Jay Mclain
0xjaydm

Penetration Test

In my analysis, I discovered several significant security risks that could be exploited by an entry-level threat. Through a data scrape tool I developed, I was able to obtain potentially sensitive information from the surface web. Furthermore, during a more thorough search, I uncovered public access to hidden directories, developer pages, open ports with unused processes, and more.

Mitigation

To address these risks, it is crucial to train [REDACTED] staff to exercise caution when using their work email. I recommend the following measures:

- Users should avoid signing up for subscriptions using their business email.
- User passwords should be randomized and longer to enhance security.
- 2FA should be standard across every user login, ideally not a phone number.
- Only key staff members should have access to the WordPress backend, even if it's a user account. Privileges can be escalated to admin as needed.
- Users should be educated about common phishing tactics, as they are often the cause of breaches, especially considering the wide access of emails I discovered.

Socials

To improve security on [REDACTED] social platforms, the following steps are recommended:

- Enable two-factor authentication (2FA) on all social media accounts using Google Authenticator or similar instead of relying on phone-based authentication, which can be easily spoofed.
- Create dummy email accounts, not associated with the domain, for each social media account. ProtonMail, with its end-to-end encryption, is a recommended option. This approach increases the attack surface for hackers and prevents overlapping vulnerabilities.

- Avoid sharing business emails publicly, except for submissions@[REDACTED].com. Auto-forwarding can be set up to personal business emails for convenience.

Website

Ideally, it would be prudent to switch to a different website provider, as WordPress is known for its instability and security vulnerabilities. However, if [REDACTED] chooses to remain with the current host provider, the following website vulnerability mitigation techniques should be implemented:

- Three critical hidden directories, which can be seen under **Sensitive Information**, should be further concealed or redirected to publicly accessible parts of the website. This can be achieved using Apache service, which is often already running on WordPress sites. By setting up a .htaccess file and building rules, these directories can be hidden or redirected to return a 404 error page.
- A non-essential SSH process is running on port 443, potentially exposing default credentials. Disabling SSH is recommended as it is unused and poses a vulnerability.
- An FTP service is running on port 8080, allowing anonymous login. Since this is not needed for a music company, disabling FTP is recommended to prevent data exfiltration.
- A publicly available developer page, though seemingly benign, can be exploited for social engineering attacks. Disabling this page is advised.
- HTTP headers can provide insights into potential exploits that attackers can leverage. [REDACTED] is currently running nine headers, some of which may not be essential for the website's functionality. Disabling, removing, or implementing these headers can enhance security.

Sensitive Information / Vulnerabilities

During my investigation, I obtained user information, including passwords and personal details. While some passwords may be hashed, they can be easily unhashed using various methods. I have left some of each hash and password out intentionally.

User: **[REDACTED]**

Pass: **[REDACTED]**

—---

User: **[REDACTED]**

Pass: **[REDACTED]**

—--

User: **[REDACTED]**

Pass: **[REDACTED]**

—--

User: **[REDACTED]**

Pass: **[REDACTED]**

—--

User: **[REDACTED]**

Pass: **[REDACTED]**

—--

User: **[REDACTED]**

Pass: **[REDACTED]**

—--

User: **[REDACTED]**

Pass: **[REDACTED]**

Name: **[REDACTED]**

Address: **[REDACTED]**

—--

Name: **[REDACTED]**

Pass: **[REDACTED]**

Address: **[REDACTED]**

Web ID: **[REDACTED]**

Facebook ID: **[REDACTED]**

Mobile Phone: **[REDACTED]**

—---

FTP

While interacting with the **FTP** (file transfer protocol) service, I noticed that by default there is an anonymous login that can be used via the sftp command with the IP address:

sftp [IP ADDRESS]

User: anonymous

Password:

(intentionally left blank)

Additionally, although the port is wrapped (or hidden) I can find that [REDACTED] runs FTP via the return of enumerated info: **ftp.[REDACTED].com**

Hidden Directories

Was able to identify hidden directories using gobuster, which should normally not be available to the public.

/security.txt

/robots.txt

/.well-known/security.txt

Interior Pages

dev.[REDACTED].com

[REDACTED].com/wp-login.php

ftp.[REDACTED].com

[REDACTED].com/wp-content/media

‘

Conclusion

In conclusion, I am grateful to [REDACTED] for giving me the opportunity to perform a comprehensive penetration test, which allowed me to gain valuable real-world experience in the field of cybersecurity. I am confident that the information I have provided will be of great value in enhancing your security measures. I am always ready and willing to assist in implementing the mitigation techniques that I have suggested.