Sri Lanka Institute of Information Technology

Cyber Security Assignment (2025)

Weak Authentication & identification Vulnerability

Bug Bounty Report- 09

IT23363366

TABLE OF CONTENT

Title 3

Scope and Objective 3

Enumeration & Reconnaissance 3

  Tools Used 3

  Steps Taken 3

Vulnerability Description 5

Affected components 5

Proof of Concept (PoC) 5

Impact Assessment 6

Remediation / Recommendations 6

Network / Access Control Recommendations 7

Conclusion 7

References 7

1. Title

Report Title: Weak Authentication & identification Vulnerability in WordPress Admin Portal
Reported By: Raahim Mahmooth
Tested On: https://slsportisotonic.com/
Platform: https://hackerone.com/

2. Scope and Objective

This report documents a **weak authentication vulnerability** discovered during a penetration test conducted on the WordPress website at **slsportisotonic.com**. The test focused on identifying authentication weaknesses using brute force and dictionary-based attacks to test the strength of passwords protecting sensitive administrative pages.

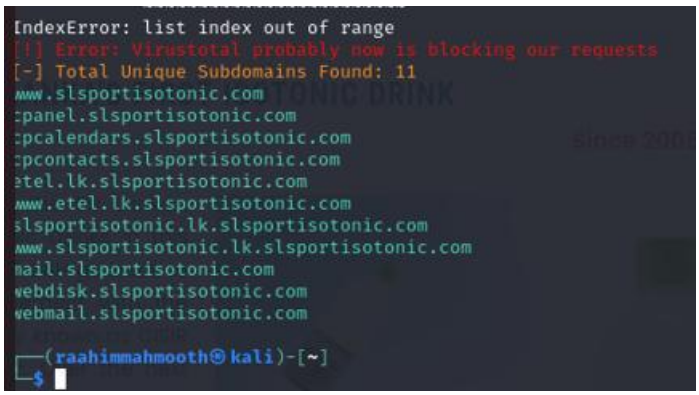
3. Enumeration & Reconnaissance

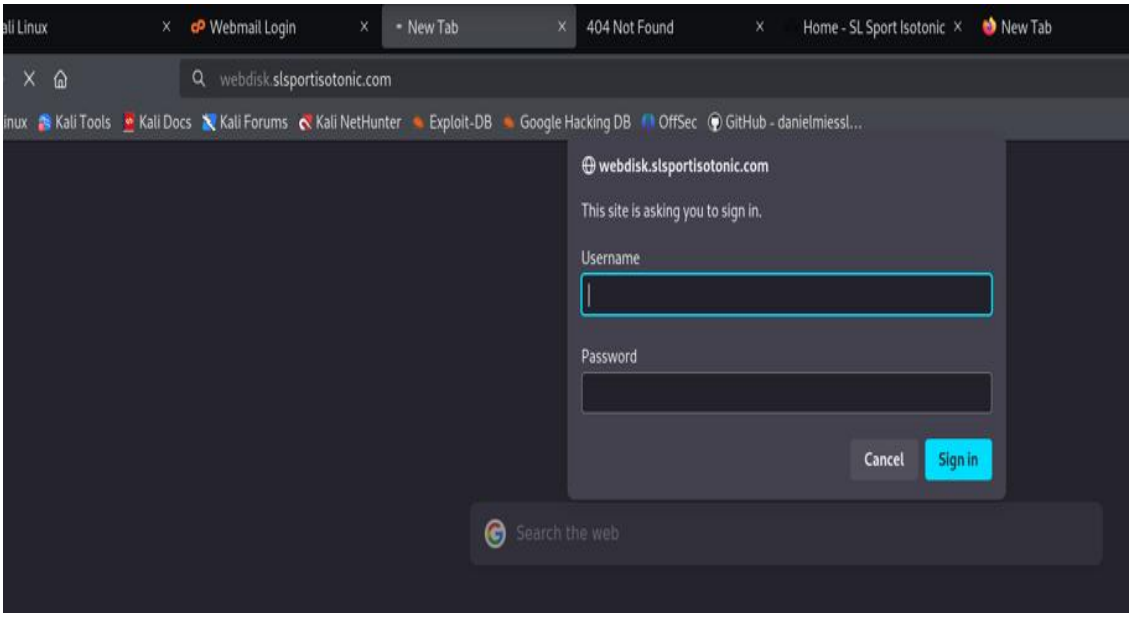
Tools Used

- **Sublist3r**: Subdomain enumeration tool.
- **Go Buster**: Directory listing tool.
- **Hydra:** Bruteforce,password cracking tool

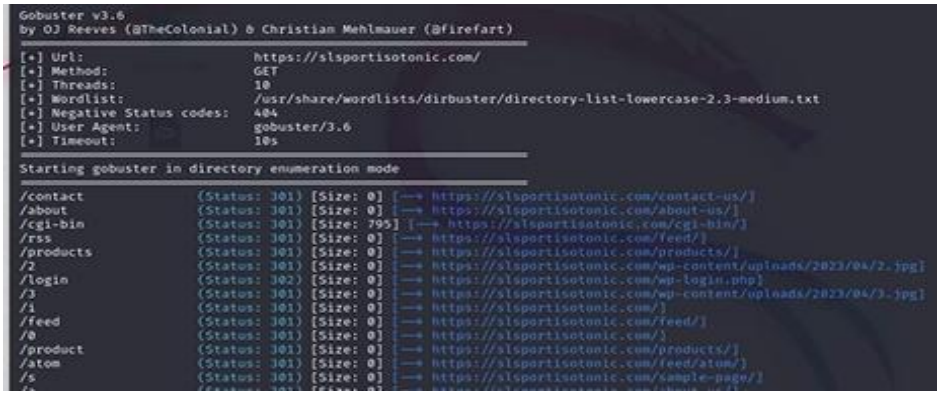
Steps Taken

- **Subdomain enumeration**: Using **Sublist3r**, I discovered multiple subdomains associated with the target, such as **webmail .slsportisotonic.com** and **cpcontacts .slsportisotonic.com**. However, these required credentials for access.
- Network devices such as routers typically utilize **basic authentication** to control access to their **administrative interfaces.**





- **Directory enumeration**: With **GoBuster**, I was able to discover the `/wp-login.php` directory, which indicated the presence of a WordPress login page.



4. Vulnerability Description

- **Vulnerability Type**: Weak Authentication / Brute Force
- **Severity**: **High**
- **Impact**: Successful brute force attack allowed access to an admin portal, enabling unauthorized control over the website's backend.

5. Affected components

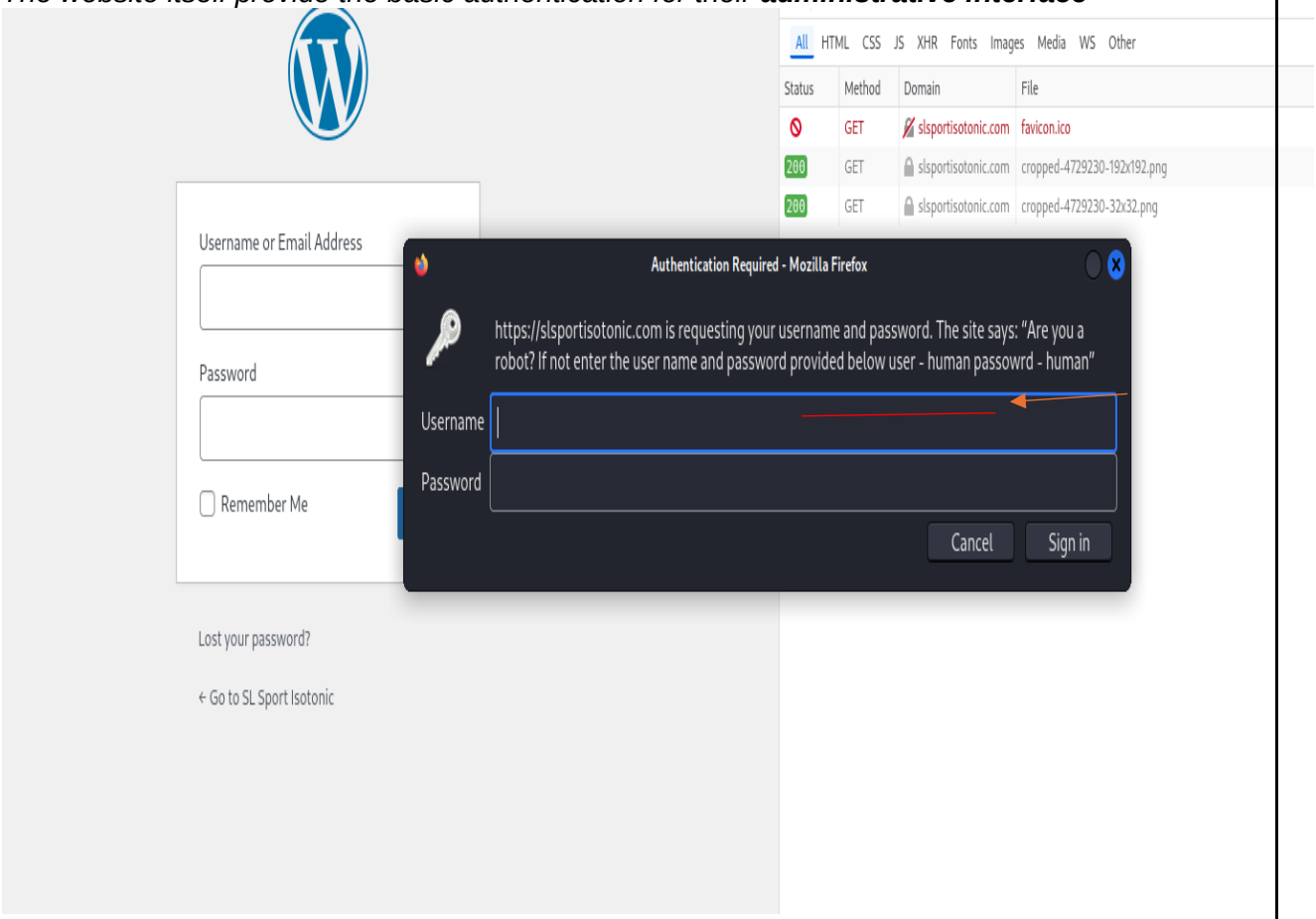
- Endpoint: **https://slsportisotonic.com /wp-login.php**

6. Proof of Concept (PoC)

- **Access the Login Page of Admin**: **Navigate** to https://slsportisotonic.com/

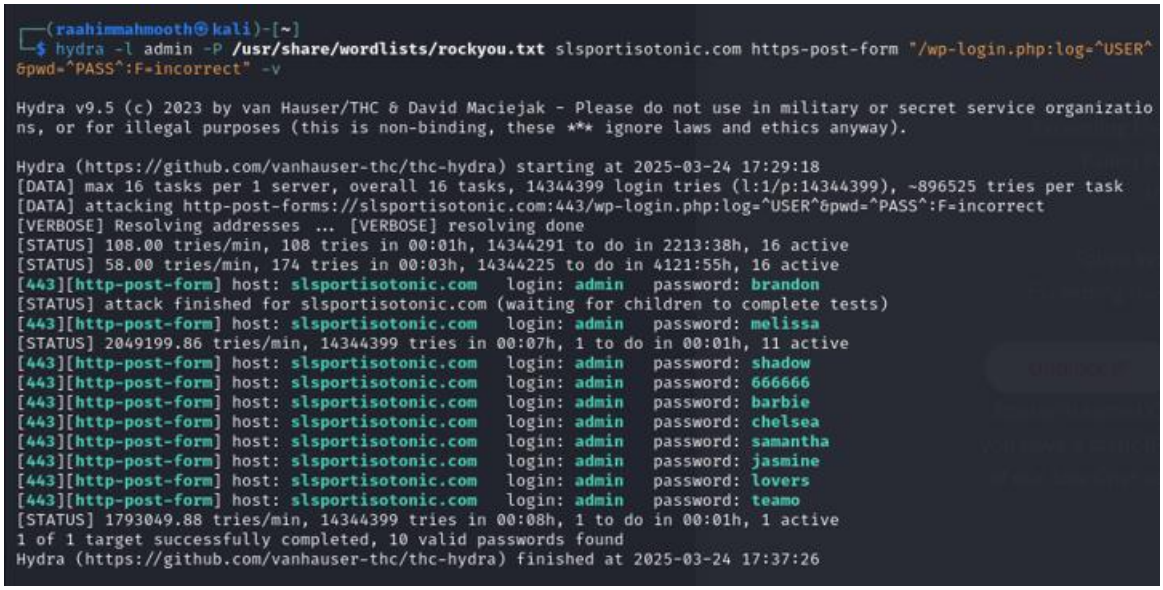
  *(If we **/admin** in the website it will redirect to wp-login page the default password is human username is human to access the admin login)*

  *The website itself provide the basic authentication for their **administrative interface***



- **Password Cracking**: Use Hydra to perform a brute-force attack on the login form.
  - Command*:* `hydra -l admin -P rockyou.txt https-post-form "wp-login.php:log=^USER^&pwd=^PASS^:F=incorrect"`

- Hydra output showing successful password crack.



- **Video**: A video demonstrating will be added in the zip file

7. Impact Assessment

- **Risk**: By gaining access to the WordPress admin panel, an attacker could potentially:
  - Alter or delete website content.
  - Access sensitive user data.
  - Install malicious code or backdoors.
- This issue, if exploited, can cause severe damage to the target website's integrity and its users' data.

8. Remediation / Recommendations

To resolve this vulnerability, I recommend the following:

1. **Implement Strong Password Policies**: Enforce the use of complex passwords that cannot be easily cracked.
2. **Multi-Factor Authentication (MFA)**: Enable MFA for all administrative accounts to add an additional layer of protection.
3. **Rate Limiting**: Introduce rate-limiting to prevent brute-force attacks from succeeding.

4. **IP Blocking**: Temporarily block IP addresses that have made multiple failed login attempts.
5. **CAPTCHA Protection**: Add CAPTCHA or similar protections on the login form to prevent automated attacks.

9. Network / Access Control Recommendations

- Restrict access to the WordPress admin panel to specific internal IPs or VPN access, ensuring only authorized personnel can access it remotely.(this mechanism in place there reducing the impact also the company has a threat by insider attack)

10. Conclusion

The vulnerability discovered in the identification authentication (OWASP Top 10: A7) mechanism of the WordPress admin portal presents a critical security risk, as it allows unauthorized access using easily guessable passwords. I highly recommend applying the suggested remediation measures to prevent any exploitation.

11. References

- OWASP Top 10: A7 - Identification and Authentication Failures
    - **CVE Reference: CWE-300: Channel Accessible by Non-Endpoint**
    - **CWE-521: Weak Password Requirements**