

Отчёт по индивидуальному проекту этап №5

Основы информационной безопасности

Паращенко А.Д.

8 октября 2024

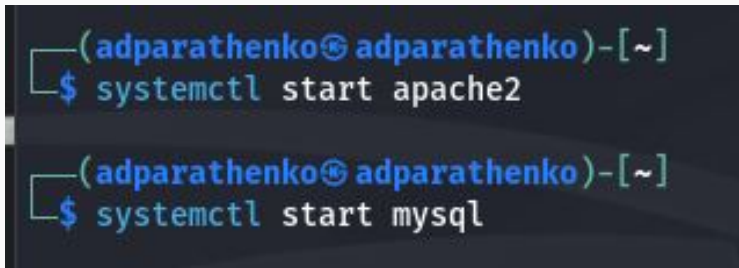
Российский университет дружбы народов, Москва, Россия

Цель работы

Научиться использовать на практике Burp Suite.

Выполнение лабораторной работы

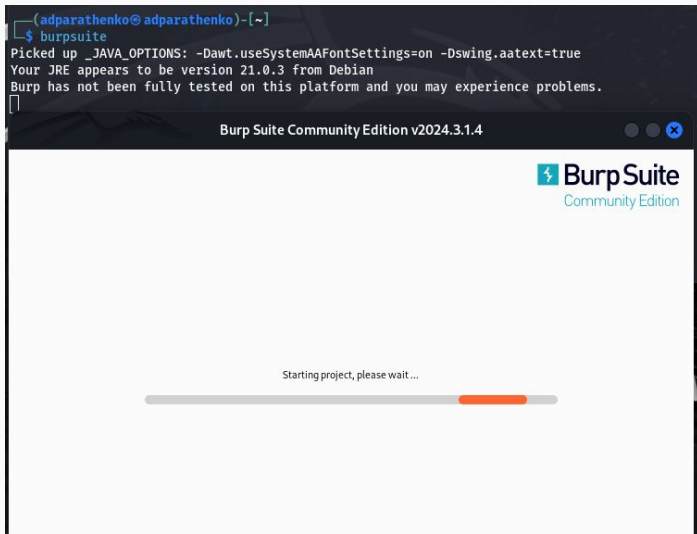
Запускаем локальный сервер, на котором откроем веб-приложение DVWA для тестирования инструмента Burp Suite. (рис. (fig:001?))

A terminal window with a dark background and light blue text. The prompt is '(adparathenko@adparathenko)-[~]'. The first command entered is '\$ systemctl start apache2'. The second command entered is '\$ systemctl start mysql'.

```
(adparathenko@adparathenko)-[~]  
$ systemctl start apache2  
  
(adparathenko@adparathenko)-[~]  
$ systemctl start mysql
```

Рис. 1: Запуск Apache2

Запускаем Burp Suite. (рис. (fig:002?))



Изменяем настройки в Proxy на *Intercept is on*. рис. (fig:003?))

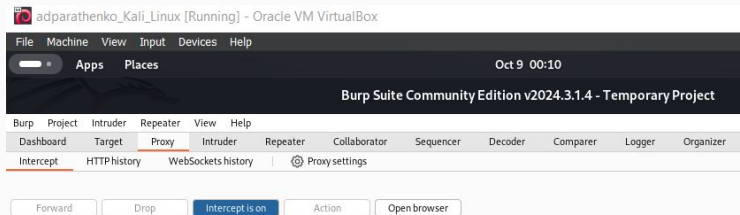
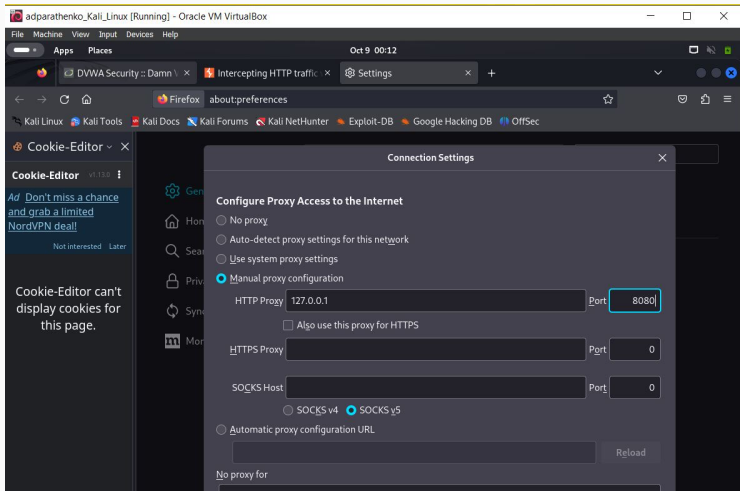


Рис. 3: Intercept is on

Изменяем настройки сервера в браузере для работы с Proxu и захватом данных с помощью Burp Suite. (рис. (fig:004?))



Устанавливаем параметр `network_allow_hijacking_localhost` на `true`. (рис. (fig:005?))

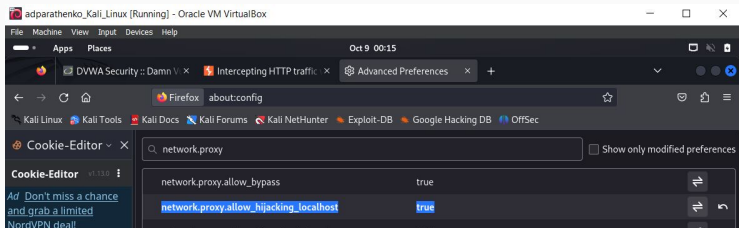


Рис. 5: `network_allow_hijacking_localhost`

В браузере заходим на DVWA и во вкладке Proxy появляется захваченный запрос. нажимаем Forward, чтобы загрузить страницу. (рис. (fig:006?))

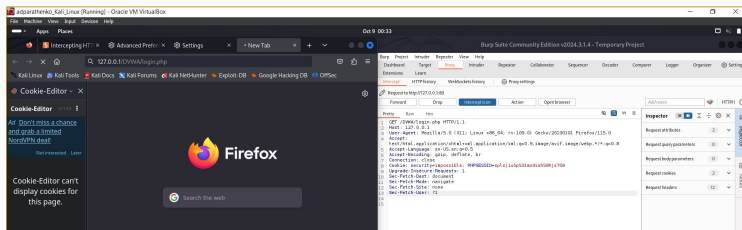


Рис. 6: Захваченный запрос

Загрузилась страница авторизации. (рис. (fig:007?))

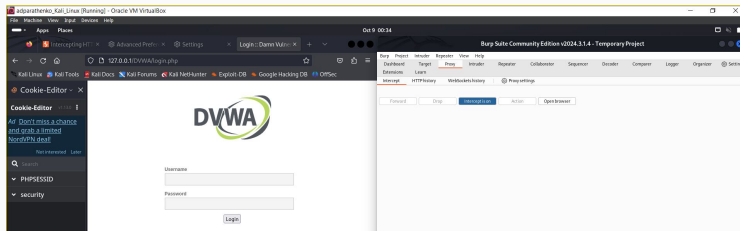
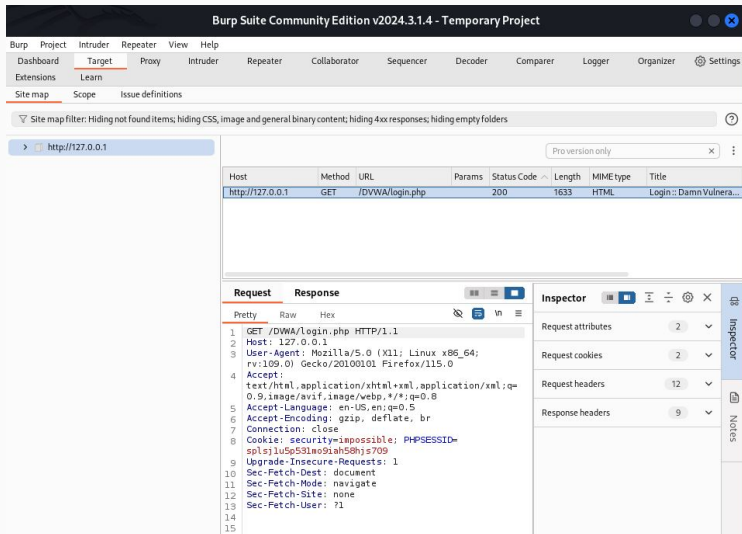


Рис. 7: Страница авторизации

Историю запросов можно посмотреть во вкладке Target. (рис. (fig:008?))



Вводя случайный логин и пароль, в запросе мы увидим введенные данные. (рис. (fig:009?))

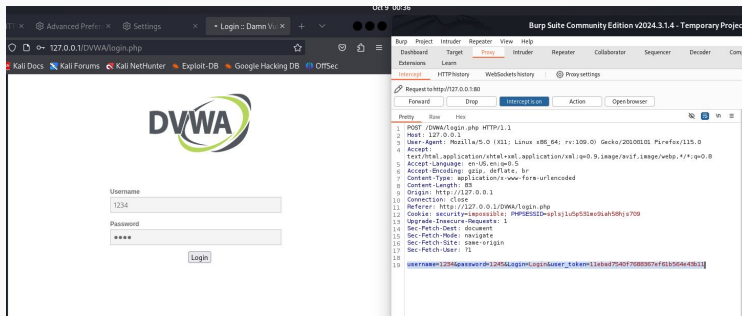
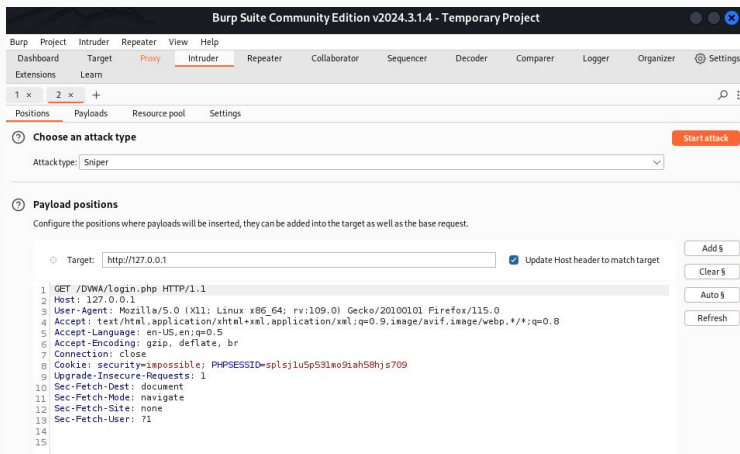
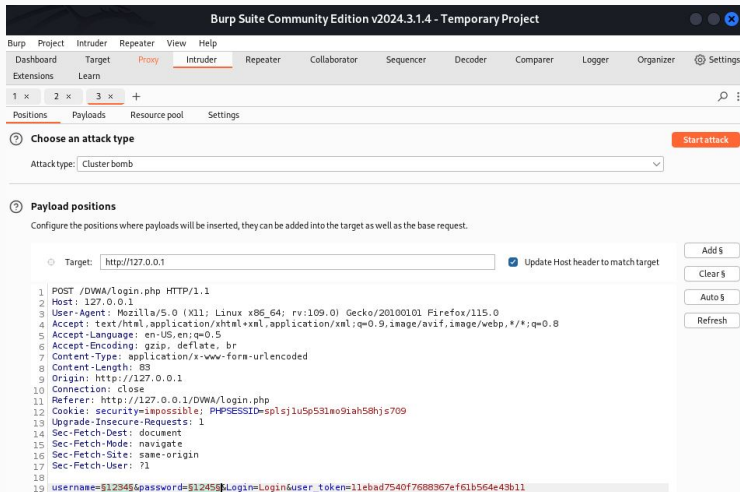


Рис. 9: случайный логин и пароль

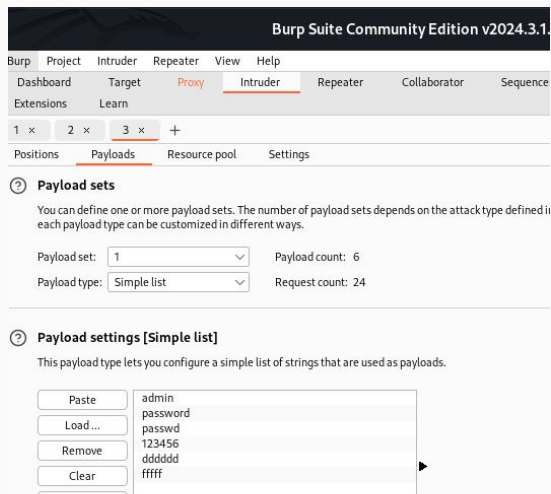
Находим этот запрос во вкладке Target и, нажимая на правую кнопку мыши, нажимаем на Send to Intruder. Попадая во вкладку мы видим вид атаки. (рис. (fig:010?))



Меняем вид атаки на Cluster bomb и выделяем специальными знаками данные ввода, которые хотим подбирать, в нашем случае, это логин и пароль. (рис. (fig:011?))



Далее добавляем 2 списка параметров для подбора логина и пароля. (рис. (fig:012?)) -(рис. (fig:013?))



Запускаем атаку и получаем результаты перебора. (рис. (fig:014?))

2. Intruder attack of http://127.0.0.1							
Attack Save							
2. Intruder attack of http://127.0.0.1							
Results Positions Payloads Resource pool Settings							
Intruder attack results filter: Showing all items							
Request	Payload 1	Payload 2	Status code	Response ...	Error	Timeout	Length
0			302	15			476
1	admin	admin	302	28			475
2	password	admin	302	29			476
3	passwd	admin	302	46			475
4	123456	admin	302	46			476
5	dddddd	admin	302	56			475
6	fffff	admin	302	185			476
7	admin	password	302	23			476
8	password	password	302	11			475
9	passwd	password	302	26			476
10	123456	password	302	18			475
11	dddddd	password	302	26			475
12	fffff	password	302	27			476
13	admin	pass	302	23			476
14	password	pass	302	19			475
15	passwd	pass	302	17			475
16	123456	pass	302	10			475
17	dddddd	pass	302	19			476
18	fffff	pass	302	12			475
19	admin	aaaaaaa	302	28			476
20	password	aaaaaaa	302	25			476
21	passwd	aaaaaaa	302	25			476

У всех вариантов перебора, кроме одного, *location: login.php*. (рис. (fig:015?))

2. Intruder attack of http://127.0.0.1

Attack Save

2. Intruder attack of http://127.0.0.1

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response ...	Error	Timeout	Length	C
0			302	15			476	
1	admin	admin	302	28			475	
2	password	admin	302	29			476	
3	passwd	admin	302	46			475	

Request Response

F Raw Hex Render

```

1 HTTP/1.1 302 Found
2 Date: Tue, 08 Oct 2024 21:46:35 GMT
3 Server: Apache/2.4.59 (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=krchjm2sresktqcaf5dvq8bj4; expires=Wed, 09 Oct 2024 21:46:35 GMT; Max-Age=86400; pa
  SameSite=Strict
8 Location: login.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
  
```

А у пары *admin password* результат *location: index.php*. Это показывает нам, что это верная пара логин-пароль. (рис. (fig:016?))

2. Intruder attack of http://127.0.0.1

Attack Save

2. Intruder attack of http://127.0.0.1 Atta

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response ...	Error	Timeout	Length	Corr
0			302	15			476	
1	admin	admin	302	28			475	
2	password	admin	302	29			476	
3	passwd	admin	302	46			475	
4	123456	admin	302	46			476	
5	dddddd	admin	302	56			475	
6	fffff	admin	302	185			476	
7	admin	password	302	23			476	
8	password	password	302	11			475	

Request Response

Pretty Raw Hex Render

```

1 HTTP/1.1 302 Found
2 Date: Tue, 08 Oct 2024 21:46:38 GMT
3 Server: Apache/2.4.59 (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=1b236j3qdmehjnb98ns6cr742a; expires=Wed, 09 Oct 2024 21:46:38 GMT; Max-Age=86400; pat

```

Чтобы ещё раз проверить результат мы отправляем эту пару на повторную проверку *Send to Repeater*. (рис. (fig:017?))

Request	Payload 1	Payload 2
0		
1	admin	admin
2	password	admin
3	passwd	admin
4	123456	admin
5	dddddd	admin
6	fffff	admin
7	ad	
8	pa	

Result #7

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Request	Response
1	HTTP/1.1 301

Получаем тот же результат *location: index.php.* (рис. (fig:018?))

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows a POST request to `/DWA/login.php` with various headers and a body containing login credentials. The 'Response' pane on the right shows a 302 Found status with a `Location: index.php` header. The 'Inspector' pane on the far right highlights the selected text 'Location: index.php'.

Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Target: `http://127.0.0.1` | HTTP/1

Request

```

1 POST /DWA/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/DWA/login.php
12 Cookie: security=impossible: PHPSESSID=
  splsjluSp53lno9iah58hs709
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=
  11ebad7540f7688367ef61b564e43b11
  
```

Response

```

1 HTTP/1.1 302 Found
2 Date: Tue, 08 Oct 2024 21:56:50 GMT
3 Server: Apache/2.4.59 (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=
  idkf6u89cuqvup2d1mn3tgguc9; expires=Wed,
  09 Oct 2024 21:56:50 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
  
```

Inspector

Selection: 19 (0x13)

Selected text

Location: index.php

Request attributes: 2

Request query parameters: 0

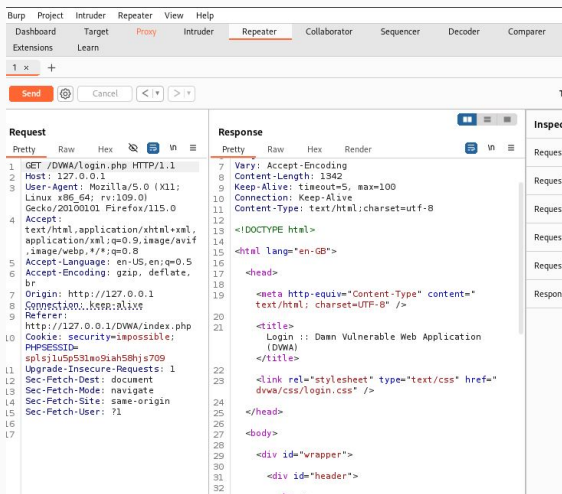
Request body parameters: 4

Request cookies: 2

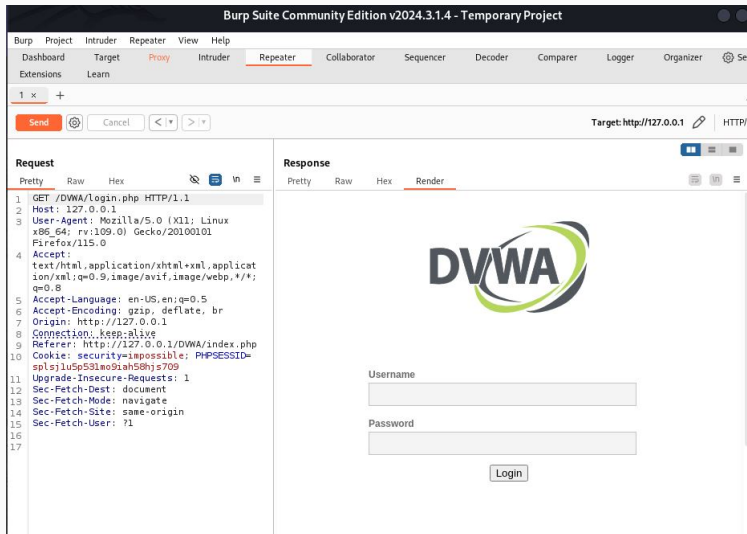
Request headers: 16

Response headers: 11

Нажимаем на *Follow redirection* и получаем неcompiled html код в окне Response.
(рис. (fig:019?))



В подокне Render получаем вид страницы в браузере. (рис. (fig:020?))



Вывод

В результате выполнения работы мы научились использовать инструмент Burp Suite и перебором возможных пар подобрали пару логин-пароль для входа на сайт.

Список литературы

- 1) Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.