

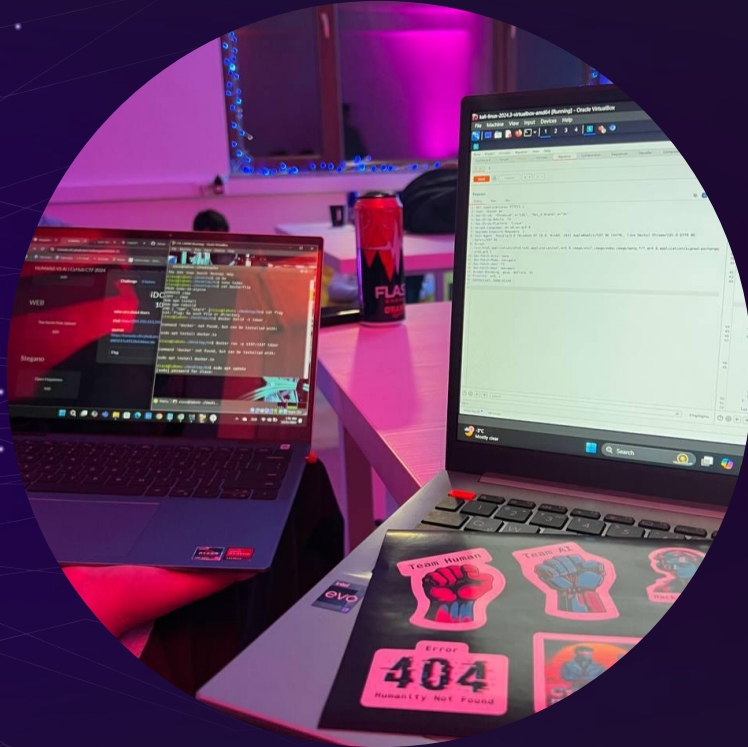
Penetration Testing and Ethical Hacking

«Patch early, scan often, trust nothing»



~Tamara Babakhanyan

Ինչու՞ Cyber security



Երկար ուսումնասիրելուց և տարբեր ուղղությունների ծանոթանալուց հետո հասկացա, որ ցանկացած ուղրտի հիմքում ընկած է տեղեկատվության՝

- Ստացումը
- Փոխանցումը
- Պահպանումը

Եվ շատ կարևոր է, որ այդ տեղեկատվական հաղորդակցությունները լինեն ապահով, ճիշտ և բարեխղճորեն կառավարվող: Այս է պատճառը, որ ինձ համար ինֆորմացիոն տեխնոլոգիաները դարձան այն ուղրտը, որը ինձ թույլ կտար ստեղծագործել և կիրառել հասանելի ինֆորմացիան առաջ քաշվող խնդիրներին լուծում տալու համար:

Relq technology school?

- **Building cloud based server**

AWS,SSH,Ubuntu,Linux,Apache2,
FireWall,VirtualBox,PortManagment,
Brute Force,IPtables

- **Mastering vulnerabilities
And Network scanning**

WEB security,TryHackMe,Nmap,Python,
RootMe,OWASP,Pentesting,Metasploitable

- **PortSwigger and
BurpSuite**

PortSwigger,Metasploit,Ruby Basics,msfVenom
Reverse Shell,Vulnhub

- **Malware Development**

WireShark,MalWare,Reverse Engineering,
"ransomware", "RAT", "keylogger", "spyware",
"adware", "contact/cookie stealer"

- **Windows server and
Active Directory**

Windows Server,Runas,CS,CVE,
DNS/DHCP Setup,Virtual Machine,
Testing by Kali Linux,Crack Map,BackDoor

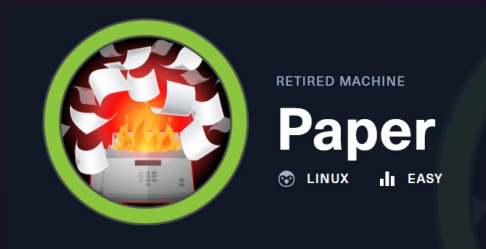
- **OSINT investigation**

OSINT,Open-Source intelligence,
GEO location,Digital footprint,Researching,
Maltego,Google Dorking,OSINT Tools



HACKTHEBOX

Starting out in Cybersecurity, HackTheBox (HTB) has been the go-to resource provided to me or anyone interested in Penetration Testing and Ethical Hacking for that matter.



- 22/tcp SSH
- 80/tcp HTTP
- 443/tcp SSL/HTTP

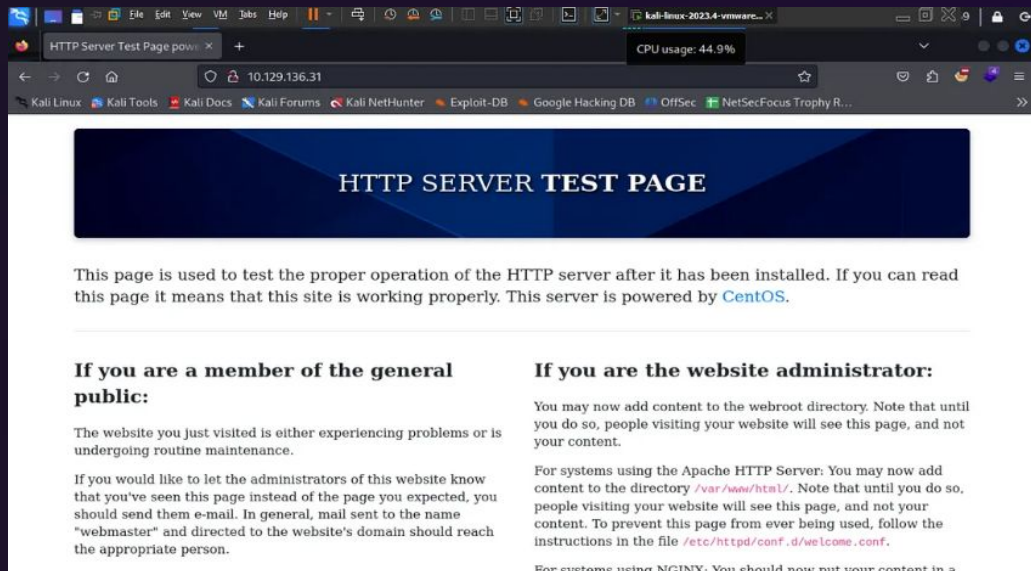
3 ports open



Lets Use Nmap

```
Host is up (0.41s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   2048 10:05:ea:50:56:a6:00:cb:1c:9c:93:df:5f:83:e0:64 (RSA)
|   256  58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
|_  256  31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
80/tcp    open  http         Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_ http-title: HTTP Server Test Page powered by CentOS
|_ http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
443/tcp   open  ssl/http     Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_ http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_ http-title: HTTP Server Test Page powered by CentOS
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US
|_ Subject Alternative Name: DNS:localhost.localdomain
```

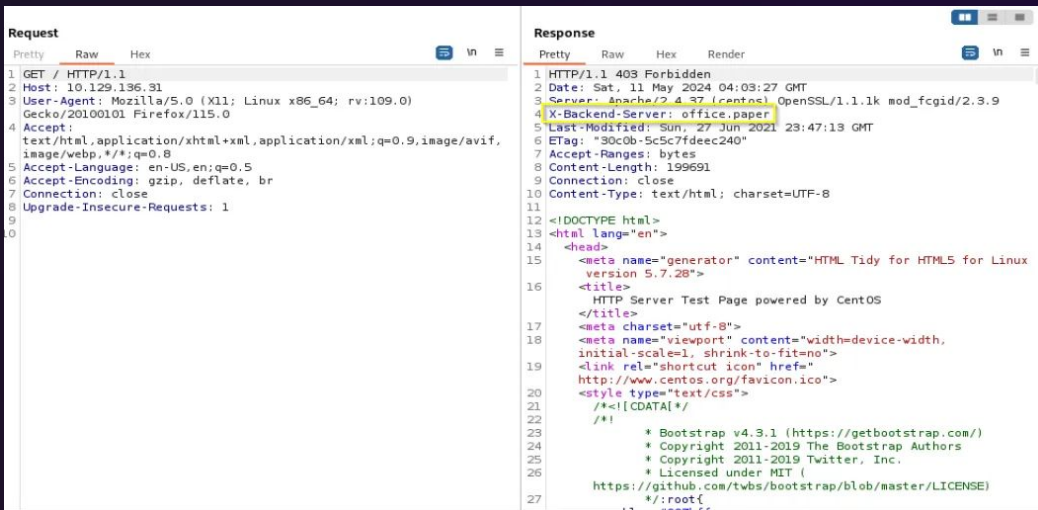
Let's check website



There are nothing interesting...



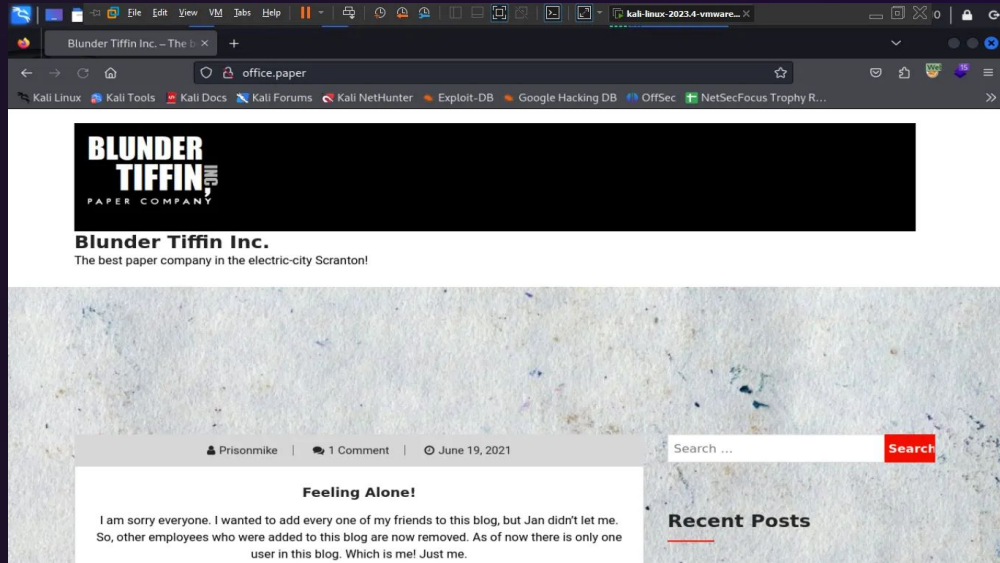
Let's Use BurpSuite



Burp Suite can identify common security flaws such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more. By sitting between the user's browser and the web application, Burp Suite acts as a proxy server.

I found a subdomain in this response header so I'll add this subdomain in the host's file. Office.paper

I check Office.paper domain



WordPress is a web content management system. It was originally created as a tool to publish blogs but has evolved to support publishing other web content, including more traditional websites

This website uses **WordPress** so I'll use *wpscan* to scan the website.

I need to scan all plugins by
wpscan

```
Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid,
| - X-Powered-By: PHP/7.2.24
| - X-Backend-Server: office.paper
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] WordPress readme found: http://office.paper/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] WordPress version 5.2.3 identified (Insecure, released on
| Found By: Rss Generator (Passive Detection)
| - http://office.paper/index.php/feed/, <generator>https://
| - http://office.paper/index.php/comments/feed/, <generator>
```

```
(kali㉿kali)-[~]
$ wpscan --url "http://office.paper/"
```

I googled to search 5.2.3 for any exploit for this version after that I
found this CVE (CVE-2019-17671)

0
DAY

Sebastian Neef - 0daywork

home

Proof of Concept for "Wordpress <=5.2.3: viewing unauthenticated posts" (CVE-2019-17671)

A couple of days [WordPress released 5.2.4](#) with a few security patches. *Props to J.D. Grimes who found and disclosed a method of viewing unauthenticated posts.* caught my attention, but I couldn't find a public Proof of Concept, so I set out to reverse engineer the published patch.

Information Gathering

My first step was to find as much information as possible about the bug as I couldn't find a PoC. I compared the statements from different security companies. Most recited the same phrase of "possibility to view unauthenticated posts":

- <https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html>
- <https://blog.wpscan.org/wordpress-5-2-4-security-release/>
- https://www.reddit.com/r/netsec/comments/d9k72/wordpress_524_security_release_breakdown/f3vbuyh/
- ...

I discovered the relevant patch in the WordPress SVN repo / [Github repo mirror](#) by selecting the branch `5.2-branch` and going through the list of [most recent commits](#), looking for a commit that mentions `unauthenticated posts` or `viewing posts` or something similar. [Commit f82ed753cf00329a5e41f2cb6dc521085136f308](#) looked interesting!

Analysing the Patch

site benötigt Cookies, um ohne Einschränkungen genutzt werden zu können. [Mehr erfahren](#)

Verstanden

6:47 PM 5/3/2023

I check the website and found some secret URL

Inside the FBI, Agent Michael Scarn sits with his feet up on his desk. His robotic butler Dwigt....

Secret Registration URL of new Employee chat system


<http://chat.office.paper/register/8qozr226AhkCHZdyY>

I am keeping this draft unpublished, as unpublished drafts cannot be accessed by outsiders. I am not that ignorant, Nick.

Also, stop looking at my drafts. Jeez!

← → ↺ ⌂ 🔍 chat.office.paper/register/8qozr226AhkCHZdyY ☆ 📧 ⬇️ 📁 🏠 🌐 📱

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec NetSecFocus Trophy R...



Register a new account

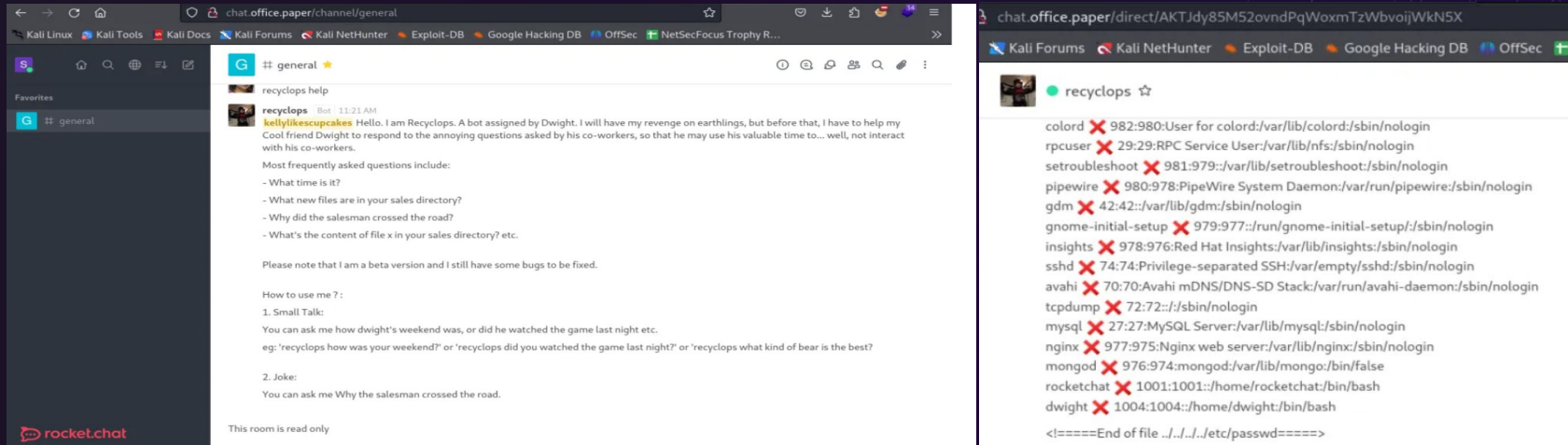
Back to login

By proceeding you are agreeing to our [Terms of Service](#), [Privacy Policy](#) and [Legal Notice](#)

Powered by [Open Source Chat Platform Rocket.Chat](#)

“We have rocket chat so let’s
register by email and password for
login to the chat.”

After Login i found this chat and there some interesting messages



In this rocket.chat i found that this user is bot and i can use some linux commands
And we can read some information about passwords base-by using etc/passwd

Հնորհակալութիւն

«Patch early, scan often, trust nothing»