روشهای نفوذگری در وب

مترجم: امیر حسین شریفی
منبع: Hacking Exposed Web Application

هدف اصلی این سلسله مقالات شناساندن روشهای نفوذگری در برنامه کاربردی تحت وب می باشد که می تواند برای خوانندگان قابل لمس، قابل توسعه و همچنین به صورت عملی، انجام پذیر باشد. همه اینها تجاربی می باشد که در سالیان دراز کسب شده است و به صورت حرفه ای تنظیم شده است. هدف از بیان این مطالب شناساندن نقاط ضعف برنامه های کاربردی و سرورهای وب به معماران و مهندسان نرم افزار و برنامه نویسان وی می باشد که با شناختن نقاط ضعف با تلاش در جهت پیدا کردن آنها در رفع آن کوشش کنند. قدمهای اولیه در این روشها به شرح ذیل می باشد:

- **شناسایی اولیه**
- **نفوذ در سرورهای وب**
- **پیمایش برنامه کاربردی**
- **حمله به مکانسیمهای احراز هویت**
- **حمله به روشهای کسب مجوز**[1]
- **اجرای یک تحلیل عملی**
- **آلوده کردن داده های اتصالی**
- **حمله به واسط مدیریت**
- **حمله به مشتری**
- **مروری کوتاه بر حملات DoS**[2]

ما در این سلسله مقالات قصد داریم اینگونه حملات را ، توضیحی مختصر ، علمی و عملی دهیم تا یک راهنمای جامع و کوچکی برای تمام مدیران شبکه و مهندسان نرم افزار و برنامه نویسان وب باشد تا بتوانند یک برنامه کاربردی محکم و استوار بنا کنند تا دست مریض احوالان از آن موصون باشد.

1 - Attack the Authorization Schemes
2 - Denial Of Service

شناسایی اولیه

اولین قدم در این روش ، جمع آوری اطلاعات از هدف می باشد و در این بخش روشهای جمع آوری اینگونه اطلاعات را بیان می کنیم. همچنین به تمام جوانب و لایه های برنامه کاربردی و سرور وب پی خواهیم برد. در این قسمت به سوالات زیر پاسخ داده می شود:

برای اتصال با برنامه کاربردی وب از چه مرورگرهایی می توان استفاده کرد؟

آیا برنامه خاصی نیاز می باشد تا بتوان با برنامه ارتباط برقرار کرد؟

از چه پروتکلی برای انتقال داده استفاده می شود؟

از طریق چه پورتهایی؟

چه تعداد سرور در حال حاضر وجود دارد؟

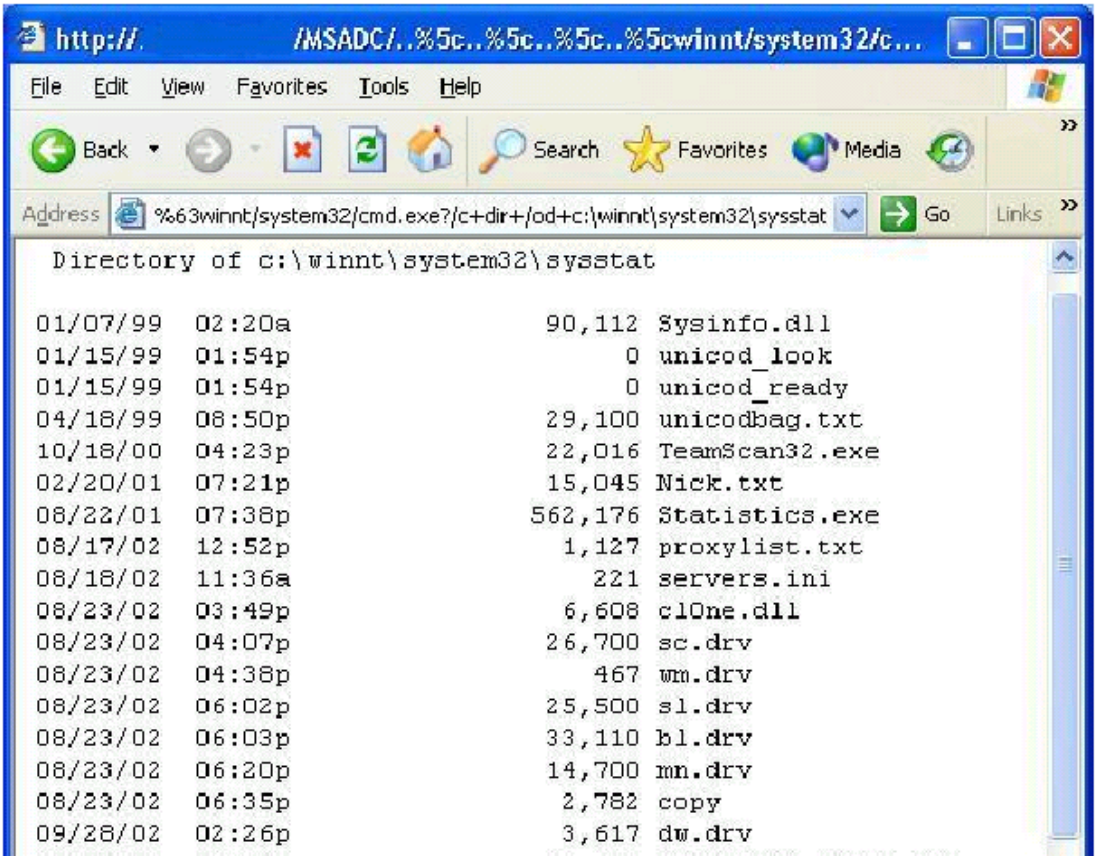
از چه مدلی برای طراحی سرورها استفاده شده است؟

آیا برای بعضی از عملکردهای سایت ، از سرورهای خارجی کمک گرفته شده است؟

در این بخش با ابزارهای شناسایی و تکنیک های آن آشنا می شویم.

حمله به سرورهای وب

تعداد بی شماری از سوراخهای امنیتی که در سرورهای وب وجود دارد و یا به وجود می آید امروزه نقل و نبات مجالس هکر ها و بچه هکرها شده است. معمولا اولین قدمی که یک هکر برای حمله به یک سایت انجام می دهد چک کردن و پیدا کردن سوراخهای امنیتی سرور سایت می باشد. اگر با یک مدیر تنبل سرو کار دارید ، یک سرور وب را در اختیار خواهید داشت!! در این فصل به روشهای نفوذ در سرورهای وب و معرفی ابزارهای پویش می پردازیم که همه این حملات از طریق پورت 80 انجام می شود.



پیمایش برنامه کاربردی

اگر در مرحله قبل به هیچ سوراخ و ضعف امنیتی برخورد نکرده اید ، آفرین به طراحان برنامه کاربردی و سرور وب ! (یا بهتر است بگوییم که چه خوش شانس بوده اند !). حال تمام توجه خود را روی مولفه های به کار رفته در خود برنامه کاربردی وب جلب کنید. – چند دسته از امکانات روی سرور وب اجرا شده است؟ برنامه کاربردی را برررسی کنید تا پی ببرید که از چه تکنولوژیهایی برای طراحی برنامه کاربردی وب استفاده شده است؟ (ASP,ASP .NET , ISAPI , Java , CGI , others ?) ، ساختمان دایرکتوریها و فایلهای سایت ، هر محتوای احراز هویت و انواع احراز هویتی که استفاده می کند، پیوندهای خارجی (در صورت وجود) ، بانک ذخیره کننده انتهایی و ... . این مرحله یکی از مهمترین مراحلی می باشد که شما انجام می دهید و اگر این مرحله را به خوبی انجام دهید احتمال پیروز شدن شما به حداکثر می رسد.

حمله به مکانسیمهای احراز هویت

اگر در مرحله قبل هر محتوای احراز هویتی را که کشف کرده اید باید به دقت مورد تحلیل و بررسی قرار دهید. باید گفت حساس ترین داده های سایت در این قسمت تولید و محافظت می شود.برای اینکه به قدرت مولفه های احراز هویت پی ببرید راههایی وجود دارد. از جمله : حملات

کلمات رمز قابل حدس ، دزدی نشانه ها از کوکیها و ... . در این قسمت این مبحث را به صورت جزیی تر بیان می کنیم.

حمله به رویه های کسب مجوز[3]

وقتی یک کاربر احراز هویت شد، قدم بعدی ، حملات دسترسی به فایلها و اشیاء می باشد این موضوع از طرق مختلفی انجام می شود. از طریق تکنیکهای پیمایش دایرکتوریها ، تغییر قانون کاربر (به عنوان مثال به وسیله تغییر دادن داده های فرم ها و یا کوکیها) ، درخواست اشیای مخفی به وسیله نامهای قابل حدس، حملات جستجوهای قانونی ، تونل زدن از طریق دستورات ویژه به سرور SQL و ... .

همچنین در بخشهایی از این مقالات درباره مهمترین جنبه های صدور مجوزها ، نگهداشتن وضعیت ، مفصل بحث خواهیم کرد.

اجرای یک تحلیل عملی

یکی دیگر از مراحل بحرانی در این روشها ، انجام یک تجزیه و تحلیل واقعی روی توابع منحصر به فرد برنامه های کاربردی می باشد. در اصل یک تحلیل عملی ، شناسایی هر مولفه از توابع برنامه کاربردی می باشد. برای مثال تنظیم ورودیها ، تصدیق ، تنظیم پیگردیها و تلاش برای تزریق داده های غلط برای هر ورودی. فرایند تلاش برای تزریق داده های اشتباه برای تست کردن مرکز امنیت برنامه کاربردی می باشد و گهگاهی به آن حملات صحت ورودی ها [4] گفته می شود.

آلوده کردن اتصالات داده ای

بعضی از ویران کننده ترین حملات روی برنامه های کاربردی وب ، روی پایگاه داده انتهایی انجام می شود. همه افراد معمولا علاقمند می باشند که داده های مشتری های خود را به صورت ذخیره شده داشته باشند. برای این منظور راههای بی شمار زیادی برای اتصال برنامه های کاربردی وب و بانکهای اطلاعاتی وجود دارد. همیشه تولید کنندگان برنامه های کاربردی بیشتر روی کارآمدی اینگونه برنامه ها تکیه می کنند تا روی امنیت آن ! ما در این بخش روی استخراج داده ها از طریق برنامه کاربردی و همچنین به دست گرفتن کنترل سیستم عامل از طریق استفاده از دستورات SQL ! صحبت خواهیم کرد.

3 - Authorization
4 - Input Validation Attacks

حمله به واسط مدیریت

تا الان هیچ بحثی درباره سرویسهای ضروری که در کنار برنامه های کاربردی وب ، به کار می روند ، حرفی به میان نیامده است. یکی از این سرویسهای ضروری ، **مدیریت راه دور** [5] می باشد. این امر به مدیران سایتها این امکان را می دهد که هنگامیکه داده و یا یک پیکربندی نیاز به تغییر و یا به روز رسانی داشته باشد ، بتوانند به راحتی از راه دور این کار را انجام دهند.

پس همیشه یک وسیله و یا یک پورتی برای مدیران شبکه و سایتها موجود است تا به وسیله آن بتوانند یک ارتباط راه دور با سرور ، محتواها و یا پایگاه داده انتهایی داشته باشند.

در این قسمت نیز کمی درباره واسط ارتباطی مدیریت سرور وب بحث خواهیم کرد.

حمله به مشتری

در خیلی از مواقع پیش می آید که علیه معماری برنامه های کاربردی وب حملاتی انجام شده است. البته این اشتباهی است که معمولا قابل برآورد نمی باشد و از همین جا بود که حملات ویران کننده ای علیه کاربران برنامه های کاربردی نیز اتفاق افتاد. از جمله این حملات اسکریپتهای تقلبی سایت [6] – به اختصار XSS یا CSS– می باشد که حملات شبیه آن علیه سایتهای مشهور eBay ، E*Trade ، Citigroup و Hotmail اتفاق افتاده است و خیلی راحت می تواند توسط یک سایت نا اهل پیاده سازی شود و به میلیونها نفر فرستاده شود و یا در گروهای خبری مشهور ، سایتهای چت و .... به سرعت منتشر شود. اگر به نظر شما این موضوع می تواند خیلی ناجور باشد این فصل را حتما مطالعه کنید.

مروری کوتاه بر حملات DoS[7]

خیلی باید خوشبین و پر مدعا باشیم که یک نفوذگر نتواند از طریق این روشهای نفوذگری به برنامه کاربردی ما حمله کند. اما یک نوع حمله دیگر می باشد که چاره ای برای آن اندیشیده نشده است. و آن عدم پذیرش سرویس [8] می باشد و این یک حقیقت تلخی می باشد که دنیای اینترنت با آن مواجه می باشد. همانطور که از نامش پیداست ، حملات DoS در اصل باعث رد کردن درخواست های مشروع کاربران برنامه کاربردی می باشد. البته این حمله به صورتهای مختلفی انجام می شود ، از جمله تحمیل یک سیلی از ترافیک بیخود به سایت، که باعث می شود درخواستهای مشروع کاربر نیز پذیرفته نشود. حملات Dos علیه سرورها را در مبحث حمله به سرورها و حملات DoS علیه برنامه های کاربردی را در فصلی جدید توضیح می دهیم. همچنین توضیح مختصری نیز درباره حملات DDoS[9] یا DoS توزیع شده خواهیم داد.

5 - Remote Management
6 - Cross-Site scripting
7 - Denial Of Service
8 - Denial Of Service (DoS)
9 - Distributed DoS