پروژه پایانی امنیت سیستم های کامپیوتری

استاد : دکتر دیانت

دانشجویان: سارا سادات یونسی - ۹۸۵۳۳۰۵۳
فاطمه عسگری - ۹۸۴۷۱۴۱۴

نیم‌سال دوم
سال تحصیلی ۱۴۰۱-۱۴۰۲

۱.سوال اول

۱.وب سایتی آسیب پذیری SQL دارد ابزاری طراحی کنید که بتواند این آسیب پذیری را کشف و SQL injection انجام دهد می توانید از ابزار sqlMap نمونه برداری کنید برای تست ابزار خود می توانید آزمایشگاه تست نفوذ رایگان DVWA استفاده کنید.

پاسخ

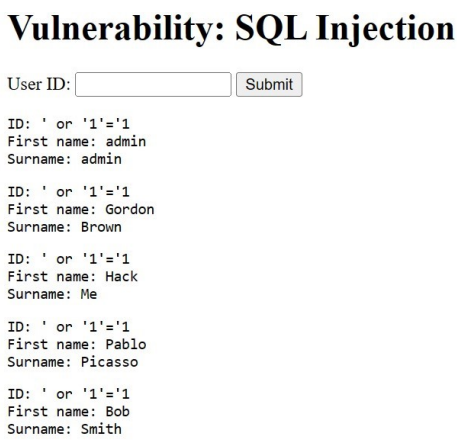
گام های طی شده به شرح زیر است:

- INJECTION SQL چیست؟

- injection Sql ، یکی از رایج‌ترین روش‌های حملات نفوذی به پایگاه داده است. در این نوع حمله، هکر با استفاده از ورودی‌هایی که به پایگاه داده فرستاده می‌شوند، توانایی اجرای دستورات SQL را دارد و می‌تواند اطلاعات محرمانه را از پایگاه داده دریافت کند، داده‌های موجود را تغییر دهد یا حتی پایگاه داده را به صورت کامل نابود کند.برای مثال، فرض کنید یک وب سایت دارای فرم ورود کاربر است که نام کاربری و رمز عبور را از کاربر دریافت می‌کند و سپس آن‌ها را برای استعلام صحت به پایگاه داده ارسال می‌کند. اگر هکری توانسته باشد ورودی‌های فرم را تغییر دهد و یا کدهایی را از طریق فرم اجرا کند، می‌تواند دسترسی به پایگاه داده را به دست آورده و اطلاعات محرمانه را به دست آورد. به عنوان مثال، با وارد کردن یک عبارت SQL نفوذی مانند “’ OR ’۱’=’۱’” به جای نام کاربری و رمز عبور، هکر می‌تواند دسترسی کامل به پایگاه داده را به دست آورد.برای جلوگیری از حملات نفوذی SQL، باید از روش‌هایی مانند استفاده از پارامترهای مشخص در دستورات SQL، استفاده از تابع‌های پیش‌فرض مانند PDO و mysqli در زبان‌های برنامه‌نویسی و استفاده از فیلترینگ و اعتبارسنجی داده‌های ورودی استفاده کرد. همچنین، باید به روزرسانی‌های امنیتی پایگاه داده و سیستم‌های مورد استفاده برای اجرای برنامه‌های وب انجام داده شود. هکرها با وارد کردن کوئری‌هایی که حاوی دستورات SQL هستند، تلاش می‌کنند به پایگاه داده دسترسی پیدا کنند. برخی از کوئری‌هایی که هکرها ممکن است وارد کنند عبارتند از: UNION: SELECT این کوئری برای ادغام دو جدول با ساختار مشابه استفاده می‌شود. هکر با استفاده از این کوئری، می‌تواند اطلاعاتی را که در جدول دیگری وجود دارد، به جدول فعلی اضافه کند OR: ۱=۱ این کوئری برای بررسی موجود بودن یک شرط در دستور SELECT استفاده می‌شود. اگر هکر این کوئری را وارد کند، شرطی که می‌خواهد بررسی شود را تائید خواهد کرد. DROP: TABLE این کوئری برای حذف یک جدول از پایگاه داده استفاده می‌شود. با وارد کردن این کوئری، هکر می‌تواند جدولی را از پایگاه داده حذف کند. INSERT: users INTO این کوئری برای اضافه کردن یک رکورد جدید به جدول کاربران استفاده می‌شود. با وارد کردن این کوئری، هکر می‌تواند یک رکورد جدید با اطلاعاتی که می‌خواهد، به جدول کاربران اضافه کند. قسمت اول پروژه

یک کد پایتون برای تست نفوذ به دیتابیس مجازی Appli- Web Vulnerable (Damn DVWA cation) است که با استفاده از زبان پایتون نوشته شده است.در این برنامه، یک لیست از پارامترهای مختلف برای تست نفوذ به دیتابیس تنظیم شده است. هر پارامتر شامل دو فیلد است: name و payload. فیلد name عنوان پارامتر را مشخص می‌کند و فیلد payload حمله‌ای است که به سمت دیتابیس ارسال می‌شود. این حملات شامل استفاده از injection SQL هستند.سپس، توابعی تعریف شده‌اند و تابع sendrequest وظیفه ارسال درخواست با پارامترهای مشخص شده را دارد و محتوای دریافتی را در یک فایل مشخص ذخیره می‌کند. تابع main هم مسئول اجرای برنامه است. این تابع

ابتدا پارامترهای لیست paramslist را برای تست نفوذ به دیتابیس ارسال می‌کند و محتوای دریافتی را در فایل‌های مجزا ذخیره می‌کند.در این کد، مقدار cookies نیزset شده است. این مقدار همراه با هر درخواست ارسال می‌شود تا سرور بتواند اعتبار شناسه جلسه را بررسی کند و اجازه دسترسی به سیستم را بدهد.در نهایت، هر فایل خروجی در پوشه ReceivedhtmlResponses ذخیره می‌شود که با استفاده از مقدار outputfile در تابع sendrequest تعیین شده است.چند نمونه عکس از خروجی فایل های html: AlwaysTrueScenario:



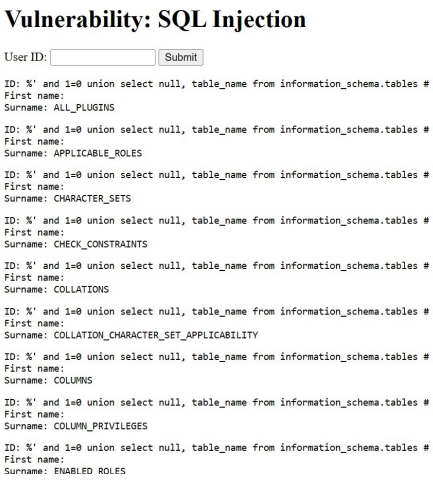
Vulnerability: SQL Injection

User ID: Submit

```
ID: ' or '1'='1
First name: admin
Surname: admin

ID: ' or '1'='1
First name: Gordon
Surname: Brown

ID: ' or '1'='1
First name: Hack
Surname: Me

ID: ' or '1'='1
First name: Pablo
Surname: Picasso

ID: ' or '1'='1
First name: Bob
Surname: Smith
```

شکل ۱: html shape ۱

- Displayalltablesininformationschema:



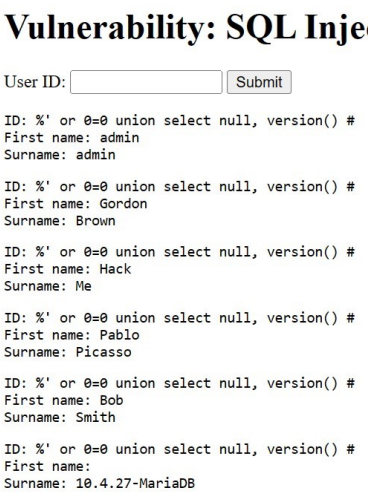
Vulnerability: SQL Injection

User ID: Submit

```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ALL_PLUGINS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: APPLICABLE_ROLES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHECK_CONSTRAINTS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMN_PRIVILEGES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ENABLED_ROLES
```

شکل ۲: html shape ۲

- DisplayDatabaseVersion



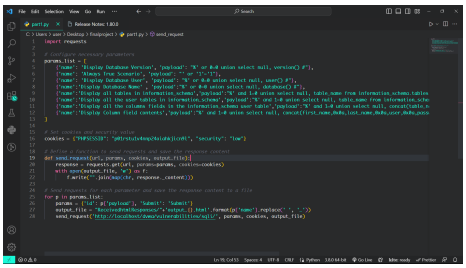
Vulnerability: SQL Injection

User ID: Submit

```
ID: %' or 0=0 union select null, version() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, version() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, version() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, version() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, version() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, version() #
First name:
Surname: 10.4.27-MariaDB
```

شکل ۳: html shape ۳

-
- کد اجرایی



شکل ۴: کد اجرایی

۲.سوال دوم

ابزار های تست نفوذ وب را بررسی کنید و یک سناریو در این سطح به دلخواه پیاده سازی کنید و یک سناریو در این سطح به دلخواه پیاده سازی کنید . میتواند برای پیاده سازی سناریو خود از DVWA استفاده کنید.

پاسخ

گام های طی شده به شرح زیر است:

- قسمت دوم پروژه

- در ابتدا چند ابزار تست نفوذ را بررسی می کنیم:

- به طور کلی، ابزارهای تست نفوذ به دو دسته تقسیم می‌شوند:

- ابزارهای تست نفوذ شبکه: این ابزارها برای بررسی آسیب‌پذیری‌های شبکه مورد استفاده قرار می‌گیرند و شامل ابزارهایی مانند Nmap، Wireshark، Metasploit Aircrack-ng، و Nessus می‌شوند.

- ابزارهای تست نفوذ برنامه‌های کاربردی: این ابزارها برای بررسی آسیب‌پذیری‌های برنامه‌های کاربردی مانند وب‌سایت‌ها و برنامه‌های موبایل استفاده می‌شوند و شامل ابزارهایی مانند Burp Suite، OWASP ZAP، Sqlmap و Acunetix می‌شوند.

- OWASP ZAP: Proxy Attack Zed OWASP یا به اختصار ZAP، ابزاری متن‌باز و رایگان برای تست نفوذ بر روی برنامه‌های کاربردی و وب‌سایت‌هاست. این ابزار به صورت خودکار آسیب‌پذیری‌های موجود در برنامه‌های کاربردی را شناسایی می‌کند و به کارشناسان امنیتی اجازه می‌دهد تا این آسیب‌پذیری‌ها را بررسی و رفع کنند. ZAP قابلیت‌های متعددی دارد که شامل تست نفوذ، بررسی آسیب‌پذیری‌های XSS و SQL، injection بررسی امنیت SSL/TLS و بسیاری از ویژگی‌های دیگر است.

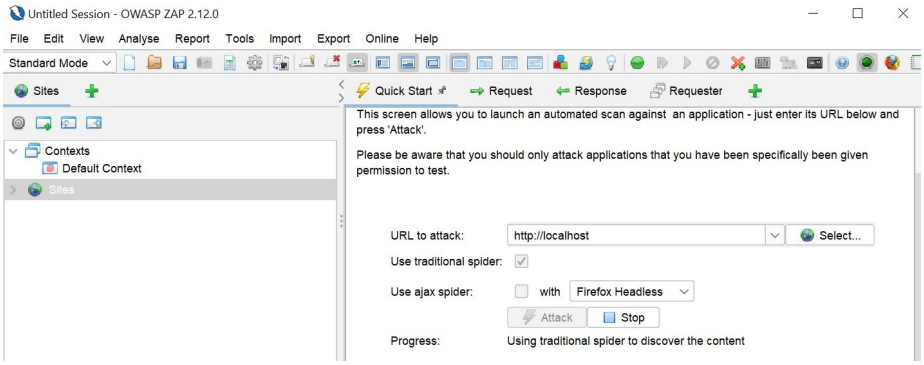
- Sqlmap Sqlmap ابزاری متن‌باز و رایگان برای تست نفوذ به دیتابیس‌های مختلف است. با استفاده از این ابزار، کارشناسان امنیتی می‌توانند آسیب‌پذیری‌های موجود در دیتابیس‌ها را شناسایی کنند و به دسترسی غیرمجاز به داده‌های حساس جلوگیری کنند. Sqlmap قابلیت‌های متعددی دارد که شامل تست نفوذ به دیتابیس‌های MySQL، Oracle، PostgreSQL- Mi crosoft SQL Server و بسیاری دیگر است.

- Acunetix Acunetix یک ابزار تجاری برای تست نفوذ به وب‌سایت‌ها است. این ابزار به کارشناسان امنیتی اجازه می‌دهد تا آسیب‌پذیری‌های موجود در وب‌سایت‌ها و برنامه‌های وب را شناسایی و رفع کنند. Acunetix دارای قابلیت‌هایی مانند تست نفوذ به برنامه‌های وب، بررسی آسیب‌پذیری‌های XSS و SQL، injection بررسی امنیت SSL/TLS و بسیاری از ویژگی‌های دیگر است. به عنوان یک ابزار تجاری، Acunetix دارای قیمتی است که برای استفاده تجاری توصیه می‌شود. ZAP OWASP با استفاده از روش‌های تست خودکار و دستی، به کاربر اجازه می‌دهد تا به صورت جامع و کامل از امنیت وب‌سایت خود آگاهی پیدا کند و در صورت وجود آسیب‌پذیری، اقدام به رفع آن کند. این ابزار امکان انجام تست‌های پویا و استاتیک را دارد و قابلیت انجام تست‌های خودکار را نیز داراست.

- ZAP، OWASP از پروتکل‌های HTTP و HTTPS پشتیبانی می‌کند و به کاربر اجازه می‌دهد تا با استفاده از آن، ترافیک HTTP و HTTPS را مانیتور و تحلیل کند. همچنین، این ابزار به

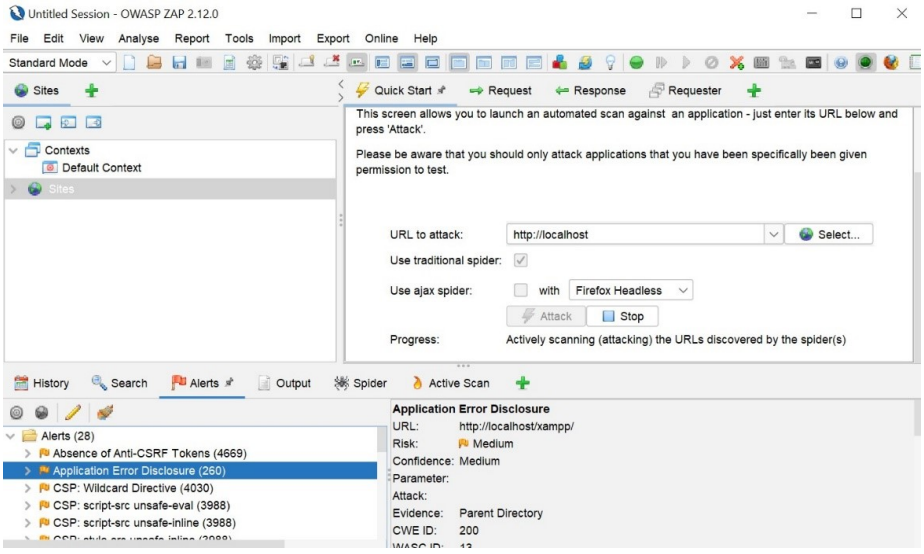
کاربر اجازه می‌دهد تا به صورت دستی یا خودکار، فرایند تست را برای تست نفوذ به وب‌سایت‌ها شروع کند.

ZAP OWASP یکی از ابزارهای محبوب و پرکاربرد در زمینه تست نفوذ وب‌سایت‌ها است و به دلیل ویژگی‌های قابل تنظیم و امکانات بالایی که دارد، به عنوان یکی از بهترین ابزارهای تست نفوذ در حوزه امنیت وب‌سایت‌ها شناخته می‌شود. در ابتدا url لوکال هاست به صورت زیر وارد میکنیم:



شکل ۵: تصویر url

– و یکسری alert به تعداد۲۸ تا به ما میدهد:



شکل ۶: تصویر alart

- لیستی از آسیب‌پذیری‌هایی که ZAP OWASP در localhost درdvwa بخش "Alerts" نمایش داده می‌شود. هر آسیب‌پذیری یک عنوان (نام) دارد که با کلیک کردن روی آن، جزئیات بیشتر در مورد آن آسیب‌پذیری نمایش داده می‌شود.در لیستی از آسیب‌پذیری‌هایی که شما در بخش "Alerts" در ZAP OWASP هست، هر آسیب‌پذیری با یک شماره شناسایی و یک نام مشخص شده است. برخی از آسیب‌پذیری‌های مشخص شده در این لیست عبارتند از:

- Tokens: Anti-CSRF of Absence - به وجود آمدن این آسیب‌پذیری نشان می‌دهد که بر روی صفحات وب، از توکن‌های CSRF استفاده نشده است.

- Disclosure: Error Application - این آسیب‌پذیری به وجود می‌آید زمانی که سایت وب، خطایی را به کاربر نمایش می‌دهد که می‌تواند اطلاعات حساس را نشان دهد.

- Directive: Wildcard CSP: - این آسیب‌پذیری به وجود می‌آید زمانی که سیاست امنیتی محتوای CSP به صورت نادرست تنظیم شده است.

- unsafe-eval: script-src CSP: - این آسیب‌پذیری به وجود می‌آید زمانی که از فانکشن eval در کد JavaScript سایت وب استفاده شده است.

- Browsing: Directory - این آسیب‌پذیری به وجود می‌آید زمانی که دسترسی به لیست فایل‌های موجود در دایرکتوری‌های سایت وب فعال شده است.

- Header: Anti-clickjacking Missing - این آسیب‌پذیری به وجود می‌آید زمانی که از سربرگ‌های امنیتی ضد کلیک جکینگ استفاده نشده است.

- Library: JS Vulnerable - این آسیب‌پذیری به وجود می‌آید زمانی که نسخه‌ای ازکتابخانه‌های جاوااسکریپت استفاده شده در سایت وب، قابلیت‌های امنیتی ناکافی دارد.

- Missing: Header X-Content-Type-Options - این آسیب‌پذیری به وجود می‌آید زمانی که سربرگ‌های امنیتی X-Content-Type-Options فعال نشده است.

- User Controllable HTML Element Attribute (Potential): (XSS) این آسیب‌پذیری به وجود می‌آید زمانی که کاربر می‌تواند ورودی‌های HTML را تغییر دهد و در نتیجه، به حملات XSS منجر شود. توصیه می‌شود که با دقت به تمامی آسیب‌پذیری‌های شناسایی شده توسط ZAP OWASP توجه کنیدو سعی کنید آن‌ها را برطرف کنید تا امنیت سایت وب شما بهبود یابد.

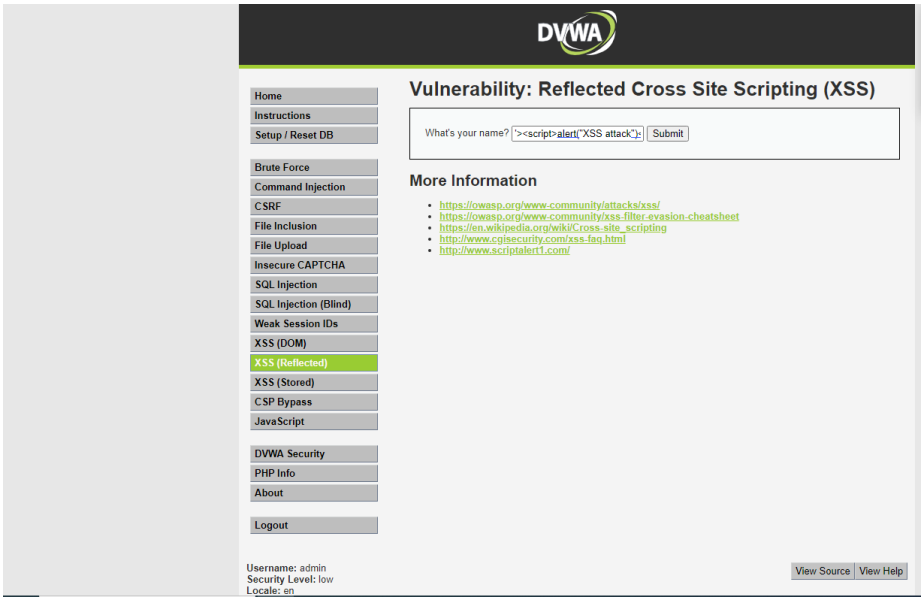
- یک حمله ازمایشی XSS نیز در DVWA انجام دادیم:

- حمله‌ی XSS به معنی اجرای کدهای مخرب در مرورگر کاربر است، که توسط یک مهاجم انجام می‌شود. در این حمله، مهاجم با استفاده از یک کد مخرب به صورت ناشناس، کدی را در صفحه‌ی وبی که توسط کاربر باز می‌شود قرار می‌دهد. این کد مخرب می‌تواند اطلاعات حساس کاربر را ربوده یا به سرور مهاجم ارسال کند.در DVWA، برای آزمایش آسیب‌پذیری XSS، یک فرم ورودی وجود دارد که در آن کاربر می‌تواند یک پیام را وارد کند. اگر این فرم به درستی

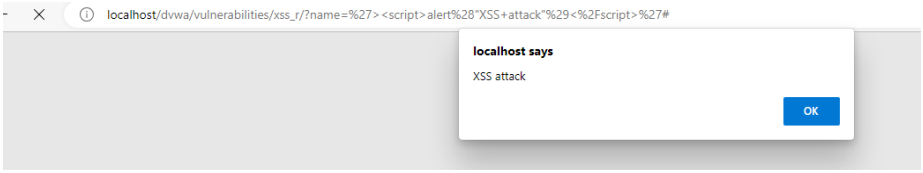
اعتبارسنجی نشود، مهاجم می‌تواند با وارد کردن کدهای مخرب، نفوذ به صفحه‌ی وب کاربر کند و اطلاعات حساس را برداشته یا به سرور خود منتقل کند.به طور کلی، آزمایش روی DVWA نشان می‌دهد که چگونه یک آسیب‌پذیری XSS می‌تواند برای دستیابی به اطلاعات حساس کاربران و نفوذ به سیستم‌ها و شبکه‌ها استفاده شود. این آزمون به کارشناسان امنیتی کمک می‌کند تا با آسیب‌پذیری‌های این نوع آشنا شوند و راهکارهایی برای جلوگیری و رفع آن‌ها پیاده کنند.

- مهاجم می‌تواند HTML و جاوا اسکریپت را در فرم و پست‌های API قرار دهد که اجازه می‌دهد کد به طور خودکار در مرورگر اجرا شود.

- در قسمت XSS(Reflected) یک فرم ساده هست که باید اسم را وارد کنیم اگر عبارت ‘><script>alert(“XSS attack!”)</script>’ وارد کنیم مشاهده می کنیم:



شکل ۷: تصویر ۶



شکل ۸: تصویر ۷

۳.سوال سوم

در مورد تمام جوانب اسیب پذیری SQL و متد های وقوع آن تحقیق کنید و راه های جلوگیری از آن را نیز ذکر کنید.

- Injection یکی از مهم‌ترین آسیب‌پذیری‌های امنیتی در برنامه‌های وب است که می‌تواند به افشای اطلاعات حساس کاربران و حتی در برخی موارد به کنترل کامل سیستم منجر شود. در ادامه به بررسی تمام جوانب آسیب‌پذیری SQL و راه‌های جلوگیری از آن پرداخته‌ایم:

- متدهای وقوع Injection: SQL

- Injection SQL می‌تواند از طریق ورودی‌های مختلف به برنامه‌ی وب وارد شود. برخی از متدهایی که برای وقوع Injection SQL مورد استفاده قرار می‌گیرند عبارتند از:

- ۱. ورودی‌های فرم: نفوذ کننده می‌تواند با استفاده از ورودی‌هایی که در فرم‌های برنامه‌ی وب وجود دارند، دستورات SQL خود را به پایگاه داده ارسال کند.

- ۲. پارامترهای :URL در برخی برنامه‌های وب، پارامترهایی به صورت URL درخواست شده توسط کاربران به برنامه‌ی وب ارسال می‌شوند. نفوذ کننده می‌تواند با استفاده از این پارامترها، دستورات SQL خود را به پایگاه داده ارسال کند.

- ۳. ورودی‌های :HTTP در برخی برنامه‌های وب، ورودی‌های HTTP نیز به عنوان ورودی‌های برنامه‌ی وب استفاده می‌شوند. نفوذ کننده می‌تواند با استفاده از این ورودی‌ها، دستورات SQL خود را به پایگاه داده ارسال کند.

- ۴. فایل‌های بارگذاری شده: در برخی برنامه‌های وب، کاربران می‌توانند فایل‌هایی را برای بارگذاری در برنامه‌ی وب ارسال کنند. نفوذ کننده می‌تواند با استفاده از این فایل‌ها، دستورات SQL خود را به پایگاه داده ارسال کند.

- راه‌های جلوگیری از Injection: SQL برای جلوگیری از وقوع Injection، SQL می‌توانید از راه‌های زیر استفاده کنید:

- ۱. استفاده از Statements: Prepared استفاده از Statements Prepared برای ارسال دستورات SQL به پایگاه داده، جلوگیری از Injection SQL را فراهم می‌کند. در Prepared Statements، بجای ارسال دستورات SQL به پایگاه داده، از پارامترهایی استفاده می‌شود که قبل از ارسال به پایگاه داده، توسط برنامه‌ی وب پر شده و سپس به پایگاه داده ارسال می‌شوند.

- ۲. فیلتر کردن ورودی‌های کاربران: برنامه‌ی وب باید ورودی‌های کاربران را فیلتر کند تا اطمینان حاصل شود که دستورات SQL نامناسب به پایگاه داده ارسال نمی‌شود. برای فیلتر کردن ورودی‌ها، می‌توانید از توابعی همچون ‘htmlspecialchars’ و ‘mysqlirealescapestring’ استفاده کنید.

- ۳. محدود کردن دسترسی به پایگاه داده: برای جلوگیری از Injection، SQL باید دسترسی به پایگاه داده را محدود کنید و فقط به کاربرانی که نیاز به دسترسی دارند، دسترسی را اعطا کنید.

- ۴. به‌روزرسانی نرم‌افزار: برای جلوگیری از آسیب‌پذیری‌های امنیتی، باید نرم‌افزارهای مورد استفاده‌ی خود را به‌روز کنید و به‌صورت دوره‌ای به بررسی آن‌ها بپردازید.

- ۵. استفاده از ابزارهای امنیتی: برای جلوگیری از SQL Injection، می‌توانید از ابزارهای امنیتی مثل فایروال و نرم‌افزارهای ضد ویروس استفاده کنید تا به سیستم خودتان امنیت بیشتری ببخشید.

- دلیل رواج حملات Injection SQL در این بخش به علل فراگیر شدن Injection SQL در وردپرس می پردازیم.

- اکثر پایگاه داده ها بر مبنای SQL هستند.

- وردپرس پرکاربردترین CMS از SQL استفاده می کند.

- تقریبا همه سایت ها دارای فیلدهای ورودی مانند فرم ها هستند.

- کاربر گسترده و دسترسی راحت به ابزارهای Injection SQL

- عدم نیاز به دانش فنی برای استفاده از آن

- روش های شناسایی و مقابله با حملات Injection SQL چنانچه سایت شما با حملات تزریق SQL شده است. در این بخش به شما نحوه روش های شناسایی Injection SQL را آموزش می دهیم.

- ۱- استفاده از اسکنرهای آسیب پذیر مانند WPScan یا ThreatPass

  این پلاگین ها باید به صورت دوره ای از نظر عملکرد بررسی شوند.

- ۲- کنترل آسیب

  ممکن است مهاجم دیتابیس شما را از هر نقطه ای مورد حمله قرار دهد. امتیازات ادمین را برای دسترسی به دیتابیس محدود کنید. تا هکر تنها به دیتابیس به صورت فقط خواندنی دسترسی داشته باشد و نمی تواند کاری انجام دهد.

- ۳- پاکسازی فایل های UDF

  یکی دیگر از راه های جلوگیری از حملات Injection SQL این است که فایل های UDF که مهاجمان از آنها برای حمله استفاده می کنند را پاکسازی کنید.

- ۴- گرفتن بک آپ به صورت دوره ای

  از سایت خود بک آپ های دوره ای داشته باشید و آن را در جای امن نگه دارید.

- ۵- پاکسازی پایگاه داده

۱- همه جداول خود را با استفاده از دستور نمایش جداول جست و جو کنید و به دنبال جدولی به نام Sqlmap باشید.

- ۲- اگر جدول Sqlmap را پیدا کردید نشان می دهد که برای مقابله با وب سایت شما ایجاد شده است. با استفاده از دستور زیر آن را حذف کنید. ؛tables ؛show

- ۳- با کد زیر به دنبال کاربران جدید یا غریبه در دیتابیس خود باشید. Sqlmap TABLE DROP

- $_{T}IMESTAMP(STR_{T}O_{D}ATE(sept222020, 4-$UNIX < u.created AND u AS users FROM * Select .

'malicious'@'localhost'؛ USER DROP

- ۵- رمزهای عبور خود را با استفاده از دستور زیر تغییر دهید.

md۵(rand()))))؛ sha(concat(pass، concat('ZZZ'، = pass SET users UPDATE

- ۶- اجرای حملات شبیه سازی شده

تست نفوذ یا بررسی امنیت وب سایت تان برای محافظت از سایت شما حیاتی است. شما می توانید از یک متخصص کمک بگیرید تا حملات شبیه سازی شده را روی سایت تان اجرا کند. به این صورت می توانید تمامی حفره های امنیتی را قبل از نفوذ مهاجم شناسایی کرده و پوشش دهید.

علاوه بر مواردی که برای شناسایی حملات Injection SQL ذکر شد، این نکات نیز اهمیت دارند: اگر پورت ۳۳۰۶ شما باز است آن را مسدود کنید، دسترسی کاربران دیتابیس را به بخش های ساس محدود کنید، پسورد رمزنگاری شده خود را نیرومندتر کنید.

روش های شناسایی حملات injection sql

.اگر انواع حملات را بشناسید و با راه های نفوذ هکرها آشنا شوید این مزیت را دارد که اقدامت پیشگیرانه را انجام دهید اقدمات ساده از تغییر هاست تا تغییر پیشوند جداول وردپرس به افزایش امنیت کمک می کند.
جلوگیری از حملات Injection SQL قبل از اینکه حمله اتفاق افتد باید از آن جلوگیری کنید. در این بخش به راه های مقابله با حملات injection sql می پردازیم.

- ۱- محدود کردن استفاده از فرم های ورود

تا حد امکان استفاده از فرم های ورودی مانند پاپ آپ های اشتراک را به حداقل برسانید.

- ۲- استفاده از تم ها و افزونه های امن و معتبر

تم و افزونه های خود را از مارکت های معتبر تهیه کنید و هرگز از افزونه های نال شده استفاده نکنید.. به افزونه های ثبت نام و فرم های تماس دقت کنید زیرا ممکن است هر ورودی کاربر تهدیدی برای سایت شما باشد.

- ۳- نسخه وردپرس خود را پنهان کنید

یکی از راه هایی که می توانید سایت خود را از نفوذ حفظ کنید این است که نسخه وردپرس خودتان را با استفاده از کد زیر مخفی کنید.

$$_{a}ction(wp_{h}ead, wp_{g}enerator); 4 - \text{remove}$$

به کاربران دیتابیس خود امتیازات اضافه ندهید. تغییراتی که آنها می توانند روی سایت شما بدهند باید به شیوه ای باشد که تنها بتوانند وظایف خود را انجام بدهند.

نکته: هرگز اطلاعات کاربر اصلی (همه دسترسی ها را دارد) را برای دسترسی به پایگاه داده به سایر کاربران ارائه ندهید.

- ۵- اطلاعات ارسال شده کاربران را بررسی و تایید کنید

یکی دیگر از روش های جلوگیری از Injection SQL بررسی کاراکترهای ورودی کاربران است. برای مثال اگر فیلد ایمیل است دقت کنید که حتما در قالب ایمیل باشد. در تمام بخش ها این احراز را انجام دهید. در صورت صحیح و استاندارد بودن کاراکترها، آن داده تایید شود. دقت کنید هر فیلد ورودی می تواند مستعد حمله و نقوذ باشد.

با استفاده از زبان برنامه نویسی php اطلاعات ارسالی کاربران را کنترل کنید.

برای مثال برای اعداد کد زیر به کار می رود.

$$_{d}igit().\text{ctype}$$

$$_{a}lpha()6 - \text{ctype}$$

در کد های سایت خود مقادیر کوئری های خودتان را داخل تک کوتیشن قرار دهید. برای مثال فرمت اول نسبت به فرمت دوم بیشتر در معرض هک و نفوذ است.

$$\text{id } _{u}ser = \text{id WHERE users FROM name SELECT}$$

$$\text{id' } _{u}ser = \text{id WHERE users FROM name SELECT}$$

- ۷- اجتناب از استفاده از کاراکترهای خاص در کدها

یکی دیگر از راه های جلوگیری از Injection SQL در وردپرس این است که در کوئری ها از کاراکترهای خاص مانند (“)، (‘)، x۰۰ ، ۱a استفاده نکنید. این کاراکترها پر خطر هستند و می توانند در طول حمله استفاده شوند. بهتر است یک کد جایگزین برای آنها در نظر بگیرید.

- ۸- آپدیت وردپرس و افزونه ها

دقت کنید که همیشه وردپرس تان به روز باشد. به علاوه به روزرسانی قالب و افزونه های خود را نیز به صورت دوره ای انجام دهید. استفاده از قالب یا افزونه های نال شده امکان نفوذ را بیشتر می کند. بایستی از افزونه

های معتبر در سایت خود استفاده کنید.

- ۹- استفاده از فایروال

وجود یک فایروال سایت شما را در برابر Injection SQL و سایر حملات محافظت می کند. چند نمونه فایروال وردپرس security WP one in all wordfence، security، itheme و غیره هستند. به علاوه از هاست خود بپرسید که چه امکانات و راه حل ها امنیتی برای وب سایت شما دارد.