Bug Bounty Report:

[PayPal - Subdomain paydiant.com]

1. Target Information

- **Main Domain:** PayPal
- **Tested Subdomain:** paydiant.com
- **IP Address:** 3.33.139.32

2. Scope Confirmation

- This testing was performed within the guidelines set by the PayPal bug bounty program, which lists specific in-scope subdomains and assets for authorized testing.

3. Tools Used and Their Functions

Subfinder

- **Function:** Subfinder is a subdomain enumeration tool used to discover additional subdomains associated with a target domain.
- **Purpose in Testing:** The tool helped ensure that paydiant.com was a legitimate subdomain of PayPal and identified any additional subdomains that could be investigated further for potential vulnerabilities.
- **Potential Impact if Vulnerabilities Found:** If any unprotected or misconfigured subdomains were discovered, they could potentially lead to a subdomain takeover, which might allow attackers to impersonate the company or launch further attacks.

FFuF (Fuzz Faster U Fool)

- **Function:** FFuF is a tool used for content discovery, capable of identifying hidden directories, files, and parameters through brute-forcing.
- **Purpose in Testing:** FFuF was used to search for hidden directories or sensitive files on paydiant.com that might reveal information or contain weaknesses.
- **Potential Impact if Vulnerabilities Found:** If sensitive data (such as configuration files, backups, or admin portals) were exposed, attackers could leverage this information for further exploitation, potentially leading to data leakage or unauthorized access.

httprobe

- **Function**: httprobe is a tool that checks the HTTP and HTTPS status of a list of domains to verify live targets.
- **Command Used**: cat domain.txt | sudo httprobe > live_domain.txt
- **Purpose in Testing**: Used to identify live domains from a list of subdomains, ensuring that only active, reachable domains were tested.
- **Potential Impact**: Ensures that time and resources are focused on live domains, reducing unnecessary requests and enhancing targeting accuracy.

Nmap

- **Function:** Nmap is a network scanning tool used to discover open ports, services, and their versions on a target host.
- **Purpose in Testing:** Nmap was used to scan 3.33.139.32 (the IP associated with paydiant.com) to identify any open ports and active services.
- **Potential Impact if Vulnerabilities Found:** Unsecured open ports or vulnerable services could allow attackers to exploit misconfigured services or known vulnerabilities in those versions, potentially leading to unauthorized system access or denial-of-service attacks.

Metasploit

- **Function:** Metasploit is a penetration testing framework with modules for exploitation, payload delivery, and post-exploitation.
- **Purpose in Testing:** Metasploit was used to test any identified services and open ports for known exploits or misconfigurations.
- **Potential Impact if Vulnerabilities Found:** Successfully exploiting a service could allow unauthorized access or privilege escalation within the target's infrastructure.

SQLMap

- **Function:** SQLMap is an automated tool for detecting and exploiting SQL injection vulnerabilities in web applications.
- **Purpose in Testing:** SQLMap was used to test paydiant.com for potential SQL injection vulnerabilities, specifically in any input fields or URL parameters.
- **Potential Impact if Vulnerabilities Found:** If SQL injection vulnerabilities were present, attackers could potentially extract sensitive data from the database, manipulate data, or bypass authentication measures.

Manual XSS Testing

- **Method Used:** A manual test was performed by injecting <script>alert('XSS')</script> into input fields to test for reflected XSS vulnerabilities.
- **Purpose in Testing:** This test was conducted to see if user input was unsafely reflected back onto the web page.
- **Potential Impact if Vulnerabilities Found:** If reflected XSS was found, attackers could exploit this to execute arbitrary JavaScript in users' browsers, potentially stealing session cookies or redirecting users to malicious sites.

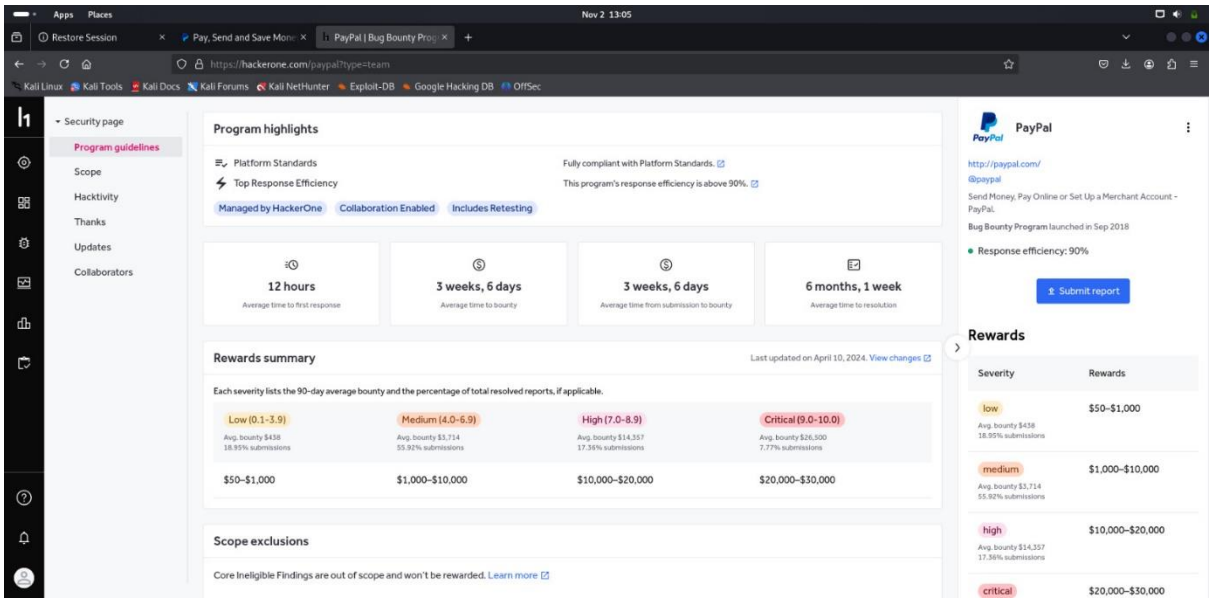
4. Findings

- **Summary:** Despite thorough testing using automated tools and manual methods, no vulnerabilities were found on paydiant.com.
- **Results:** All tests, including attempts to identify XSS, SQL injection, subdomain takeover potential, and IDOR vulnerabilities, yielded no findings.

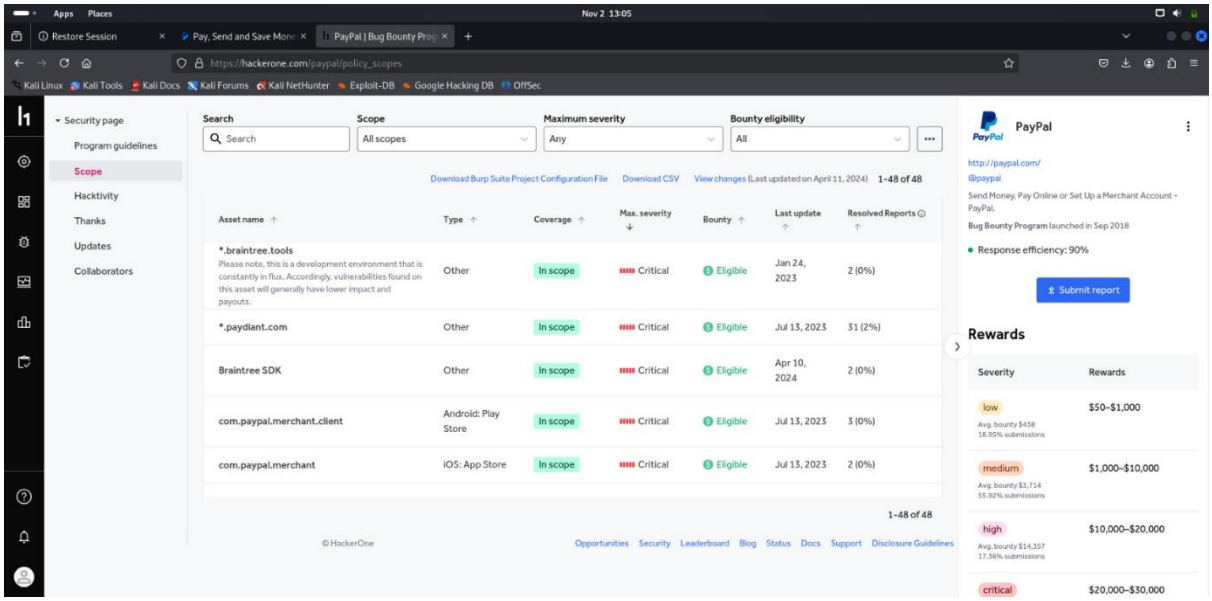
5. Conclusion

- Overall Security Posture: paydiant.com appears to have robust security measures in place, and no exploitable vulnerabilities were found during this round of testing.

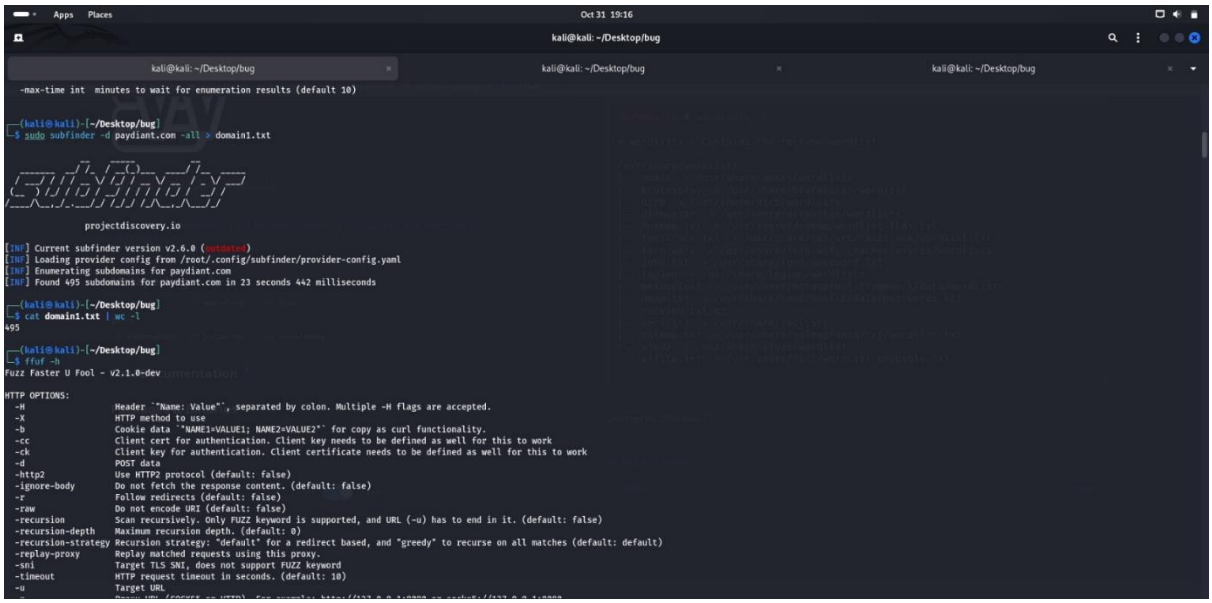
6. Documentation (Proof of Concept):



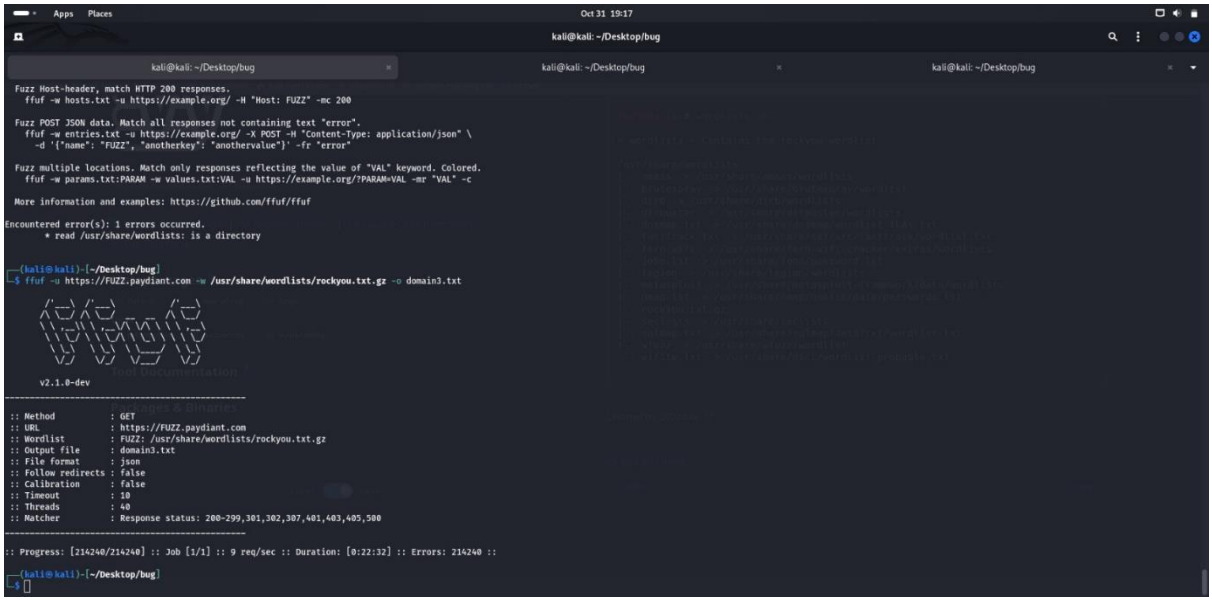
PayPal Bug Bounty Program



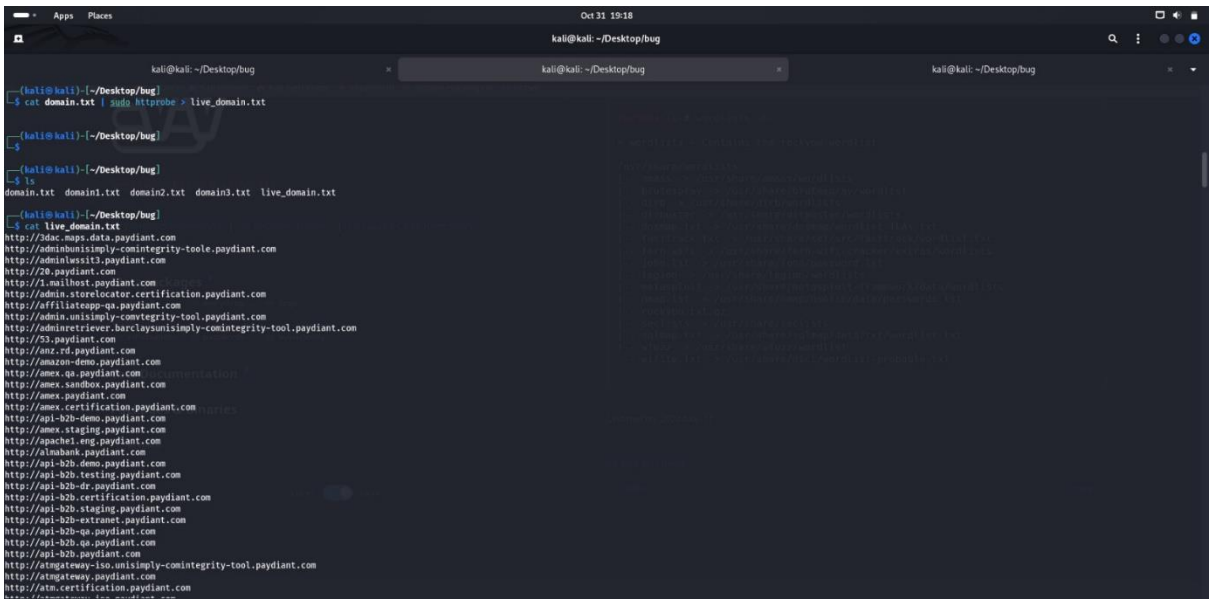
In Scope Assets



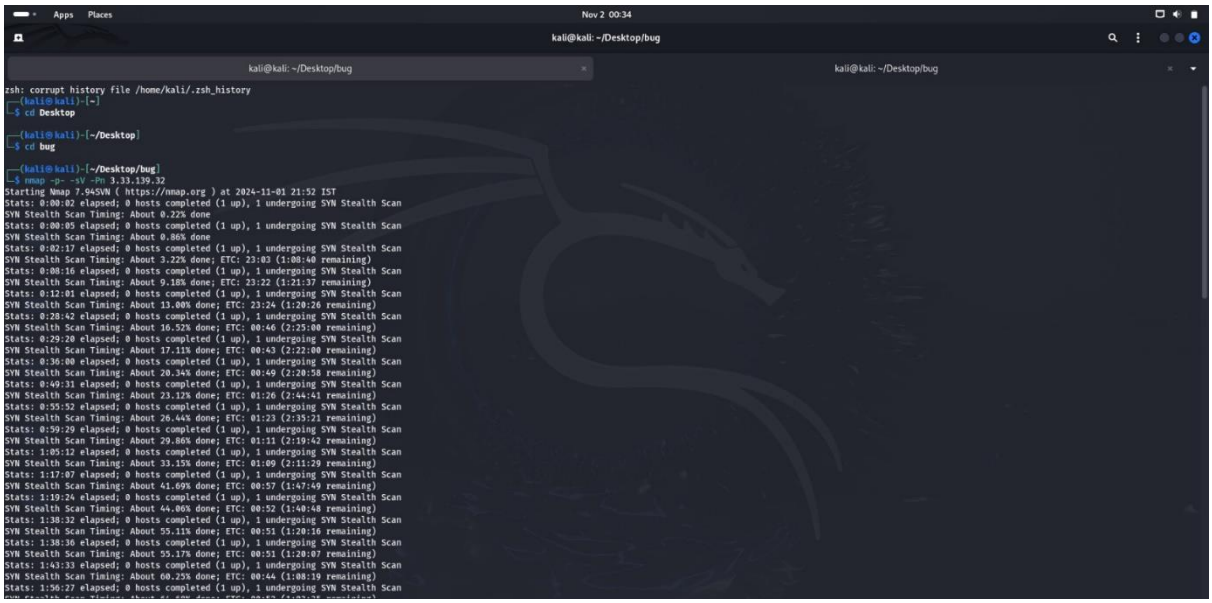
Execution of Subfinder tool



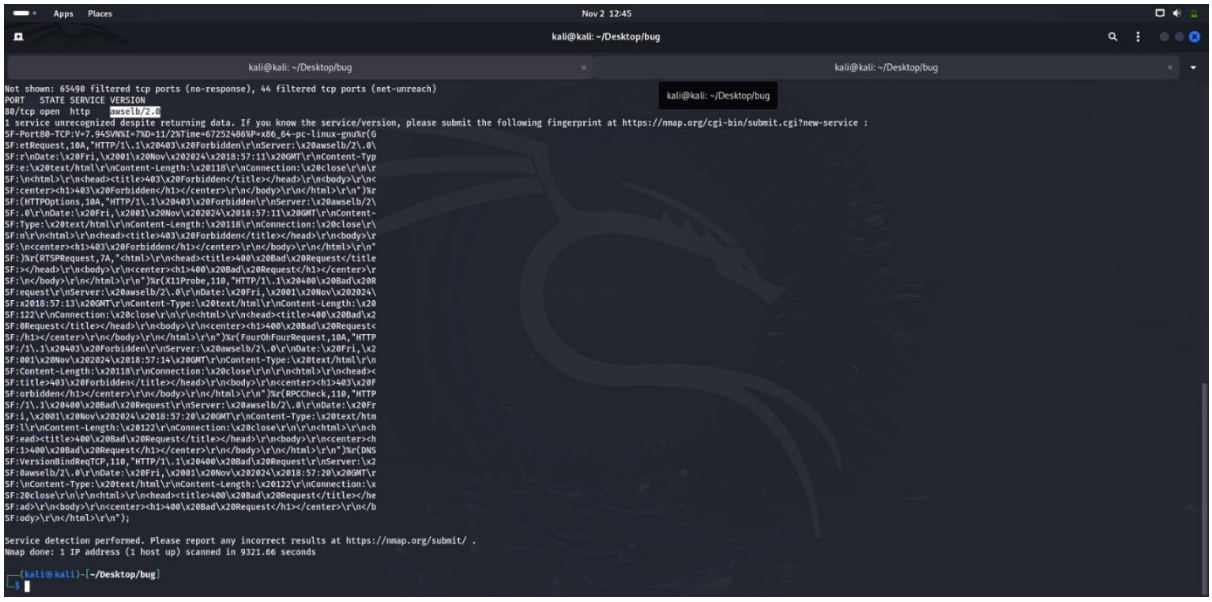
Execution of ffuf tool



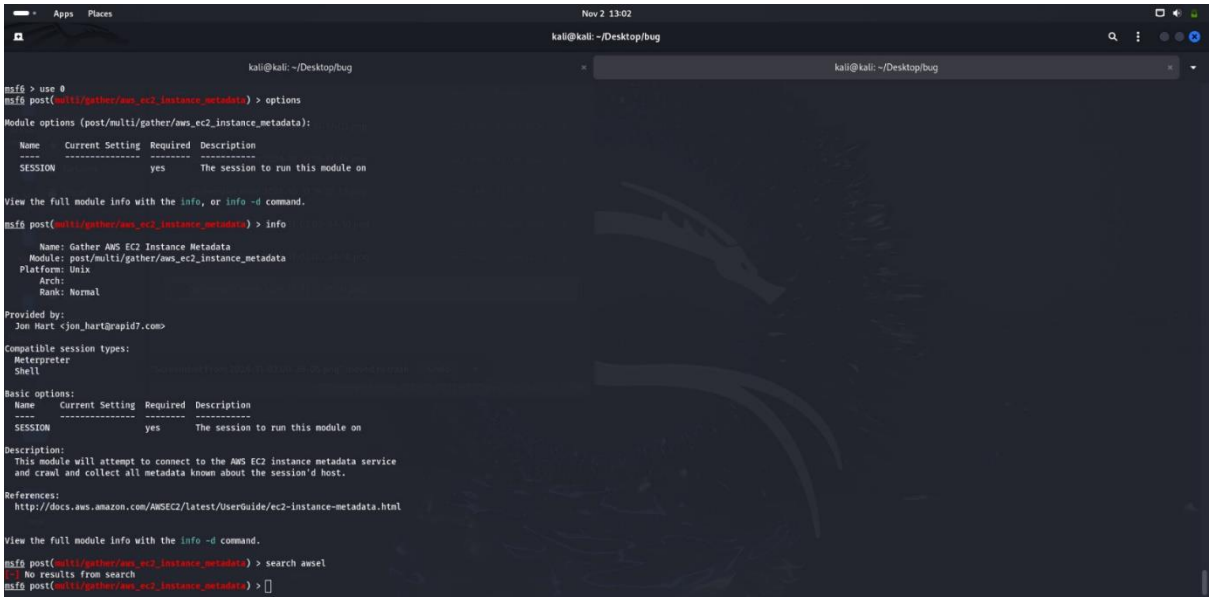
Execution of httprobe



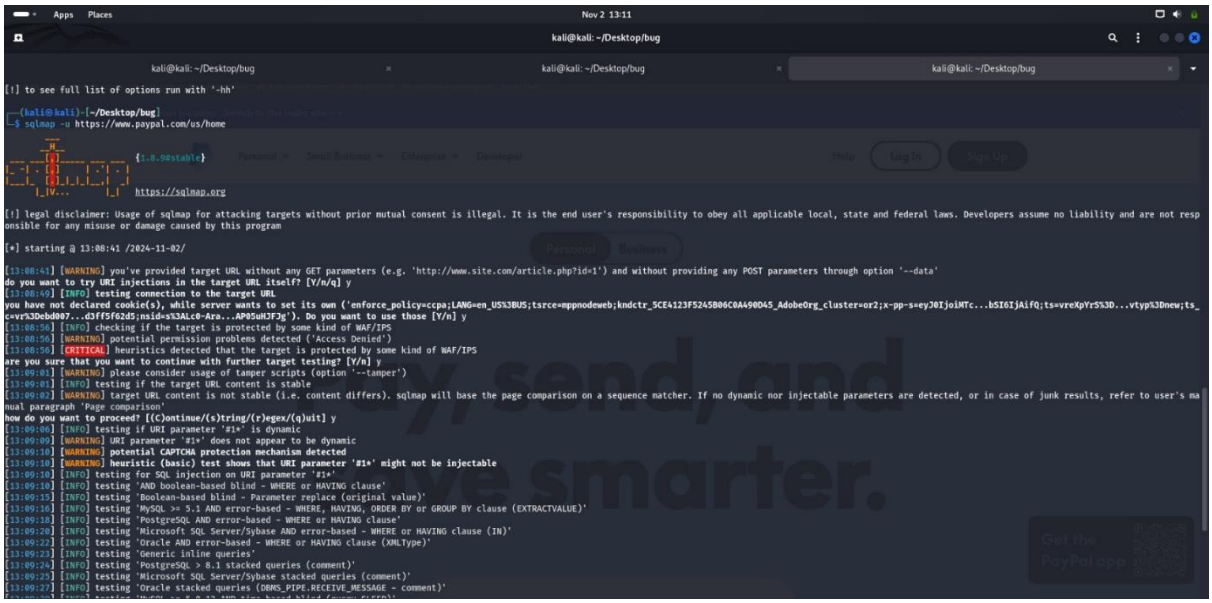
Execution of Nmap scan



Result of Nmap scan

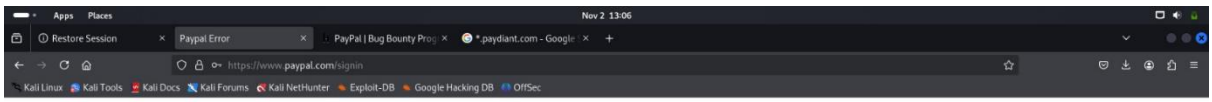


Use of Metasploit tool



Execution of SQLmap tool

Result of SQLmap tool



Access Denied.

You don't have permission to access "/signin" on this server.

Reference #17305329830b515dd17cfaae0dc00f1

Timestamp: 1730532983

Manual XSS testing