

Индивидуальный проект №4

Использование nikto

Машков И. Е.

08 марта 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Машков Илья Евгеньевич
- Студент 2-го курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132231984@pfur.ru
- <https://github.com/7S7eVe7N7>

Научиться использовать Burp Suite.

```
(iemashkov@iemashkov)-[~]  
$ sudo systemctl start apache2  
[sudo] пароль для iemashkov:  
  
(iemashkov@iemashkov)-[~]  
$ sudo systemctl start mysql  
  
(iemashkov@iemashkov)-[~]  
$ 
```

Рис. 1: Запуск локального сервера

Выполнение лабораторной работы

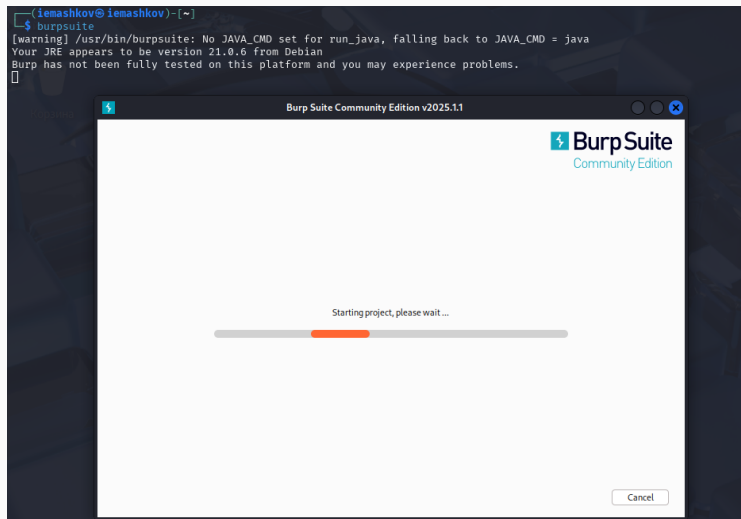


Рис. 2: Запуск приложения

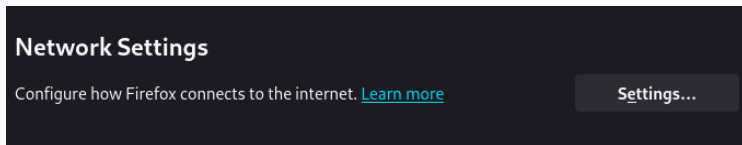


Рис. 3: Сетевые настройки браузера

Выполнение лабораторной работы

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

Port

0

SOCKS Host

Port

0

☐ SOCKS v4

☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

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

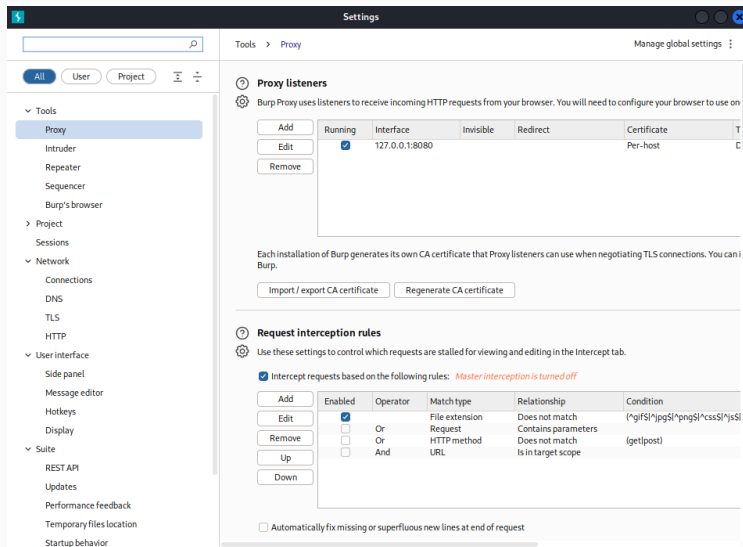
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

Cancel

OK

Выполнение лабораторной работы



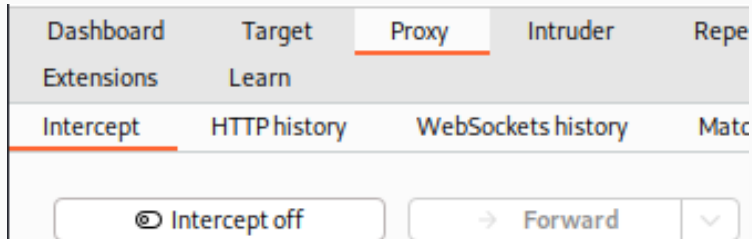


Рис. 6: Настройки Proxy

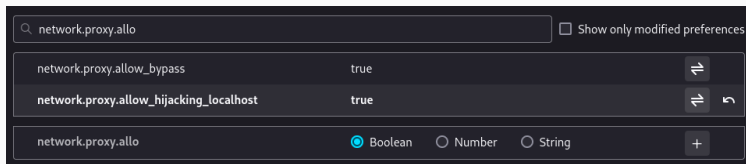


Рис. 7: Настройки параметров

Выполнение лабораторной работы

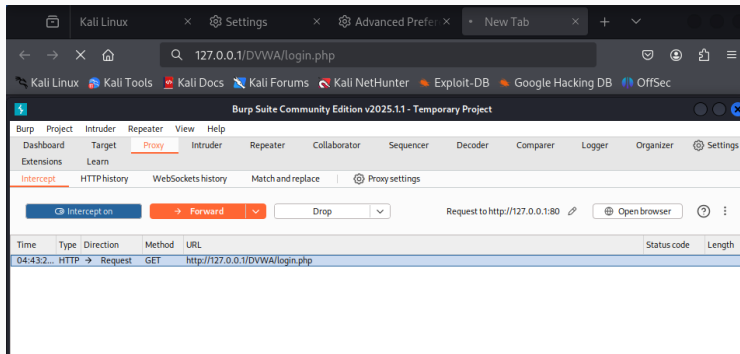


Рис. 8: Получаемые запросы сервера

Выполнение лабораторной работы

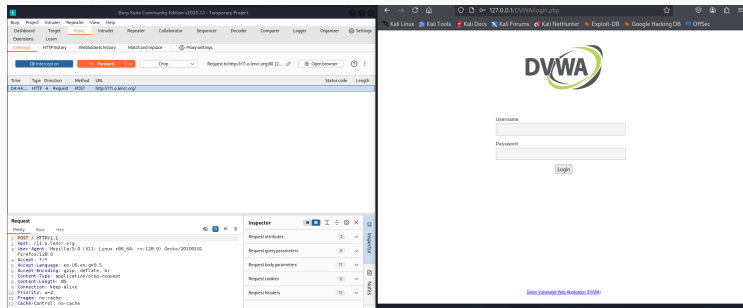


Рис. 9: Страница авторизации

Выполнение лабораторной работы

Burp Suite Community Edition v2025.1.1 - Temporary Project

Menu: Burp Project Intruder Repeater View Help

Sub-menu: Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Sub-menu: Extensions Learn

Sub-menu: Site map Scope Issue definitions

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Site map: > http://127.0.0.1

Pro version only

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://127.0.0.1	GET	/DVWA/login.php		200	2011	HTML	Login:: Damn Vulnera...

Request Response

Inspector

Request attributes 2

Request headers 12

Response headers 13

Notes

```
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:128.0) Gecko/20100101
  Firefox/128.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14
15
```

Выполнение лабораторной работы

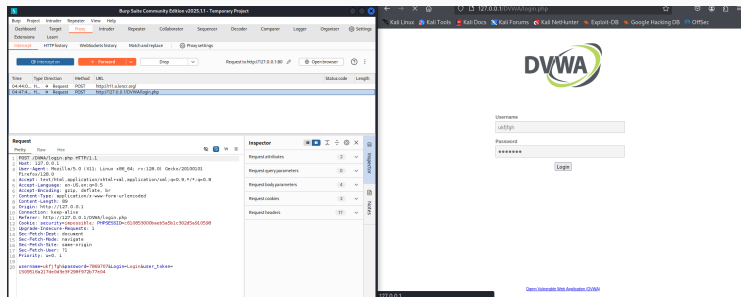


Рис. 11: Ввод случайных данных

Выполнение лабораторной работы

Burp Suite Community Edition v2025.1.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

Site map Scope Issue definitions

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

> http://127.0.0.1

Pro version only

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://127.0.0.1	GET	/DVWA/login.php				HTML	Login :: Damn Vulnerable...

Request Response

Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Lin
  x86_64; rv:128.0) Gecko/20100101
  Firefox/128.0
4 Accept:
  text/html,application/xhtml+xml,e
  ion/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, b
7 Connection: keep-alive
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14
15
```

Inspector

Notes

http://127.0.0.1/DVWA/login.php

- Add to scope
- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Organizer Ctrl+O
- Send to Comparer (request)
- Send to Comparer (response)
- Show response in browser
- Request in browser
- Engagement tools [Pro version only]
- Compare site maps
- Add notes
- Highlight
- Delete item
- Copy URL
- Copy as curl command (bash)
- Copy links
- Save item
- Site map documentation

Выполнение лабораторной работы

The screenshot displays the Burp Suite Community Edition v2025.1.1 interface. The 'Intruder' tab is active, showing a 'Sniper attack' configuration. The target is set to 'http://127.0.0.1', and the 'Update Host header to match target' checkbox is checked. The 'Positions' section includes 'Add \$', 'Clear \$', and 'Auto \$' buttons. The main area shows the HTTP request details for a POST to '/DWA/login.php'.

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,*/*;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: 89
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=c610853000baeb5a5b1c302d5a910598
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=ukfj fgh&password=7869707&Login=Login&user_token=1509516a217de0d3e3f298f972b77e04

Выполнение лабораторной работы

The screenshot displays the Burp Suite Community Edition v2025.1.1 interface. The 'Intruder' tab is active, showing a 'Cluster bomb attack' configuration. The target is set to 'http://127.0.0.1'. The attack is configured with 4 positions. The payload list contains a single entry: a POST request to '/DWA/login.php' with various headers and a body containing a username and password. The 'Start attack' button is visible.

Burp Suite Community Edition v2025.1.1 - Temporary Project

Dashboard Target **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

1 x 4 x +

Cluster bomb attack Start attack

Target http://127.0.0.1 Update Host header to match target

Positions Add \$ Clear \$ Auto \$

```
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,*/*;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: 89
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=c610853000baeb5a5b1c302d5a910598
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=$ukfjfqh$password=$7869707$&Login=Login&user_token=1509516a217de0d3e3f298f972b77e04
```

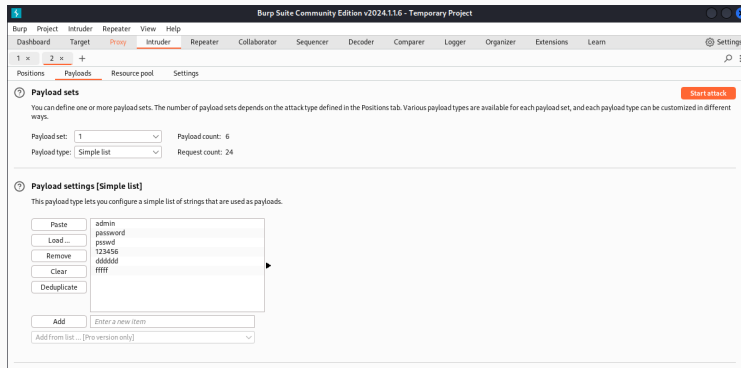


Рис. 15: Первый Simple list

Выполнение лабораторной работы

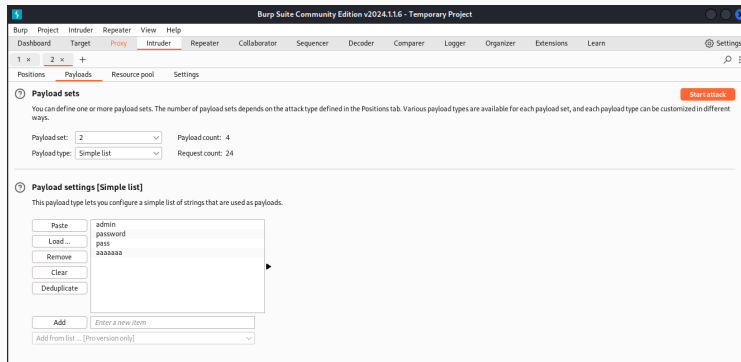


Рис. 16: Второй Simple list

Выполнение лабораторной работы

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

Filter Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			302	7			476	
1	admin	admin	302	13			476	
2	password	admin	302	3			476	
3	passwd	admin	302	4			476	
4	123456	admin	302	2			476	
5	admin	admin	302	3			476	
6	BTI	admin	302	5			476	
7	admin	password	302	3			476	
8	password	password	302	6			476	
9	passwd	password	302	6			476	
10	123456	password	302	2			476	
11	admin	password	302	3			476	
12	BTI	password	302	3			476	
13	admin	pass	302	2			476	
14	password	pass	302	2			476	
15	passwd	pass	302	3			476	
16	123456	pass	302	3			476	
17	admin	pass	302	2			476	
18	BTI	pass	302	2			476	
19	admin	aaaaaaa	302	10			476	
20	password	aaaaaaa	302	9			476	
21	passwd	aaaaaaa	302	7			476	
22	123456	aaaaaaa	302	5			476	
23	admin	aaaaaaa	302	4			476	
24	BTI	aaaaaaa	302	7			476	

Finished

Рис. 17: Запуск атаки

Выполнение лабораторной работы

Result 1 | Intruder attack

Payload1: admin
Payload2: admin
Status code: 302
Length: 475
Timer: 13

Previous
Next

Request
Response

PrettyRawHexRender

1 HTTP/1.1 302 Found
2 Date: Thu, 09 May 2024 14:47:26 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=hqle0nfenbtgo6dcc2ok3edu83; expires=Fri, 10 May 2024 14:47:26 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: login.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=99
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14

0 highlights

Выполнение лабораторной работы

Result 7 | Intruder attack

Payload 1: admin
Payload 2: password
Status code: 302
Length: 415
Timer: 3

Previous
Next

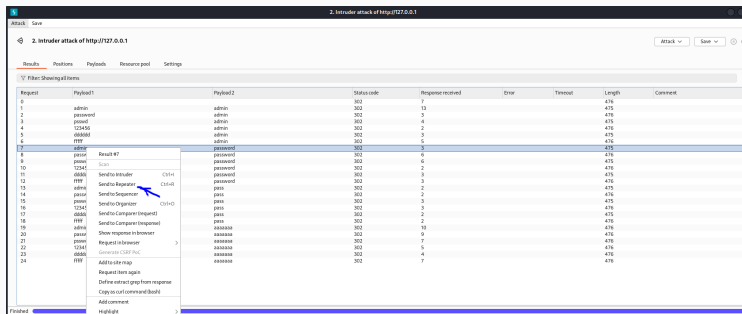
Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Thu, 09 May 2024 14:47:27 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=f12tf6kskiqgdp9g0mju7e4oc3; expires=Fri, 10 May 2024
  14:47:27 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=97
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14
```

0 highlights

Выполнение лабораторной работы



Attack Save

2. Intruder attack of http://127.0.0.1

Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
0			302	7			476	
1	admin	admin	302	13			475	
2	password	admin	302	3			476	
3	pass	admin	302	4			475	
4	123456	admin	302	2			476	
5	0x0x0x	admin	302	3			475	
6	HTTP	admin	302	5			476	
7	admin	password	302	3			475	
8	pass	Result #7	302	6			476	
9	pass	scan	302	6			475	
10	12345	password	302	2			476	
11	0x0x0x	Send to Intruder	302	3			475	
12	HTTP	Send to Sequencer	302	3			476	
13	admin	Send to Sequencer	302	2			475	
14	pass	Send to Sequencer	302	2			476	
15	pass	Send to Sequencer	302	3			475	
16	12345	pass	302	1			476	
17	0x0x0x	Send to Campaign (request)	302	2			475	
18	HTTP	Send to Campaign (request)	302	2			476	
19	admin	pass	302	19			475	
20	pass	Show response in browser	302	9			476	
21	pass	Request in browser	302	7			476	
22	12345	Convert GZIP file	302	5			476	
23	0x0x0x	Add to site map	302	4			476	
24	HTTP	Request here again	302	7			476	
		Define extract group from response						
		Copy as curl command (bash)						
		Add comment						
Finished		Highlight						

Рис. 20: Дополнительная проверка результата

Выполнение лабораторной работы

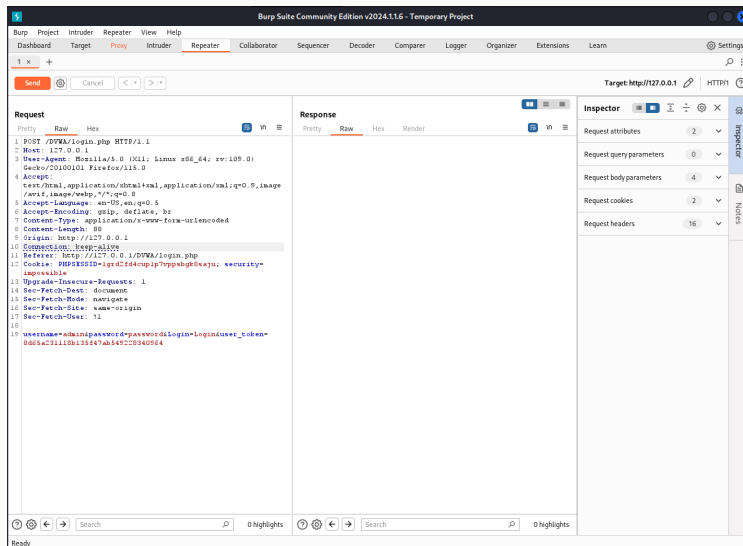


Рис. 21: Вкладка Repeater

Выполнение лабораторной работы

Burp Suite Community Edition v2024.1.16 - Temporary Project

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

1 x +

Send Cancel < + > + Follow redirection

Target: http://127.0.0.1 HTTP/1

Request

Pretty Raw Hex

```
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=1grdZf44cuplp7oppabgk8waju; 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: 11
18
19 username=admin&password=password&login=login&user_token=
  0d6fa231118b135f47ab649220340964
```

Response

Pretty Raw Hex Render

```
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=dv7q7lwvmslu7vb7mc7b086c9;
  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
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 4

Request cookies 2

Request headers 16

Response headers 11

476 bytes | 1,006 millis

Выполнение лабораторной работы

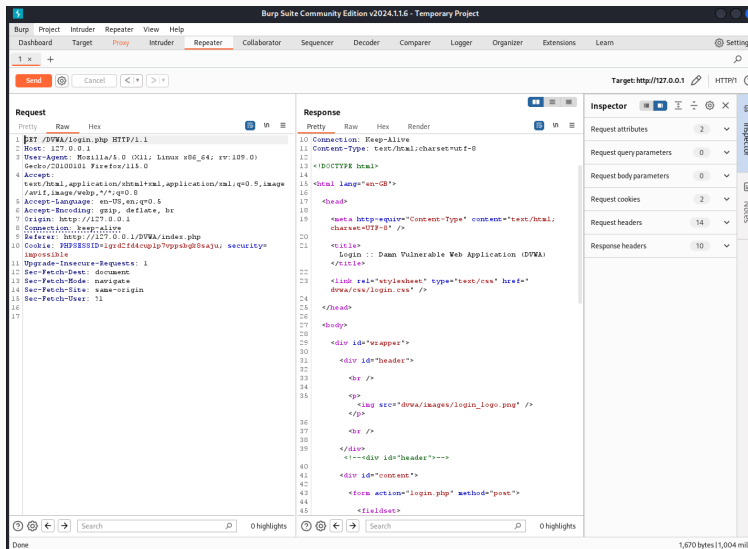


Рис. 23: Именование в окне Response

Выполнение лабораторной работы

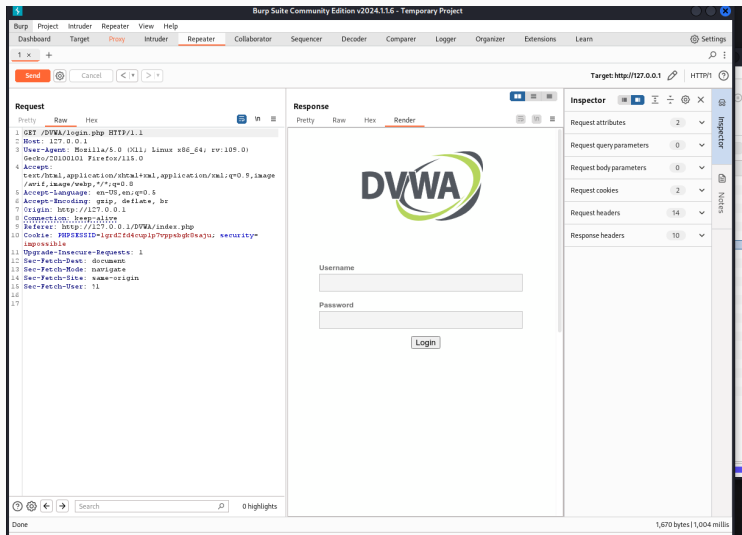


Рис. 24: Полученная страница

При выполнении лабораторной работы научился использовать инструмент Burp Suite.