بسم الله الرحمن الرحیم

مرور آموزشهای مبحث

کشف آسیب پذیری در وبسایت ها و نرم افزارهای تحت وب

Web Applications Vulnerability Detection Tutorials

- مولف: گروه مدیریت کانال The Hacking
- ویراستار: مهران صاحب کوهی

- تاریخ نگارش: دی ماه 1394
- کانال ما را در تلگرام دنبال کنید: https://telegram.me/thehacking

پیشگفتار:

پس از به پایان رسیدن آموزشهای مبحث کشف آسیب پذیری در وبسایت ها و نرم افزارهای تحت وب در کانال تلگرام The Hacking به نشانی https://telegram.me/thehacking، همانند دیگر مباحث تصمیم گرفتیم تا مطالب آموزشی که در کانال قرار داده شده اند را سرجمع و در قالب یک مقاله در اختیار شما کاربران و دانش پژوهان فعال عرصه فناوری اطلاعات قرار دهیم.

نکته ای را باید بیان نماییم؛ اینکه برخی از آموزشها و ویدئوها که به صورت ضمیمه شده در کانال قرار گرفته اند، را باید مستقیماً از کانال دانلود کنید. بیشتر آموزشها سعی شده به صورت متنی باشند و برخی از آموزشهای ویدئویی را در کانال آپارات The Hacking به نشانی http://aparat.com/thehacking می توانید مشاهده و دانلود نمایید.

معرفی کوتاه کانال The Hacking:

کانال The Hacking، کانال The Hacking یک کانال تلگرام است که روزانه مطالب مفیدی در زمینه هک و امنیت را در اختیار کاربران خود قرار می دهد. نمونه فعالیت های این کانال به شرح زیر است:

- ✓ آموزش هک و امنیت و روشهای نفوذ و تست نفوذ به صورت کاملاً حرفه ای
- ✓ ارائه نرم افزارها و مقالات مرتبط
- ✓ ارائه نکات مهم جهت افزایش امنیت در دنیای مجازی
- ✓ بررسی روشهای امنیت در مسنجر تلگرام

و...

آدرس کانال The Hacking در تلگرام:

https://telegram.me/thehacking

ویدئوهای کانال The Hacking را می توانید از آدرس زیر در آپارات مشاهده و دانلود کنید:

Http://aparat.com/thehacking

هشدار: تمامی آموزشها و مطالب موجود در این مقاله فقط جنبه آموزشی داشته و هرگونه استفاده نابجا بعهده کاربر می باشد.

از تمامی دوستان و کاربران عزیزی که در ارائه این آموزشها به نحوه احسن ما را یاری نمودند، تشکر میکنیم.

Milad Hacking – Mohammad Reza Mokhtari – Mohammad Ghasemi

Mahdi Ardestani – Arash Khazaei - Mr.G}{o$t – Sajjad Teymoori

مقدمه:

میزان استفاده از برنامه های تحت وب (Web Application) و نیز وبسایت ها در اینترنت روز به روز در حال گسترش است و موضوعات و ایده های جدیدی برای ایجاد یک وبسایت از سوی افراد مطرح می شوند. هرکسی با هر شغل و در هر رده سنی با توجه به نیاز خود و استفاده ای که از اینترنت دارد، اقدام به راه اندازی یک وبسایت می کند. از افراد حقیقی و حقوقی که قصد حضور در اینترنت برای انتشار اطلاعات و معرفی محصولاتشان گرفته تا دانش آموزان و دانش جویان همگی به نوعی از وبسایت های اینترنتی استفاده میکنند.

در این بین نفوذگران نیز در بین بازدیدکنندگان این وبسایت ها قرار دارند و با اهداف مختلفی مانند نشان دادن ضعف ها و اشکالات امنیتی موجود یا انجام یک عملیات خرابکارانه و سرقت اطلاعات به این وبسایت ها نفوذ می کنند. این افراد با بهره گیری از تکنیک ها و فنون خاص و نیز سوء استفاده از آسیب پذیری های موجود اقدام به نفوذ میکنند.

ما در این سلسله آموزشها قصد داریم تا شما را با این فنون و تکنیک ها برای کشف آسیب پذیری و ضعف و اشکال موجود در وبسایت ها آشنا و ابزارهای مورد استفاده برای این امور را معرفی و نحوه کارشان را شرح دهیم.

پس با ما همراه باشید...

ضمناً این مقاله حتماً دارای اشکالات نحوی و فنی بوده که از شما عزیزان و اساتید خواهشمندیم تا در صورت مشاهده هرگونه اشکال مارا در ارائه مطالب آموزشی بهتر یاری فرمایید. همچنین می توانید انتقادات و پیشنهادات سازنده خود را با ما اط طریق مراجعه به نشانی https://fullsecurity.org در میان بگذارید.

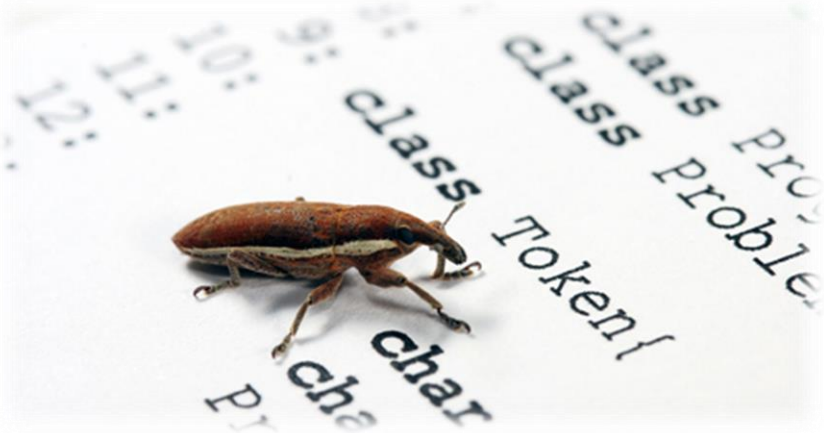
با تشکر

گروه مدیریت کانال The Hacking

دی ماه 1394

برای شروع ابتدا به بیان مفاهیم و تعاریف این مبحث می پردازیم:

1. باگ چیست؟



ابتدا به تاریخچه این کلمه می پردازیم:

باگ از نظر لغوی یعنی حشره کوچک است. این اصطلاح را اولین بار گریس هوپر خانمی که در دانشگاه هاروارد مشغول تحصیل و تحقیق در رشته کامپیوتر بود، به کار برده است. او که در حال کار با کامپیوترهای Mark II و Mark IIIبود، یک بار با مشکل مواجه شد و تکنسین هایی که برای بررسی مشکل و تعمیر کامپیوتر، آن را باز کرده بودند سوسکی را پیدا کردند که وارد دستگاه شده بود و آن را از کار انداخته بود.البته در حقیقت این واژه را اولین بار همان تکنسین هایی که این حشره را داخل دستگاه یافته بودند، به شوخی به کار برده بودند البته این تکنسین ها یا خانم هوپر اولین کسانی نبودند که از این واژه برای اشاره به یک ایراد در دستگاهی استفاده می کردند. آنها صرفاً برای نخستین بار از این اصطلاح در دنیای کامپیوتر استفاده کردند، ولی اعتقاد بر این است که اصطلاح Debug توسط همین افراد ابداع شد.

آسیب پذیری یا همان Vulnerability نیز برگرفته از همین اصطلاح است. اکثر نفوذگران به ضعف های امنیتی موجود در برنامه ها و وبسایت ها باگ یا Vulnerability می گویند. باگ مشکلی است که در یک برنامه رخ داده و باعث از کار انداختن کلی آن یا اجرا نکردن دستور یا دستورات بعدی به صورت ناقص یا کامل می گردد.اغلب این مشکلات در هنگامی رخ می دهد که دادهای دریافتی از سوی کاربر فیلتر نشده و برنامه سعی به اجرا کردن آن می کند برای نمونه می توان انجام عمل تقسیم را بیان کرد. فکر کنید برنامه دو متغیر را دریافت می کند به طوری که متغیر اول عدد صورت و متفیر دوم عدد مخرج می باشد اگر کاربر ابتدا عدد ۶ و سپس عدد ۳ را وارد کند برنامه در خروجی خود عدد ۲ را نمایش خواهد داد حال اگر کاربر در صورت یک عدد(مثلا ۶) و در مخرج یک حروف الفبا یا عدد صفر را وارد کند به نظر شما عکس العمل برنامه چه خواهد بود؟

همانطور که می دانیم در ریاضیات تقسیم عدد بر حروف الفبا و صفر تعریف نشده است پس برنامه با حالتی از پیش تعریف نشده برخورد می کند و چون قابلیت اجرا کردن آنها را ندارد هنگ می کند و خروجی منطقی را تحویل نمی دهد و این مشکل در زمانی خطرناکتر می شود که برنامه قصد انجام عملیاتی خاص و مهم همچون چک کردن نام کاربری و کلمه ی عبور را داشته باشد.فکر کنید در یک صفحهء وبسایت که قسمت ورود کاربر تهویه شده است پیج بدون فیلتر کردن داده های ورودی از طرف کاربر فقط سعی به اجرا کردن آنها را دارد در این هنگام کاربری اسکریپتی را وارد می کند و چون این داده ها فقط پردازش می شوند پس می تواند برای سایت یک عامل خطرناک محسوب شده و باعث اختلال در عملکرد آن گردد.

2. اکسپلویت چیست؟

تعریف کوتاه اکسپلویت: نفوذ بر اساس نتیجه گیری و گرفتن خروجی های حاصل از برنامه ها و ابزارها

اغلب موارد هکرها و برنامه نویس ها هنگامی که سعی به نفوذ به یک کامپیوتر یا یک برنامه را دارند مداوم به آنها داده هایی را تحویل می دهند که برنامه آنها را پردازش کند و خروجی خود را نمایش دهد در این هنگام نفوذگر با تناسب بستن میان داده ها و خروجی ها به عملکرد کلی برنامه پی برده و سعی می کند که با داده هایی که برنامه برای انجام آنها دچار خطا می شود به انها صدمه وارد کند. و از جهتی چون چک کردن برنامه های مختلف و کدها وقت زیادی را می گیرد فرد نفوذگر وقتی نحوه ی صدمه زدن به برنامه را کشف کرد برنامه ای را برای این منظور می نویسد که خودکار کارهای مورد نظر وی را انجام دهد.به همین دلیل هنگامی که یک مشکل امنیتی پیدا می شود فرد برنامه نویس کدی را با مضمون اکسپلویت قرار می دهد که نقش وی را بهتر و سریع تر انجام دهد.

ما ، تو صنف خودمون(!) ، به باگ میگیم سوتی های برنامه نویس! ☺

یکی از معروف ترین وبسایت هایی که اقدام به انتشار اکسپلویت میکند، وبسایت Exploit Database است:

https://www.exploit-db.com

3. شل چیست؟ و شل گرفتن چیست؟

شل در لغت به معنی پوسته است و در سیستم عامل های لینوکس جزء قسمت هایی است که رابط کاربر بین سخت افزار می باشد.در مفاهیم هکینگ هنگامی که شخص نفوذگر با استفاده ابزارها و کارهای خود می تواند به سیستم مورد نظر خود نفوذ کند و کنترل سیستم را به دست بگیرد اصطلاحاً می گویند شل گرفته است و می تواند تصمیمات خود را عملی گرداند.

4. تارگت چیست؟

تارگت معمولاً یک مشخصات نسبتاً دقیقی از سیستم هدف است. مثلاً عبارت Win XP SP3 en بیانگر این است که سیستم هدف دارای سیستم عامل ویندوز ایکس پی سرویس پک 3 انگلیسی است. از این اطلاعات معمولاً در اغلب اکسپلویتها استفاده می شود.

معرفی نرم افزار Acunetix Web Vulnerability Scanner:

اکانتیکس یک اسکنر امنیتی جهت پیدا کردن باگ ها و حفره های امنیتی وب سایت ها میباشد که با استفاده از اسکنر امنیتی اکانتیکس میتوان اقدام به شناسایی و سپس رفع آسیب پذیری های یک وب سایت نمود.امروزه تقریبا 70 درصد سایت های اینترنتی باگ و راه های نفوذ دارند بدون آنکه خودشان اطلاعی داشته باشند. اکانتیکس یک ابزار محبوب و شناخته شده در بین هکر ها میباشد که ورژن 10 این اسکنر چندین ماه قبل ارایه شد.

برخی از قابلیت های اسکنر امنیتی اکانتیکس

- امکان اسکن قدرتمند وبسایت ها برای یافتن باگ های SQL injection و Cross site scripting و سایر اسیب پذیری های موجود
- قابلیت اسکن هزاران صفحه با سرعت بالا
- قابلیت پیدا کردن نوع وب سرور و اسکریپت
- قابلیت پیدا کردن صفحات لاگین سایت ها
- قابلیت پیدا کردن فولدر های یک سایت
- قابلیت بروت فورس صفحات لاگین
- قابلیت پیدا کردن ساب دامنه های یک سایت
- امکان سو استفاده از اسیب پذیری Blind Sql Injection در این اسکنر به صورت اتوماتیک

آخرین ورژن این نرم افزار را میتوانید بصورت کرک شده از لینک زیر دریافت نمایید:

http://soft98.ir/internet/webmaster-tools/14439-Acunetix-Web-Vulnerability-Scanner.html

آموزش تصویری کار با اسکنر امنیتی اکانتیکسAcunetix :

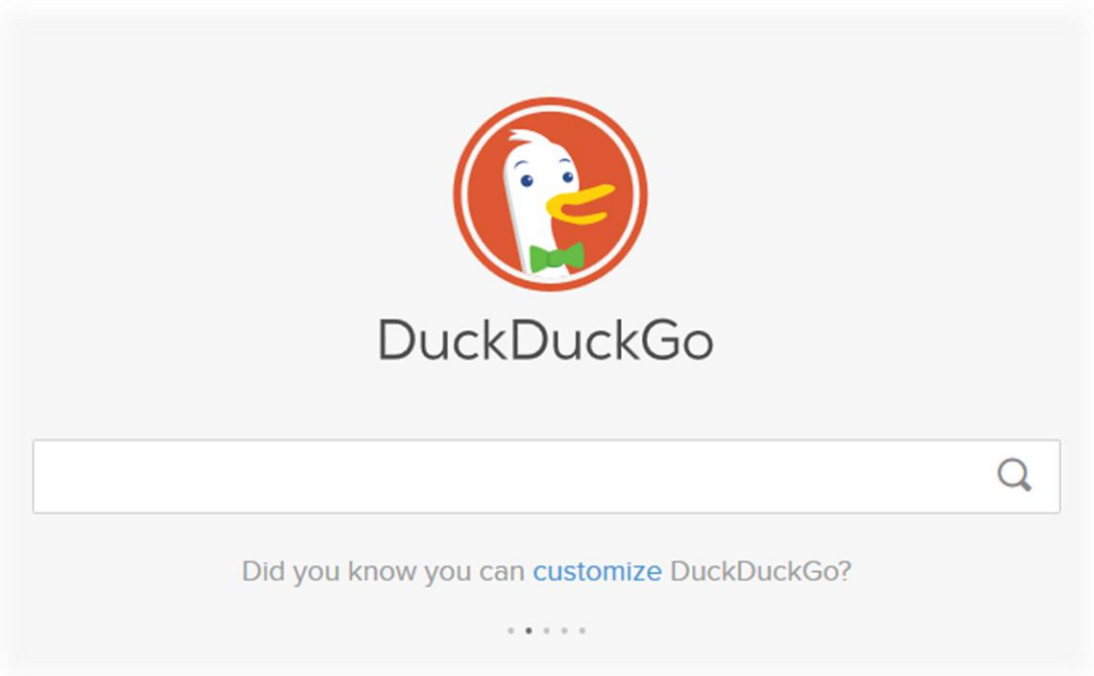
در این مجموعه آموزشی به آموزش قسمت های مختلف اسکنر اکانتیکس Acunetix پرداخته شده است که میتوان با دانلود این مجموعه اقدام به کار با بخش های مختلف اسکنر اکانتیکس Acunetix نمود همچنین با اسکن و انالیز سایت میتوان اقدام به ایمن سازی وب سایت با رفع آسیب پذیری ها نمود.

برای دریافت این آموزش تصویری از لینک زیر استفاده کنید:

http://dl.fullsecurity.org/milad/Pack%20Acunetix%20FullSecurityorg.rar

✓ رمز عبور برای فایل فشرده: fullsecurity.org

معرفی وبسایت Duckduckgo:



داک داک گو موتور جستجوی محبوب هکرها و نفوذگران است.

این موتور جستجو که همانند گوگل عمل میکند تمرکز خود را بر روی حریم خصوصی کاربران و جلوگیری از دزدی اطلاعات شخصی افراد توسط گوگل دارد. شما میتوانید از این موتور جستجو استفاده کرده بدون انکه نگران ترک شدن شما در نت و یا نقض حریم خصوصی خود باشید.

آدرس این وبسایت به صورت زیر است:

http://duckduckgo.com

معرفی حملات و آسیب پذیری موسوم به SQL Injection:

نفوذ به سایت ها و سرور ها با روش های مختلفی انجام می شود که معمولا نفوذگران با استفاده از باگ های موجود اقدام به نفوذ به اسکریپت سایت میکنند و اقدام به هک کردن سایت و سرور میکنند. حفره های مختلفی بروی سایت ها می توانند وجود داشته باشند که Sql Injection یکی از این باگ ها می باشد که نفوذگران می توانند از طریق آن به سایت هایی که این باگ را دارند نفوذ کنند. تزریق به پایگاه داده (SQL injection) نوعی از حملات هکرها به وبسایت و غالبا نرم افزارهای تحت وب است که به هکرها این امکان را می‌دهد تا به پایگاه داده یا همان Database دسترسی پیدا کنند. این نوع حملات جز متداول ترین روش‌های است که به منظور نفوذ به وبسایت ها انجام میگیرد.

نفوذگر با اجرای دستوراتی در Url سایت اقدام به نفوذبه دیتابیس و تخلیه اطلاعات پایگاه داده سایت میکند و با سرقت یوزر ها و پسورد های پایگاه داده اقدام به نفوذ به سایت میکند.

برای آشنایی بیشتر با حملات SQL Injection می توانید از مقاله زیر استفاده نمایید:

http://yon.ir/40Ll

در آموزش تصویری زیر نیز می توانید با نحوه انجام یک حمله SQL Injection آشنا شوید:

http://uploadboy.me/fdyuwk2mbc8z/Sqlinjection.rar

معرفی حملات و آسیب پذیری موسوم به LFD (Local File Disclosure/Download):

اگر برای دانلود فایلی در گوگل جستجویی کرده باشید متوجه میشوید که بعضی از سایت ها از صفحه ای برای دانلود کردن فایل به وسیله کاربر استفاده میکنند.

از اونجایی که در بیشتر موارد ورودی ها چک نمیشوند و کاربر میتواند هر فایلی رو که بخواهد دانلود کند موجب هک شدن سایت میگردد. وقتی که ورودی ها کنترل نشوند و کاربر اجازه دانلود هر فایلی رو داشته باشد میتواند فایل های مهم از جمله کانفیگ وب سایت رادانلود کرده و به صورت Remote به دیتابیس دسترسی پیدا کند و با عوض کردن پسورد مدیر سایت از داخل دیتابیس اقدام به هک کردن و تغییر چهره وب سایت کند.

باگ LFD یا Local File Download بیشتر در پوسته ها و پلاگین هایی که قابلیت دانلود فایل را به کاربران میدهد وجود دارد و همچنین در فایل هایی که در ان ها از توابعی مانند $filename و افزونه های file manager دیده شده است.

برای رفع این اسیب پذیری کافی است که فرمت قابل دانلود را تنظیم کنید و هر فرمتی قابل دانلود نباشد.

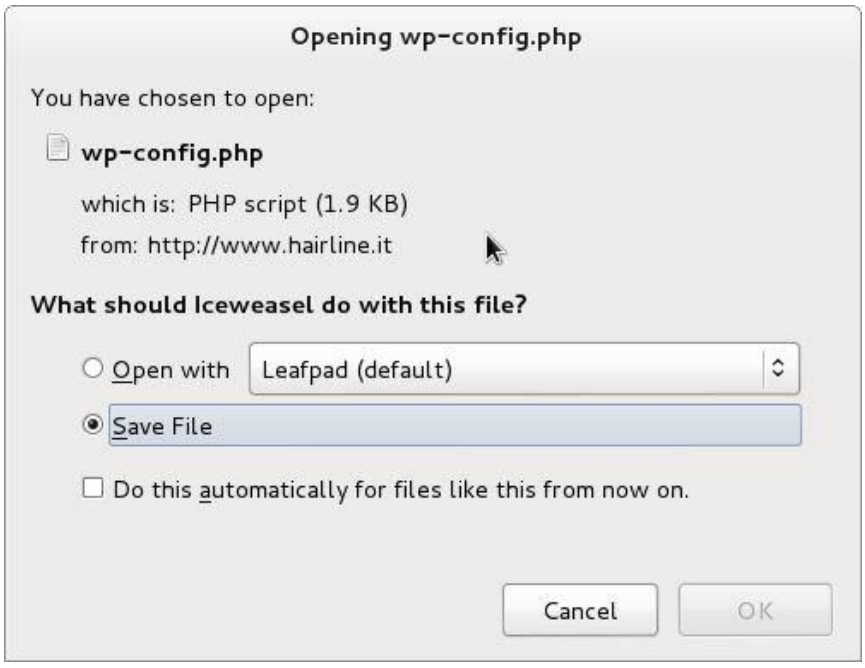
برای نمونه آدرس زیر را در نظر بگیرید:

vismatica.com/force-download.php?file=wp-config.php

در این لینک، فایل force-download.php ، کاربران را برای دانلود فایل به مکانی که فایل مورد نظر در آنجا قرار دارد، ارجاع می دهد. ما در اینجا به جای آدرس فایلی که به آن ارجاع داده شده است، آدرس فایل کانفیگ وبسایت را وارد میکنیم.

این آدرس را در نظر بگیرید:

http://www.kanazawa-adc.com/force-download.php?file=wp-config.php



در ادرس بالا مدیر سایت وردپرسی اقدام به ایجاد یک صفحه برای دانلود فایل های pdf کرده است که به دلیل فیلتر نشدن فرمت ها نفوذگر میتواند به راحتی به فایل های امنیتی از جمله فایل کانفیگ دسترسی و امکان دانلود داشته باشد. و با استفاده از این اسیب پذیری سایت به راحتی مورد نفوذ قرار میگرد.

ویدئوی مربوط به آموزش این آسیب پذیری را از آدرسهای زیر میتوانید دانلود و مشاهده کنید (با تشکر از دوست عزیز، رسول):

http://yon.ir/LFD03 http://yon.ir/LFD02 http://yon.ir/LFD01

آشنایی با حملات و آسیب پذیری موسوم به RFU یا Remote File Uploader:

همون طور که همه ما میدونیم برای اشتراک گذاشتن یک عکس یا فایل در بستر اینترنت ابتدا نیاز داریم که فایل یا عکس خودمون رو توی یک سایت اپلود کنیم تا به طول مثال بتونیم عکس یا فایلی رو برای شخصی ارسال کنیم.

بعضی از سایت هیچ محدودیتی برای اپلود فایل در نظر نگرفتن به صورت کلی هر فرمتی از قبیل php اجازه اپلود و اجرا بر روی سرور رو داده که نفوذگر میاد فایل مخرب sheller خودش رو اپلود میکنه و دسترسی کامل میگیره از سایت و با داشتن دانش کافی و تجربه بالا میتونه سرور رو هم مورد نفوذ قرار بده.

عواقب آپلود فایل بدون محدودیت میتونه متفاوت باشه به عنوان مثال وقتی نفوذگر WebShell خود را بر روی سرور اپلود و اجرا کنه یا سیستم را بطور کامل تصاحب کنه یا دسترسی به پایگاه داده داره یا انتقال و دریافت فایلهای نرم افزار کاربردی تحت وب برای او فراهم است و حتی میتواند کد صفحات به دلخواه تغییر دهد.

آشنایی با حملات و آسیب پذیری موسوم به LFI یا Local File Inclusion:

آسیب پذیری LFI مخفف عبارت Local File Inclusion میباشد که یکی از آسیب پذیری های معروف جهت نفوذ به وب سایت ها می باشد که به نفوذگر اجازه اجرای دستورات بر روی سرور را میدهد آسیب پذیری Local File Inclusion یک آسیب پذیری خطرناک می باشد که در بسیاری از کامپوننت های جوملا که بر روی هسته نصب شده اند در چند سال اخیر توسط نفوذگران مختلف شناسایی شده است.

در این آموزش میخواهیم به نحوه آشنایی با این آسیب پذیری بپردازیم که چگونه ایجاد میشود و چطور میتوان از این آسیب پذیری سو استفاده نمود برای درک اینکه چگونه آسیب پذیری های Local File Inclusion می تواند رخ دهد باید با توابع require, Include() در زبان برنامه نویسی php آشنایی نسبتا کمی داشته باشید.

این آسیب پذیری بیشتر در سورس کد هایی دیده میشود که درخواست فراخوانی یک فایل را دارند به طور مثال با استفاده از توابع Include میتوان اقدام به خواند فایل ها نمود نفوذگر با استفاده از آسیب پذیری Local File Inclusion یک نوع دسترسی محلی را به دست می آورد که برای مشاهده ی فایل های مهم سرور مورد نظر استفاده قرار میگیرد.

مهم ترین و پرکاربرد ترین روش استفاده از آسیب پذیری Local File Inclusion میتوان به خواندن فایل های مهم سیستمی و خواندن فایل کانفیگ config اشاره نمود.

ر اینجا باید اضافه کنم که علاوه بر تابع Include از توابع زیر نیز برای فراخوانی یک فایل در زبان PHP میتوان استفاده نمود که در صورت استفاده ممکن است سایت دارای این اسیب پذیری باشد:

Include_Once Require Require_once virtual

روش استفاده از این آسیب پذیری را میتوان به بروت فورس یوزر های سرور و همچنین تبدیل باگ Local File Inclusion به آسیب پذیری Remote Command Execution اشاره نمود.

در زیر آدرس یک وبسایت آسیب پذیر نسبت به LFI را مشاهده میکنید:

http://www.cncseries.ru/autohtml.php?filename=../../../../../../../../../../../../../../../etc/passwd

پس از اجرای دستور ما توانستیم فایل passwd در سرور لینوکس رو بخونیم که یوزر های سرور رو بهمون نمایش داد.

تصویری از یک سایت آسیب پذیر دارای باگ LFI:

معرفی حملات و آسیب پذیری های موسوم به XSS یا Cross Site Scripting:

آسـیب پذیری XSS مخفف Cross Site Scripting می باشـد و زمانی در یک برنامه ی رخ می دهد که ورودی بدون فیلتر پردازش شود ، در نتیجه نفوذگر به راحتی می تواند کد های خود را اجرا کند. این آسیب پذیری یک آسیب پذیری تحت کاربر یا کلاینت می باشد و با استفاده از آن به طور مستقیم نمی توان به سایت نفوذ کرد ، با استفاده از آن می توان کوکی های مدیر سایت را دزدید و سپس با استفاده از آن کوکی های به سایت نفوذ کرد. کد هایی که نفوذگر می تواند در این جملات استفاده کند زبان های تحت وب مانند html، css و javascript می باشد و نمی تواند از زبان های تحت سرور مانند php استفاده کند.

با عنوان مثال، کد های زیر به زبان php نوشـته شـده اند که یک ورودی که نام کاربر می باشـد را از آن می گیرد سـپس عبارت Hello username را چاپ می کند البته به جای username نام دریافتی را چاپ می کند:

```
<?php

$username=$_GET['name'];

echo "Hello " , $username;

?>

<form action="" method="get" />

<input type="text" name="name" />

<input type="submit" value="submit" />

</form>
```

خوب حالا کد های php را بر روی لوکال هاست یا هر جای دیگر اجرا نمایید و در کار موجود نام خود را وارد نمایید سپس بر روی submit کلیک کنید.

مشاهده می کنید که به شما سلام می کند ، Hello user.

خوب حالا به جای خود یک کد html یا جاوا اسکریپت در کادر وارد کنید سپس بر روی submit کلیک کنید.

Javascript : <script>alert(/Xss Vuln/)</script>

Html : <h1>Xss Vuln</h1>

همانطور که مشاهده کردید کد های ما اجرا شد ، به این دلیل کد های ما اجرا شدند که برنامه از هیچ فیلتری برای جلوگیری از اجرای کد ها استفاده نکرد. در صورت فیلتر نشدن دستورات و اجرای هر چیزی میتوان با استفاده از اجرای دستورات جاوا اسکریپت اقدام به نفوذ به سایت نمود.

در ادامه به آموزش کامل کشف آسیب پذیری های XSS می پردازیم:

آموزش کشف آسیب پذیری های XSS:

در این آموزش ما ابتدا به روشهای کشف وبسایت های آسیب پذیر و سپس به تست وجود آسیب پذیری در این وبسایت ها می پردازیم:

1. کشف وبسایت های آسیب پذیر: شما عزیزان می توانید از تمامی وبسایت هایی که دارای فیلدهای ورودی اطلاعاتی نظیر فیلد جستجو، فیلدهای ورود کاربر و صفحه مدیریت و ثبت نام کاربر هستند برای تست وجود آسیب پذیری استفاده نمایید و علاوه بر این می توانید از دورک گوگل زیر نیز استفاده کنید:

intext:"?search"=

2. تست وجود آسیب پذیری: پس از اینکه ما یک وبسایت برای تست وجود آسیب پذیری XSS انتخاب کردیم، اقدام به تست ورودی های این سایت برای وجود آسیب پذیری XSS می کنیم:

الف) به عنوان مثال در یک فیلد جستجو، یک رشته کاراکتر معمولی مانند BTS را وارد میکنیم. سپس به قسمت نتایج و خروجی های این فیلد می رویم. برای مشاهده خروجی ها می توان از سورس صفحه استفاده کرد. مسلماً همین رشته کاراکتر در خروجی بدون هیچ تغییری نمایش داده می شود.

ب) در این مرحله بررسی میکنیم که آیا سرور موارد ایمنی را رعایت می کند یا خیر. برای این منظور رشته کاراکتر <script> را در فیلد جستجو وارد و پس از اجرا به قسمت خروجی ها و نتایج این فیلد می رویم.

اگر این رشته کاراکتر بدون هیچ تغییری در قسمت خروجی نمایش داده شد، می توان نتیجه گرفت این وبسایت آسیب پذیری XSS را داراست اما بازهم باید تست های قوی تری را انجام دهیم...

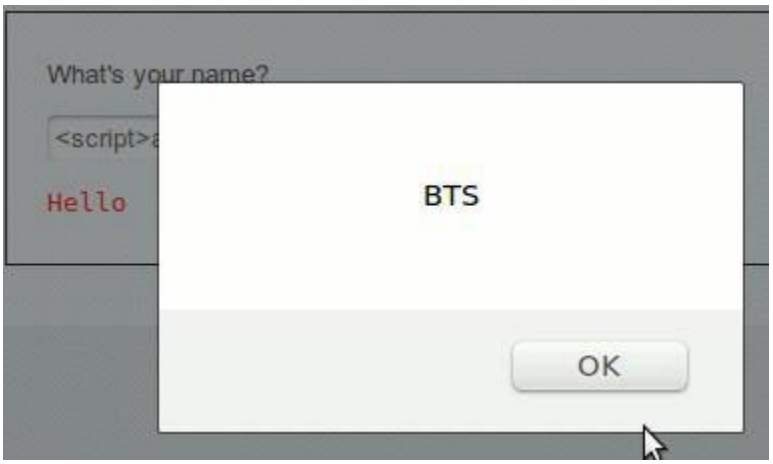
❌ اگر موارد ایمنی برای رشته کاراکتری که وارد کردیم رعایت شود، این رشته کاراکتری به صورت زیر در قسمت خروجی نمایش داده می شود:

<script>

ج) حال در این مرحله، با توجه به عملکرد سرور و فیلد جستجو در نمایش نتایج مربوطه، رشته کاراکتر زیر را وارد میکنیم:

<script>alert('BTS')</script>

اگر نتیجه عملکرد این فیلد، باز شدن یک پنجره پاپ آپ با متن BTS باشد، این وبسایت دارای XSS است که نتیجه عملکرد این فیلد به صورت تصویر زیر خواهد بود:



حال که از وجود باگ XSS در این وبسایت اطمینان حاصل کردیم، به استخراج اطلاعات و ادامه حمله می پردازیم.

آموزش دور زدن (Bypass) فیلترهای XSS:

در قسمت قبل به بیان روشهای کشف آسیب پذیری های XSS پرداختیم و بیان کردیم که چگونه برخی رشته کاراکترهای می توانند آسیب پذیر بودن یک وبسایت از نوع XSS را به ما نشان دهند. برخی از وبسایت ها هستند که از فیلترهایی موسوم به WAF استفاده و این رشته های کاراکتری را فیلتر میکنند که باعث عدم اجرای این رشته کاراکترها و اسکریپت ها می شوند.

مثلاً اسکریپت زیر '<scirpt>alert("hi")</script>' در صورت فیلتر شدن بصورت زیر تبدیل خواهد شد:

<script>alert(>xss detected<)</script>

که این اسکریپت عملکردی نخواهد داشت...

روشهای بای پس فیلترها:

1. روش بای پس magic_quotes_gpc: عبارت magic_quotes_gpc=ON یکی از تنظیمات موجود در PHP Setting که توسط فایل php.ini کانفیگ شده است می باشد که هر کاراکتر تک کوتیشن و جفت کوتیشن و کاراکتر \ را به صورت خودکار به کاراکتر / تبدیل میکند. مثلاً اسکریپت <scirpt>alert("hi")</script> پس از گذر از این فیلتر به صورت زیر تبدیل می شود:

<script>alert(/hi/)</script>

این روش فیلتر شناخته شه است و به راحتی بایپس می شودبدین صورت که کاراکترها را به صورت ASCII میکنیم. مثلاً رشته کاراکتری زیر را درنظر بگیرید:

alert("hi”);

این رشته کاراکتری پس از تیدیل به کدهای ASCII به صورت زیر خواهد بود:

String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 104, 105, 34, 41, 59)

در نتیجه اسکریپت نهایی ما به شکل زیر خواهد بود:

<script>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 104, 105, 34, 41, 59)</script>

✅ برای تبدیل رشته کاراکترها با کاراکترهای ASCII در راه وجود دارد:

الف) استفاده از افزونه Hack Bar در مرورگر موزیلا که می توانید این افزونه را از آدرس زیر دریافت و نصب کنید:

https://addons.mozilla.org/en-US/firefox/addon/hackbar/

ب) استفاده از روش اینکد کردن HEX با استفاده از وبسایت زیر:

http://centricle.com/tools/ascii-hex/

2. روش تبدیل حالت بزرگی و کوچکی حروف: برخی از مدیران وبسایت ها کلمات script و alert را در لیست فیلتر قرار میدهند که در صورت وارد کردن این عبارات در یک فیلد ورودی مانند فیلد جستجو، با پیغام خطای زیر مواجه می شویم:

" you are not allowed to search this"

این روش فیلتر را می توان با تغییر دادن حالت بزرگی و کوچکی حروف بای پس کرد بدین شکل:

<ScRipt>ALeRt("hi");</sCRipT>

این روش بای پس ممکن است بدرستی عمل نکند اما باز هم میتوان آنرا تست کرد.

3. روش افزودن یک تگ بسته به ابتدای اسکریپت: گاهی اوقات قرار دادن یک <" در ابتدای اسکریپت میتواند در بای پس فیلتر سودمند واقع گردد. مثلاً:

"><script>alert("Hi");</script>

که بصورت زیر میتواند باشد:

hxxp://vulnerable-site/search?q="><script>alert("Hi");</script>

از این مقاله می توانید برای آشنایی بیشتر با حملات و آسیب پذیری های XSS استفاده کنید:

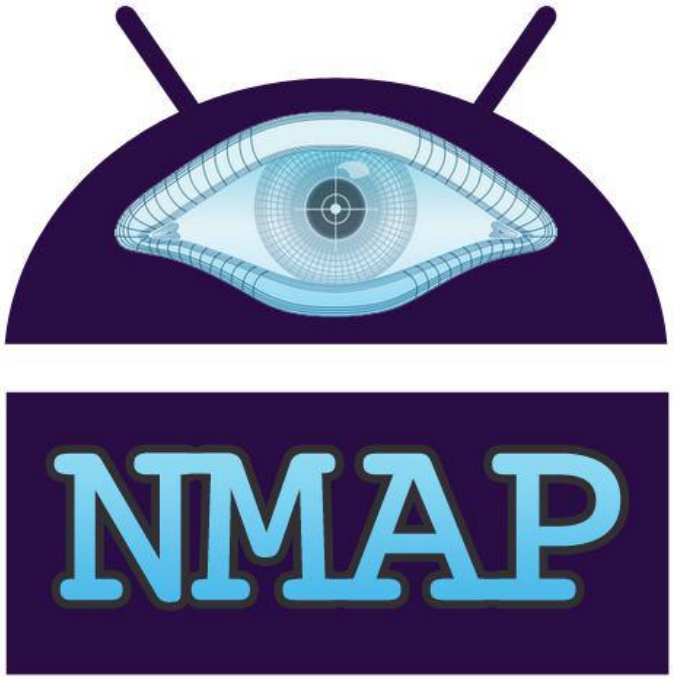
https://www.owasp.org/images/9/9d/OWASP_Attack_Category-_Cross-site_Scripting_-XSS.pdf

در این ویدئو نیز یک باگ XSS که در گوگل یافت شده است، نشان داده شده است:
http://s6.picofile.com/file/8182049918/Google_bug_xss_by_FullSecurity.mp4.html

در این ویدئو نیز با باگ XSS موجود در سایت Yahoo آشنا میشوید:
http://s4.picofile.com/file/8182048668/2014_XSS_Yahoo_com.mp4.html
در این وبسایت نیز برخی از وبسایت های بزرگ که دارای باگ XSS بوده اند، ثبت شده و می شوند:
http://www.xssed.com

در این ویدئو نیز با باگ موجود در موتور جستجوگر Yooz آشنا می شوید:
http://yon.ir/yooz1

یک هدیه از طرف کانال The Hacking



برای اولین بار در ایران

نرم افزار Nmap فارسی شده برای اندروید

نرم افزار Nmap یکی از قویترین ها در ضمینه کشف پورت و... است،اما تا کنون فقط نسخه لینوکس و ویندوز ان موجود بوده ما برای اولین بار در ایران نرم افزار Nmap که توسط تیم متخصص TheHacking فارسی شده است برای شما قرار میدهیم.

-احتیاج به روت

فارسی شده توسط Mr.G}{o$t

لینک دانلود:

http://yon.ir/nmapforapk

آموزش تصویری ایجاد بک دور در وردپرس ورژن 4

به طور معمول بعد از گرفتن دسترسی از سایت امکان از بین رفتن دسترسی نفوذگر نیز وجود دارد یکی از راه های دسترسی همیشگی از سایت ایجاد درب پشتی در سایت میباشد.

در این آموزش تصویری که توسط مدیران این کانال آماده شده است با ویرایش صفحه لاگین وردپرس اقدام به ایجاد بک دور در سایت وردپرسی میکنیم همچنین بعد از اپدیت وردپرس دسترسی ممکن است دسترسی از بین برود با این روش حتی در صورت اپدیت سایت وردپرسی میتوان اخرین پسورد مدیر را بدست آورد همچنین میتوانید پرمیشن فایل صفحه لاگین را ویرایش کنید تا در صورت اپدیت بکدور در اسکریپت سایت باقی بماند

این روش در وردپرس ورژن 4 تست شده و قابل استفاده میباشد.

لینک دانلود

http://s6.picofile.com/file/8191661042/create_backdoor_to_wordpress_2015_by_FullSecurity.rar.html

آموزش تصویری ایمن سازی وردپرس

در این فیلم آموزشی که به زبان انگلیسی میباشد نحوه ایمن سازی و محافظت وب سایت وردپرسی از هک شدن را یاد خواهید گرفت:

http://s6.picofile.com/file/8182296300/How_to_Secure_Wordpress_by_fullsecurity_org.avi.html

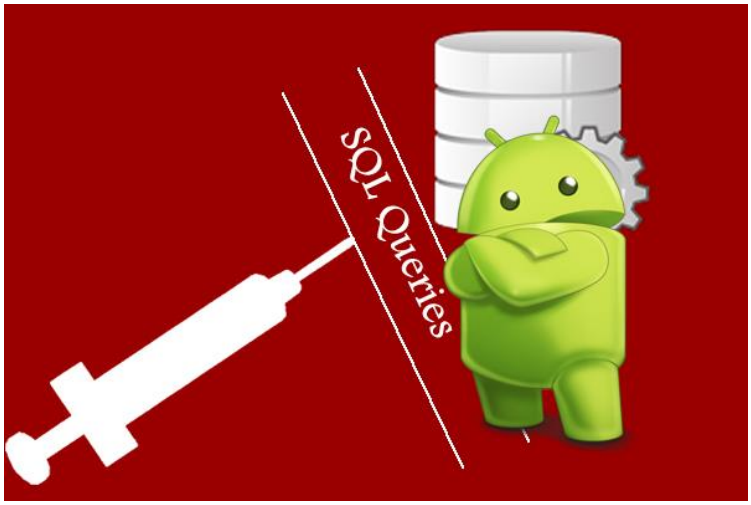
آموزش نفوذ به یک سایت وردپرسی با استفاده از Wpscan:

Wpscan یک ابزار برای نفوذ به وبسایت های وردپرسی است که در کالی لینوکس موجود می باشد. در این آموزش تصویری با نحوه نفوذ به یک سایت وردپرسی با استفاده از این ابزار آشنا می شوید:

http://s4.picofile.com/file/8182049126/Wordpress_Hacking_BruteForce_Wpscan_by_Fullsecurity.avi.html

معرفی نرم افزار Droid SQLi:

Android SQL Injection Tool



یک نرم افزار همانند هویج در ویندوز برای نفوذ با باگ sqli در اندروید استفاده میشود

نحوه استفاده به این صورت است که ادرس قسمت اسیب پذیر سایت را در نرم افزار وارد کرده و عملیات نفوذ را طی میکنید.

برای دانلود این اپلیکیشن اندرویدی از لینک زیر استفاده کنید:

http://yon.ir/droidsqli

برای مشاهده آموزش تصویری این اپلیکیشن نیز میتوانید از لینک زیر استفاده کنید:

http://www.aparat.com/v/tyj6i

معرفی اسکریپت امنیتی RIPS

اگر دقت کرده باشید برنامه های وجود داره که با استفاده از اسکن سایت میان حفره های مدیریت محتوا رو تا حد خوبی شناسایی میکنن یکی از محبوب ترین این ابزار ها اکانتیکس Acunetix هست که با دادن ادرس سایت اقدام به کشف و شناسایی حفره های اسکریپت میکنه. البته این روز ها با کانفیگ مناسب سرور ها این اسکنر در مواردی نمیتونه حتی سایت رو شروع به اسکن کنه چه برسه به کشف حفره ها دلیلش هم اینه تعداد درخواست های زیاد این اسکنر به سرور باعث میشه سرور تشخیص بده ای پی مورد نظر داره حملات تکذیب سرور انجام میده و ای پی رو بلاک کنه که در این شرایط اسکنر Acunetix نمیتونه کارش رو ادامه بده . اسکریپتی قبلا عرضه شده بود به نام RIPS که با نصب این اسکریپت امکان این رو داشتیم سورس فایل های اسکریپت رو توی این اسکریپت به انالیز بگذاریم تا این اسکریپت امنیتی تشخیص بده سورس فایل داره اسیب پذیری هست یا خیر

این اسکریپت از حفره های

Code Execution

Command Execution

Cross-Site Scripting

Header Injection

File Disclosure

File Inclusion

File Manipulation

LDAP Injection

SQL Injection

Unserialize with POP

XPath Injection

پشتیبانی میکنه و تا حد خوبی امکان شناسایی حفره های بالا توی اسکریپت رو داره همچنین یکی از موارد مفیدی که میتونیم بهش اشاره کنیم شناسایی بک دور ها توی اسکریپت هست.

قابلیت های کلی :

- بررسی و ارائه ی آمار آسیب پذیری ها
- گروه بندی کردن آسیب پذیری ها
- توضیحات در رابطه با هر باگ و روش استفاده
- ساخت اکسپلویت برای هر باگ
- آمار فایل ها
- لیست فانکشن ها
- نمایش سورس کد و آدرس فایل بررسی شده
- جست و جو در میان کدها
- لیست ورودی ها
- شناسایی بکدور در اسکریپت

و چندین قابلیت دیگر همه از کارایی های RIPS می باشد .

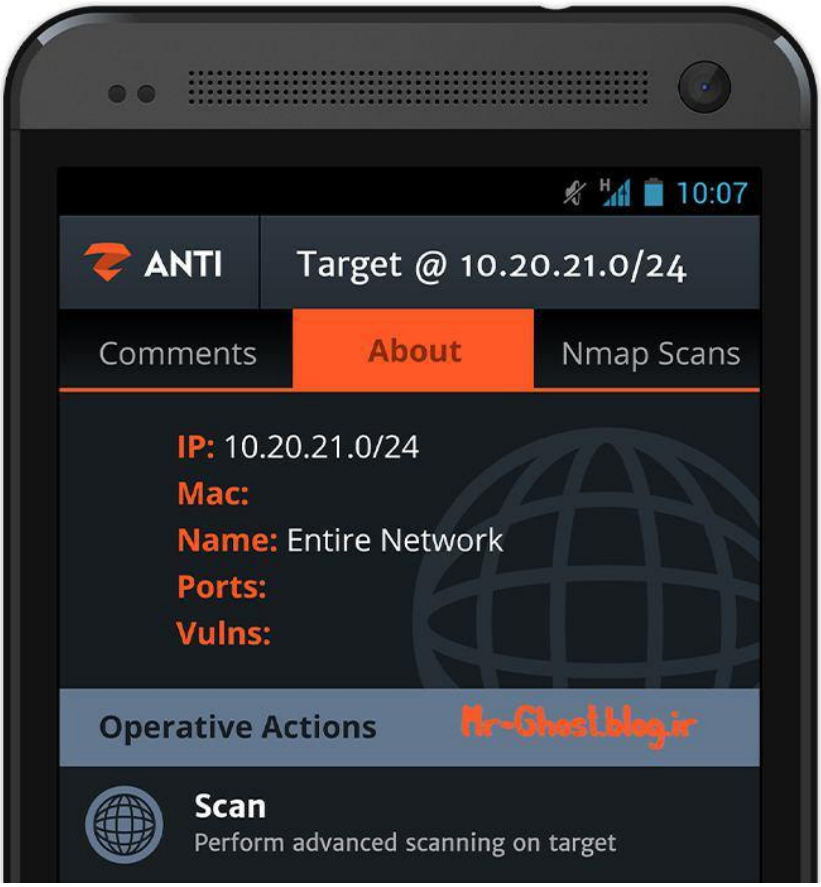
دوستان عزیز میتوانید از لینک زیر اقدام به دانلود کنید.

http://sourceforge.net/projects/rips-scanner/files

برای دانلود آموزش تصویری نحوه استفاده از این اسکریپت نیز از لینک زیر استفاده کنید:

http://s3.picofile.com/file/8188430834/New_Find_Bug_By_Milad_Hacking_FullSecurity_org.rar.html

آموزش Sniff با نرم افزار zANTI در اندروید



با استفاده از این آموزش میتوانید به راحتی رمز های وارد شده،بطور مثال: شخصی وارد حساب کاربری اش مثلاً در blogfa میشود. و به محض وارد شدن به حسابش،نام کاربری و پسورد آن برای شما به نمایش در می آید

نکته: نرم افزار zANTI احتیاج به دسترسی Root دارد

برای دانلود آموزش تصویری این برنامه از لینک زیر استفاده کنید:

http://yon.ir/Mitma

آموزش ساخت رام (بدون برنامه نویسی)

با استفاده از این آموزش میتوانید خیلی ساده و بدون دانش برنامه نویسی رام شخصی خودت را بسازید!

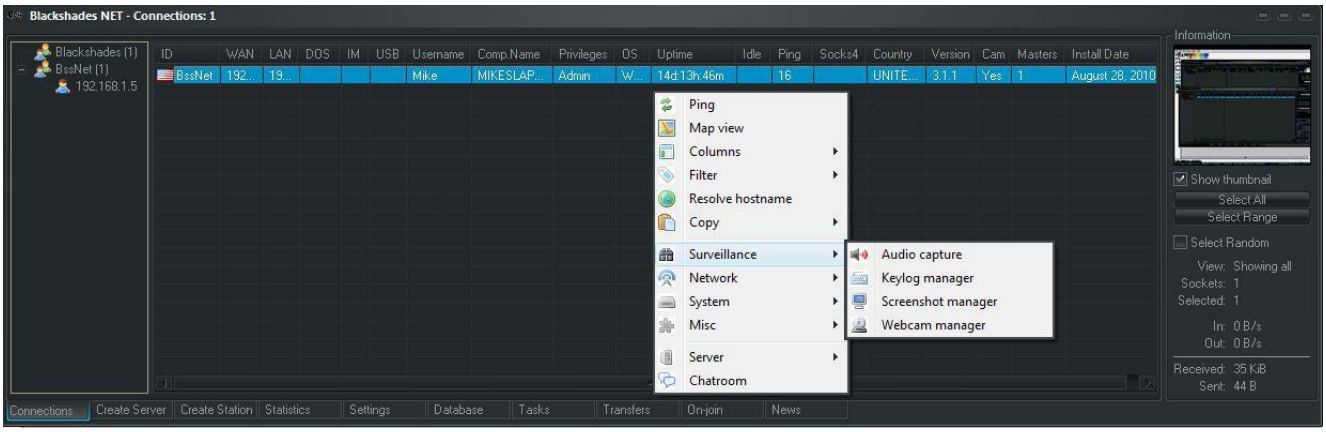
توسط این آموزش میتوانید:

- نام رام را تغییر دهید
- به رام شخصیتان آهنگ و عکس اضافه کنید
- برنامه های دلخواه خود را جزو برنامه های سیستمی قرار دهید
- و.....

دانلود ویدیو آموزشی از لینک زیر:

http://s3.picofile.com/file/8231041142/Make_A_Personal_ROM_Thehacking_Mr_G_o_t_.rar.html

معرفی رات Black Shades



Black Shades

یک رات فوق العاده به اعتقاد بیشتر کاربرانی که از رات ها استفاده میکنند میباشد حتی Back Shades را میتوان یک پله بالاتر از رات DarkComet هم دید. قابلیت های این رات قدرتمند را میتوان با ثبات و ارزان و همچنین قابل اعتماد و محیط آسان و کار پسند اشاره نمود که همگی قابلیت های یک رات بزرگ برای انجام پروژه های بزرگ میباشد Black Shades با زبان دات نت نوشته شده است و قابل اجرا بر روی تمامی نسخه ها از ویندوز قابل اجرا میباشد. نکته جالب را میتوان به برنامه نویس این رات اشاره کرد که برنامه نویس رات Black Shades توسط FBI و از آن به دلیل حمله به کاربران از طریق شبکه اجتمای فیسبوک دستگیر شد. رات ها به نفوذگران امکان هک کردن سیستم عامل هایی همچون ویندوز را میدهند.

پایان –

برای مشاهده آموزشهای بیشتر می توانید کانال ما را در تلگرام دنبال کنید:
Telegram.me/thehacking

برای مشاهده ویدئوها نیز میتوانید کانال مارا در آپارات دنبال کنید:
Aparat.com/thehacking