HTB - Paper

Nmap

- sC: default scripts
- sV: show versions
- oA: output all formats

> *CentOS, for Apache server*
>
> *Self-signed certificate: not verified by other orgs*

Feroxbuster/gobuster

- 403: access forbidden
- 301: page moved

Burpsuite

- found x-backend server: office.paper
- check with `banner-plus` nmap script

<script src="https://gist.github.com/littleairmada/b04319742c29efe44d5662d842c20e1c.js"></script>

Look at `office.paper`

- check WordPress
  - view source: v 5.2.3
  - 2019

Wpscan

- to check wordpress
- quickscan first
- Enumerate later
  - all plugins: `ap`
  - plugin detection: aggressive

WP exploits

`?static=1&order=asc`

=> 404

=> gewoon

Secret Registration URL of Employee chat system

- add to `/etc/hosts`
- open link in registration link
  - registering (rocket chat)
  - searchsploit check
  - text recyclops for OS commands
  - `cat ../../../etc/passwd`
  - `/proc/self/environ`
  - => Dwight runs it & password
- `cat /proc/self/stat`
- `cat /proc/2530/cmdline`

SSH

- `ps -ef --forest`
  - to look at bot_restart.sh
  - executes by Dwight => not useful
- look at Rocketchat code
- `cd /var/www/html/`

Linpeas

- http server & wget on remote
- `CVE-2021-3560`
- run polkit.sh
- `su - secnigma`
- `sudo su -`

NoSQL injection from exploitdb

- pip3 install oathtool
- => no result