

مقدمه و هدف از پروژه

هدف از این پروژه تست و یافتن شکاف های امنیتی در برنامه مورد نظر با ابزارهای معرفی شده است.

معرفی کامل برنامه مورد آزمون

این برنامه که سبدگردانی یا PRX نام دارد به این شکل است که کاربران که شامل دو دسته حقیقی و حقوقی میشوند، ابتدا با شماره تلفن خود در سامانه ثبت نام میکنند و با استفاده از سرویس OTP این شماره ارزیابی میشود و سپس وارد سامانه میشوند. در سامانه بسته به نوع حقیقی یا حقوقی بودن باید اطلاعاتی در قالب فرم هایی پر کرده و در نهایت در یک پرسشنامه شرکت کرده. نتایج این فرم ها و پرسشنامه ها به بخش R&D ارسال شده و متخصصین این بخش با توجه به اطلاعات کاربر و نتایج پرسشنامه میزان ریسک پذیری وی را ارزیابی میکنند و نسبت به آن صندوق سرمایه گذاری مناسب را پیشنهاد میکنند.

* به علت زیاد بودن اطلاعات و جداول فقط تعدادی از آن ها برای نمونه نمایش داده میشود.

نمونه اطلاعاتی که در قالب مشتری حقیقی گرفته میشود:

جدول مشخصات مشتری:

نام خانوادگی:	نام پدر:	نام:
تاریخ تولد:	محل صدور:	کد ملی:
وضعیت تأهل: مجرد □ متأهل □	جنسیت: مرد □ زن □	شماره شناسنامه:
تلفن همراه:	تلفن منزل:	کد پستی:
بهترین زمان برای تماس تلفنی:		دورنگار:
نشانی محل سکونت:		
پست الکترونیک:		

۱- مشخصات عمومی مشتری و افراد تحت تکفل:

۱-۱- مشخصات عمومی افراد تحت تکفل خود را در جدول زیر قید نمایید (شامل همسر، فرزندان و سایر افراد تحت تکفل):

[illegible]

۱-۲- در جدول زیر وضعیت درآمدی خود را قید نمایید:

مبلغ در آمد اصلی و مستمر	سایر درآمدها و عایدات موردی	کمک‌های سایر افراد تحت تکفل در هزینه‌های شما	مبلغ هزینه‌های مستمر و دائمی شما	مبلغ هزینه‌های موردی و اتفاقی شما (در هر ماه)	مبلغ مشارکت شما در هزینه‌های سایرین

۱-۴- وضعیت تحصیلی خود را در جدول زیر قید نمایید:

مدرک تحصیلی	رشته تحصیلی	سال اخذ مدرک	صادر کننده مدرک
□ زیر دیپلم			
□ دیپلم			
□ فوق دیپلم			
□ کارشناسی			
□ کارشناسی ارشد			
□ دکتری			

۱-۵- مشاغلی که در حال حاضر به آنها مشغول هستید و مشاغلی که سابقاً به آنها مشغول بوده‌اید را به ترتیب در جدول زیر بیان کنید:

[illegible]

نمونه اطلاعاتی که در قالب مشتری حقوقی گرفته میشود:

جدول مشخصات مشتری:

نام:		
شماره ثبت:	تاریخ ثبت:	محل ثبت:
کد / شناسه ملی:		
موضوع فعالیت اصلی شرکت طبق اساسنامه:		
موضوع فعالیت اصلی شرکت بر مبنای عملکرد واقعی سه سال گذشته:		
کد پستی:	تلفن ثابت:	
دورنگار:	بهترین زمان برای تماس تلفنی:	
نشانی:		
پست الکترونیک:		
نام نماینده:	کد ملی:	تلفن همراه:

۱-۱- مشخصات عمومی ترکیب هیئت مدیره

ردیف	نام و نام خانوادگی	سمت	مقطع تحصیلی	رشته تحصیلی	سوابق اجرایی	میزان آشنایی با بازار سرمایه (کم، متوسط، خوب)	تجربه سرمایه گذاری شخصی در بورس (دارد، ندارد)
۱							
۲							
۳							

۱-۲- مشخصات عمومی کارشناسان و مدیران بخش سرمایه‌گذاری شرکت

ردیف	نام و نام خانوادگی	سمت	مقطع تحصیلی	رشته تحصیلی	سوابق اجرایی	میزان آشنایی با بازار سرمایه (کم، متوسط، خوب)	تجربه سرمایه گذاری شخصی در بورس (دارد، ندارد)
۱							
۲							
۳							

بعضی اطلاعات بین مشتری حقوقی و حقیقی ثابت است که در قالب کاربر ذخیره میشود مانند:

۲- هدف از سرمایه گذاری:

باتوجه به اینکه تصمیم به ایجاد سبد اوراق بهادار در اوراق بهادار گرفته‌اید، هدف خود را از این سرمایه گذاری بیان کنید:

☐ حفظ ارزش دارایی.

☐ استفاده از عایدات سرمایه گذاری جهت تأمین هزینه‌های خود و افراد تحت تکفل.

☐ استفاده از عایدات سرمایه گذاری به عنوان درآمد ثانویه (جهت افزایش رفاه زندگی).

☐ تأمین وجه مورد نیاز جهت خرید مسکن.

☐ سایر موارد، به تفصیل شرح داده شود:

.....

.....

.....

۳- برنامه‌های آتی:

برنامه‌های آتی، مبالغ مورد نیاز برای اجرای برنامه‌های آتی و موعد زمانی اجرای برنامه‌های آتی خود را به تفصیل شرح دهید.

.....

.....

.....

۴- تجربیات سرمایه گذاری: لطفاً ۵ تجربه اخیر خود در زمینه سرمایه گذاری‌های قبلی را در جدول زیر درج نمایید:

ردیف	نوع سرمایه گذاری	مبلغ سرمایه گذاری	مدت سرمایه گذاری (به ماه)	مبلغ سود یا ضرر	توصیف شما از سود یا ضرر سرمایه گذاری				در صورتی که سرمایه گذاری را به نقد تبدیل نموده‌اید، دلیل تبدیل را بیان کنید
					سود زیاد	سود کم	ضرر کم	ضرر زیاد	
۱									
۲									
۳									
۴									
۵									

۵- دارایی‌ها و ترکیب آن‌ها: لطفاً نوع و ارزش و دارایی‌ها و همچنین درصد تقریبی هر یک از آن‌ها، از کل دارایی‌های خود را در جدول زیر تعیین کنید :

ردیف	نوع دارایی	ارزش روز دارایی‌ها	درصد از کل دارایی‌ها
۱	ساختمان و ملک		
۲	خودرو		
۳	طلا و ارز		
۴	سهام		
۵	اوراق مشارکت دولتی و شرکتی		
۶	وجه نقد / مطالبات از سایر اشخاص / حساب پس انداز و سپرده بانکی		
۷	سایر دارایی‌ها		
جمع			

نمونه ای از پرسشنامه کاربر حقیقی و حقوقی:

ب) پرسشنامه

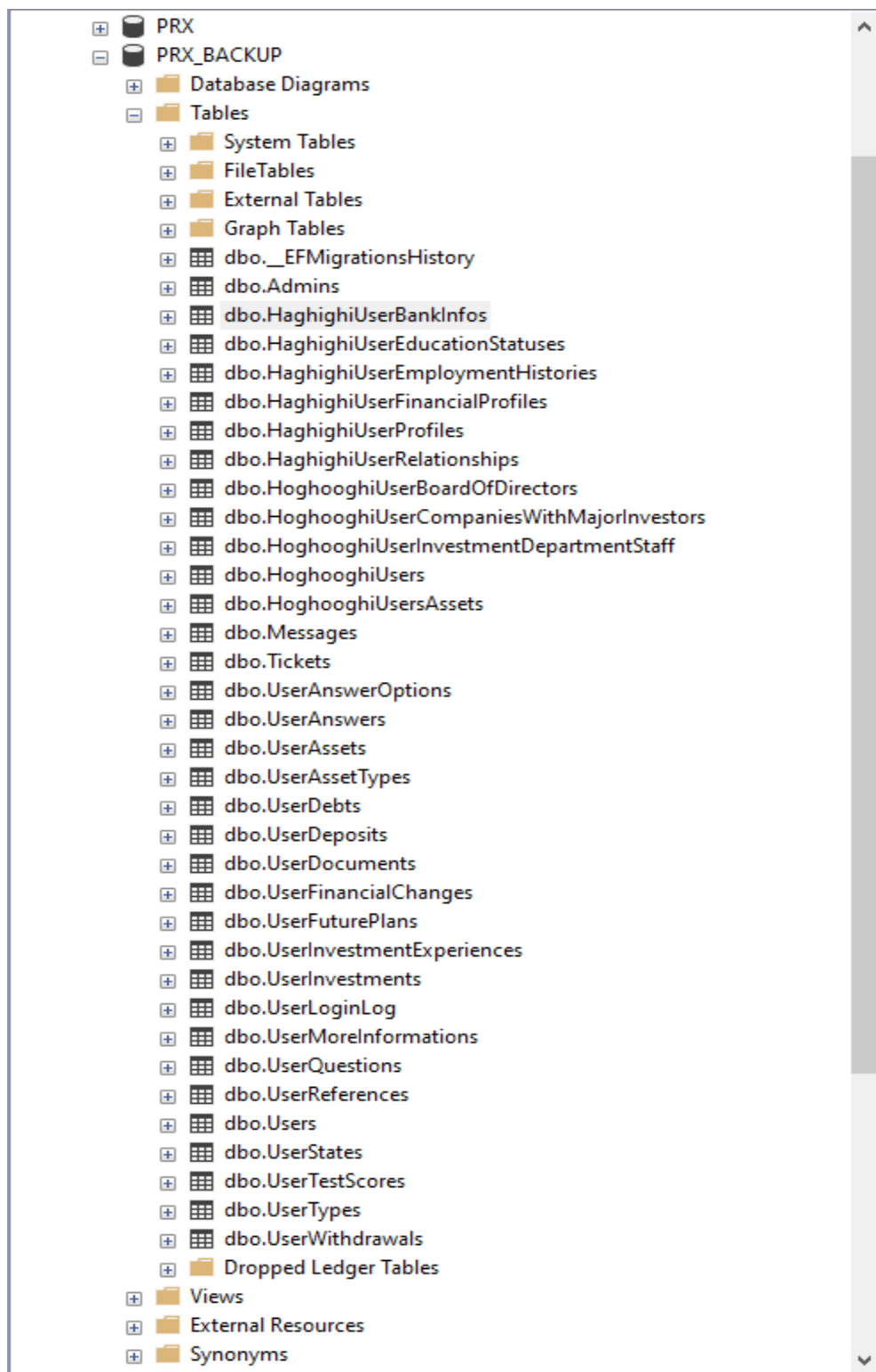
۱- معمولاً وضعیت پس انداز شما به چه صورت است؟

- ☐ الف- درآمدهای معمول من به میزانی نبوده است که بتوانم پس اندازی داشته باشم.
- ☐ ب- معمولاً بیش از ۵۰٪ پس انداز من به صورت نقد و شبه نقد (شامل سپرده بانکی و اوراق مشارکت) بوده است.
- ☐ ج- معمولاً کمتر از ۵۰٪ پس انداز من به صورت نقد و شبه نقد (شامل سپرده بانکی و اوراق مشارکت) بوده است.
- ☐ د- اصولاً پس انداز خود را به صورت نقد یا شبه نقد نگهداری نمی کنم و در اولین فرصت آن را در سایر دارایی های مالی یا دارایی های فیزیکی مختلف سرمایه گذاری می کنم.

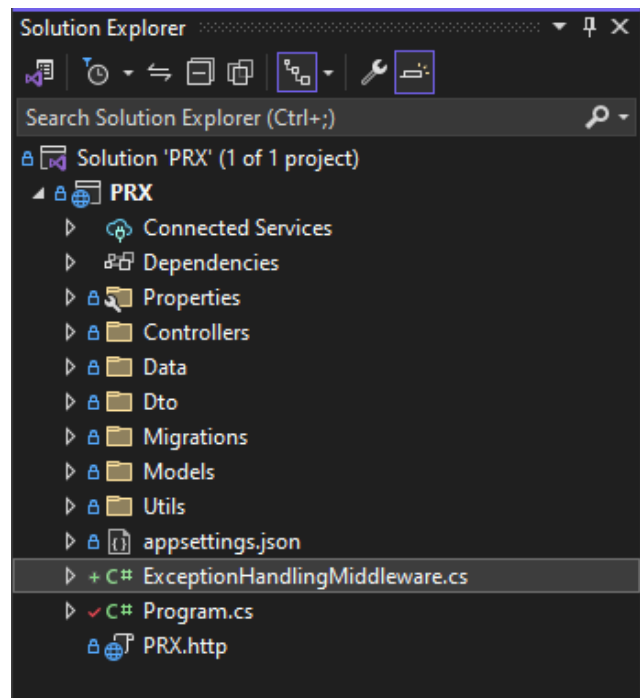
۲- میزان آشنایی شما با امور سرمایه گذاری در اوراق بهادار چقدر است؟

- ☐ الف- به هیچ وجه با سرمایه گذاری در اوراق بهادار آشنایی ندارم.
- ☐ ب- تا حدودی با سرمایه گذاری در اوراق بهادار آشنا هستم ولی درک کاملی از آن ندارم.
- ☐ ج- با سرمایه گذاری در اوراق بهادار آشنا هستم. عوامل مختلفی که بر بازده سرمایه گذاری مؤثر هستند را درک می کنم.
- ☐ د- آشنایی زیادی با سرمایه گذاری در اوراق بهادار دارم. در اتخاذ تصمیمات سرمایه گذاری خود، از تحقیقات انجام شده و سایر اطلاعات مرتبط استفاده می کنم. عوامل مختلفی که بر بازده سرمایه گذاری مؤثر هستند را درک می کنم.

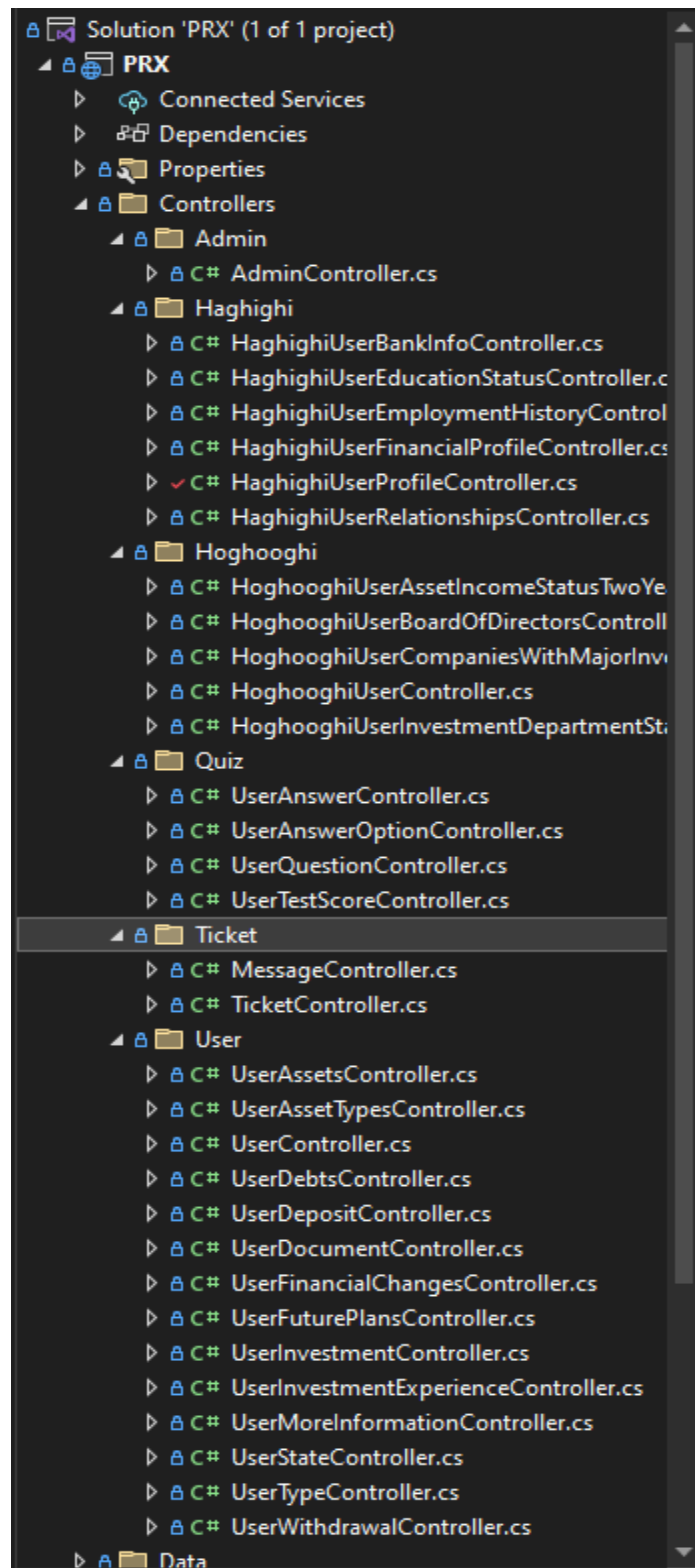
نمای کلی دیتابیس و جدول های آن به شکل زیر است:



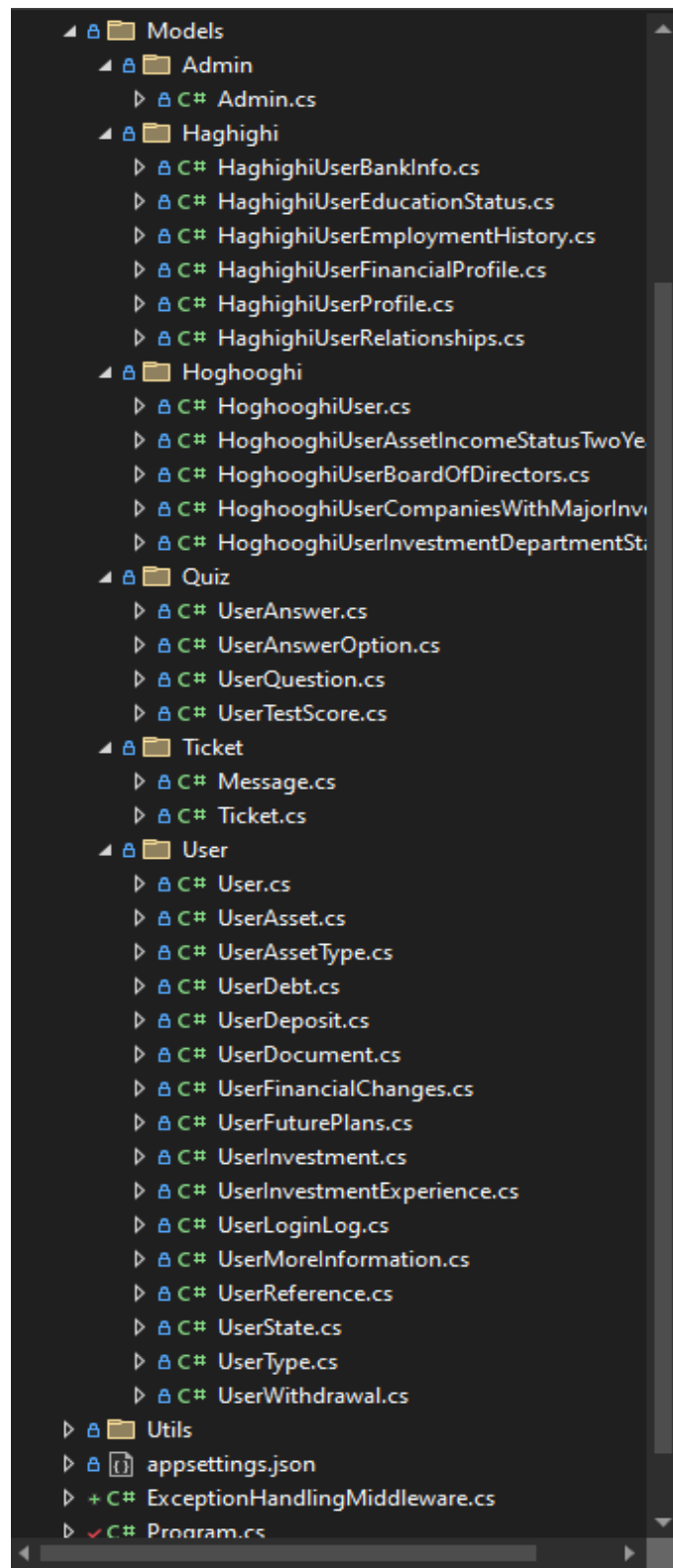
نمای کلی پروژه در ویژوال استودیو به شکل زیر است:




کنترلر ها :



مدل های برنامه:




بخشی از نمای کلی Swagger برای تست API های بک اند:

 **Swagger**
OpenAPI SMART BEAR

Select a definition PRX v1

PRX API v1 OAS3
<http://172.21.18.73:5032/swagger/v1/swagger.json>

Authorize 

Admin	▼
HaghighiUserBankInfo	▼
HaghighiUserEducationStatus	▼
HaghighiUserEmploymentHistory	▼
HaghighiUserFinancialProfile	▼
HaghighiUserProfile	▼
HaghighiUserRelationships	▼
HoghooghiUser	▼
HoghooghiUserAssetIncomeStatusTwoYearsAgo	▼
HoghooghiUserBoardOfDirectors	▼

نمای Swagger برای User :

Users



GET	/api/Users/PhoneExistance/{phoneNumber}	✓	🔒
POST	/api/Users	✓	🔒
POST	/api/Users/verify-otp	✓	🔒
POST	/api/Users/login	✓	🔒
POST	/api/Users/logout	✓	🔒
GET	/api/Users/{id}	✓	🔒
PUT	/api/Users/{id}	✓	🔒
DELETE	/api/Users/{id}	✓	🔒
GET	/api/Users/Admin	✓	🔒
GET	/api/Users/Admin/{id}	✓	🔒
PUT	/api/Users/Admin/{id}	✓	🔒
DELETE	/api/Users/Admin/{id}	✓	🔒
DELETE	/api/Users/Admin/Clear	✓	🔒

نیازمندی های آزمون

برنامه باید تمام ورودی های کاربر را برای جلوگیری از تزریق SQL ارزیابی کند.
برنامه باید تعداد زیادی درخواست را بدون به خطر انداختن امنیت انجام دهد.
تمام فیلدهای ورودی کاربر باید برای آسیب پذیری های تزریق SQL آزمایش شوند.

حوزه مورد آزمون

حوزه مورد بررسی آزمون امنیت در سیستم تحت وب است.

ابزار مورد استفاده

SQLMap

یک ابزار تست نفوذ متن باز است که برای شناسایی و بهره برداری از آسیب پذیری های تزریق SQL در برنامه های وب استفاده می شود. این ابزار می تواند به طور خودکار آسیب پذیری های تزریق SQL را شناسایی کند و اطلاعات حساس مانند نام کاربری و رمز عبور را دریافت کند.

قابلیت ها

- شناسایی آسیب پذیری های تزریق SQL مانند SQL Injection
- تست خودکار برای شناسایی و بهره برداری از آسیب پذیری های SQL Injection
- ارائه گزارش جامع از آسیب پذیری ها و اطلاعات به دست آمده.

طرح آزمون

شناسه طرح آزمون:

به عنوان مثال میتوان شناسه این طرح آزمون را PRX-TP01 گذاشت.

مقدمه:

این طرح آزمون برای پروژه PRX تهیه شده است که شامل بررسی و شناسایی آسیب پذیری های امنیتی مانند تزریق SQL می باشد.

اقلام مورد آزمون:

اندپوینت مربوط به کاربر

جدول اطلاعات کاربر

دیتابیس

ویژگی هایی که مورد آزمون قرار میگیرند:

امنیت اطلاعات کاربران در برابر حمله تزریق sql

امنیت اطلاعات دیتابیس در برابر حمله تزریق sql

امنیت اطلاعات url در برابر حمله تزریق sql

ویژگی هایی که مورد آزمون نیستند:

رابط کاربری

اندپوینت های برنامه به غیر از کاربران

جدول های برنامه به غیر از کاربران

سیستم احراز هویت

روش انجام آزمون:

استفاده از ابزار SQLMap برای شناسایی آسیب پذیری های تزریق SQL در محیط CMD

معیار پذیرش یا رد آزمون:

با استفاده از خروجی های SQLMap که باید نشان دهد در برابر تزریق آسیب پذیر نیست.

خروجی (تحویلی) های آزمون:

گزارش پروژه

تسک ها:

اجرای پروژه در Local Host

نصب کتابخانه SQLMap

اجرای دستورات CMD برای تست URL با ابزار SQLMap

تکمیل گزارش پروژه

نیازمندی محیطی:

Visual Studio

SQL Server Management Studio

Chrome or Microsoft Edge

CMD

Python

Clone SQLMap Library

تخصیص وظایف:

آزمونگر : محمد مهدی نظری

دولوپر: محمد مهدی نظری

زمان بندی:

تحويل گزارش تا 10 تیر 1403

ریسک ها:

به علت تست تزریق امکان از دست رفتن یا تغییر داده در دیتابیس وجود دارد که برای این مورد از یک دیتابیس پشتیبان استفاده میکنیم برای اینکه اگر برنامه نسبت به تزریق آسیب پذیر بود داده های حیاتی از دست نروند.

سند موارد آزمون

مواردی که در این آزمون بررسی خواهد شد با استفاده از sqlmap شامل :

بدست آوردن اینکه آدرس در مقابل حمله SQL Injection آسیب پذیر هست یا نه (TC01):

ورودی:

```
C:\Users\M.Nazari\Downloads\sqlmapproject-sqlmap-b256269>python sqlmap.py -u "http://172.21.18.73:5033/api/Users/47" --batch --dump --level 5 --risk 3
```

خروجی:

```
[09:42:51] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'  
[09:42:51] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'  
[09:42:51] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'  
[09:42:51] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'  
[09:42:51] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'  
[09:42:51] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'  
[09:42:51] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'  
[09:42:51] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'  
[09:42:51] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'  
[09:42:51] [INFO] testing 'Oracle time-based blind - Parameter replace (heavy queries)'  
[09:42:51] [INFO] testing 'SQLite > 2.0 time-based blind - Parameter replace (heavy query)'  
[09:42:51] [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'  
[09:42:51] [INFO] testing 'SAP MaxDB time-based blind - Parameter replace (heavy query)'  
[09:42:51] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'  
[09:42:51] [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - Parameter replace (heavy query)'  
[09:42:51] [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'  
[09:42:51] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'  
[09:42:51] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'  
[09:42:51] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'  
[09:42:51] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'  
[09:42:52] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'  
[09:42:52] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'  
[09:42:52] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'  
[09:42:52] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'  
[09:42:52] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'  
[09:42:52] [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'  
[09:42:52] [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'  
[09:42:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
[09:42:53] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'  
[09:42:54] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'  
[09:42:56] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'  
[09:42:57] [WARNING] parameter 'Host' does not seem to be injectable  
[09:42:57] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') a  
nd/or switch '--random-agent'  
[09:42:57] [WARNING] HTTP error codes detected during run:  
404 (Not Found) - 1 times, 400 (Bad Request) - 9370 times  
[*] ending @ 09:42:57 /2024-06-30/
```


بدست آوردن شمای دیتابیس (TC02)

ورودی:

```
C:\Users\M.Nazari\Downloads\sqlmapproject-sqlmap-b256269>python sqlmap.py -u "http://172.21.18.73:5033/api/Users/47" --schema --level 5 --risk 3
```

خروجی:

```
[10:09:16] [INFO] testing 'HSQLDB > 2.0 AND time-based blind (heavy query - comment)'
[10:09:16] [INFO] testing 'HSQLDB > 2.0 OR time-based blind (heavy query - comment)'
[10:09:17] [INFO] testing 'Informix AND time-based blind (heavy query)'
[10:09:17] [INFO] testing 'Informix OR time-based blind (heavy query)'
[10:09:17] [INFO] testing 'Informix AND time-based blind (heavy query - comment)'
[10:09:17] [INFO] testing 'Informix OR time-based blind (heavy query - comment)'
[10:09:17] [INFO] testing 'ClickHouse AND time-based blind (heavy query)'
[10:09:18] [INFO] testing 'ClickHouse OR time-based blind (heavy query)'
[10:09:18] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[10:09:18] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[10:09:18] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[10:09:18] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (subtraction)'
[10:09:18] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[10:09:18] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
[10:09:18] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[10:09:18] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[10:09:18] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[10:09:18] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[10:09:18] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[10:09:18] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'
[10:09:18] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[10:09:18] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'
[10:09:18] [INFO] testing 'Oracle time-based blind - Parameter replace (heavy queries)'
[10:09:18] [INFO] testing 'SQLite > 2.0 time-based blind - Parameter replace (heavy query)'
[10:09:18] [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'
[10:09:18] [INFO] testing 'SAP MaxDB time-based blind - Parameter replace (heavy query)'
[10:09:18] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'
[10:09:18] [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - Parameter replace (heavy query)'
[10:09:18] [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'
[10:09:18] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'
[10:09:18] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[10:09:18] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
[10:09:18] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[10:09:18] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[10:09:18] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'
[10:09:18] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'
[10:09:18] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'
[10:09:18] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[10:09:18] [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[10:09:18] [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[10:09:18] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[10:09:20] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[10:09:21] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[10:09:23] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[10:09:25] [WARNING] parameter 'Host' does not seem to be injectable
[10:09:25] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') a
nd/or switch '--random-agent'
[10:09:25] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times, 400 (Bad Request) - 28667 times

[*] ending @ 10:09:25 / 2024-06-30/
```

بدست آوردن فیلدهای جدول ها (TC03)

ورودی:

```
C:\Users\M.Nazari\Downloads\sqlmapproject-sqlmap-b256269>python sqlmap.py -u "http://172.21.18.73:5033/api/Users/47" --tables --level 5 --risk 3
```

خروجی:

```
10:21:16 [INFO] testing 'SAP MaxDB OR time-based blind (heavy query)'
10:21:16 [INFO] testing 'SAP MaxDB AND time-based blind (heavy query - comment)'
10:21:16 [INFO] testing 'SAP MaxDB OR time-based blind (heavy query - comment)'
10:21:16 [INFO] testing 'HSQLDB >= 1.7.2 AND time-based blind (heavy query)'
10:21:17 [INFO] testing 'HSQLDB >= 1.7.2 OR time-based blind (heavy query)'
10:21:17 [INFO] testing 'HSQLDB >= 1.7.2 AND time-based blind (heavy query - comment)'
10:21:17 [INFO] testing 'HSQLDB >= 1.7.2 OR time-based blind (heavy query - comment)'
10:21:17 [INFO] testing 'HSQLDB > 2.0 AND time-based blind (heavy query)'
10:21:17 [INFO] testing 'HSQLDB > 2.0 OR time-based blind (heavy query)'
10:21:17 [INFO] testing 'HSQLDB > 2.0 AND time-based blind (heavy query - comment)'
10:21:18 [INFO] testing 'HSQLDB > 2.0 OR time-based blind (heavy query - comment)'
10:21:18 [INFO] testing 'Informix AND time-based blind (heavy query)'
10:21:18 [INFO] testing 'Informix OR time-based blind (heavy query)'
10:21:18 [INFO] testing 'Informix AND time-based blind (heavy query - comment)'
10:21:18 [INFO] testing 'Informix OR time-based blind (heavy query - comment)'
10:21:18 [INFO] testing 'ClickHouse AND time-based blind (heavy query)'
10:21:18 [INFO] testing 'ClickHouse OR time-based blind (heavy query)'
10:21:19 [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE (EXTRACTVALUE)'
10:21:19 [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
10:21:19 [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
10:21:19 [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (subtraction)'
10:21:19 [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
10:21:19 [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
10:21:19 [INFO] testing 'MySQL time-based blind - Parameter replace (tool)'
10:21:19 [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
10:21:19 [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
10:21:19 [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
10:21:19 [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
10:21:19 [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'
10:21:19 [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
10:21:19 [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'
10:21:19 [INFO] testing 'Oracle time-based blind - Parameter replace (heavy queries)'
10:21:19 [INFO] testing 'SQLite > 2.0 time-based blind - Parameter replace (heavy query)'
10:21:19 [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'
10:21:19 [INFO] testing 'SAP MaxDB time-based blind - Parameter replace (heavy query)'
10:21:19 [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'
10:21:19 [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - Parameter replace (heavy query)'
10:21:19 [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'
10:21:19 [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'
10:21:19 [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
10:21:19 [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
10:21:19 [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
10:21:19 [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
10:21:19 [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'
10:21:19 [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'
10:21:19 [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'
10:21:19 [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'
10:21:19 [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
10:21:19 [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
10:21:19 [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
10:21:21 [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
10:21:22 [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
10:21:23 [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
10:21:25 [WARNING] parameter 'Host' does not seem to be injectable
10:21:25 [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') a
nd/or switch '--random-agent'
10:21:25 [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times, 400 (Bad Request) - 15797 times

[*] ending @ 10:21:25 /2024-06-30/
```

بدست آوردن رمزهای هش شده (tc04)

ورودی:

```
C:\Users\M.Nazari\Downloads\sqlmapproject-sqlmap-b256269>python sqlmap.py -u "http://172.21.18.73:5033/api/Users/47" -D PRX_BACKUP -T Users -C password --dump
```

خروجی:

```

[+] H
[+] (1.8.6.5#dev)
[+] https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:49:58 /2024-06-30/

[11:49:59] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] Y
[11:50:04] [INFO] testing connection to the target URL
[11:50:04] [INFO] testing if the target URL content is stable
[11:50:04] [INFO] target URL content is stable
[11:50:04] [INFO] testing if URI parameter '#1' is dynamic
[11:50:04] [WARNING] URI parameter '#1' does not appear to be dynamic
[11:50:04] [WARNING] heuristic (basic) test shows that URI parameter '#1' might not be injectable
[11:50:04] [INFO] testing for SQL injection on URI parameter '#1'
[11:50:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:50:04] [WARNING] reflective value(s) found and filtering out
[11:50:04] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:50:04] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:50:04] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:50:04] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IV)'
[11:50:04] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:50:04] [INFO] testing 'Generic inline queries'
[11:50:04] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:50:04] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:50:04] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:50:04] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[11:50:04] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:50:04] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:50:04] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[11:50:07] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:50:07] [WARNING] URI parameter '#1' does not seem to be injectable
[11:50:07] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=spacecomment') and/or switch '--random-agent'
[11:50:07] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times, 400 (Bad Request) - 72 times

[*] ending @ 11:50:07 /2024-06-30/

```

داده آزمون

Level -> 5

Risk -> 3

url -> http://172.21.18.73:5033/api/Users/47

table -> Users

field -> password

سند نتایج اجرای آزمون

خلاصه آزمون ها :

تعداد تست های اجرا شده : 4

تعداد تست های قبول شده: 4

تعداد تست های رد شده: 0

درصد قبولی تست ها : تست های اجرا شده / تست های قبول شده = $4/4 = 100\%$

نتایج جزیی تست ها:

تست کیس 1

آزمونگر: محمد مهدی نظری

شرح: چک کردن کلی تزریق پذیر بودن برنامه

نتیجه مورد انتظار: اجازه تزریق نباید داده شود

نتیجه به دست آمده: برنامه تزریق پذیر نیست

وضعیت: موفقیت آمیز

تست کیس 2

آزمونگر: محمد مهدی نظری

شرح: به دست آوردن شمای کلی دیتابیس با تزریق

نتیجه مورد انتظار: اجازه تزریق نباید داده شود

نتیجه به دست آمده: برنامه تزریق پذیر نیست

وضعیت: موفقیت آمیز

تست کیس 3

آزمونگر: محمد مهدی نظری

شرح: بدست آوردن جدول های دیتابیس با تزریق

نتیجه مورد انتظار: اجازه تزریق نباید داده شود

نتیجه به دست آمده: برنامه تزریق پذیر نیست

وضعیت: موفقیت آمیز

تست کیس 4

آزمونگر: محمد مهدی نظری

شرح: بدست آوردن رمز های کاربران با تزریق

نتیجه مورد انتظار: اجازه تزریق نباید داده شود

نتیجه به دست آمده: برنامه تزریق پذیر نیست

وضعیت: موفقیت آمیز

جمع بندی

موفقیت‌ها:

1. شناسایی و جلوگیری از تزریق SQL

تمامی تست کیس‌های مربوط به شناسایی تزریق SQL با موفقیت انجام شد و هیچ آسیب‌پذیری تزریق SQL در دریافت اطلاعات کاربر یافت نشد.

تست‌های انجام شده نشان داد که پیاده‌سازی امنیتی برنامه در مقابل حملات تزریق SQL مقاوم است.

2. بازیابی اطلاعات پایگاه داده

تست‌های مربوط به بازیابی طرح (Schema) پایگاه داده و داده‌های حساس کاربران نیز موفقیت‌آمیز بود و نشان داد که هیچ اطلاعات حساسی به صورت غیرمجاز قابل دسترسی نیست.

رمزهای عبور کاربران به صورت هش شده و با استفاده از الگوریتم‌های قوی رمزنگاری شده‌اند که این امر امنیت داده‌های کاربران را تضمین می‌کند.

مشکلات و کمبودها

1. عدم دسترسی به محیط تست

در برخی از مراحل اولیه تست، دسترسی به محیط تست با مشکلاتی همراه بود که باعث تأخیر در اجرای تست‌ها شد.

کمبود منابع سخت‌افزاری مناسب برای اجرای تست‌ها با تعداد بالای درخواست‌ها.

2. مشکلات فنی ابزارهای تست

در برخی موارد، ابزار SQLMap با مشکلات فنی مواجه شد که نیاز به عیب‌یابی و پشتیبانی فنی داشت. ناسازگاری‌های جزئی بین نسخه‌های مختلف ابزارهای تست و محیط توسعه.

3. محدودیت‌های زمانی

محدودیت‌های زمانی برای اجرای تمامی تست‌ها و تحلیل نتایج به صورت دقیق و جامع. نیاز به برنامه‌ریزی بهتر و تخصیص زمان کافی برای اجرای تست‌های دستی و خودکار.

راه‌حل‌های پیشنهادی

1. ایجاد محیط تست پایدار

ایجاد یک محیط تست مجزا و پایدار با منابع سخت‌افزاری مناسب که به صورت دائمی در دسترس تیم تست باشد. استفاده از سرویس‌های ابری برای ایجاد محیط‌های تست با قابلیت مقیاس‌پذیری بالا.

2. آموزش و پشتیبانی فنی

آموزش تیم تست در مورد ابزارهای تست مانند SQLMap و نحوه استفاده بهینه از آنها. ایجاد یک تیم پشتیبانی فنی برای رفع مشکلات و ناسازگاری‌های ابزارهای تست.

3. بهبود زمان‌بندی و مدیریت پروژه

ایجاد یک برنامه زمان‌بندی دقیق و واقع‌بینانه برای اجرای تمامی تست‌ها. تخصیص زمان بیشتری برای تحلیل نتایج و تهیه گزارش‌های جامع و کامل.

استفاده از ابزارهای مدیریت پروژه برای پیگیری و کنترل دقیق تر زمان بندی ها و وظایف.

4. تست های دوره ای و مستمر

اجرای تست های امنیتی به صورت دوره ای و مستمر به منظور اطمینان از حفظ امنیت نرم افزار در طول زمان. ایجاد رویه های تست خودکار که به صورت مداوم و با هر تغییر در کد منبع اجرا شوند.

نتیجه گیری

این پروژه با موفقیت به اتمام رسید و تمامی تست کیس ها نتایج مثبتی داشتند که نشان دهنده امنیت بالای نرم افزار در برابر حملات تزریق SQL است. با این حال، شناسایی و رفع مشکلات و کمبودهای موجود می تواند به بهبود کیفیت و امنیت نرم افزار در پروژه های آینده کمک کند. استفاده از راه حل های پیشنهادی نیز می تواند موجب افزایش کارایی و موفقیت در اجرای تست های امنیتی شود.