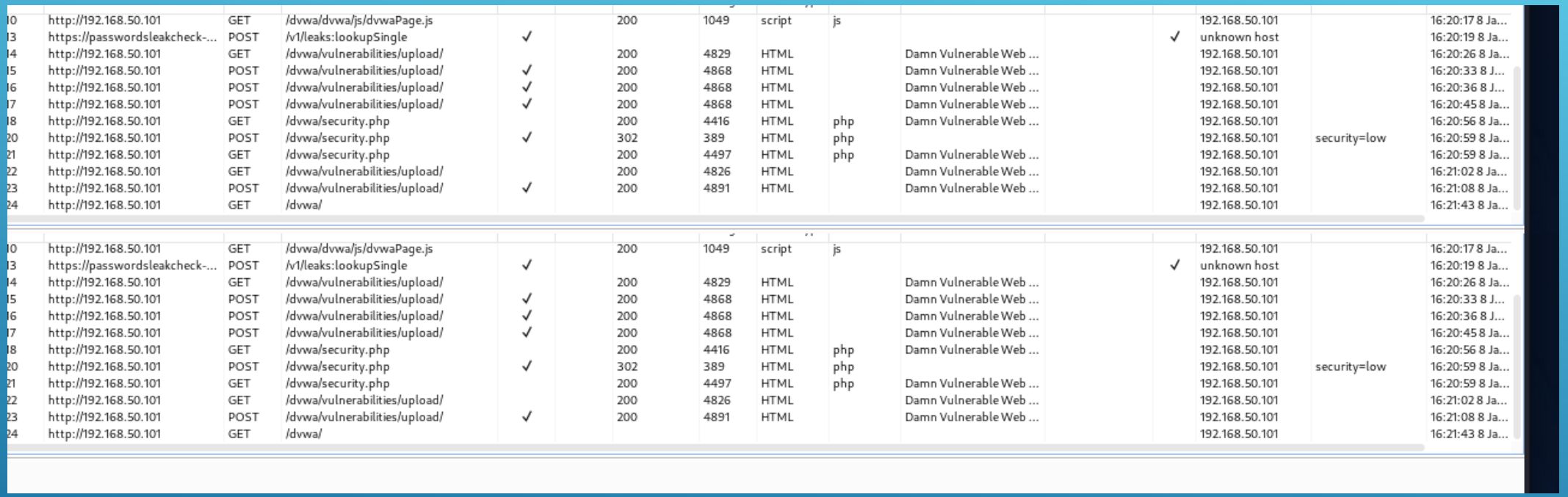
S6L1

La traccia di oggi consisteva nel sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in php sull'indirizzo Ip di metasploitable 192.168.50.101

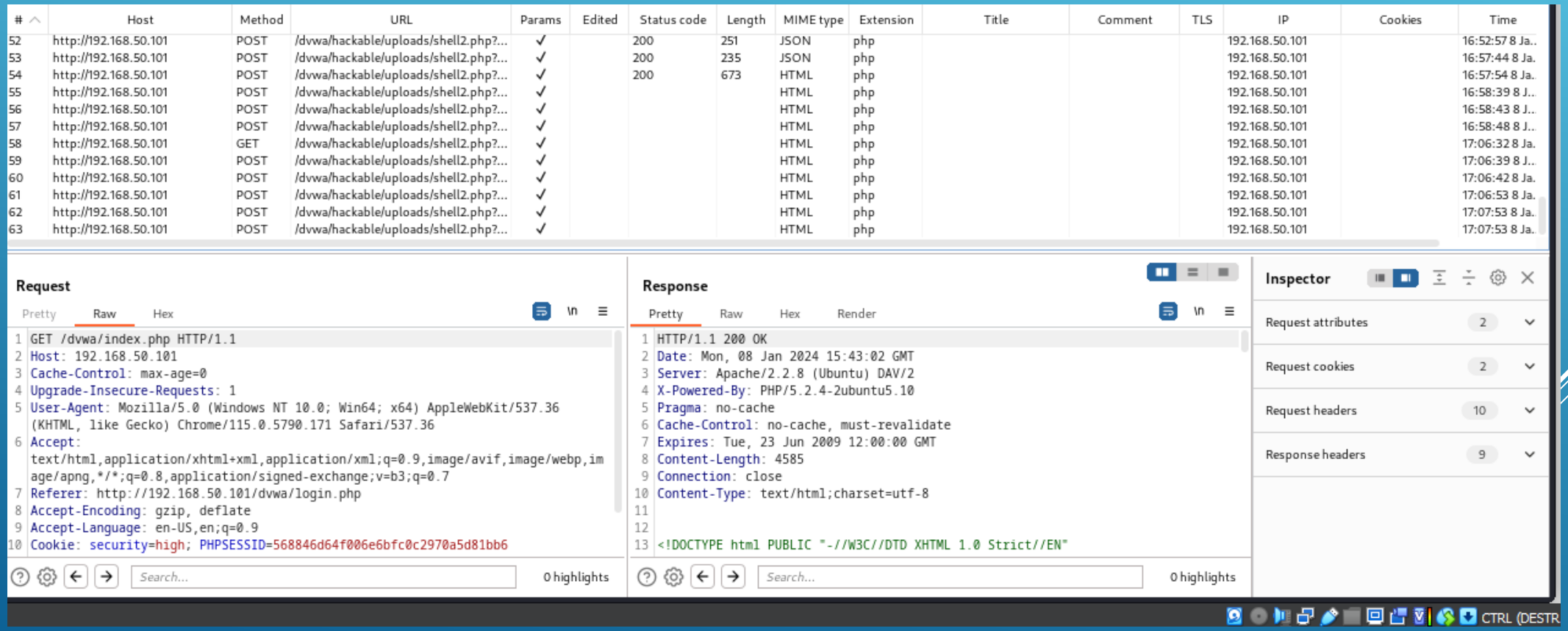
INTERCETTARE TRAMITE BURPSUITE E ANALIZZARE OGNI RICHIESTA VERSO LA DVWA



10	http://192.168.50.101	GET	/dvwa/dvwa/js/dvwaPage.js			200	1049	script	js			192.168.50.101		16:20:17 8 Ja...
13	https://passwordsleakcheck-...	POST	/v1/leaks:lookupSingle	✓							✓	unknown host		16:20:19 8 Ja...
14	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4829	HTML		Damn Vulnerable Web ...		192.168.50.101		16:20:26 8 Ja...
15	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web ...		192.168.50.101		16:20:33 8 J...
16	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web ...		192.168.50.101		16:20:36 8 J...
17	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web ...		192.168.50.101		16:20:45 8 Ja...
18	http://192.168.50.101	GET	/dvwa/security.php			200	4416	HTML	php	Damn Vulnerable Web ...		192.168.50.101		16:20:56 8 Ja...
20	http://192.168.50.101	POST	/dvwa/security.php	✓		302	389	HTML	php			192.168.50.101	security=low	16:20:59 8 Ja...
21	http://192.168.50.101	GET	/dvwa/security.php			200	4497	HTML	php	Damn Vulnerable Web ...		192.168.50.101		16:20:59 8 Ja...
22	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web ...		192.168.50.101		16:21:02 8 Ja...
23	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web ...		192.168.50.101		16:21:08 8 Ja...
24	http://192.168.50.101	GET	/dvwa/									192.168.50.101		16:21:43 8 Ja...

10	http://192.168.50.101	GET	/dvwa/dvwa/js/dvwaPage.js			200	1049	script	js			192.168.50.101		16:20:17 8 Ja...
13	https://passwordsleakcheck-...	POST	/v1/leaks:lookupSingle	✓							✓	unknown host		16:20:19 8 Ja...
14	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4829	HTML		Damn Vulnerable Web ...		192.168.50.101		16:20:26 8 Ja...
15	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web ...		192.168.50.101		16:20:33 8 J...
16	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web ...		192.168.50.101		16:20:36 8 J...
17	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4868	HTML		Damn Vulnerable Web ...		192.168.50.101		16:20:45 8 Ja...
18	http://192.168.50.101	GET	/dvwa/security.php			200	4416	HTML	php	Damn Vulnerable Web ...		192.168.50.101		16:20:56 8 Ja...
20	http://192.168.50.101	POST	/dvwa/security.php	✓		302	389	HTML	php			192.168.50.101	security=low	16:20:59 8 Ja...
21	http://192.168.50.101	GET	/dvwa/security.php			200	4497	HTML	php	Damn Vulnerable Web ...		192.168.50.101		16:20:59 8 Ja...
22	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web ...		192.168.50.101		16:21:02 8 Ja...
23	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web ...		192.168.50.101		16:21:08 8 Ja...
24	http://192.168.50.101	GET	/dvwa/									192.168.50.101		16:21:43 8 Ja...

IN FINALE ABBIAMO ESEGUITO LO STESSO PROCEDIMENTO CON UNA SHELL IN PHP PIÙ COMPLESSA SEMPRE TRAMITE BURPSUITE CON IL COMANDO GET



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time
52	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	251	JSON	php				192.168.50.101		16:52:57 8 Ja..
53	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	235	JSON	php				192.168.50.101		16:57:44 8 Ja.
54	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	673	HTML	php				192.168.50.101		16:57:54 8 Ja.
55	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		16:58:39 8 J..
56	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		16:58:43 8 J..
57	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		16:58:48 8 J..
58	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		17:06:32 8 Ja.
59	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		17:06:39 8 J..
60	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		17:06:42 8 Ja.
61	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		17:06:53 8 Ja.
62	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		17:07:53 8 Ja.
63	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		17:07:53 8 Ja.

Request

Pretty Raw Hex

```
1 GET /dvwa/index.php HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
  age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://192.168.50.101/dvwa/login.php
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: security=high; PHPSESSID=568846d64f006e6bfc0c2970a5d81bb6
```

Search... 0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 15:43:02 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Pragma: no-cache
6 Cache-Control: no-cache, must-revalidate
7 Expires: Tue, 23 Jun 2009 12:00:00 GMT
8 Content-Length: 4585
9 Connection: close
10 Content-Type: text/html;charset=utf-8
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
```

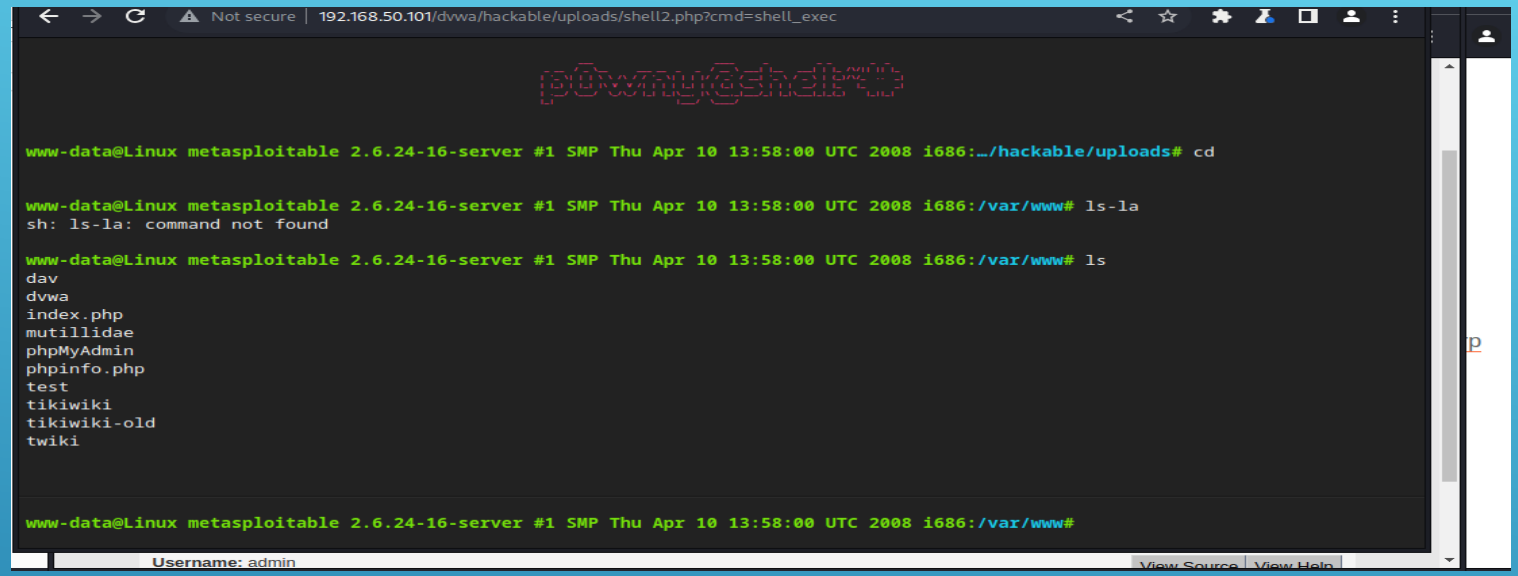
Search... 0 highlights

Inspector

- Request attributes 2
- Request cookies 2
- Request headers 10
- Response headers 9

CTRL (DESTR

Come si può notare nella shell più complessa non possiamo interagire su di essa nella seconda Immagine su burpsuite phpsessid si evidenziano i cookie di sessione



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time
59	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	235	JSON	php				192.168.50.101		17:06:39 8 J...
60	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	721	HTML	php				192.168.50.101		17:06:42 8 Ja...
61	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	673	HTML	php				192.168.50.101		17:06:53 8 Ja...
62	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	741	HTML	php				192.168.50.101		17:07:53 8 Ja...
63	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	721	HTML	php				192.168.50.101		17:07:53 8 Ja...
64	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell2.php?...	✓		200	15474	HTML	php	p0wny@shell:~#			192.168.50.101		17:10:46 8 Ja...
65	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	251	JSON	php				192.168.50.101		17:11:14 8 Ja...
66	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	235	JSON	php				192.168.50.101		17:11:36 8 Ja...
67	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	275	JSON	php				192.168.50.101		17:11:42 8 Ja...
68	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓		200	352	JSON	php				192.168.50.101		17:11:47 8 Ja...
69	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell2.php?...	✓		200	15474	HTML	php	p0wny@shell:~#			192.168.50.101		17:12:48 8 Ja...
70	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell2.php?...	✓				HTML	php				192.168.50.101		17:12:51 8 Ja...

Request

Pretty Raw Hex

```
1 GET /dvwa/index.php HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
  age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://192.168.50.101/dvwa/login.php
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: security=high; PHPSESSID=568846d64f006e6bfc0c2970a5d81bb6
```

Search... 0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 15:43:02 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Pragma: no-cache
6 Cache-Control: no-cache, must-revalidate
7 Expires: Tue, 23 Jun 2009 12:00:00 GMT
8 Content-Length: 4585
9 Connection: close
10 Content-Type: text/html;charset=utf-8
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
```

Search... 0 highlights

Inspector

- Request attributes 2
- Request cookies 2
- Request headers 10
- Response headers 9