به نام خدا

دستکاری تاریخچه به صورت بین سایتی

OWASP Attack Category: Cross Site History Manipulation (XSHM)

توضیحات

XSHM یک SOP (مخفف Same Origin Policy به معنای سیاست های یکسان بودن مبداء و ماهیت) برای تهدیدات امنیتی است. SOP به عنوان مهمترین مفهوم امنیتی در مرورگرهای جدید است. SOP به این معناست که صفحات وب با مبداء و ماهیت های مختلف در طراحی (مثل تفاوت در پروتکل ها) نمی توانند با یکدیگر ارتباط برقرار کنند. تهدید XSHM زمانی رخ می دهد که شی Historyی مرورگر در سمت کلاینت، بر اساس هر سایت به صورت مناسب جداسازی نشده باشد. دستکاری و تغییر تاریخچه ی مرورگر ممکن است منجر به ایجاد مشکل در SOP شود و برای هکر امکان حمله ی CSRF و سایر اکسپلوییت ها را فراهم سازد. از قبیل: تجاوز به حریم شخصی کاربری، تشخیص وضعیت لاگین، نگاشت منابع، بدست آوردن اطلاعات حساس، ردیابی فعالیت های کاربر و دزدیدن پارامترهای URL.

عوامل ریسک

دستکاری تاریخچه مرورگر باعث مشکلات SOP و تجاوز به حریم شخصی کاربران می شود. با استفاده از CSRF و دستکاری history، علاوه بر یکپارچگی یا همان Integrity [مترجم: از پارامترهای امنیت]، محرمانگی یا همان confidentiality نیز مورد حمله قرار می گیرد. همچنین می توانیم به بازخوردها از مبداء های مختلف دسترسی پیدا کرده و اطلاعاتی از سایت های دیگر بدست آوریم.

tamadonEH@gmail.com
https://twitter.com/tamadonEH

مباحث زیر بر اساس حمله ی XSHM بدست می آیند:

* افشای شرط ها به صورت بین سایتی (Cross-site)

* تشخیص لاگین

*تشخیص وضعیت

*بدست آوردن اطلاعات

*ردیابی کاربران به صورت بین سایتی (Cross-site)

*مورد یابی (enumeration) پارامتر/URLها به صورت بین سایتی (Cross-site)

افشای شرط ها به چه معناست؟

افشای شرط ها (condition leakage) زمانی رخ می دهد که هکر بتواند به مقادیر حساس موجود در جملات شرطی موجود در برنامه ی مورد حمله دسترسی پیدا کند. برای مثال اگر یک سایت شامل عبارت منطقی زیر باشد:

```
Page A: If (CONDITION)
            Redirect(Page B)
```

هکر می تواند CSRF را اجرا کرده و بر اساس بازخورد، به مقادیر موجود در شرط پی برد. این حمله از طرف سایت هکر انجام می شود و سپس سایت هکر یک درخواست بین سایتی را به سایت قربانی ارسال می کند و با دستکاری شی History یک بازخورد از اطلاعات افشاء شده ی درخواستی از سایت قربانی به دست می آورد. در مثال بالا بیان این نکته ضروری است که می توان دستور redirect در کد را به روشنی ظاهر کرد و یا آن را به وسیله ی عملگرهای محیطی کامل کرد.

روند حمله:

۱. ساخت یک IFRAME با آدرس صفحه ی B یعنی src=Page B

۲. مقدار فعلی طول History را به خاطر بسپارید.

۳. src مربوط به IFRAME را به صفحه ی A تغییر دهید.

۴. اگر مقدار طول History تغییر نکرد، یعنی این که شرط جمله درست (TRUE) بوده است.

tamadonEH@gmail.com
https://twitter.com/tamadonEH

تشخیص لاگین

دموی زیر در صورتی که فردی به وسیله ی IE در فیس بوک لاگین کرده باشد، وضعیت او را نمایش می دهد. «آیا من در حال استفاده از فیس بوک هستم؟»

بدست آوردن اطلاعات بین سایتی

دست یافتن به اطلاعات حساس از روی صفحه ی یک مبداء متفاوت در صورتی که یک شرط برای ریدایرکت پیاده سازی شده باشد، امکان پذیر است: فرض کنید که در یک برنامه ی مدیریت منابع انسانی (HR) که دسترسی به صورت عمومی نیست. یک کاربر قانونی بتواند کارمندان را با استفاده از نام، حقوق یا موارد دیگر جستجو کند. در صورتی که جستجو هیچ نتیجه ای نداشت، برنامه یک فرمان ریدایرکت اجرا کرده و کاربر را به صفحه ی «پیدا نشد» ریدایرکت کند. برای این کار از URL زیر استفاده می کنیم:

```
http://Intranet/SearchEmployee.aspx?
name=Jon&SalaryFrom=3000&SalaryTo=3500
```

و هکر با مشاهده ریدایرکت به «پیدا نشد» می تواند به اطلاعات حساسی در خصوص حقوق کاربر برسد. روند این حمله به صورت زیر است:

۱. یک IFRAME با آدرس NotFound.aspx بسازید.

۲. مقدار فعلی طول Hisory را به خاطر بسارید. ۳. مقدار src در IFRAME را به «SearchEmployee.aspx?name=Jon&SalaryFrom=3000&SalaryTo=3500» تغییر دهید.

۴. اگر مقدار طول History ثابت ماند؛ یعنی اینکه جستجو هیچ نتیجه ای نداشته است.

با تکرار حمله ی بالا با مقادیر مختلف برای پارامتر حقوق،هکر می تواند به اطلاعات حساسی مثل مقدار حقوق هر کارمند دسترسی پیدا کند. این مورد یک حمله ی جدی از افشاسازی بین سایتی است. اگر صفحه ای قبلا برای جستجو در قسمت فرمانِ شرط یک ریدایرکت را اجرا کند به صورت بالقوه به XSHM آسیب پذیر بوده و خروجی آن در افشاءسازی بسیار شبیه XSS خواهد بود. برنامه ممکن است به خودیِ خود نسبت به XSS در امان باشد اما اجرای آن از یک سایت دیگر و توسط یک IFRAME درون آن، می تواند آن را آسیب پذیر کند.

حملات مشابه:

Cross-site Scripting (XSS)

Cross-Site Request Forgery (CSRF)

آسیب پذیر های مشابه:

Cross Site Scripting Flaw

منابع:

Presentation in OWASP Israel Local Chapter Meeting (Feb-2010)

Cross site history manipulation (XSHM) Guide

Checkmarx identifies new web browser vulnerability, InfoSecurity Magazine, January 27, 2010

Demo for Internet Explorer users - "Am I using Facebook?"

Wikipedia: Same Origin Policy (SOP)

لینک مقاله:

https://www.owasp.org/index.php/Cross_Site_History_Manipulation_%28XSHM%29

تاریخ ساخت: Feb 9, 2010 یا ۲۰ بهمن ۱۳۸۸

تاریخ تحقیق: August 25, 2014 یا ۳ شهریور ۱۳۹۳

/* تصحیح این مقاله، چه در ترجمه و چه در مباحث علمی ، توسط شما دوستان باعث خوشحالی خواهد بود. لطفا آن را با tamadonEH@gmail.com مطرح نمایید.*/

برای مشاهده لیست مقالات کار شده توسط گروه ما به لینک زیر مراجعه فرمایید:

https://github.com/tamadonEH/list/blob/master/list.md

tamadonEH@gmail.com
https://twitter.com/tamadonEH