به نام خدا

Spoofing Method of Hacking

Spoofing یک روش معتبر است که توسط خیلی از سایت های بزرگ امروزی برای رسیدن به مقاصد خودشان استفاده میشود. سایت های بزرگ امروزی اکثرا به یکی از روش های زیر محافظت می شوند:

- htaccess. : در این روش فایل htaccess. در منطقه محافظت شده ی سایت قرار می گیرد که در آن آدرس فایلی که پسوردها در آن قرار گرفته وجود دارد.

- سایت مخفی: در این روش User & Pass های شما توسط برنامه های سایت با Database پسوردها مطابقت داده می شود و شما در صورت مطابقت داشتن پسورد به یک URL انتقال داده می شوید که این URL هر بار تغییر می کند.

- Referal: این موضوع این مطلب آموزشی است. سایت محافظت شده وقتی به شما اجازه دسترسی می دهد که شما فقط و فقط از طریق یک URL مشخص به سایت وارد شده باشید.

این روش هم از یک فایل htaccess. استفاده می کند ولی با این تفاوت که به جای داشتن آدرس فایل محتوای User&Pass ها در آن یک سری خطهای "Mod_rewrite" قرار دارد. برای مثال:

Example Code

```
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://WebMaster_Domain.index.html or blablabla_domainyoutrust.*$
RewriteRule .*\ blabla...
```

شما نیازی به داشتن همه این دستورات ندارید و این فقط یک نمونه برای آشنایی بود. وقتی که فایل htaccess. **چک می کند که شما از طریق** URL **مشخص وارد شدید یا نه دو حالت پیش می آید:**

اول- شما از طریق URL **مشخص وارد شدید بنابراین شما اجازه داخل شدن دارید.**

دوم- شما از URL **مشخص وارد نشده اید و اجازه ی داخل شدن ندارید و** Browser **شما به صفحه ای انتقال داده می شود که در آن پیام** Error **درج شده است.**

حال شروع به توضیح کامل این روش و طریقه نفوذ به آن را به طور کامل توضیح می دم:

اطلاعات مقدماتی

HTTP چیست؟

مجموعه ای از روش ها و قوانینی که برای انتقال اطلاعات برای روی شبکه ی تار عنکبوتی چهانی (World Wide Web) مورد استفاده قرار می گیرد.

اگر اطلاعات طبق این قوانین منتقل نشوند پیام Error ظاهر می شود. انتقال دهندگان اطلاعت در HTTP شامل درخواست کننده ی اطلاعات (Client) و فرستندگان اطلاعات که می تواند هم یک سایت و هم یک شخص دیگر باشد (Server)، نامیده می شوند.

در هر درخواستی که از سوی Client به Server فرستاده می شود شامل بخشی به نام "HTTP Header" می باشد. خود HTTP Header شامل تعدادی "Header Fields" می باشد.

Header Fields ها برای مشخص کردن نوع درخواست و برنامه ای که درخواست را به سرور ارسال کرده است به کار می رود تا سرور با توجه به نوع برنامه اطلاعات را اسال کند، به عنوان مثال Windows Media Player نمی تواند فایل های txt را باز کند. در زیر یک نمونه "HTTP Header" را مشاهده می کنید:

Example Code

```
GET http://www.microsoft.com/ HTTP/1.0
Accept: image/jpeg, image/pjpeg, application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows 98)
Host: www.microsoft.com
Proxy-Connection: Keep-Alive
```

در ادامه ربط این موضوع با Referer را توضیح می دهم...

یکی از Header Field ها "Referer Field" می باشد که معمولا به شکل زیر می باشد:

CODE

```
Referer: http://www.somesite.tk/programs.htm
```

وقتی که شما به وسیله یک Browser (Internet Explorer, NetScape, Opera, NeoPlanet, HotJava, Mozilla, Cubic Eye) وارد سایتی می شوید، Browser، "Referer Field" را به آخرین URL که درخواست شما به آن فرستاده شده تغییر می دهد.

به عنوان مثال هر وقت شما به سایت Google.com بروید و بعد روی لینک Add your ad to google today کلیک کنید، آخرین صفحه ای که شما بازدید کردید Google.com می باشد.
بنابراین "Referer Field" به صورت اتوماتیک و کاملا مخفی به این صورت تنظیم خواهد شد:

Example Code

```
Referer: http://www.google.com/
```

تنها حالتی که درخواست شما "Referer Field" ندارد حالتی است که شما به تازگی Browser را باز کرده باشید و URL مربوط را تایپ یا Copy/Paste کنید. در بقیه حالات هر وقت شما روی یک لینک کلیک کنید همیشه دارای " Referer Field" هستید.

Referer برای این به کار می رود که سایت ها با مشاهده ی اینکه بیشتر **Visitor** های خود از طریق کدام سایت وارد شدند (یا همین تبلیغات که با هر بار کلیک مقداری پول به **WebMaster** سایت داده می شود) یا اینکه شما می خواهید قسمتی از سایت در اختیار عموم نباشد و فقط کسی که از **URL** مشخص و خاصی وارد شده به محتویات سایت دسترسی داشته باشد.

خوب حالا فهمیدیم که Referer ها برای چه به کار می روند؟

حالا ممکن است این سوال برای شما پیش بیاید که چطور می شود Referer رو تغییر داد به چیزی که ما می خواهیم؟ یک Browser درخواست را به وسیله Request-URL و HTTP Headers تولید می کند و به سایت مورد نظر می فرستد. بنابراین چرا برنامه ی خود شما این کار را نکند و مشخصات را به هر چی می خواهید تغییر ندهد و برای سرور نفرستد؟

خوب البته که این کار امکان پذیر است!

بنابراین اگر شما می خواهید به یک سایت بگویید که من از سایت **http://www.google.com** آمدم (در صورتیکه واقعا اینطور نیست) شما فقط باید یک برنامه ای بنویسید که یک درخواست بسازد و در "**Referer Field**" عبارت فوق یعنی **htt://www.google.com** را وارد کند!

به این صورت:

Example Code

```
GET http://www.microsoft.com/directx HTTP/1.0
Accept: */*
Referer: http://www.google.com/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows 98)
Host: www.microsoft.com
```

خوب این درخواست می گوید که شما از طریق گوگل به سایت http://www.microsoft.com/directx رفتید. آیا واقعا اینطور می باشد؟

Referer URL ها برای امنیت به کار می روند!

بعضی سایت ها متاسفانه یا خوشبختانه از **Referer URL** ها برای امنیت سایت استفاده می کنند و به عنوان مثال یک **User** فقط هنگامی اجازه دارد که به یک صفحه در قسمت **Protect** شده ی سایت دسترسی داشته باشد که از یکی **Referer URL** خاص وارد شده باشد.

بعضی سایت ها (نه همه ی آنها) از این روش استفاده می کنند!

در این روش وقتی شما **User&Pass** را وارد **Form** می کنید و بر روی **Submit** کلیک می کنید اطلاعات شما به یک **CGI Script** بر روی سرور فرستاده می شود و اگر **User&Pass** درست باشد شما به **URL** محافظت شده تغییر جهت می دهید.

برای مثال:

http://www.somesite.com/login.cgi ========> http://www.somesite.com/confidentialdata/

حالا وقتی **URL** فوق یعنی **http://www.somesites.com /confidentialdata/** درخواست می شود سرور **Referer URL** را چک می کند.

چرا؟ خوب به دلیل اینکه فقط CGI Script اجازه دارد که شما را Refer دهد در URL محافظت شده، فقط در هنگامی که User&Pass شما درست باشد.

عبور کردن از روش امنیت Referer

همه چیزهایی که شما نیاز دارید این است که referrer URL و Protected URL را پیدا کنید و ...

شما می توانید از برنامه مورد علاقه خودتون برای Edit کردن Request (درخواست) استفاده کنید و Referer URL رو به CGI Script و Target را به URL مخفی تغییر دهید.

فقط مهم ترین موضوع پیدا کردن Referer و URL مخفی، صحیح است. پیدا کردن Referer زیاد سخت نیست، تنها کاری که شما باید انجام دهید این است که به جای User & Pass هر چیزی قرار دهید و Submit را بفشارید. آن URL که بعد از کلیک کردن روی Submit به نمایش در می آید همان Referer URL می باشد.

البته من خودم شخصا فکر می کنم که استفاده از Source File در HTML مطمئن تر باشه، به این صورت که Source File HTML را با Notepad باز کنید و به دنبال چیزی شبیه نوشته زیر بگردید:

Example Code

```
<form method=post action="http://www.somesite.com/login.cgi">
```

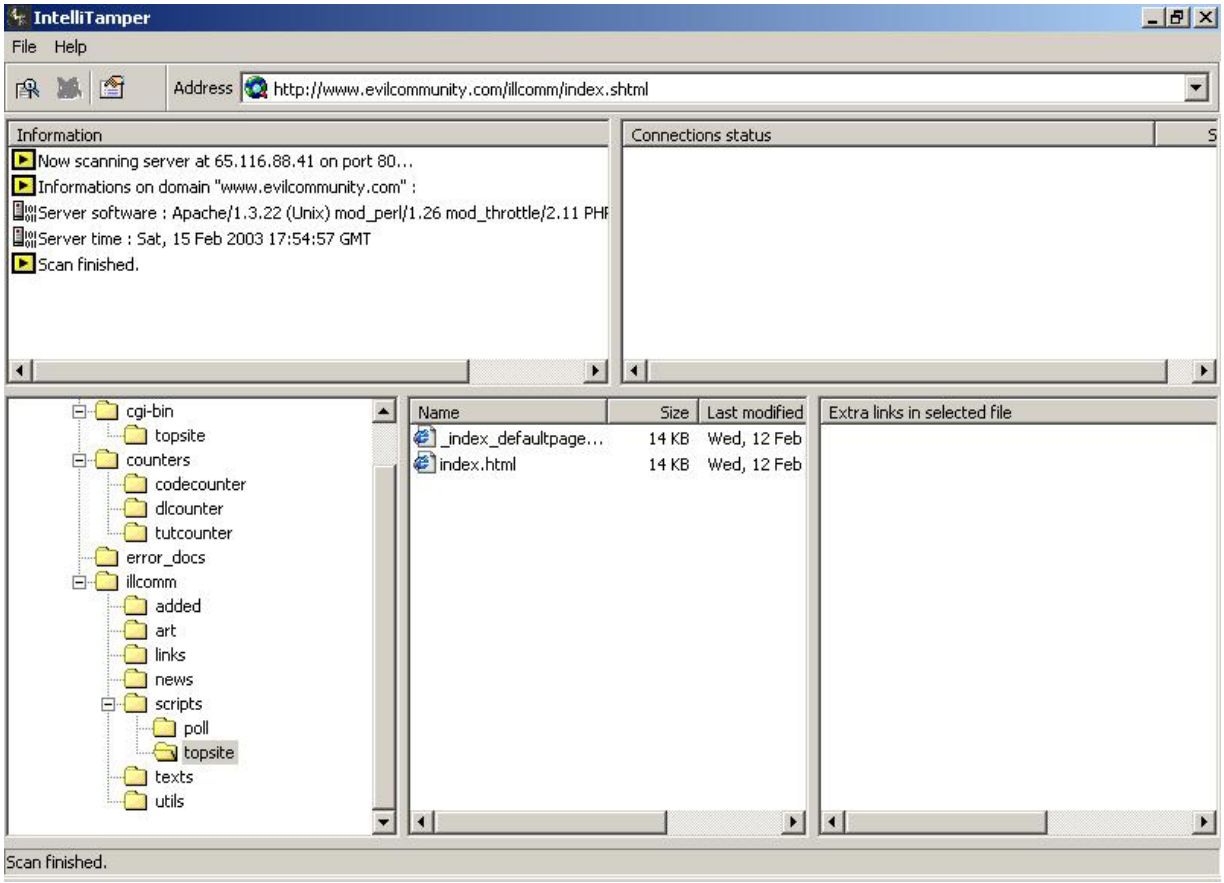
وقتی این نوشته را پیدا کردید، http://www.somesites.com/login.cgi همان referer شماست!

برای پیدا کردن URL مخفی:

راحت ترین کار این است که شما یک User & Pass از آن سایت داشته باشید و به URL مورد نظر دست پیدا کنید. البته در بیشتر حالات شما ممکن است که نتوانید به User & Pass درست دست پیدا کنید. برای این حالات من توصیه می کنم که برنامه هایی مثل:

Intellitamner

را دانلود کنید. سایت را برای Dir هایی مثل secret، content و ... سرچ کنید و URL فایل های HTML درون آن را پیدا کنید.



در بعضی مواقع ممکن است که نتایج حاصلاز Search مطلوب نباشد یا سایت مورد نظر درخواست مربوط بـه Search را قبـول نکند!

در ادامه چند برنامه و طریقه استفاده از بهترین آنها را توضیح می دهم....

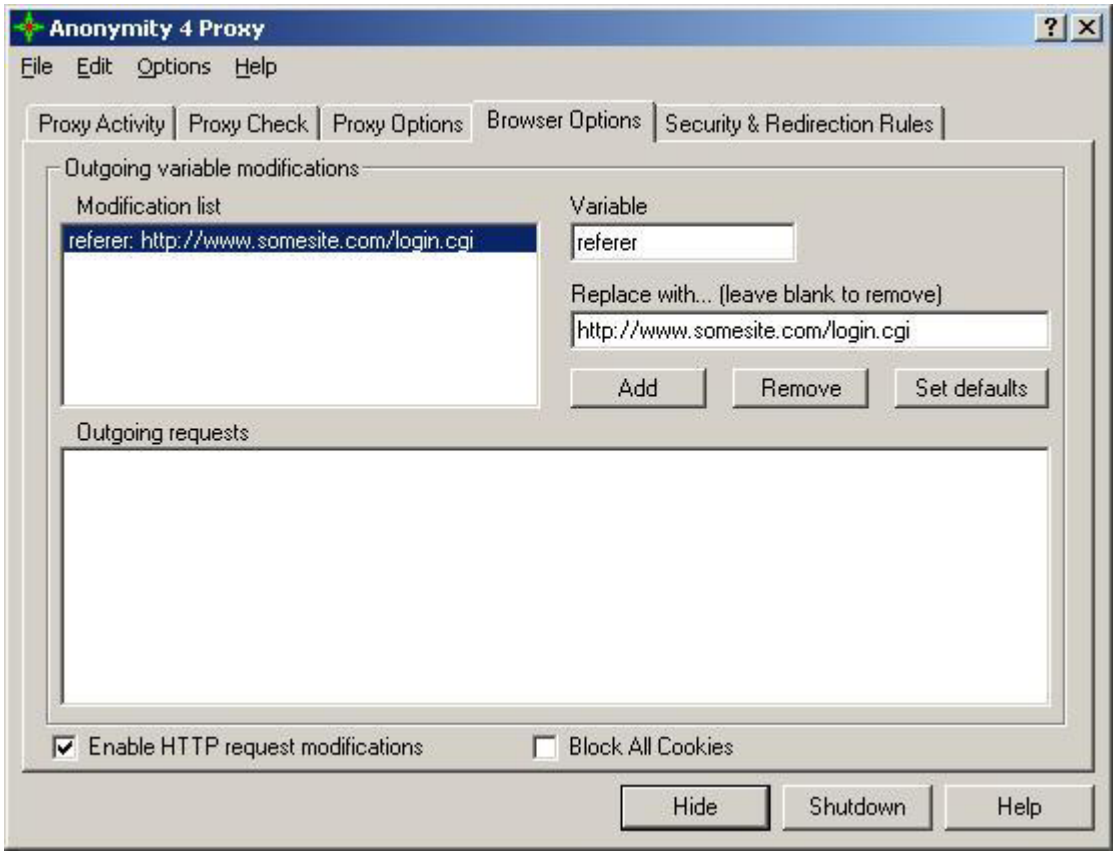
چند برنامه وجود دارد که می توانید از آنها برای Edit کردن request استفاده کنید:

A4 Proxy (Anonymity 4 Proxy)

RefCheat by Ksoze

M-Spoofer

A۴ Proxy



این برنامه انتخاب خود من هست که از امکانات خوبی برخوردار است. شما می توانید علاوه بر Edit کردن Request، از یـک Proxy Server هم استفاده کنید:

برای تنظیم این برنامه:

۱- به برگه ی "Browser Option" مراجعه کنید.

۲- در قسمت "Variable" عبارت "Referer" را تایپ کنید.

۳- در قسمت "Replace with"، URL مربوط به Referer را تایپ کنید به عنوان مثال:

http://www.somesites.com/login.cgi

۴- قسمت Add را بفشارید.

خوب در سمت چپ این را مشاهده می کنید:

Example Code

```
referer: http://www.somesite.com/login.cgi
```

خوب حالا به URL مخفی بروید! به همین سادگی!

خوب در پایان شاید شما متوجه شده باشید که این خیلی روش ساده ای برای نفوذ است. پس چرا دیگران از این روش استفاده نمی کنند؟

خوب در جواب باید بگم که فقط افراد محدودی از این روش آگاهی دارند و خیلی از این افراد نمی خواهند که با دیگران در میان بگذارند و افرادی هم که اطلاع ندارند براشون مهم نیست!!!

پایان مقاله

Written by: **wolf_of_night**

Mail: **sarve_paidar@yahoo.com**

Report any typing mistake in the text

Crouz Security Team

Czar Admins
Rara Avis Member
Oxlip Site
Ubiquitous and
Zealot men