CyberApolis Water Breach Report

Payton Sinclair

Department of Homeland Security

December 10th, 2025

Table of Contents

Executive Summary

Due to the attack and take over of the CyberApolis Water Company by the terrorist group the Carbon Spector who opened the flood gates of the dam in an attempt to flood the city of CyberApolis, I executed an infiltration into the CyberApolis Water Company's systems in order to regain control of the dam and avert the destruction of CyberApolis.

The infiltration was done by gathering as much information on the company as possible both front facing and internal. This was done by identifying employees who may have sensitive credentials that could be used to access the company, scanning and scraping all of the publicly available information about the company and its employees, utilizing tools that scan the company's network in an attempt to find vulnerabilities, and then exploiting said vulnerabilities once found in order to gain access to the network through an employees' poor use of their sensitive account information. I utilized an exploit on the website to gather usernames and passwords that I could use to get into the employee portal. I cracked those passwords, and used them to access the systems in order to shut the flood gates of the dam.

As it stands, the CyberApolis Water Company is extremely vulnerable to numerous attacks due to the inherent vulnerabilities in their website, and the weakness of their employees' sensitive data and credentials. In order to mitigate the risk, the website needs to be improved by someone with security in mind in order to fix the vulnerabilities inherently present in the website. Employees need to be required to have much more secure passwords, with a longer minimum length, and the addition of symbols. Additionally, the website also needs to have stronger authentication for the employees, such as two factor authentication in order to prevent attackers from accessing their accounts so easily. These things will dramatically improve the poor security of the CyberApolis Water Company and can help deter problems in the future.

Introduction

During pre-engagement activities, I was informed that the CyberApolis Water Company had been taken over and captured by a terrorist organization known as the Carbon Spector. I was informed that Carbon Spector had taken employees of the CyberApolis Water Company hostage and that they aim to open the flood gates of the dam to flood the city of CyberApolis. I have been tasked by the Department of Homeland Security to hack into the CyberApolis Water Company, gain access to the HMI controls, and shut down the dam's flood gates before a disaster befalls CyberApolis. I was given no restrictions in the methods for this task, and therefore, used any means necessary to gain access and complete the task handed to me. This task was given to me with no information outside of the address to the website being http://water.cyberapolis.gov.

Reconnaissance

I started with reconnaissance, and began by going to the http://water.cyberapolis.gov website in order to figure out what information I could glean from the website.

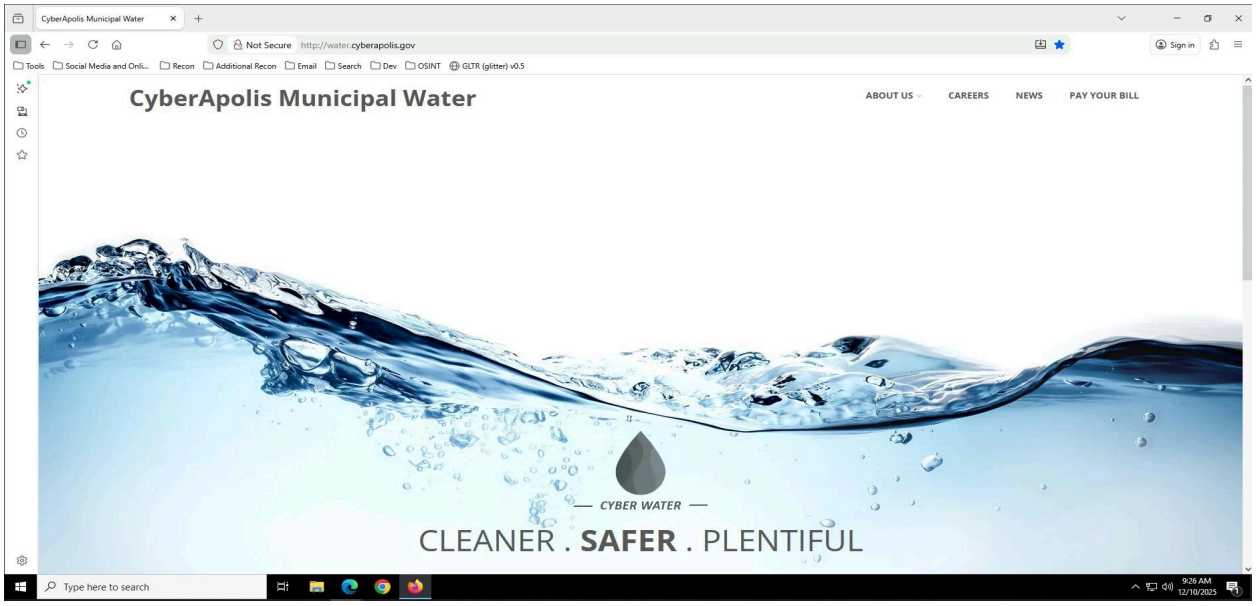


Figure R1 : Water Company Website

First, I went to the about us page to identify potential individuals with information I could use to access the company's water systems. The page gave me eight individuals who may have information I could use to access the company's systems.

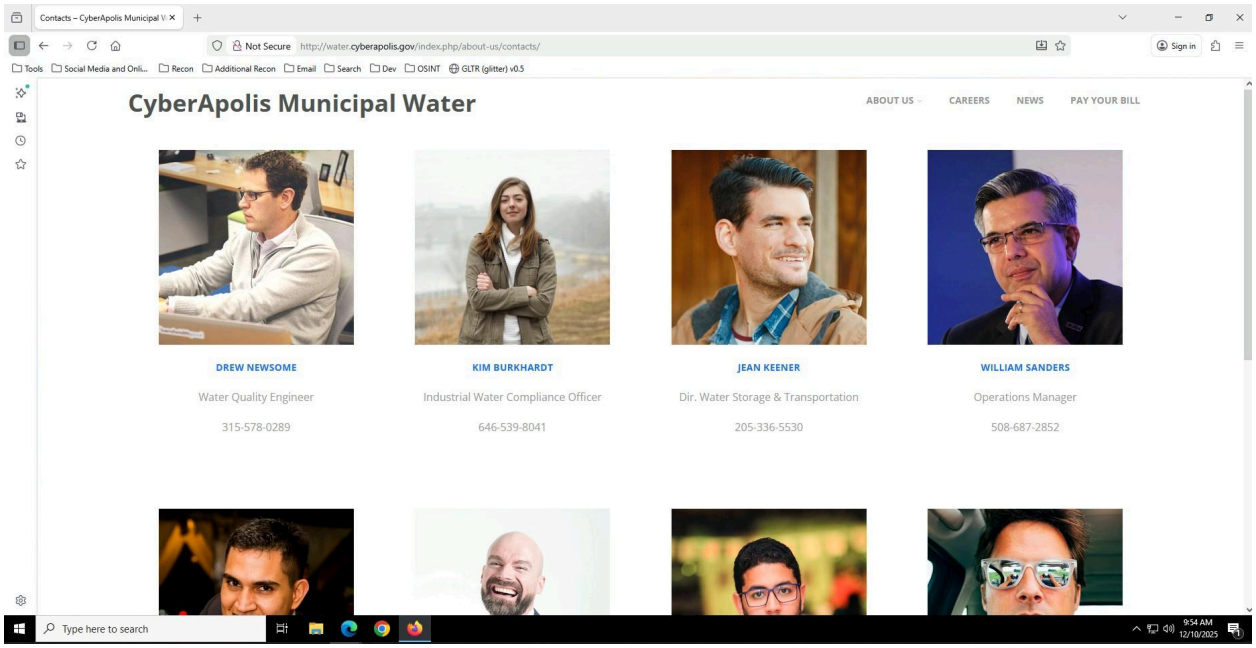


Figure R2 : Potential Executive Targets

My next course of action was to search for all eight of these individuals's social media accounts, as well as the company as a whole, to identify information about them.

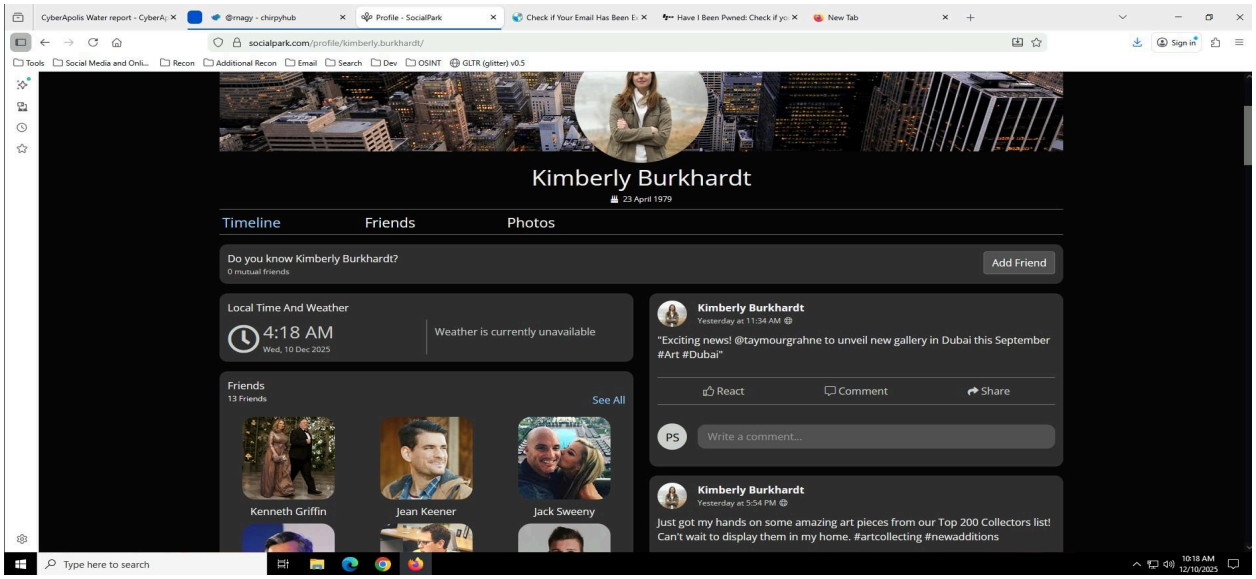


Figure R3 : Social Media Accounts

I didn't determine anything of note from the social media accounts, so I went to the reports page on the Water Company's website, downloaded the reports, and recovered metadata from them using exiftool on the windows terminal. William Sander's account name is sandersw.

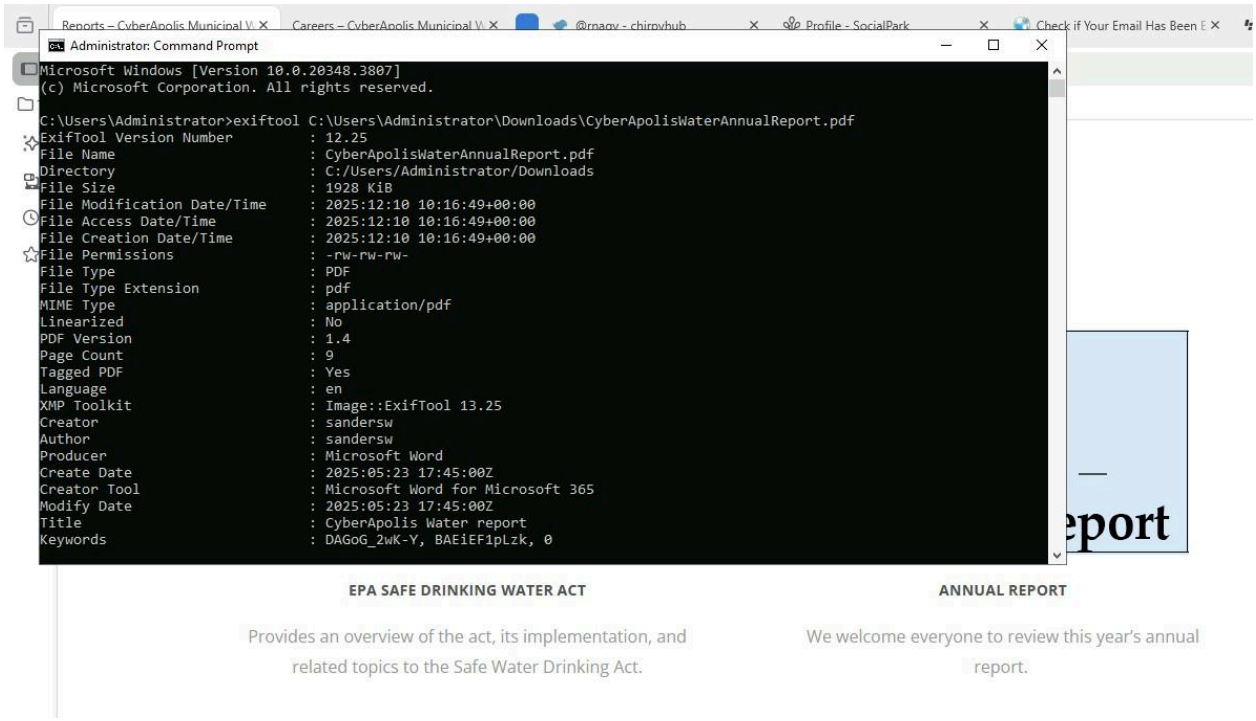


Figure R4 : Exiftool Metadata

I then looked at the source for the contacts page, and found two emails for people who weren't on the contact list, but were listed as part of the board. These emails confirmed to me the layout of the company email being @water.cyberapolis.gov.

Figure R5 : Page Source Information

Then I finally checked for a robots.txt file and a sitemap.xml file. I didn't find either, but I was directed to a url not found page that gave me some information on the server version and on what port it was running.

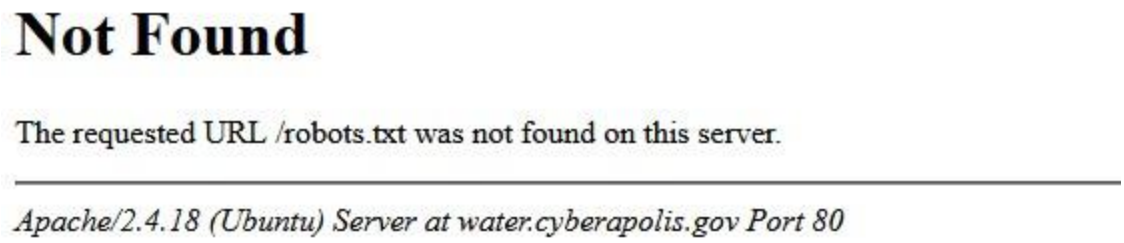


Figure R6 : URL Not Found Page

Scanning

I then began scanning the website for vulnerable ports starting with confirming the host is up. This helped me confirm the IP address for the website being (10.139.40.217).

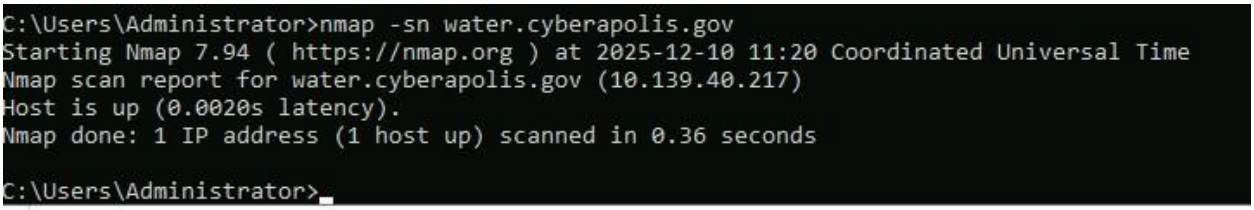


Figure S1 : Host Confirmed Up

I then conducted a scan of all open TCP ports on the water.cyberapolis.gov website. This scan revealed that only 4 ports were open, those being port 21 for FTP, port 22 for SSH, port 29 for finger, and port 80 for HTTP. FTP is the file transfer protocol, but isn't secure and can be exploited by attackers. SSH is the secure shell, which could be exploited if an attacker obtained admin credentials. The finger service is a very old protocol used to get information about system users. (Mitigation suggestion) The HTTP service hosts the web server for the website.

```
C:\Users\Administrator>nmap -sS -p- -T4 10.139.40.217
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-10 11:30 Coordinated Universal Time
Nmap scan report for water.cyberapolis.gov (10.139.40.217)
Host is up (0.00069s latency).
Not shown: 65531 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
79/tcp open  finger
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 8.72 seconds

C:\Users\Administrator>
```

Figure S2 : Open Ports

I then scanned for the versions of the services running on the open ports to look for vulnerabilities. Ftp is on version vsftpd 3.0.3, SSH is running OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0), finger's version went unidentified, and http is running Apache httpd 2.4.18.

```
C:\Users\Administrator>nmap -sV -sC -p 21,22,79,80 10.139.40.217
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-10 11:47 Coordinated Universal Time
Nmap scan report for water.cyberapolis.gov (10.139.40.217)
Host is up (0.0010s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 05:86:ad:4b:95:03:e6:33:5f:18:66:74:f2:f9:27:f1 (RSA)
|   256 63:40:a8:fc:ad:f3:56:32:44:bf:65:99:2b:46:8a:fa (ECDSA)
|_  256 f2:6d:44:5d:99:29:31:8b:e1:0b:fa:31:cd:10:5d:df (ED25519)
79/tcp open  finger?
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: CyberApolis Municipal Water
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.24 seconds

C:\Users\Administrator>
```

Figure S3 : Service Versions

I quickly followed this up by just conducting a scan to identify the OS. Which ended up being a Linux Kernel in the 3.X family, likely, 3.10-3.13. This is an outdated OS and should be updated.

```
C:\Users\Administrator>nmap -O water.cyberapolis.gov
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-10 11:56 Coordinated Universal Time
Nmap scan report for water.cyberapolis.gov (10.139.40.217)
Host is up (0.0039s latency).
Not shown: 996 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
79/tcp open  finger
80/tcp open  http
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10 - 3.13
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds

C:\Users\Administrator>
```

Figure S4 : OS Version

Finally, I wrapped up the vulnerability scanning with a ZAP scan, checking for vulnerabilities in the website that could be exploited. The scan uncovered several high priority vulnerabilities, the two most important being ”Remote OS Command Injection” and “SQL Injection”. The first of the two means that ZAP detected a field that would accept user input and run it as a system command, the other means zap detected a field that is vulnerable to SQL injection, potentially allowing me to gather user and employee data from the back end database.

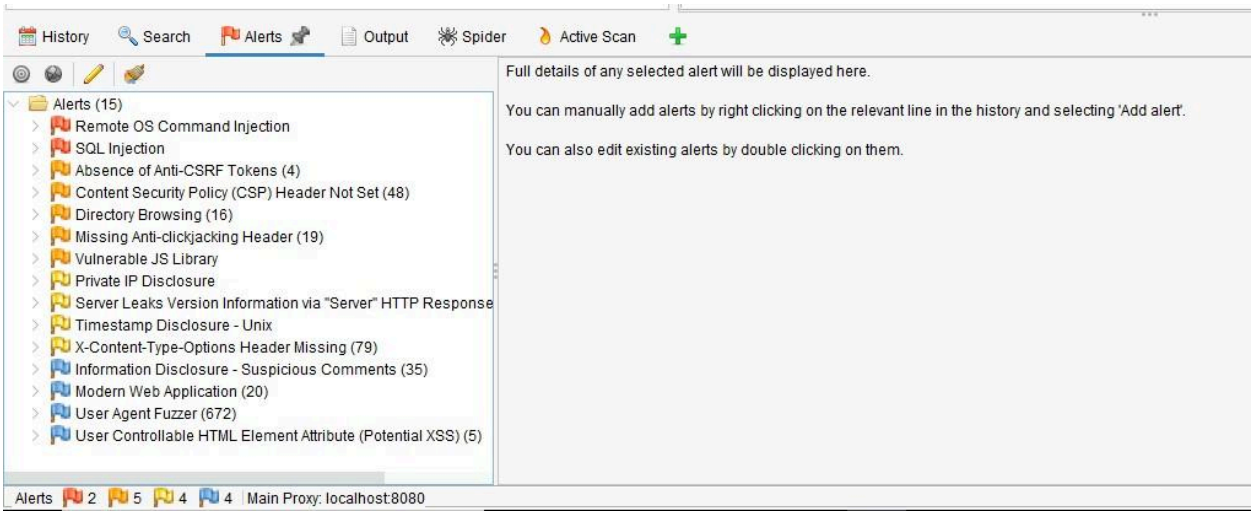


Figure S5 : Zap Scan Vulnerabilities

Exploitation

Now it is time for exploitation of the discovered vulnerabilities. To do this, I used the fact I know that this website is running on Linux OS, and has a Remote OS Command Injection vulnerability to type commands into whatever fields I could find. The vulnerable field is the three fields in the pay your bill tab of the water company's website water.cyberapolis.gov/index.php/pay-your-bill/

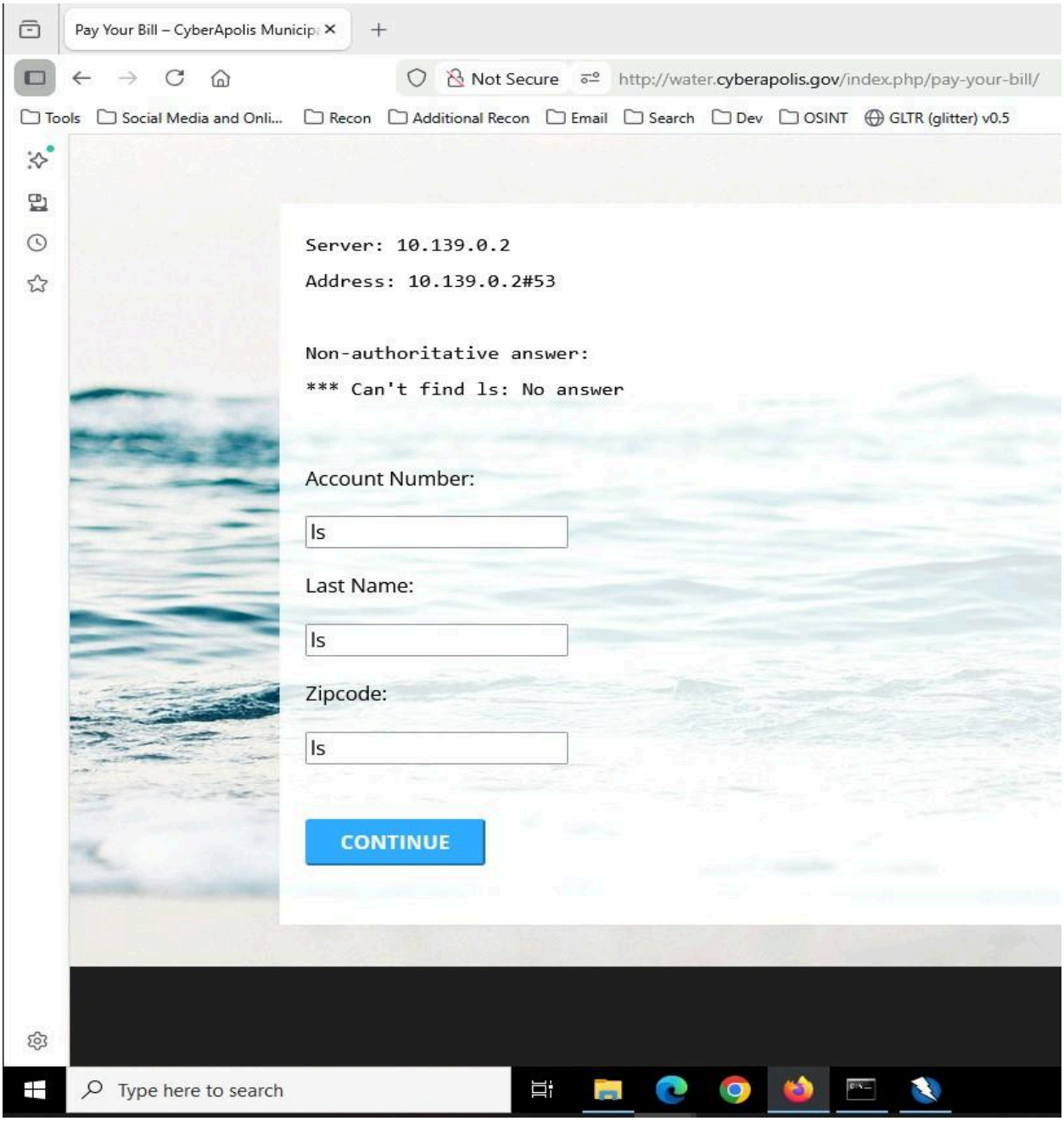


Figure E1 : Injection Field Discovered

I then exploited the field with a Linux command to get the files on the server.

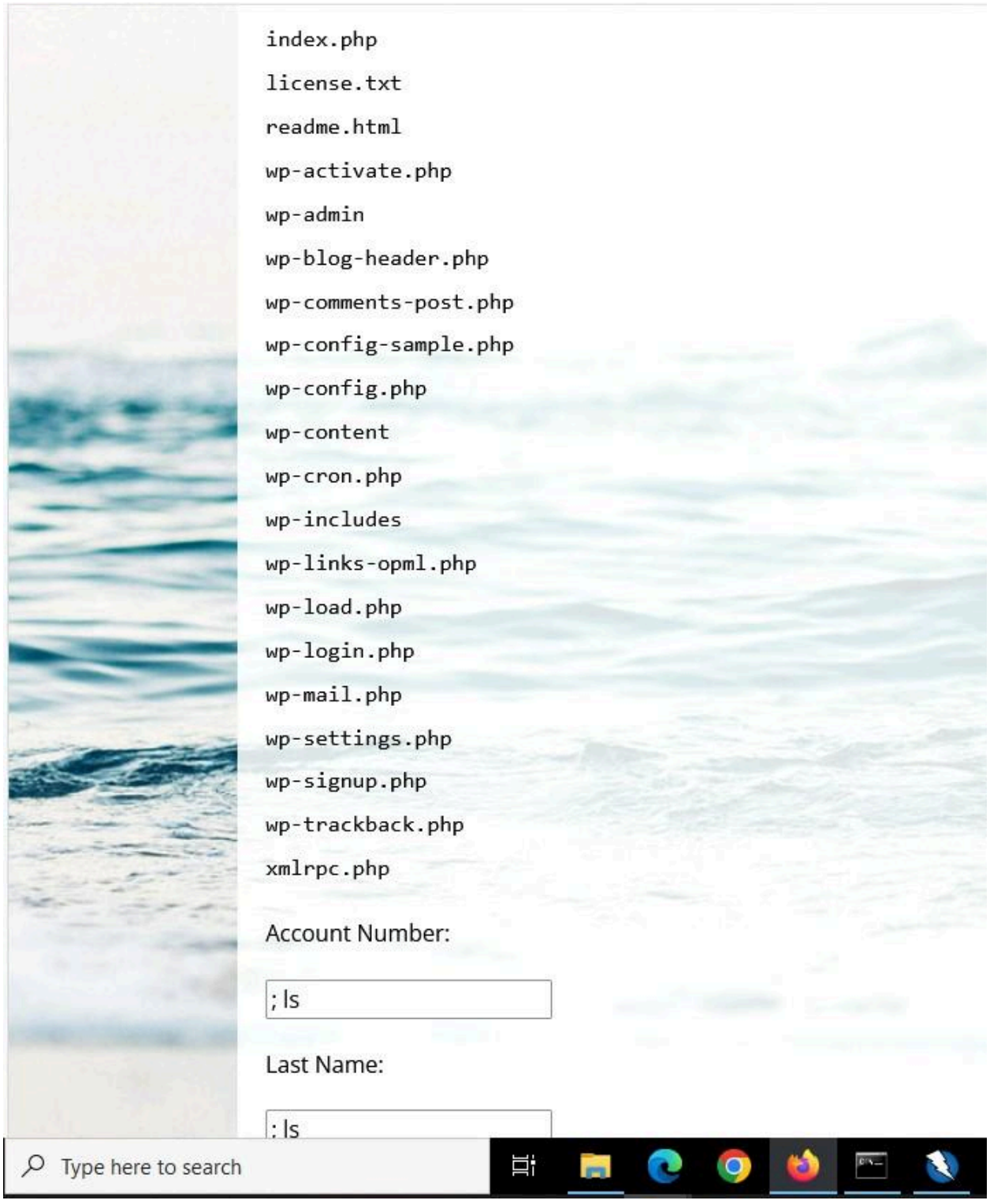


Figure E2 : Command Injection to Gather Files on Server

Next I used the cat command to read the contents of the wp-config.php file in order to get the credentials to the SQL database so that I can get login details for the employee portal.

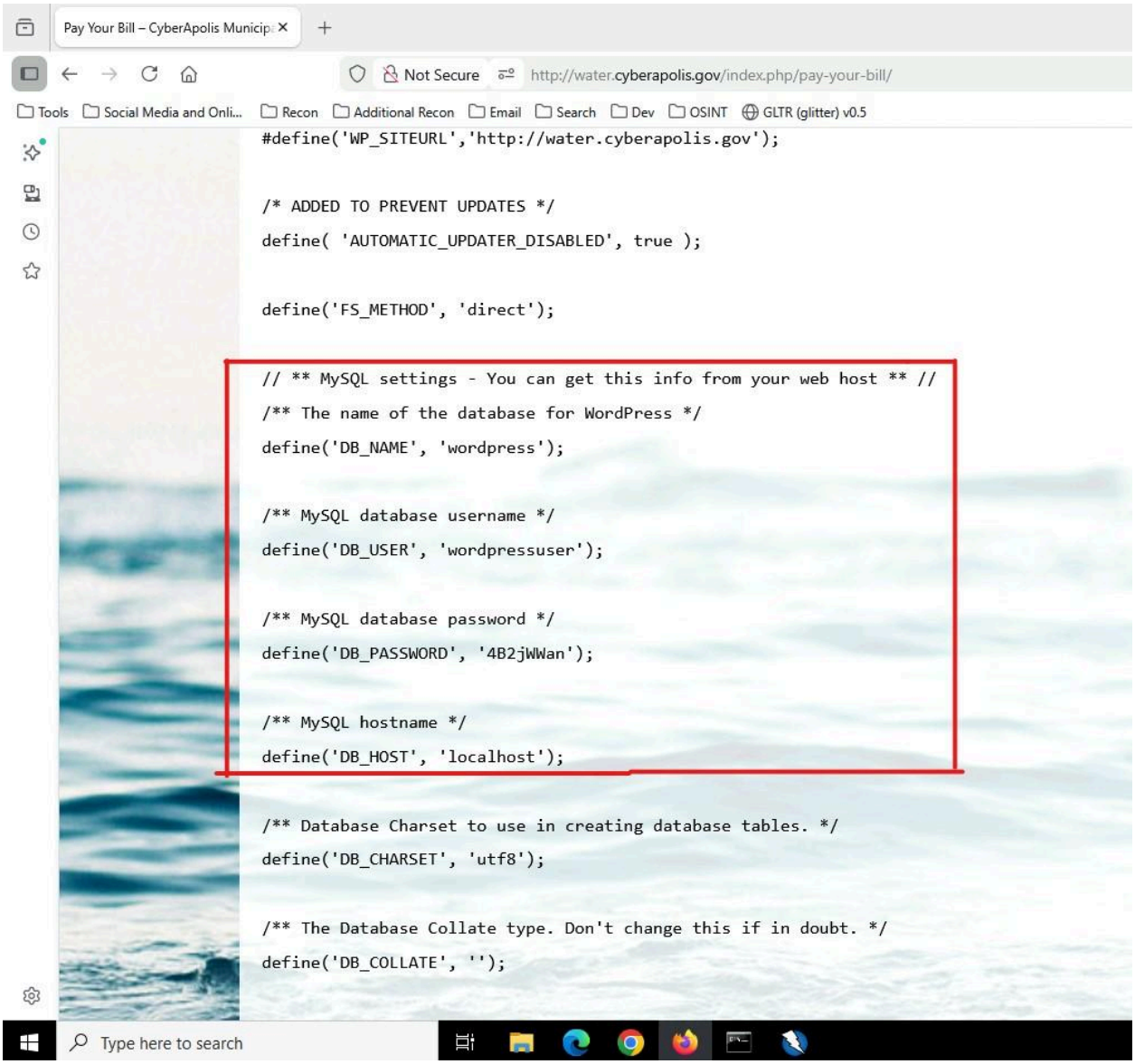


Figure E3 : Collection of MySQL Credentials

Now that I have the MySQL credentials to work with, I next ran the “; mysqldump -u wordpressuser -p4B2jWWan? wordpress wp_users > /tmp/out.txt” code in the vulnerable field to log into MySQL, get usernames and passwords, and dump them into a text file. I then used the cat command on the dumped text file to get the usernames and passwords. This gave me the

usernames, emails, and password hashes for administrator, jhuag, and nmiller, who was one of our people of interest earlier. His data may become very useful, as well as the administrator.

```
LOCK TABLES `wp_users` WRITE;
/*!40000 ALTER TABLE `wp_users` DISABLE KEYS */;
INSERT INTO `wp_users` VALUES (1,'administrator','$P$Btl4QxtImnxuw2cg7WZuckFYs1.6kI0','administrator','uacyber@ephibian.com','','2016-08-01
23:44:41','',0,'administrator'),(2,'jhaug','$P$BJf5symeHmoPIxygDerx3KWID1LBn0.','jhaug','jhaug@ephibian.com','','2016-08-02
18:25:56','',0,'jhaug'),(3,'nmiller','$P$B6r9Dtcb34jTYaiGZ9TNXcBUPcH2pW.','nmiller','nmiller@ephibian.com','','2016-08-02
20:57:33','',0,'Norman Miller');
/*!40000 ALTER TABLE `wp_users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

Figure E4 : MySQL Access and Exploitation

Now that I have usernames and password hashes, I exported them to a text file, used WinSCP to transfer my file from my Windows system to my Kali Linux system, and used John the Ripper to crack the password hashes. However, here John the Ripper failed to crack the hashes, and I didn't have the right formatting for them, so instead, I switched back to command injection instead of MySQL, used the cat /etc/shadow command to get usernames and hashes in the correct format, for the people of interest on the contact page.

I then grabbed almost all of the people of interest who were on the contact page being Drew Newsome, Kim Burkhardt, Jean Keener, William Sanders, William Gilbert, Kenneth Griffin, Richard Nagy, and Jack Sweeny. John the Ripper was able to crack the passwords of William Sanders, Jean Keener, and William Gilbert.

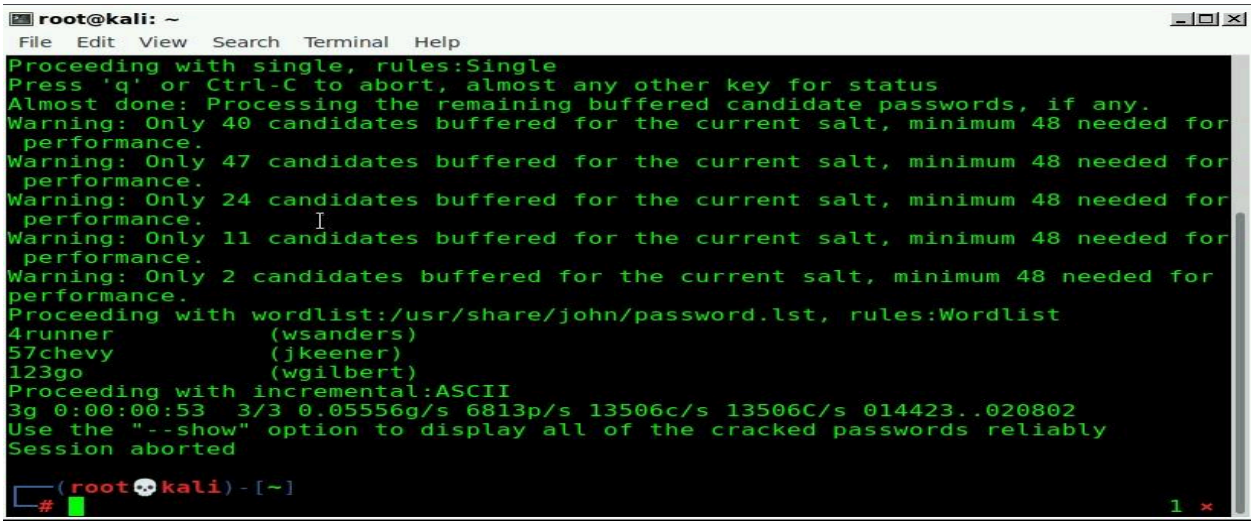
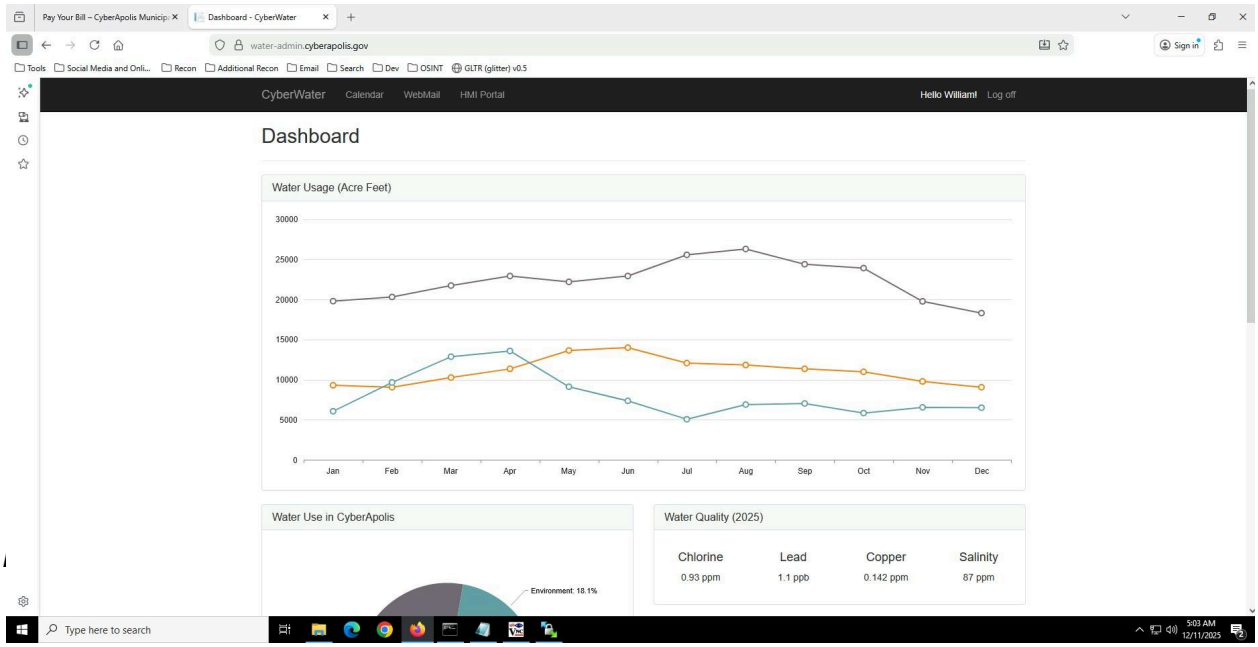


Figure E5 : Shows the Output of John the Ripper

Post Exploitation

With my new usernames and passwords, I now went to log into the employee portal.



Now that I have successfully gotten into the employee dashboard, I need to gain access to the HMI's controls and close the flood gates of the dam. The login credentials of William Sanders didn't work for the HMI portal, and neither did the other two individuals whose passwords I cracked, however, the username for William Sanders, wsanders, is different from the one I found in the metadata of the reports put out by the water company, so I tried logging in using that username and password. I was successful.

Post Exploitation

I have managed to log into the HMI portal using the login credentials of William Sanders.

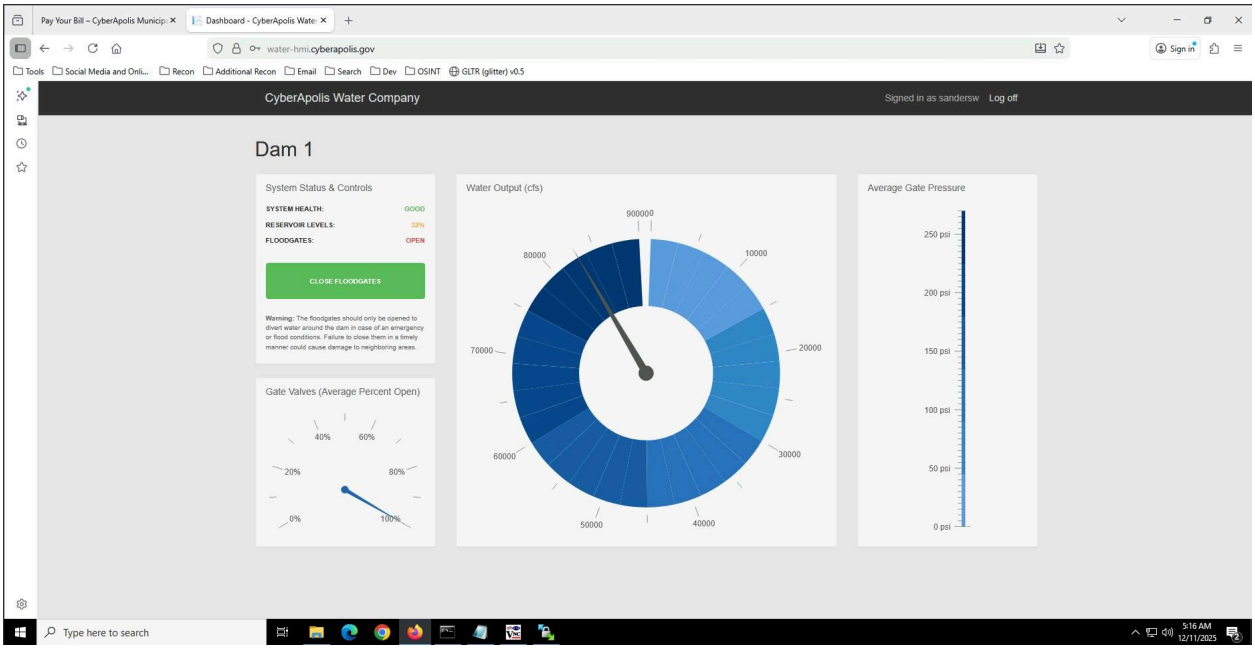


Figure P1 : Shows the HMI Portal Accessed.

All I need to do now is close the flood gates to save CyberApolis.

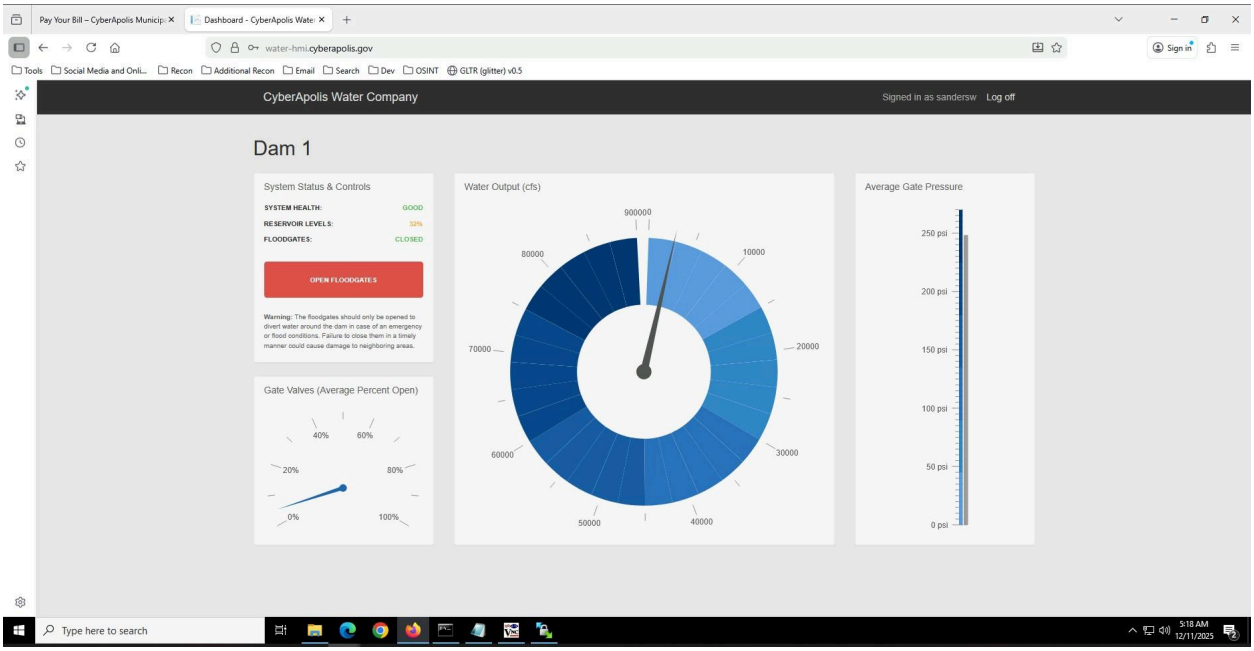


Figure P2 : CyberApolis is Saved

Summary and Mitigations

This report details the steps and techniques used to successfully infiltrate the CyberApolis Water Company's internal network. Those steps being reconnaissance, scanning exploitation, and post exploitation. This report shows through these steps that there are several high priority security risks that cause the CyberApolis Water Company to be vulnerable to multiple attack surfaces, and put the employees at risk.

The report began with the reconnaissance phase where target individuals were acquired, and sensitive public data was learned about them such as their emails, email formats and usernames. In the scanning phase, ports were discovered to be open, with insecure services running on them, and vulnerabilities were found on the web server, including two that could serve as an entire attack surface with which to infiltrate the system on. Those being the remote OS command injection, and the SQL injection vulnerabilities. These vulnerabilities both allow you to look through the company's internal databases by passing commands through an insecure field on the website. This allowed for the exploitation of the website, gathering usernames and passwords that were cracked and used to gain entry into the employee portal. In the post exploitation phase, we simply had total access to the portal, and to the HMI controls where we were able to shut down the flood gates.

In order to mitigate the risk that this report has brought to light, it is recommended to reconfigure the insecure fields on the website so that they aren't easy attack vectors into the website. It is recommended to shut down unnecessary ports such as port 79 hosting a legacy program that can be used as an attack vector. It is also recommended to maintain and keep up to date all protocols that are being run. Another major recommendation to mitigate risk to the company is to improve employee credential security. Make it a policy to have a strong password with a minimum length and symbols included, and enable some sort of two factor authentication to make it more difficult for attackers to gain easy entry once obtaining a username and password.