

Индивидуальный проект этап 5

Информационная безопасность

Ким И. В. НФИбд-01-21

Российский университет дружбы народов, Москва, Россия

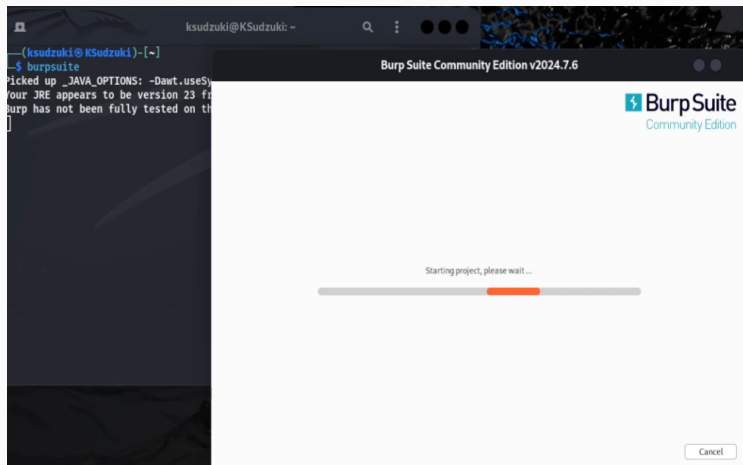
Цели и задачи

Научиться пользоваться Burp Suite

Выполнение работы

```
(ksudzuki@KSudzuki)-[~]  
$ sudo service mysql start  
  
(ksudzuki@KSudzuki)-[~]  
$ sudo service apache2 start
```

Запустил Burp Suite



Настроил прокси в браузере

Connection Settings

×

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy

127.0.0.1

Port

8080

☒ Also use this proxy for HTTPS

HTTPS Proxy

127.0.0.1

Port

8080

SOCKS Host

127.0.0.1

Port

8080

☐ SOCKS v4

☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

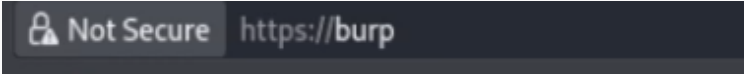
Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

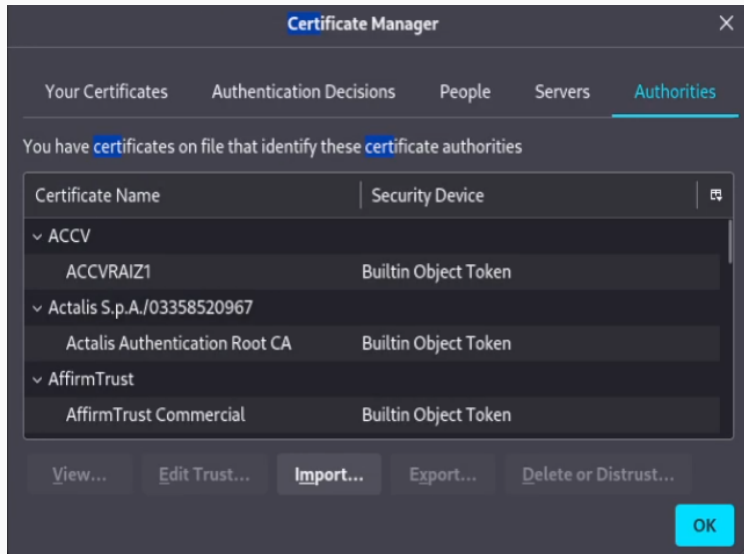
☐ Do not prompt for authentication if password is saved

Зашёл на сайт burp и скачал сертификаты



A screenshot of a web browser's address bar. On the left, there is a warning icon (a padlock with a diagonal line through it) followed by the text "Not Secure". To the right of this, the URL "https://burp" is displayed. The entire address bar has a dark, semi-transparent background.

Установил сертификаты в браузер



Перезапустил BurpSuite и зашёл на наш сайт dvwa/login.php

Burp Suite interface showing the HTTP history tab. The interface includes a menu bar (Burp, Project, Intruder, Repeater, View, Help) and a toolbar with various tools like Extensions, Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Learn. The Proxy tab is active, showing a list of intercepted HTTP requests.

Time	Type	Direction	Host	Method	URL
20:35:41 12 Oct 2024	HTTP	→ Request	r10.o.lencr.org	POST	http://r10.o.lencr.org/
20:38:43 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gatewayAdapt-gls2rus
20:40:05 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gatewayAdapt-gls2rus
20:40:05 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gatewayAdapt-gls2rus
20:40:05 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gatewayAdapt-gls2rus
20:40:06 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gatewayAdapt-gls2rus
20:41:30 12 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/dvwa/index.php
20:42:39 12 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/dvwa/login.php
20:42:45 12 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/dvwa/login.php

Во вкладке Проху отображаются запросы на вход

Бурп Project Intruder Repeater View Help

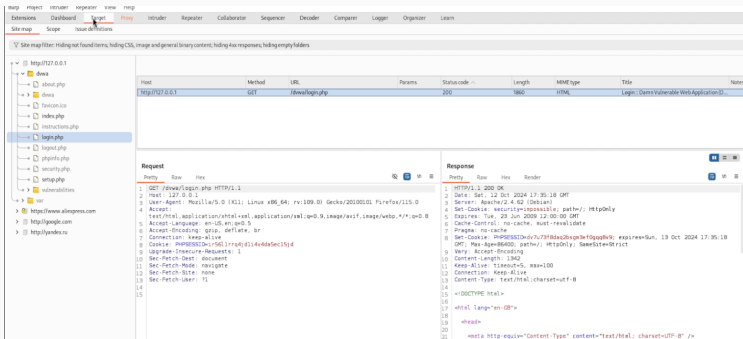
Extensions Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Learn

Intercept HTTP history WebSockets history Proxy settings

Interception Forward Drop

Time	Type	Direction	Host	Method	URL
20:35:41 12 Oct 2024	HTTP	→ Request	r10.o.lencr.org	POST	http://r10.o.lencr.org/
20:38:43 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gateway/dapt-gla2rus
20:40:05 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gateway/dapt-gla2rus
20:40:05 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gateway/dapt-gla2rus
20:40:05 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gateway/dapt-gla2rus
20:40:06 12 Oct 2024	HTTP	→ Request	aliexpress.ru	GET	https://aliexpress.ru/gateway/dapt-gla2rus
20:41:30 12 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/dwaa/index.php
20:42:39 12 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/dwaa/login.php
20:42:45 12 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/dwaa/login.php

Во вкладке target мы можем посмотреть данные о цели



The screenshot shows the Burp Suite interface with the 'Target' tab selected. The site map on the left shows a tree structure with 'dms' selected. The main panel displays a table of site map items, with 'http://127.0.0.1' selected. Below the table, the 'Request' and 'Response' tabs are visible, showing the details of the selected item.

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes
http://127.0.0.1	GET	/dms/login.php		200	1860	HTML	Login - Dams Vulnerable Web Application (2...	

Request

```
1 GET /dms/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 Connection: keep-alive
8 Cookie: PHPSESSID=7u73f8da2b3e70q9w9; expires=Sun, 13 Oct 2024 17:35:18 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14
15
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Sat, 12 Oct 2024 17:35:18 GMT
3 Server: Apache/2.4.62 (Debian)
4 Set-Cookie: sessionid=7u73f8da2b3e70q9w9; path=/; HttpOnly
5 Expires: Tue, 23 Jun 2009 12:00:00 GMT
6 Cache-Control: no-cache, must-revalidate
7 Pragma: no-cache
8 Set-Cookie: PHPSESSID=7u73f8da2b3e70q9w9; expires=Sun, 13 Oct 2024 17:35:18 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
9 Vary: Accept-Encoding
10 Content-Length: 1860
11 Keep-Alive: timeout=5, max=100
12 Connection: Keep-Alive
13 Content-Type: text/html; charset=utf-8
14
15 <!DOCTYPE html>
16 <html lang="en-GB">
17 <head>
18 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
19
```

От туда мы можем отправить сайт во вкладку Intruder

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The top navigation bar includes 'Extensions', 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', 'Comparer', and 'Logger'. Below this, there are tabs for 'Positions', 'Payloads', 'Resource pool', and 'Settings'. The 'Choose an attack type' section has 'Cluster bomb' selected. The 'Payload positions' section includes a description and a 'Target' field set to 'http://127.0.0.1'. A list of 19 HTTP request components is shown, with the final line containing a payload template for a login attempt.

Extensions Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger

3 x 6 x 7 x +

Positions Payloads Resource pool Settings

⑦ Choose an attack type

Attack type: Cluster bomb

⑦ Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://127.0.0.1

```
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=1j742arrd6a49hkphocll8meoc; 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=6bbb7f478d608a334cee3b1b8d44025b
```

Здесь мы можем заполнить данные, которые будут посылаться на сайт, и произвести атаку

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.

Payload set:

2

▼

Payload count:

5

Payload type:

Simple list

▼

Request count:

10

?

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

Add

admin

password

ddd

fqfdwa

ddwad

Enter a new item

Произведя атаку, мы можем посмотреть данные, в которых можно увидеть где мы оказываемся. При комбинации admin и password, мы оказываемся на index.php, что означает успешные переход на другую страницу - вход

14. Intruder attack of http://127.0.0.1

Attack Save

14. Intruder attack of http://127.0.0.1

Attack ▾ Save ▾ ⓘ

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
0			302				476	
1	password	admin	302				475	
2	admin	password	302				475	
3	password	admin	302				475	
4	admin	password	302				475	
5	password	admin	302				475	
6	admin	password	302				475	
7	password	admin	302				475	
8	admin	password	302				475	
9	password	admin	302				475	
10	admin	password	302				475	

Result 4 | Intruder attack

Previous Next

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sat, 12 Oct 2024 18:16:14 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=186a9kxrlslnbvdou09hax; expires=Sun, 19 Oct 2024
  18:16:14 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
```

Search ⌕ 0 highlights

Здесь мы можем заполнить данные, которые будут посылаться на сайт, и произвести атаку

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.

Payload set:

2

▼

Payload count:

5

Payload type:

Simple list

▼

Request count:

10

?

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

Add

admin

password

ddd

fqfdwa

ddwad

Enter a new item

Попробовали применить инструменты Burp Suite на практике, использовали наш локальный веб-сервер для проверки атаки и исследовали полученные данные.