به نام خدا

پروژه ۱۰ آسیب پذیری اول اپلیکیشن های تحت وب در سال ۲۰۱۳ از اواسپ،

شماره ۴ ارجاع مستقیم به شیءها به صورت ناامن

OWASP Top 10 Project 2013 - A4 Insecure Direct Object References

ویژگی های این مورد Application Specific

انواع کاربران سیستم شما را مورد مطالعه قرار می دهد. آیا تمام کاربران تنها به انواع مشخص و تحت کنترلی از داده های سیستم دسترسی دارند؟

قابلیت اکسپلوییت شدن: آسان (حالت وسط؛ یعنی ۲ از ۳)

هکری که به عنوان کاربری مجاز برای سیستم شناخته می شود، می تواند به آسانی مقدار پارامترهایی که به صورت مستقیم جهت ارجاع استفاده می شوند را به نوعی تغییر دهد که به شی دیگری که برای آن مجاز نیست، ارجاع داده شود. آیا دسترسی افزایش یافته است؟

میزان شیوع: رایج (بدترین حالت؛ یعنی ۲ از ۳)
قابلیت شناسایی: آسان (راحت ترین حالت؛ یعنی ۳ از ۳)

برنامه های کاربردی معمولا از یک نام واقعی و یا کلید یک شیء در زمان تولید و ساخت یک صفحه ی وب استفاده می

کنند. معمولا برنامه ها کاربران را به منظور اعتبارسنجی برای شیء هدف صحت سنجی نمی کنند که نتیجه ی آن، رخنه ی ارجاع مستقیم به شیءها به صورت ناامن می شود. آزمایشگر (هکر) به راحتی می تواند مقادیر این پارامترها را به منظور تشخیص این نوع از رخنه، دستکاری کند. در تحلیل و آنالیز کدها، صحت سنجی مناسب و بر اساس اعتبارسنجی به سرعت نمایان می شود.

میزان تاثیر آن: متوسط (حالت میانی؛ یعنی ۲ از ۳)

این نوع از رخنه می تواند تمام داده ها که توسط پارامترها ارجاع داده می شوند را در خطر قرار دهد. مگر اینکه شیء ارجاعی، غیرقابل پیش بینی باشد. برای هکر دسترسی به تمام داده های فعال از این نوع، آسان خواهد بود.

تاثیر آن در تجارت:

ارزش تجاریِ داده های منتشر و ظاهر شده را مورد مطالعه قرار می دهد.

آیا ممکن است به واسطه ی این آسیب پذیری به شهرت شما آسیب برسد؟

آیا من یک آسیب پذیری از این نوع هستم؟

بهترین راه برای فهمیدن این موضوع که آیا برنامه نسبت به ارجاع مستقیم به شیءها به صورت ناامن آسیب پذیر است یا خیر این است که تمام اشیاء ارجاعی به صورت مناسب حمایت و محافظت شوند. برای رسیدن به این هدف موارد زیر را مورد مطالعه قرار دهید:

۱- در ارجاعات مستقیم به منابع *محدود و کنترل شده*، آیا در صورت درخواست کاربر مجاز به یک صفحه ی مشخص، برنامه می تواند کار صحت سنجی را به درستی انجام دهد؟

۲- اگر ارجاع به صورت ارجاع *نامستقیم* بود، آیا نگاشت به ارجاعِ مستقیم جهت محدود ساختن مقادیر مجاز برای کاربر جاری، با شکست مواجه می شود؟

بازبینی کدهای برنامه به سرعت مشخص می کند که آیا این رویکرد به صورت امن پیاده سازی شده است و یا خیر. مورد آزمایش قرار دادن نیز می تواند جهت هویت سنجی ارجاع به شی ها به صورت مستقیم موثر بود و امن بودن آن را مشخص کند. عموماً ابزارهای خودکار نمی توانند جهت پیدا کردن این آسیب پذیری مفید باشند. چراکه این گونه ابزارها نمی توانند مشخص کنند که چه کارهایی جهت محافظت لازم است و یا کدام امن و کدام ناامن است.

چگونه از این آسیب پذیری جلوگیری کنم؟

جهت پیشگیری از ارجاع مستقیم به شیءها به صورت ناامن لازم است که رویکردی برای محافظت از اشیاء قابل دسترسی هر کاربر انتخاب شود. (برای مثال شماره شیء و نام فایل):

۱- *برای هر کاربر یا نشست از ارجاع غیرمستقیم به شی استفاده کنید.* این اقدام از هدف قرار دادن مستقیم هکر به منابع غیرمجاز جلوگیری می کند. برای مثال به جای کلیدهای دیتابیس، از یک لیست بازشونده ی ۶ تایی از منابع مجاز برای کاربر جاری که از عدد ۱ تا ۶ برای مشخص کردن مقداری که کاربر انتخاب کرده است، استفاده کنید. برنامه برای هر کاربر می بایست یک ارجاع غیرمستقیم را نگاشت کند که به کلید واقعی دیتابیس روی سرور بازگردد. EASPI از اواسپ شامل نگاشت های ارجاع دسترسی به صورت تصادفی و ترتیبی می شود که برنامه نویسان با استفاده از آن می توانند ارجاع به شیء ها به صورت مستقیم را از برنامه های خود حذف کنند.

۲- *دسترسی را چک کنید.* هرگونه استفاده از ارجاع به شیءها به صورت مستقیم از یک محل غیرقابل اعتماد را باید از لحاظ کنترل و دسترسی و به منظور اطمینان یافتن از اینکه کاربر برای شیءای که درخواست کرده مجاز است است و یا خیر، چک کنید.

سناریوهای حمله در قالب مثال:

برنامه از داده های بدون صحت سنجی در فراخوانی های SQL که به اطلاعات حساب ها دسترسی دارد، استفاده می کند:

```
String query = "SELECT * FROM accts WHERE account = ?";
PreparedStatement pstmt = connection.prepareStatement(query , … );
pstmt.setString( 1, request.getParameter("acct"));
ResultSet results = pstmt.executeQuery( );
```

هکر به راحتی پارامتر 'acct' را با توجه به شماره حسابی که می خواد در مرورگرش تغییر می دهد. اگر صحت سنجی به صورت نامناسبی انجام نشده باشد، هکر به جای اینکه تنها به حساب مشتری ای که مشخص شده دسترسی یابد، می تواند به تمام حساب های کاربری دسترسی پیدا کند.

```
http://example.com/app/accountInfo?acct=notmyacct
```

منابع:

در مورد سایر منابع نیز، یا ترجمه ی آن ها در گروه موجود است و یا در حال ترجمه ی آن هستیم.

منابع موجود در OWASP:

- OWASP Top 10-2007 on Insecure Dir Object References
- ESAPI Access Reference Map API
- ESAPI Access Control API (را مشاهده کنید isAuthorizedForData(), isAuthorizedForFile(), isAuthorizedForFunction())

برای نیازمندی های کنترل دسترسی اضافی، ASVS requirements area for Access Control (V4) را مشاهده کنید.

منابع خارجی:

- CWE Entry 639 on Insecure Direct Object References
- CWE Entry 22 on Path Traversal (مثالی است از حمله ی ارجاع به شیء به صورت مستقیم که توسط گروه هم ترجمه شده است)

لینک مقاله: https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

/* 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:

http://tamadon.net/list