

CyberApolis Water Breach Report

Christopher Wilson

Department of Homeland Security

February 27, 2024

Table of Contents:

Executive Summary	3
Introduction	4
1. Reconnaissance	5
2. Scanning	6
3. Exploitation	8
4. post-exploitation	10
5. Summary and Mitigation	11
6. Synopsis	12

Executive Summary:

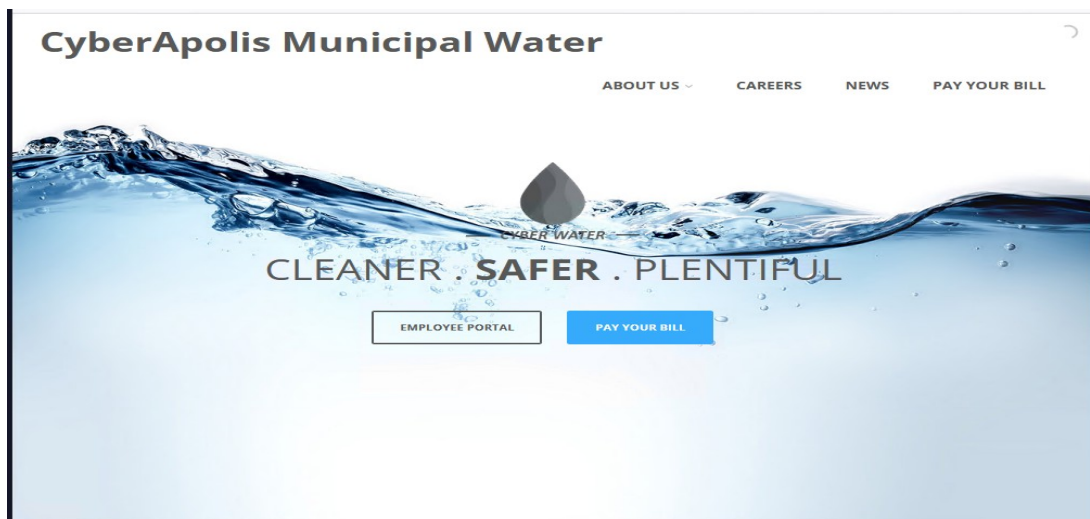
In a robust and orchestrated response to the cyber-attack on the CyberApolis Water Company, a meticulous counter-operation unfolded in phases, showcasing the resilience and preparedness of our cybersecurity team. Starting with an in-depth reconnaissance phase, we targeted pivotal access points, successfully uncovering credentials to the employee portal—a significant breakthrough. Subsequent scanning unveiled web vulnerabilities, facilitating our entry into the portal. This gateway yielded valuable data, including an employee's personal communications. With rigorous metadata analysis, an alternate pathway emerged, leading us to a different username for the HMI portal. Gaining control over the HMI interface, we promptly secured the floodgates, mitigating immediate threats. Simultaneously, efforts to reinforce cybersecurity measures commenced, focusing on patching identified vulnerabilities to fortify the water company's digital infrastructure against future incursions. This cohesive strategy neutralized the immediate danger and laid the groundwork for a more secure, resilient utility framework.

Introduction:

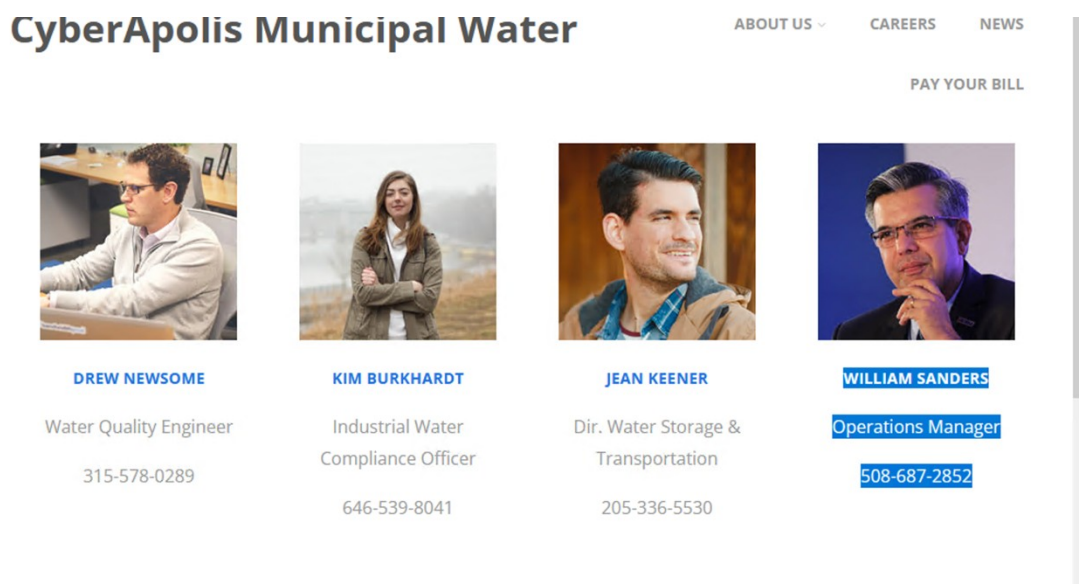
1. In a robust and orchestrated response to the cyber-attack on the CyberApolis Water Company, a meticulous counter-operation unfolded in phases, showcasing the resilience and preparedness of our cybersecurity team. Starting with an in-depth reconnaissance phase, we targeted In the wake of a digital siege on the CyberApolis Water Company by the nefarious Carbon Spector group, an emergency unfolded that threatened the city's well-being. This introduction sets the stage for a high-stakes cyber operation, detailing the critical situation where the DHS specialist is tasked with a mission crucial for the city's survival and security. The narrative unfolds to describe the specialist's mandate to infiltrate the company's compromised systems, aiming to mitigate an impending disaster. The stage is set for a detailed recount of the sophisticated strategies and decisive actions taken to safeguard CyberApolis.

Reconnaissance:

When during my reconnaissance phase I started by checking out the company's webpage <http://water.cyberapolis.gov/> to find any information I can gather

1.1

After going to the website, a Contact page with a list of different people. The organization wanted to find a target that would give us the highest privileges the organization could gain, and we pivoted from there and found William Sanders.

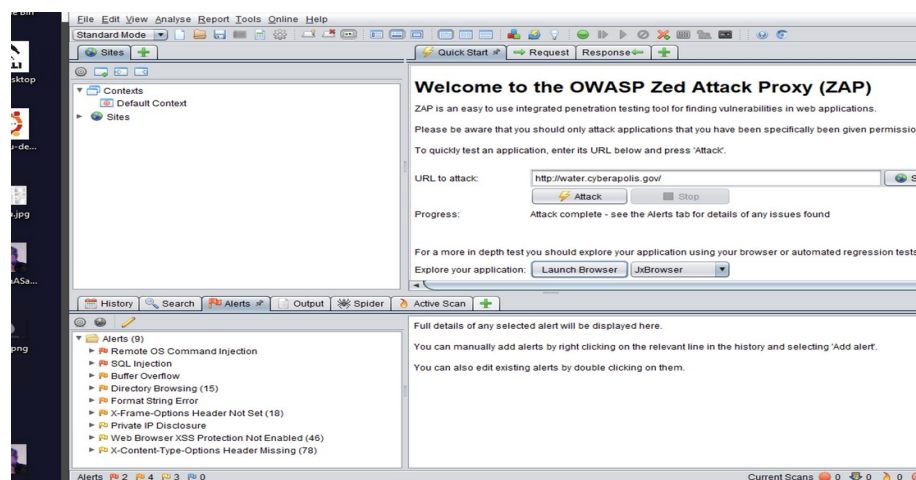
1.2

Once I found my target, I was able to being the scanning phase for infiltration.

2.Scanning:

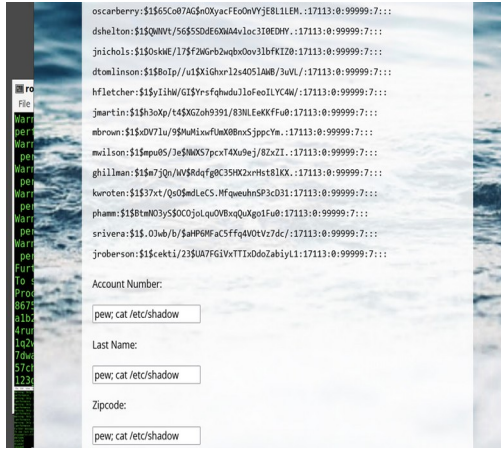
After that, it was time to begin my targeting phase; to start the process, do a zap vulnerability scan to see what vulnerabilities we would be able to find in the web application. We were able to find that there were multiple vulnerabilities, but we used the highest flags available.

2.1



Once zap was able to determine all of the flags I then set out to find the vulnerability from website that lead me to the Pay you bill here paged that had a high level flag on it for an Os command line injection attack. I then set out to exploit this vulenbility but imputing commands into find where the vulnerabilities could potentially be at so I decide to use all three to find the exploit, but the actual exploit was in last name of the pay here page and once, the the exploit was discovered I then decide to make my way through the exploit to see what I was able to get, and I was able to find a hidden file in /etc called shadow that had a list of salted md5 hashes and use names to different accounts

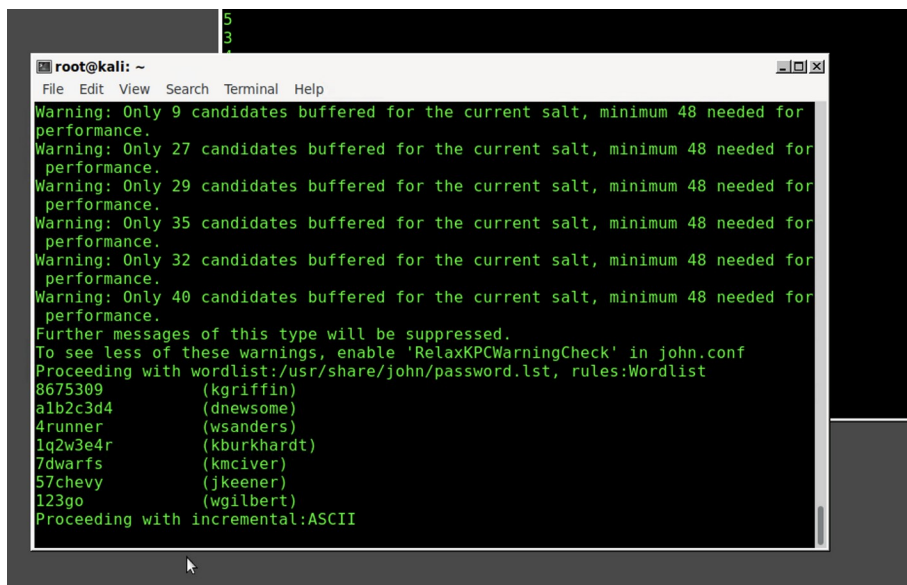
7 CyberApolis Water Breach Report 2.2



3. Exploitation:

After Being able to find this list of hashes then I decide I need to crack these different hashes using John the ripper to take these different hashes from this set list that I had made so I needed to make a file on to my computer called “stolen hashes 444” and move the file over using windows secure copy and after do that I got these usernames and passwords from John the ripper

3.1

A screenshot of a terminal window titled 'root@kali: ~'. The window shows the output of John the Ripper. It starts with several warning messages about the number of candidates buffered for the current salt, indicating that the minimum of 48 is not being reached. These warnings are suppressed. The terminal then shows the wordlist being used: 'usr/share/john/password.lst' with the rule 'Wordlist'. A list of cracked passwords and their corresponding usernames is displayed: '8675309' for '(kgriffin)', 'alb2c3d4' for '(dnewsome)', '4runner' for '(wsanders)', '1q2w3e4r' for '(kburkhardt)', '7dwarfs' for '(kmciver)', '57chevy' for '(jkeener)', and '123go' for '(wgilbert)'. Finally, it shows 'Proceeding with incremental:ASCII'.

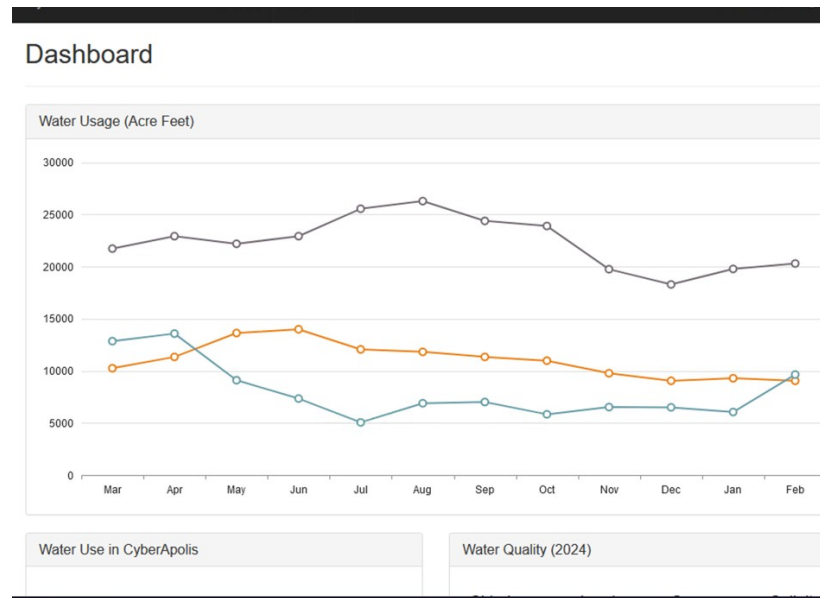
```
root@kali: ~  
File Edit View Search Terminal Help  
Warning: Only 9 candidates buffered for the current salt, minimum 48 needed for  
performance.  
Warning: Only 27 candidates buffered for the current salt, minimum 48 needed for  
performance.  
Warning: Only 29 candidates buffered for the current salt, minimum 48 needed for  
performance.  
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for  
performance.  
Warning: Only 32 candidates buffered for the current salt, minimum 48 needed for  
performance.  
Warning: Only 40 candidates buffered for the current salt, minimum 48 needed for  
performance.  
Further messages of this type will be suppressed.  
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf  
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist  
8675309      (kgriffin)  
alb2c3d4     (dnewsome)  
4runner      (wsanders)  
1q2w3e4r     (kburkhardt)  
7dwarfs      (kmciver)  
57chevy      (jkeener)  
123go        (wgilbert)  
Proceeding with incremental:ASCII
```

After I was able to obtain these usernames and passwords I then used Williams user and password for infiltration to into the employee portal and gain access to the dashboard where I was able to access the employees email along with their calendar and the HMI portal to be able to access the floodgate

9

CyberApolis Water Breach Report

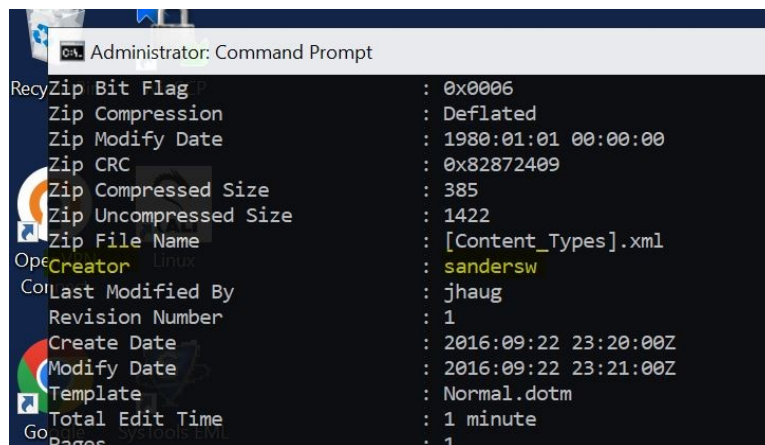
3.2



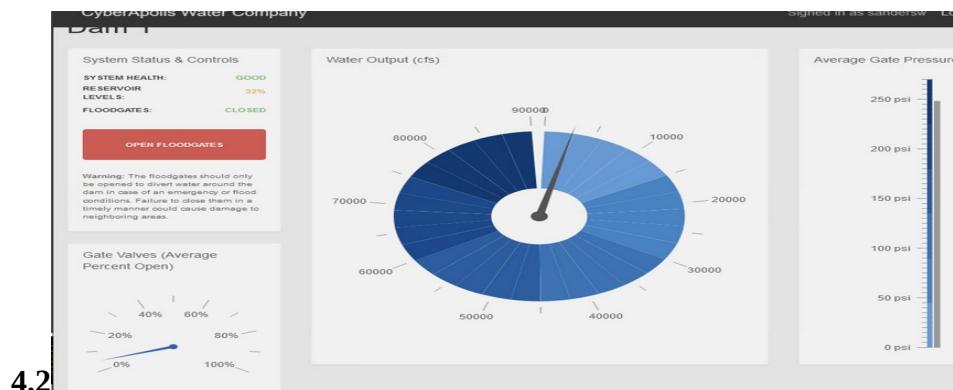
4. post-exploitation:

One the Exploration was I then moved over to the Post exploration I began my search for the username for the employee HMI portal so I decided that I needed to do back to the metadata do determine if there was any other creators of the picture that I had founding the metadata and it turns out that there had been another username that William was using under his creator tool but it came up as a different name as sandersw.

4.1



Once I had found that username I then attempted to logging in into the HMI portal with this username and the password that I had discovered in the previous steps and was able to gain access into the HMI portal and to shut the floodgates closed.



5. Summary and Mitigation:

In summary the operation commenced with a reconnaissance phase that included an analysis of the CyberApolis Water Company's website, which led to the identification of a high-priority target, William Sanders. During the scanning phase, a vulnerability scan revealed multiple high-risk vulnerabilities, with an OS command injection flaw pinpointed on the payment page.

Exploitation of this vulnerability unearthed a shadow file containing salted MD5 hashes and associated usernames. These hashes were then cracked using John the Ripper, revealing credentials that provided access to the employee portal and, crucially, the HMI controls for the floodgates.

In the post-exploitation phase, further investigation into metadata identified an alternate username, which allowed for full access to the HMI portal and the successful closure of the floodgates.

To mitigate these issues in the future, it is recommended to:

1. Regularly update and patch all systems to protect against known vulnerabilities.
2. Conduct continuous security training for employees, emphasizing the importance of secure password practices and the potential dangers of oversharing on public-facing page
3. And what is put on the internet
4. Implement rigorous, regular vulnerability scanning and penetration testing to identify and mitigate security flaws before they can be exploited.
5. Employ the principle of least privilege, ensuring employees have access only to the systems necessary for their work.
6. Utilize multi-factor authentication and encryption, especially for critical control systems like the HMI portal.

6. Synopsis

1. What Username(s) did you find that could access the Employee Portal?
Kgriffin, dnewsome, wsanders, kburkhardt, kmciver, jkeener and wgilbert

2. What password hash(es) did you find that could access the Employee Portal?
These are the password hashes

XAZKEUB/lpqkP7AQamVwS= wsanders
Pl5LymzaHtCCRJkzyQvd0= wgilbert
q9d8qZm30oTfyuougl6MZ0= Kgriffin

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

8675309
a1b2c3d4
4runner
1q2w3e4r
7dwarfs
57chevy
123go

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 other username in the metadata of the water drop

5. What vulnerabilities did you identify in the CyberApolis Water Company's website?

I was able to find that the website had was the os command line that was one of the vulnerabilities that was able to find along with SQL injection.

6. What Username(s) allowed access to the HMI Controls?

Newsomed , sandersw

7. What password(s) allowed access to the HMI controls?

a1b2c3d4 and 4runner

