بخش نخست

آشنایی با SQL Injection

چگونه از برنامه خود در برابر هکرها محافظت کنیم؟

محمد غفاری

با گذشت بیش از ده سال از حمله به پورت‌های باز و سرویس‌های رخنه‌پذیر توسط مهاجمین، امروزه مدیران سیستم با نصب دیواره‌های آتش و انجام برخی موارد امنیتی، تنها امکان مشاهده برخی سرویس‌های ضروری را فراهم می‌کنند که بسیاری از این سرویس‌ها هم پچ شده و غیرقابل نفوذ هستند. بنابراین امروزه مهاجمین سیستم‌های رایانه‌ای، استراتژی خود را از تهاجم به سیستم عامل به‌سوی تهاجم علیه برنامه‌های در حال اجرا روی سیستم عامل‌ها تغییر داده‌اند. آنچه مسلم است انگیزه اصلی این افراد در سرقت اطلاعات، سرویس‌ها و به‌طورکلی هرآنچه منفعتی برای ایشان ایجاد کند تمرکز یافته است.

بی‌گمان برنامه‌نویس باآگاهی از تهدیدهای موجود می‌تواند اقدام به ایمن‌سازی برنامه خود در برابر حملات مخرب کند. در این مقاله کوشش شده است تا برخی روش‌های رایج نفوذ و تخریب برنامه‌های تحت وب معرفی شود.

سه‌کوئل اینجکشن

در این تکنیک، مهاجم با تزریق دستورات SQL مورد نظر خود در کنار دستورات اصلی برنامه، اقدام به تخریب لایه دیتای برنامه می‌کند. در صورتی که این عمل با موفقیت انجام شود، مهاجم قادر به بازیابی، تغییر و یا حذف اطلاعات ذخیره شده در بانک اطلاعاتی خواهد بود.

با ارائه چند مثال به بررسی عملی این تکنیک می‌پردازیم:

صفحه وبی را در نظر بگیرید که برای انجام عملیاتی خاص، اقدام به دریافت شماره شناسایی از کاربر می‌کند. در صورتی که کاربر اقدام به تایپ شماره "۱۲۳۴" در فیلد مورد نظر کند، دستور زیر به بانک اطلاعاتی ارسال خواهد شد:

```
SELECT A,B
FROM testTable
WHERE id = 1234
```

در نتیجه دستور فوق، فیلدهای A و B که شماره شناسایی آنها "۱۲۳۴" است، از جدول testTable انتخاب خواهند شد.

حال در صورتی که مهاجم اقدام به تایپ عبارت "1234 OR 1=1" در فیلد فوق کند، دستور SQL به شکل زیر ارسال خواهد شد:

```
SELECT A,B
FROM testTable
WHERE id = 1234 OR 1=1
```

از آنجا که "۱=۱" موجود در قسمت شرطی دستور SELECT فوق همواره برقرار است، این عبارت منجر به خنثی شدن قسمت شرطی دستور شده و معادل با دستور زیر خواهد بود:

```
SELECT A,B
FROM testTable
```

همان‌طور که مشخص است، در نتیجه این دستور **تمام** رکوردهای موجود در جدول انتخاب خواهد شد.

بنابراین مهاجم در این بخش با آگاهی وسیع از دستورات، با قرار

عکس: mckinleys.net

دادن دستور مورد نظر خود در کنار دستور اصلی برنامه، به‌جای انتخاب رکورد مرتبط با شماره شناسایی خود، اقدام به مشاهده تمام رکوردهای جدول کرده است.

این آسیب‌پذیری می‌تواند بسیار مخرب‌تر از مورد بالا باشد. برای مثال فرض کنید اطلاعات مربوط به کاربران در جدولی به‌نام USERS ذخیره شده باشد:

حال در صورتی‌که مهاجم عبارت "DROP TABLE USERS 1234;" را در فیلد شماره شناسایی وارد سازد، دستور SQL زیر اجرا خواهد شد:

```
SELECT A,B
FROM testTable
WHERE id = 1234; DROP TABLE Users;
```

دستور فوق متشکل از دو دستور SQL است که دستور اول برای انتخاب فیلدهای A و B از جدول testTabe است، اما دستور دوم صرف‌نظر از دستور اول، منجر به حذف جدول users خواهد شد. بی‌شک در پی این حمله، ورود کاربران به سیستم مختل خواهد شد.

حال به بررسی روش‌های معمول در مقابله با سه‌کوئل اینجکشن می‌پردازیم:

- اعتبارسنجی مقادیر با تعیین نوع و تعداد کاراکترهای مجاز، انتخاب نوع داده‌ای مناسب و تعیین دامنه معتبر برای فیلدها.

در صورتی که فیلد مورد نظر در برگیرنده مقادیر عددی است، از پذیرش حروف و نشانه اجتناب کنیم.

نسبت به کاراکترها، نشانه‌ها و واژگان وارد شده توسط کاربر، به‌ویژه در موارد کلمات و نشان‌های مورد استفاده در دستورات SQL، حساسیت نشان دهیم.

انتخاب نوع داده‌ای مناسب در ساختار تشکیل دستور SQL:

```
"SELECT A,B FROM testTable
WHERE id = " + testVariable + ";"
```

در اینجا مقدار متغیر testVariable به‌عنوان مقدار id در نظر گرفته می‌شود. حال اگر مقدار id از نوع عددی باشد، انتخاب نوع داده رشته‌ای برای متغیر testVariable منجر به افزایش آسیب‌پذیری برنامه خواهد شد، چراکه در این‌صورت کاربر مجاز به وارد کردن هر ترکیبی از کاراکترها علاوه بر اعداد است.

- استفاده از حساب کاربری مشخص با سطح دسترسی محدود در اجرای دستورات بانک اطلاعاتی.
- استفاده از پارامترها و رویه های ذخیره شده در بانک اطلاعاتی.

در این‌صورت پارامترها از نظر نوع ارسال شده و طول مجاز بررسی می‌شوند، همچنین مقادیر ارسالی از نوع دستورات اجرایی در نظر گرفته نمی‌شوند.

- و سرانجام، پرهیز از نمایش صریح خطاهای موجود در اجرای دستورات به کاربر.

منابع:

wikipedia و msdn.microsoft.com

پرسش و پاسخ

کردن Deep Freeze استفاده کنید. راه دیگری که توصیه می‌کنیم تنها در صورت نیاز از آن استفاده کنید، این است که سیستم را خاموش کنید و باتری پشتیبان را از روی مادربورد بردارید.

سپس با جسمی رسانا دو قسمت فلزی محل قرارگیری باتری را به هم اتصال دهید. مدتی (حدود ۵ دقیقه) صبر کنید. سپس سیستم را بدون باتری روشن کرده و دوباره خاموش کنید. حال باتری را در جای خود قرار دهید و سیستم را راه‌اندازی کنید.

منصور آیراتین از گنبد کاووس- وقتی متنی را همرا با عکس‌هایش از یک صفحه اینترنتی کپی و به درون مایکروسافت ورد پیست می‌کنم، عکس‌ها را نشان نمی‌دهد. چطور می‌شود کاری کرد که عکس‌های داخل متن نیز نشان داده شود؟ و همچنین موقع چاپ عکس‌ها نیز چاپ شوند.

عکس‌ها به‌دلیل حجم بیشتری که نسبت به متن دارند زمان بیشتری برای دانلود شدن از اینترنت صرف می‌کنند.

بنابراین چنانچه مدتی صبر کنید عکس‌ها نیز به صفحه ورد کپی می‌شوند. البته می‌توانید در هر زمان با کلیک راست بر روی عکس و ذخیره آن بر روی سیستم خود آنها را بر روی سیستم خود داشته باشید و سپس درون متن Insert کنید.

داود قاسمی از دلیجان - فایل ekrn.exe از نود۳۲ را که باعث بالابردن پردازش CPU می‌شود را چگونه می‌توان پاک کرد؟

این فایل همان‌طور که می‌دانید از پردازش‌های آنتی‌ویروس Nod32 است که مورد نیاز این نرم‌افزار نیز هست. Nod32 را اجرا کنید وکلید F5 را بزنید. به دنبال Real-Time File System Protection بگردید. زیر عبارت Scan On تیک گزینه‌های زیر را بردارید:

File Open
File Creation
Diskette Access

در برخی موارد ویروس‌ها و بدافزارهایی نیز با همین نام اطلاعاتی از سیستم شما به اینترنت ارسال می‌کنند. این فایل‌های در پوشه System32 وجود دارند. بعد از پاک کردن آنها سیستم را با آنتی‌ویروس قوی جستجو کنید و سیستم را دوباره راه‌اندازی کنید.