

Презентация по пятому этапу индивидуального проекта

Burb Suite

Вакутайпа М.

16 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

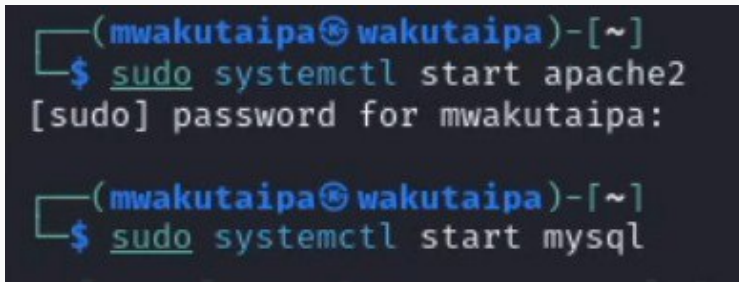
- Вакутайпа Милдред
- НКАбд 02-23
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов
- 1032239009@rudn.ru
- <https://wakutaipa.github.io/ru/>

Цель работы

Научиться использовать Burp Suite.

Выполнение лабораторной работы

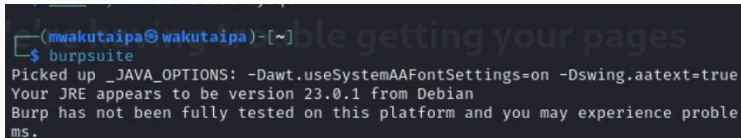
Запускаю локальный сервер DVWA:



```
(mwakutaipa@wakutaipa)-[~]  
$ sudo systemctl start apache2  
[sudo] password for mwakutaipa:  
  
(mwakutaipa@wakutaipa)-[~]  
$ sudo systemctl start mysql
```

Рис. 1: Запуск сервера

Запускаю burp suite:

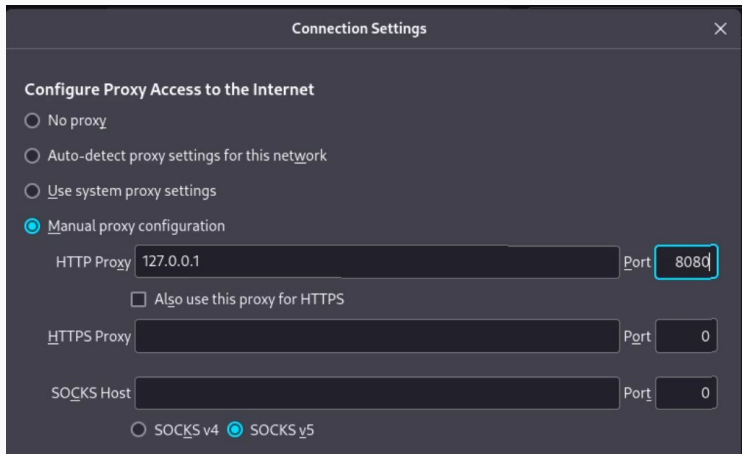
A terminal window with a dark background. The prompt is (mwakutaipa@wakutaipa)-[~]. The command \$ burpsuite has been entered. The output shows Java options, the JRE version (23.0.1 from Debian), and a warning that Burp has not been fully tested on this platform.

```
(mwakutaipa@wakutaipa)-[~]  
$ burpsuite  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
Your JRE appears to be version 23.0.1 from Debian  
Burp has not been fully tested on this platform and you may experience problems.
```

Рис. 2: Запуск Burp suite

сетевые настройки сервера

Открываю сетевые настройки браузера и изменяю настройки сервера для работы с проху и захватом данных с burp suite:



Изменяю настройки проху инструмента burp suite:

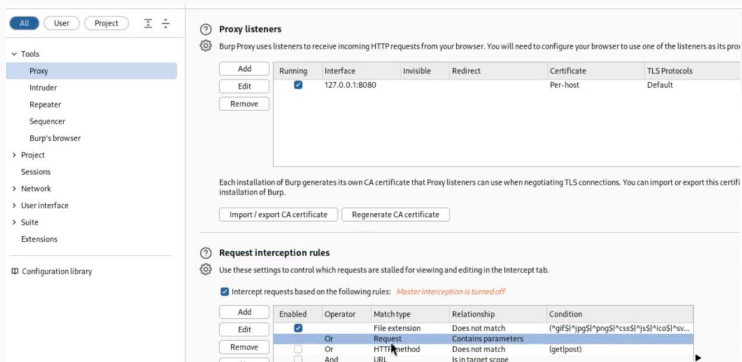


Рис. 4: настройки проху

Включаю intercept во вкладке проху:

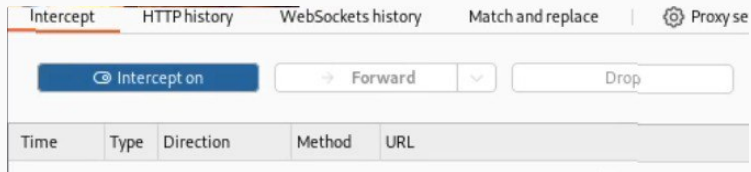


Рис. 5: Включение intercept

Установка параметра локального хоста

Необходимо установить параметр `network_allow_hijacking_localhost` на `true`, чтобы burp suite работал с локальным сервером. Я это и делала:

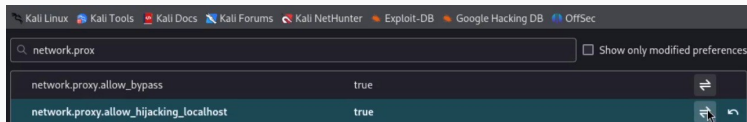
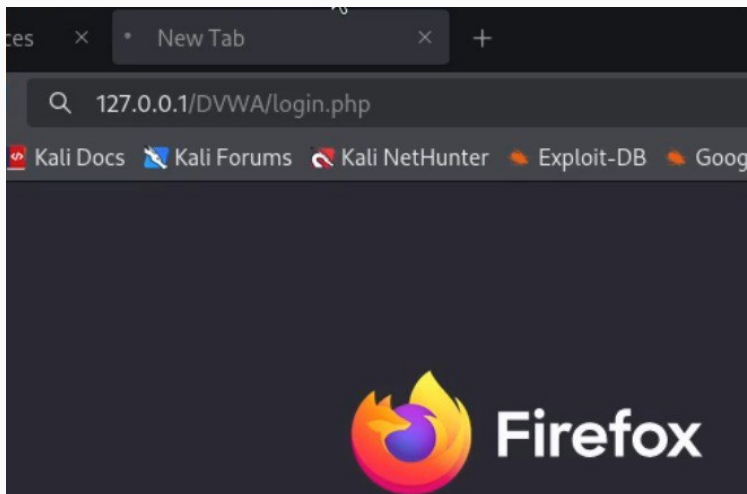
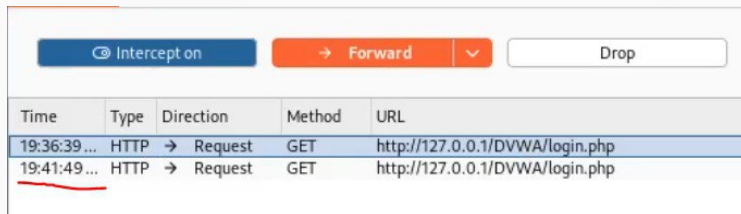


Рис. 6: Установка параметра локального хоста

Пытка зайти в dvwa

Пытаюсь зайти на dvwa в браузере и во вкладки проху появляется запрос. Нажимаю forward, чтобы загрузить страницу:





The screenshot shows the Proxy tab in Burp Suite. At the top, there are three buttons: "Intercept on" (blue), "Forward" (orange), and "Drop" (white). Below these buttons is a table of intercepted requests. The table has five columns: Time, Type, Direction, Method, and URL. Two requests are listed, both are HTTP GET requests to http://127.0.0.1/DVWA/login.php. The first request is at 19:36:39 and the second is at 19:41:49. A red line is drawn under the first request's time and type.

Time	Type	Direction	Method	URL
19:36:39 ...	HTTP	→ Request	GET	http://127.0.0.1/DVWA/login.php
19:41:49 ...	HTTP	→ Request	GET	http://127.0.0.1/DVWA/login.php

Рис. 8: вкладка proxy



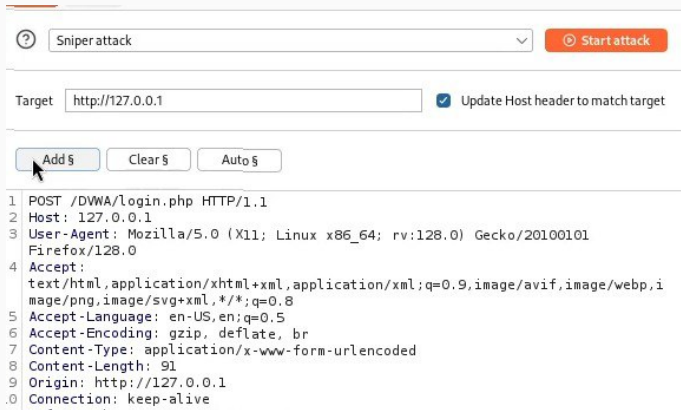
Username

Password

Login

Измененные данные

Когда пытаюсь ввести неправильные логин и пароль, в запросе появляется строка, в которой отображаются введенные данные. Этот же запрос, во вкладке target, отправил к злоумышленнику (send to intruder). Во вкладке intruder, изменяю тип атаки (на cluster bomb) и данные для входа.



Sniper attack Start attack

Target ☒ Update Host header to match target

Add \$ Clear \$ Auto \$

```
1 POST /DWWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
  Firefox/128.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
  mage/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 91
9 Origin: http://127.0.0.1
10 Connection: keep-alive
```

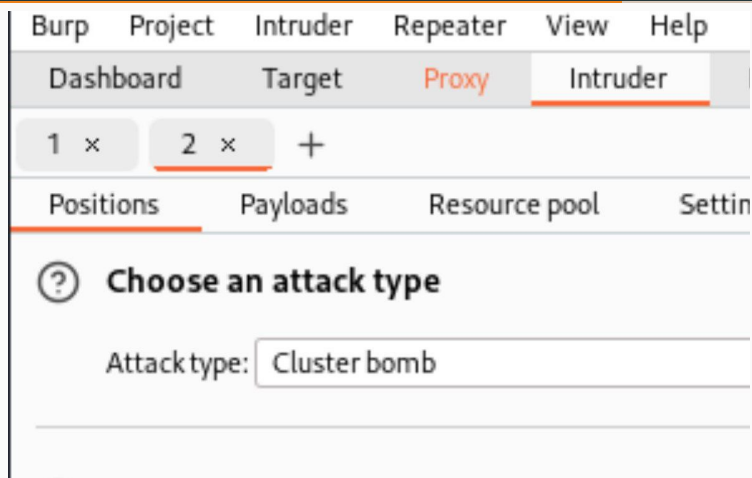



Рис. 11: Тип атака

Отметила два параметра для подбора, поэтому создала два списка со значениями для подбора в payload:

The screenshot shows the Burp Suite Intruder interface. At the top, there are tabs for Dashboard, Target, Proxy (selected), Intruder, Repeater, Collaborator, and Sequencer. Below these are buttons for 1 x, 2 x (selected), and +. The main area has tabs for Positions, Payloads (selected), Resource pool, and Settings. Under the Payloads tab, there is a section titled "Payload sets" with a help icon. It contains a description: "You can define one or more payload sets. The number of payload sets depends on the attack type c ways." Below this are two rows of configuration: "Payload set:" with a dropdown menu showing "1" and "Payload count:" with the value "6"; and "Payload type:" with a dropdown menu showing "Simple list" and "Request count:" with the value "24". Below the "Payload sets" section is another section titled "Payload settings [Simple list]" with a help icon. It contains a description: "This payload type lets you configure a simple list of strings that are used as payloads." Below this description is a list of strings: "admin", "password", "psswd", "123456", "dddddd", and "fffff". To the left of this list are five buttons: "Paste", "Load ...", "Remove", "Clear", and "Deduplicate".

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer

1 x 2 x +

Positions **Payloads** Resource pool Settings

? **Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type c ways.

Payload set: 1 Payload count: 6

Payload type: Simple list Request count: 24

? **Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate

admin
password
psswd
123456
dddddd
fffff

1 x 2 x +

Positions Payloads Resource pool Settings

? **Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type i ways.

Payload set: 2 Payload count: 4

Payload type: Simple list Request count: 24

? **Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

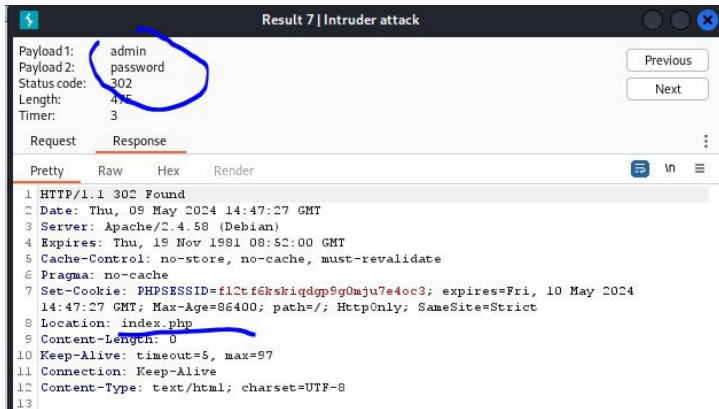
admin
password
pass
aaaaaaa

Add Enter a new item

Add from list ... [Pro version only]

Правильная пара

Далее запускаю атаку и начинаю подбор. При открытии каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В этом случае с подбором пары нас перенаправило на страницу index.php, значит пара должна быть верной:



Окна repeater и response

С использованием repeater делаю дополнительную проверку. Нажимаю send и в response получаю результат перенаправление на index.php.

The screenshot shows a network traffic analysis tool interface. At the top, there's a tab labeled '1 x' and a '+'. Below it are buttons for 'Send', a gear icon, 'Cancel', and navigation arrows. A 'Follow redirection' button is also present. The main area is split into two panels: 'Request' on the left and 'Response' on the right. Both panels have tabs for 'Pretty', 'Raw', and 'Hex'. The 'Request' panel shows a POST request to '/DVWA/login.php' with various headers and a body containing login credentials. The 'Response' panel shows an HTTP 302 Found status with headers indicating a redirect to 'index.php'.

Request

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image
  /avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 88
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/DVWA/login.php
12 Cookie: PHPSESSID=lgrd2fd4cuplp7vppsbgk8saju; security=
  impossible
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 username=admin&password=password&Login=Login&user_token=
  8d65a231118b135f47ab549228340964
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Thu, 09 May 2024 14:51:42 GMT
3 Server: Apache/2.4.58 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=dv7q7luvnslu7vb7mc7b896cr9;
  expires=Fri, 10 May 2024 14:51:42 GMT; Max-Age=86400;
  path=/; HttpOnly; SameSite=Strict
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14
```

В подокне Render получаю то, как выглядит полученная страница:

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows an HTTP GET request to `/DVWA/login.php` with various headers and cookies. The 'Response' pane on the right, set to 'Render' mode, shows the visual output of the request, which is the DVWA login page. The page features the DVWA logo at the top, followed by input fields for 'Username' and 'Password', and a 'Login' button at the bottom.

Request

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  /avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Origin: http://127.0.0.1
8 Connection: Keep-alive
9 Referer: http://127.0.0.1/DVWA/index.php
10 Cookie: PHPSESSID=lgrd2fd4cupip7vppshgk8saju; security=
  impossible
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: 11
16
17
```

Response

Username

Password

Login

Выводы

Научилась использовать Burp Suite.