iranphp articles

عنوان مقاله : نگاهی به امنیت کوکیها و session ها
نگارنده : .....
آدرس پست الکترونیک : .....
تاریخ نگارش : .....

نگاهی به امنیت کوکیها و session ها:

در رابطه استفاده کوکی و session و توابع و کار با اونها تقریبا همه کسانی که با php کار می کنند اطلاعاتی دارند و هر php نویسی حداقل یکبار از آن استفاده کرده است. اما حالا میخواهیم با هم یه نگاه دیگه به این دو تا مورد که از لحاظ امنیتی خیلی حساسند بندازیم .

بخش اسکوب در کوکی را بخاطر می آوریم. مثلا من میخواهم کوکی من در فقط مورد استفاده این فایلهای پوشه /test ، پس در بخش اسکوب می نویسم :
/testاما نکته ای که توجه ندارم ایه که دوست هکر ما میتونه از فایل /test.php هم اطلاعات کوکی را بخونه و یا فایلهای
/test/tmp/haha.phpو .... /test2.php پس باید در اسکوپ بنویسم"/test/" :

حالااگر بخواهیم کوکی مورد استفاده فایل خاصی مثل /test/cookie.php قراربگیره مینویسیم "/test/cookie.php" و درست هم مینویسیم اما اگر دوست هکر ما دوست داشته باشه از فایل /test/cookie.php-dir/haha.php اطلاعات کوکی رو بخونه ما میتونیم چیکار کنیم؟؟؟
یه راهش دستکاری تو Apache و اینکه اصلا این دوست ما دستش به اینجور فایلها نرسه که یه مقاله تو مقالات دراین باره هست .
حالا اگه خود client هک بشه و کوکی خونده بشه چی؟؟ حالا به اهمیت رمزنگاری در کوکی پی می بریم.چون اصلا اگر هکر عزیز دستش به کوکی برسه هم نمی تونه جیزی سر در بیاره!!!! درباره رمز نگاری هم که خودتون استادید و می دونید چه قدر تابع تو php در اینباره هست .

اما هنوز یه نکته کوچولو تو بخش اسکوب مونده و اون اینه که من می خوام کوکی فقط تو سایت خودم کار کنه.. پس حق دارم بنوسم :
"test.com","/tesr/"اما چرا دوست ما نباید بتونه از سایت hahatest.com با کوکی ما بازی در نیاره.. پس گزینه ای که کد شما رو حرفه ای جلوه می ده اینه ".test.com" : اما ممکنه این هکر سمج بخواد از طریق www2.test.com رو کوکی ما بازی کنه.. پس شاید کد امنتر شما دیگه بتونید بنویسید . . .

و اما در آخر شاید سایت شما نخواهد هیچ ریسکی رو تقبل کنه .. حالا دیگه وقته کار با SSL هست. اما کار کوکی با SSL لازم اینه که در آخر تابع setCookieیه عدد "۱" بنویسید و خودتون می دونید که که هنگامی که با SSL سایت شما به صورت https://test.com درمیاد .

واما کمی کار با . . . session ببینید session ها خطر پذیرند و نمیشه برای یه سایت امن کاملا روی اونها حساب کرد ، مگر با ذکر دو سه تا نکته . .

کلا session ها در پوشه /tmp ویا windows/temp ساخته میشن و این اساس خطر پذیری اونهاست. پس یه کار خوب ساخت session توی پوشه دلخواه است . یه کار خیلی معمول دیگه ریختن اطلاعات توی دیتابیس هست . من راجع این دو تا مطلب چیزی نمی نویسم چون توی انجمنها آقا نیما و دوستان ۵ تا ۶ صفحه مطلب توی این زمینه نوشتن .
اما نکته ای که ممکنه در نظر گرفته نشه استفاده از دو تابع خیلی مفید string session_encode و bool session_decode هست که خیلی مفیده و php>=4 را ساپورت میکنه .

حالا کار خوب نوشتن یه پروژه کامل با استفاده از کوکی و session و دیتابیس است که مطالبو جابندازه.فقط در آخر بگم که اینها مراحل تکمیل امنیت پروژه بود و در هر مرحله مار امنتر میشد و همه میدانیم همه سایتها نیاز به SSL ندارند .