عنوان: **باگ Directory Traversal در سایت**
نویسنده: وحید نصیری
تاریخ: ۱۳۹۱/۰۵/۰۳ ۹:۴۴
آدرس: www.dotnettips.info
برچسب‌ها: ASP.Net, Security

من فایل‌های سایت جاری رو در مسیر استاندارد app_data ذخیره سازی می‌کنم. علت هم این است که این پوشه، جزو پوشه‌های محافظت شده‌ی ASP.NET است و کسی نمی‌تواند فایلی را مستقیما از آن دریافت و یا سبب اجرای آن با فراخوانی مسیر مرتبط در مرورگر شود.
این مساله تا به اینجا یک مزیت مهم را به همراه دارد: اگر شخصی مثلا فایل shell.aspx را در این پوشه ارسال کند، از طریق مرورگر قابل اجرا و دسترسی نخواهد بود و کسی نخواهد توانست به این طریق به سایت و سرور دسترسی پیدا کند.
برای ارائه این نوع فایل‌ها به کاربر، معمولا از روش خواندن محتوای آن‌ها و سپس flush این محتوا در مرورگر کاربر استفاده می‌شود. برای نمونه اگر به لینک‌های سایت دقت کرده باشید مثلا لینک‌های تصاویر آن به این شکل است:

```
http://site/file?name=image.png
```

Image.png نام فایلی است در یکی از پوشه‌های قرار گرفته شده در مسیر app_data.
File هم در اینجا کنترلر فایل است که نام فایل را دریافت کرده و سپس به کمک FilePathResult و return File آن‌را به کاربر ارائه خواهد داد.
تا اینجا همه چیز طبیعی به نظر می‌رسد. اما ... مورد ذیل چطور؟!

لاگ خطاهای فوق مرتبط است به سعی و خطای شب گذشته یکی از دوستان جهت دریافت فایل web.config برنامه!
متدهای Server.MapPath یا متد return File و امثال آن تمامی به کاراکتر ویژه ~ (اشاره‌گر به ریشه سایت) به خوبی پاسخ می‌دهند. به عبارتی اگر این بررسی امنیتی انجام نشده باشد که کاربر چه مسیری را درخواست می‌کند، محتوای کامل فایل web.config برنامه به سادگی قابل دریافت خواهد بود (به علاوه هر آنچه که در سرور موجود است).

چطور می‌شود با این نوع حملات مقابله کرد؟
دو کار الزامی ذیل حتما باید انجام شوند:
الف) با استفاده از متد Path.GetFileName نام فایل را از کاربر دریافت کنید. به این ترتیب تمام زواید وارد شده حذف گردیده و فقط نام فایل به متدهای مرتبط ارسال می‌شود.
ب) بررسی کنید مسیری که قرار است به کاربر ارائه شود به کجا ختم شده. آیا به c:\windows اشاره می‌کند یا مثلا به c:\myapp\app_data ؟
اگر به لاگ فوق دقت کرده باشید تا چند سطح بالاتر از ریشه سایت هم جستجو شده.

نتیجه گیری:

اگر در برنامه‌های وب خود (فرقی نمی‌کند مرتبط به چه فناوری است)، نام فایلی را از کاربر جهت ارائه محتوایی به او دریافت و از این نام فایل بدون هیچ نوع بررسی خاصی، مستقیما در برنامه استفاده می‌کنید، برنامه شما به مشکل امنیتی Directory Traversal مبتلا است.

پ.ن.

-1 این باگ امنیتی در سایت وجود داشت که توسط یکی از دوستان در روزهای اول آن گزارش شد؛ ضمن تشکر!

-2 از این نوع اسکن‌ها در لاگ‌های خطاهای سایت جاری زیاد است. برای مثال به دنبال فایل‌هایی مانند DynamicStyle.aspx و css.ashx یا theme.ashx می‌گردند. حدس من این است که در یکی از پرتال‌های معروف یا افزونه‌های این نوع پرتال‌ها فایل‌های یاد شده دارای باگ فوق هستند. فایل‌های ashx عموما برای flush یک فایل یا محتوا به درون مرورگر کاربر در برنامه‌های ASP.NET Web forms مورد استفاده قرار می‌گیرند.

نظرات خوانندگان

نویسنده: فربد صالحی
تاریخ: ۱۳۹۱/۰۵/۰۳ ۱۱:۱۷

تا جایی که من متوجه شدم شما در کنترلر File، اسم فایل رو دریافت می‌کنید و اون رو به مسیری داخل App_Data نگاشت میدید و بعد فایل رو از اون مسیر به کاربر return می‌کنید. اگه به این صورته سوالی واسه من پیش اومده:
همونطور که خودتون مثال زدید مهاجم ممکنه به جای اسم فایل یک مسیر مثلا ~/web.config رو به کنترلر بفرسته، خب اگه با این مسیر به صورت یک اسم برخورد بشه مثلا میشه :

```
~/App_Data/~/web.config
```

درسته؟ یعنی در این صورت هم باز از ریشه، فایل web.config برمیگرده؟

نویسنده: وحید نصیری
تاریخ: ۱۳۹۱/۰۵/۰۳ ۱۱:۴۰

- این مورد چطور؟

```
var path = Server.MapPath("~/App_Data/../web.config");
```

حتما یکبار خروجی آن‌را دیباگ کنید؛ جالب است.
کاربر هم بجای مسیر یک تصویر یا فایل، مسیر زیر را وارد کرده:

```
../web.config
```

+ عرض کردم در راه‌حل‌های عنوان شده.
اولین بررسی دریافتی از کاربر باید این مورد باشد:

```
var fileName = Path.GetFileName("~/web.config");
```

و نه استفاده مستقیم از نام دریافتی از وب.
خروجی متد فوق (web.config خالی) دیگر به ریشه سایت و یا هیچ مسیری اشاره نخواهد کرد.

نویسنده: فربد صالحی
تاریخ: ۱۳۹۱/۰۵/۰۳ ۱۳:۴۵

اتفاقا خودم به استفاده از ".." توجه کردم، ولی چون تست نکردم این مورد رو ، تصورم این بود که تو سی شارپ جواب نمیده

نویسنده: رحمت اله رضایی
تاریخ: ۱۳۹۱/۰۵/۰۳ ۲۱:۴۹

هدف تست دیشب مشکل دیگری بود که در مطلبی جدا به آن خواهم پرداخت. اما برای اینکه بدانید برای این مورد اخیر چقدر بی توجهی می‌شود کافیست در گوگل صفحاتی را جستجو کنید که آدرسهایی اینگونه دارند و سعی کنید با تغییر آدرس، فایل web.config را دانلود کنید :

```
.../download.aspx?file=...
.../download.ashx?file=...
.../get.aspx?file=...
.../get.ashx?file=...
.../download.aspx?path=...
```

```
.../download.ashx?path=...
...
```

به این صورت جستجو کنید :

```
inurl:"/download.ashx?path="
```

سایتهای فارسی زیادی هم میتوانید پیدا کنید که این مشکل را دارند.

نویسنده: بهروز راد
تاریخ: ۱۳۹۱/۰۵/۰۴ ۷:۵۸

من این مشکل رو قبلاً در BlogEngine.NET دیده بودم که برطرفش کردن.

نویسنده: فرهاد یزدان پناه
تاریخ: ۱۳۹۱/۰۵/۰۴ ۱۴:۳۰

آیا ذخیره محتواهای ارسالی (فایل، تصویر و ...) در پایگاه داده بهتر نیست؟
همچنین پشتیبان گیری را راحت می‌کند.

نویسنده: وحید نصیری
تاریخ: ۱۳۹۱/۰۵/۰۴ ۱۴:۳۴

بله. همینطوره. به شرطی‌که امکانات سخت افزاری مهیا چنین اجازه‌ای رو به شما بدهد. مثلا سرور اختصاصی داشته باشید با RAM و CPU قابل قبول. به عبارتی در شبکه‌های خصوصی شرکت‌ها، نه سایت‌های عمومی با حداقل‌هایی که در اختیار دارند. یا پردازش ابری ... مثلا برای سازمان‌هایی که می‌تونند هزینه کنند یا دسترسی به این امکانات دارند.

نویسنده: محمد صاحب
تاریخ: ۱۳۹۱/۰۵/۰۴ ۱۵:۱۵

ممنونم خیلی جالب بود...
یک روش هم میتونه Encrypt کردن نام فایل باشه که البته سربار خودش رو داره...

نویسنده: فرهاد یزدان پناه
تاریخ: ۱۳۹۱/۰۵/۰۴ ۱۵:۵۳

بله در فضاهایی همچون Azure محدودیت هایی بر روی اندازه پایگاه داده و ... وجود دارد. ولی نه در هر نوع محیط ابری.
در ضمن الان شما برای جلوگیری از خیلی مسائل مجبور شدید یک Handler جهت پراکسی اطلاعات (چه ارسالی و چه دریافتی) ایجاد کنید که از خیلی لحاظ مشابه ذخیره فایل‌ها در پایگاه داده باشه.
در ضمن مگه اندازه فایل‌های ارسالی و ... چقدر است که نیازمند مقدار زیادی پردازش باشه. استفاده از مکانیزم‌های Cache موجود در asp.net هم می‌تونه کمک کنه.
حرف شما از خیلی لحاظ صحیحه و شکی در اون نیست ولی میشه به راه حل‌های دیگری هم فکر کرد.

نویسنده: رضوی
تاریخ: ۱۳۹۱/۰۵/۰۵ ۱۵:۸

سلام

باگهایی از این قبیل به باگهای **File Inclusion** معروفند که به دو دسته Remote File Inclusion و Local File Inclusion تقسیم می‌شوند و هکرها با استفاده از آنها می‌تواند به بسیاری از اطلاعات سرور دست پیدا کنند و یا بدون آپلود، شل بگیرند.

نویسنده: وحید نصیری
تاریخ: ۱۳۹۱/۰۵/۰۵ ۱۵:۵۹

البته در گزارشات متداول منتشره، هر دو عبارت به جای هم بکار برده می‌شوند و استفاده از file inclusion بیشتر برای سایت‌های PHP و لینوکسی مرسوم است؛ چیزی مثل این:

```
http://site.com/forcedownload.php?file=../../../../../../../../../etc/passwd
```

نویسنده: مهدی پایروند
تاریخ: ۱۳۹۱/۰۵/۱۷ ۱۳:۵۳

بله چندتایی از این سایتها رو منم تونستم ببینم، ولی نکته جالب اینه که سایتهای غیر ایرانی این مسئله رو حل کردند

نویسنده: میثم جوادی
تاریخ: ۱۳۹۱/۰۵/۳۰ ۲۰:۳۵

یه روش دیگه واسه دانلود Web.config