Cross-Site Scripting Chameleon Website

CHAMELEON

FOR OUR SMARTER WORLD

Table of Contents

Executive summary:

This report presents the findings of a Cross-Site Scripting (XSS) vulnerability assessment conducted on the City of Melbourne – open data (MOP) website The assessment aimed to identify potential XSS vulnerabilities within the web application and provide recommendations for mitigation.

Introduction

What is Cross-Site Scripting (XSS)?

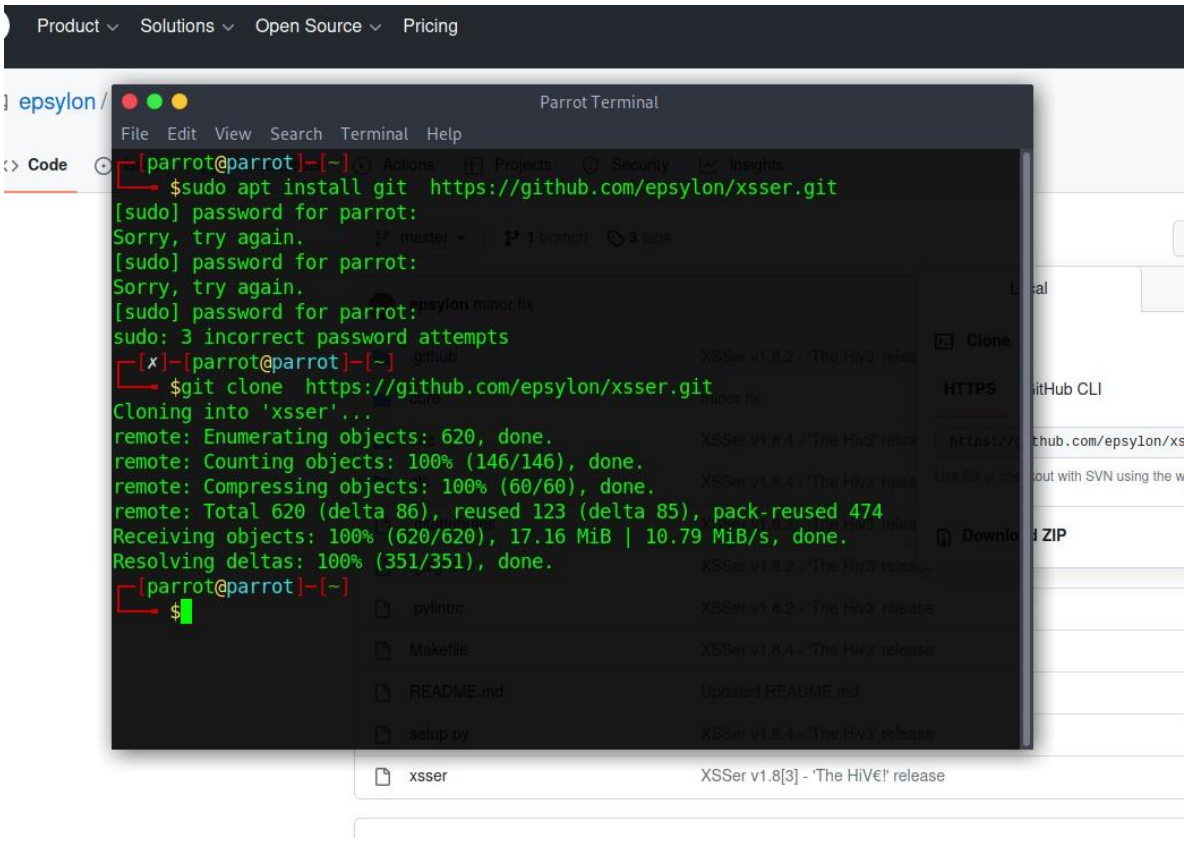
A security flaw in web applications known as cross-site scripting (XSS) allows for the insertion of malicious scripts into user-viewed web pages. These scripts may be kept on the server, diverted away from it, or subjected to user browser manipulation. Stored XSS, reflected XSS, and DOM-based XSS are the three main forms. XSS attacks can have serious repercussions, such as data theft, session hijacking, defacement, and malware propagation. Secure coding techniques like input validation and output encoding are crucial for preventing XSS attacks. Input validation libraries and common security techniques like Content Security Policy can reduce the risk posed by XSS vulnerabilities. Web developers should constantly test their applications for vulnerabilities and stay up to date on security best practises.

Tools used

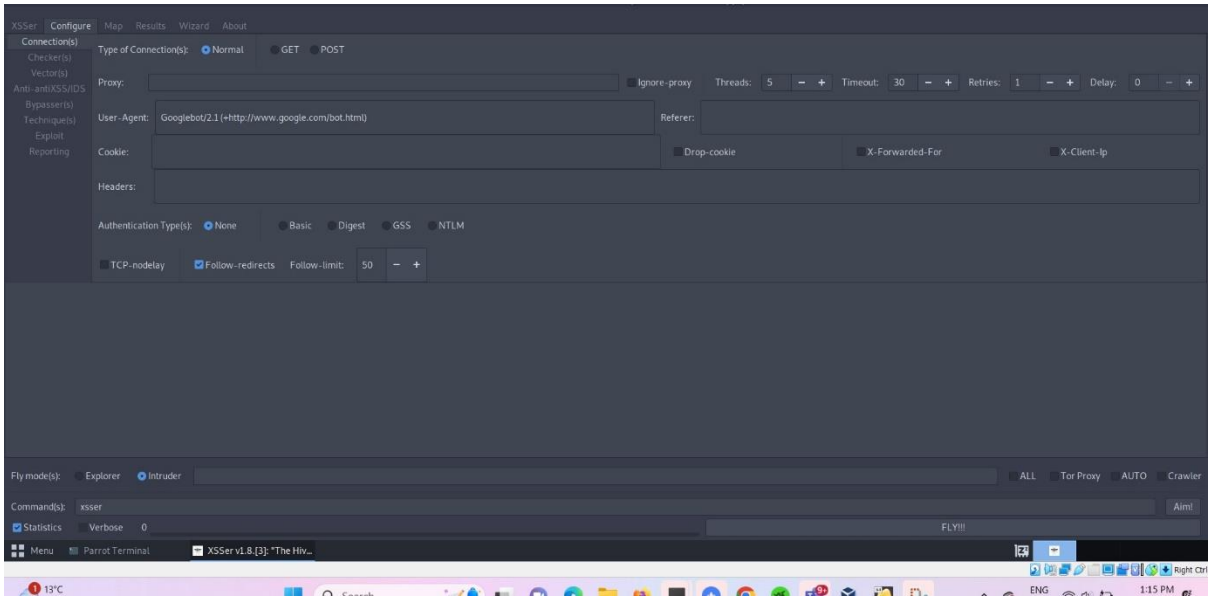
- Parrot OS
- Kali Linux
- BurpSuite
- Foxy Proxy
- OWASP
- Xsser

Results Using Xsser

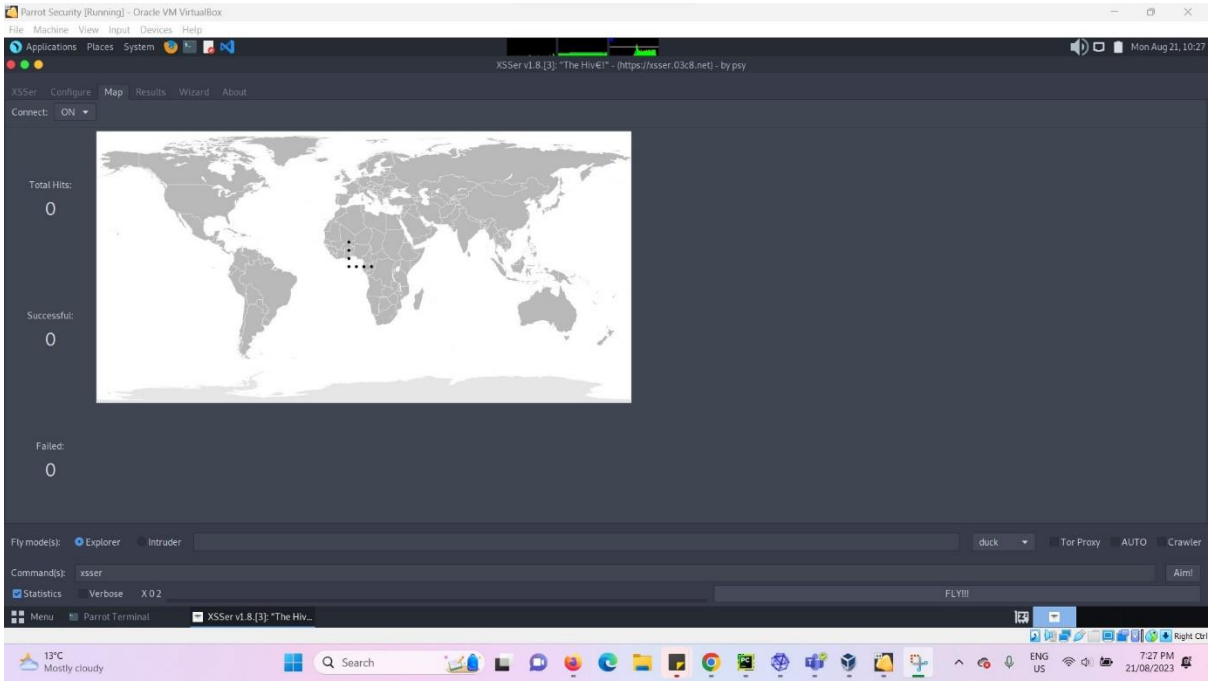
The screenshot below illustrates the required packages that needed to be downloaded.



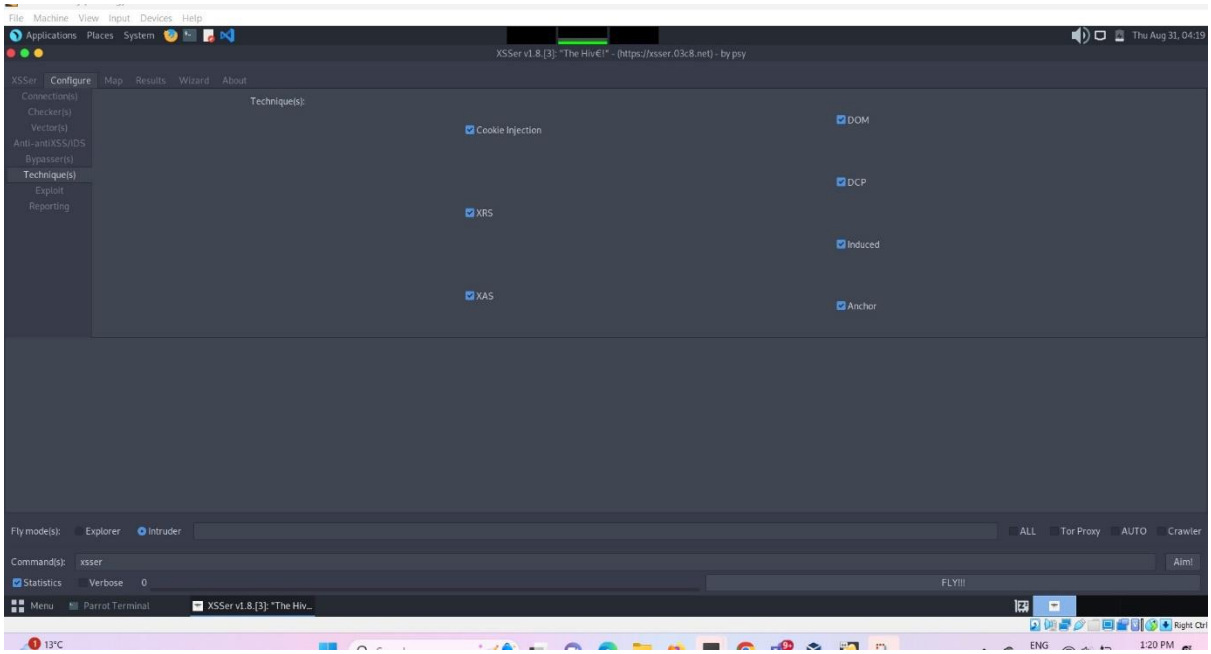
The screenshot below showcases selected options, including those for following redirects and setting the follow-limit.



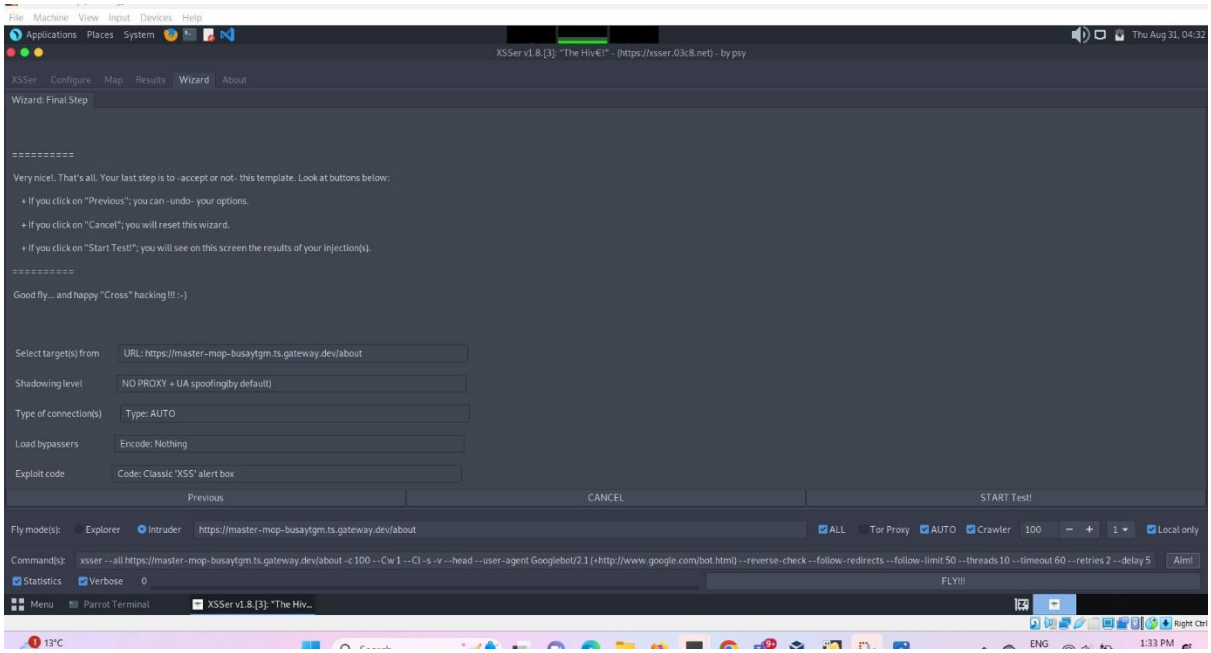
The screenshot below provides visual confirmation that the map has been successfully downloaded, marking the commencement of the attack.



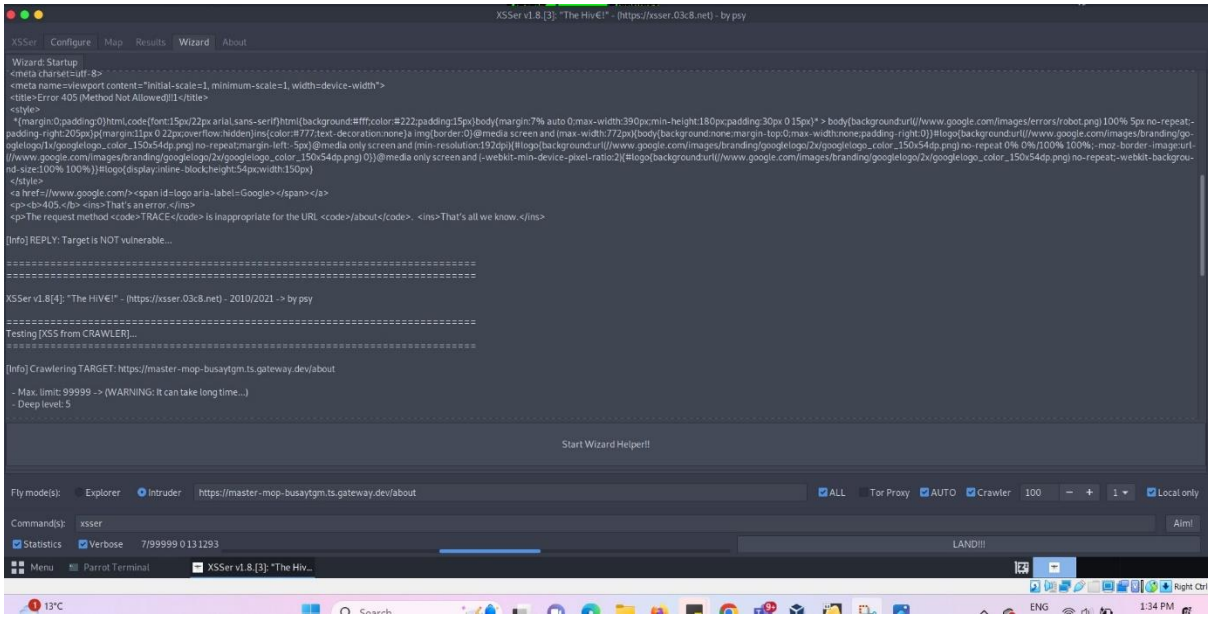
The screenshot below reveals that all available techniques have been selected, thereby broadening the scope of the attack and maximizing its chances of success.

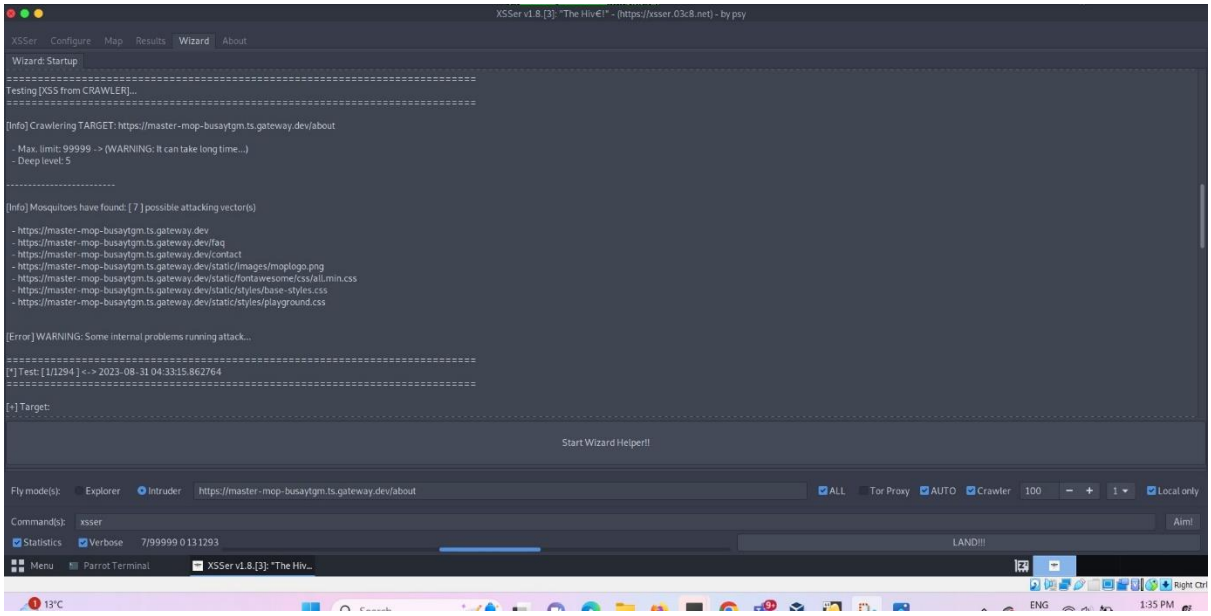


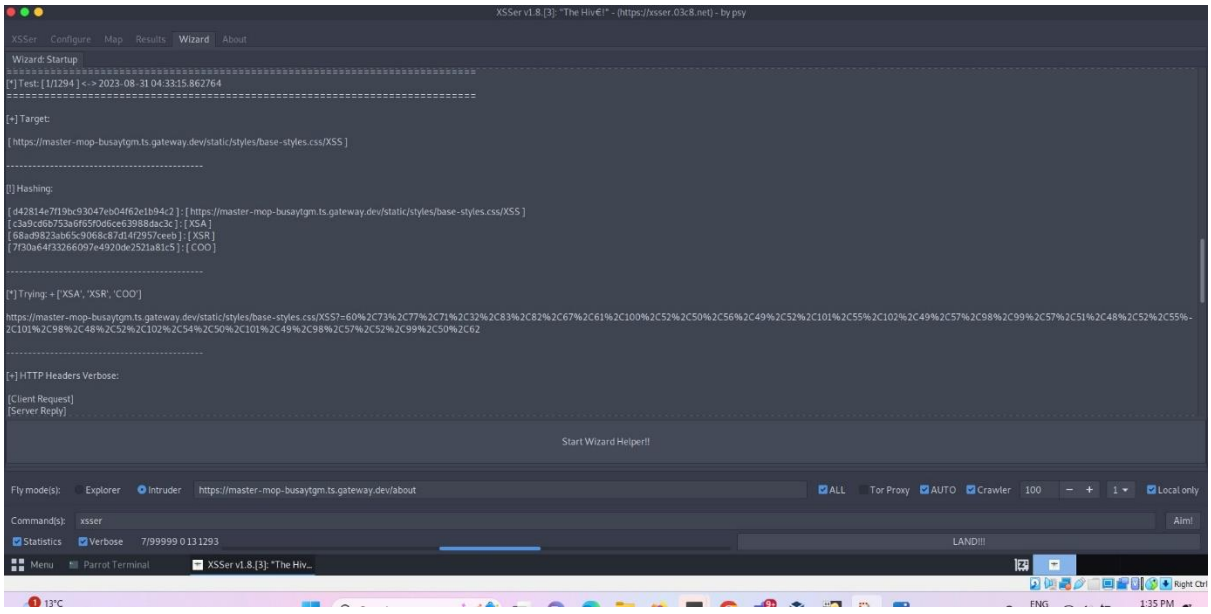
The screenshot below showcases a selection of options utilised within the Xsser Wizard.

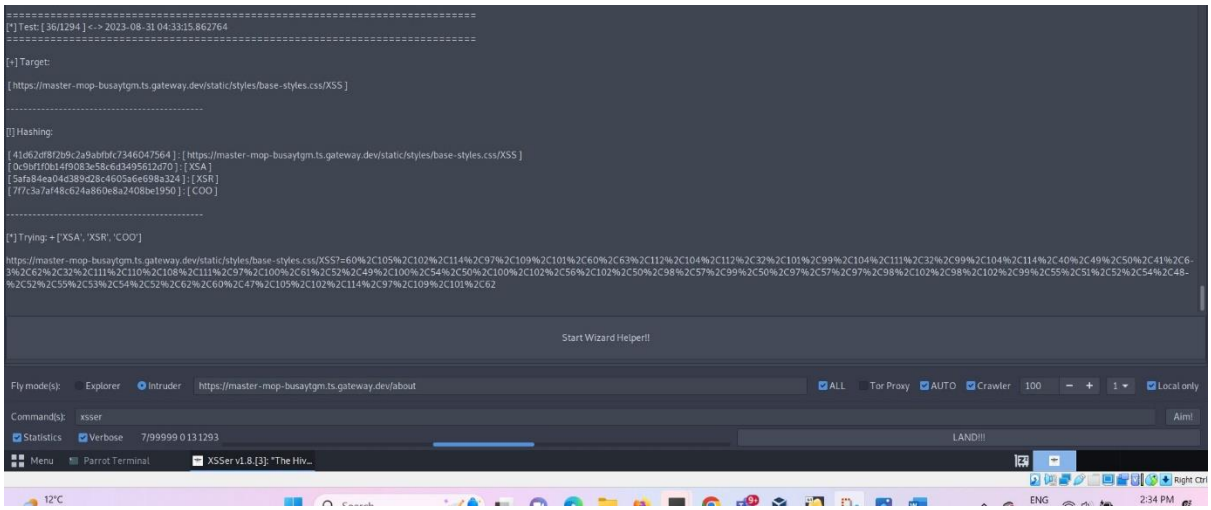


The following screenshots illustrate the outcomes of the initial scanning and attack attempt. While the attempt was not successful, it did uncover several vulnerable pages.

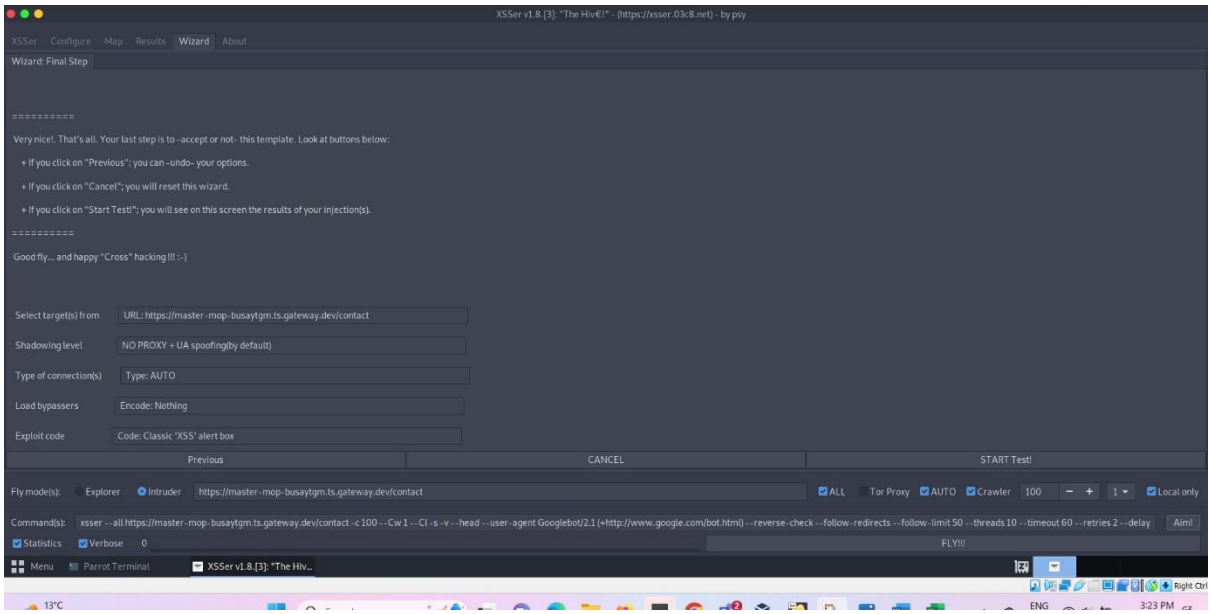



XSSer v1.8.[3]: "The Hive€!" - (https://xsser.03c8.net) - by psy
XSSer Configure Map Results Wizard About
Wizard: Startup
Testing [XSS from CRAWLER]...
[Info] Crawlering TARGET: https://master-mop-busaytgm.ts.gateway.dev/about
- Max. limit: 99999 -> (WARNING: It can take long time...)
- Deep level: 5
[Info] Mosquitoes have found: [7] possible attacking vector(s)
- https://master-mop-busaytgm.ts.gateway.dev
- https://master-mop-busaytgm.ts.gateway.dev/faq
- https://master-mop-busaytgm.ts.gateway.dev/contact
- https://master-mop-busaytgm.ts.gateway.dev/static/images/moplogo.png
- https://master-mop-busaytgm.ts.gateway.dev/static/fontawesome/css/all.min.css
- https://master-mop-busaytgm.ts.gateway.dev/static/styles/base-styles.css
- https://master-mop-busaytgm.ts.gateway.dev/static/styles/playground.css
[Error] WARNING: Some internal problems running attack...
[*] Test: [1/1294] <-> 2023-08-31 04:33:15.862764
[+] Target:
Start Wizard Helper!!
Fly mode(s): Explorer Intruder https://master-mop-busaytgm.ts.gateway.dev/about ALL Tor Proxy AUTO Crawler 100 1 Local only
Command(s): xsser Aim!
Statistics Verbose 7/99999 0 131293 LAND!!!
Menu Parrot Terminal XSSer v1.8.[3]: "The Hiv...
13°C ENG 1:35 PM


XSSer v1.8.[3]: "The Hive€!" - (https://xsser.03c8.net) - by psy
XSSer Configure Map Results Wizard About
Wizard: Startup
[*] Test: [1/1294] <-> 2023-08-31 04:33:15.862764
[+] Target:
[https://master-mop-busaytgm.ts.gateway.dev/static/styles/base-styles.css/XSS]
[!] Hashing:
[d42814e7f19bc93047eb04f62e1b94c2] : [https://master-mop-busaytgm.ts.gateway.dev/static/styles/base-styles.css/XSS]
[c3a9cd6b753a6f65f0d6ce63988dac3c] : [XSA]
[68ad9823ab65c9068c87d14f2957ceeb] : [XSR]
[7f30a64f33266097e4920de2521a81c5] : [COO]
[*] Trying: + ['XSA', 'XSR', 'COO']
https://master-mop-busaytgm.ts.gateway.dev/static/styles/base-styles.css/XSS?=60%2C73%2C77%2C71%2C32%2C83%2C82%2C67%2C61%2C100%2C52%2C50%2C56%2C49%2C52%2C101%2C55%2C102%2C49%2C57%2C98%2C99%2C57%2C51%2C48%2C52%2C55%-2C101%2C98%2C48%2C52%2C102%2C54%2C50%2C101%2C49%2C98%2C57%2C52%2C99%2C50%2C62
[+] HTTP Headers Verbose:
[Client Request]
[Server Reply]
Start Wizard Helper!!
Fly mode(s): Explorer Intruder https://master-mop-busaytgm.ts.gateway.dev/about ALL Tor Proxy AUTO Crawler 100 1 Local only
Command(s): xsser Aim!
Statistics Verbose 7/99999 0 131293 LAND!!!
Menu Parrot Terminal XSSer v1.8.[3]: "The Hiv...
13°C ENG 1:35 PM

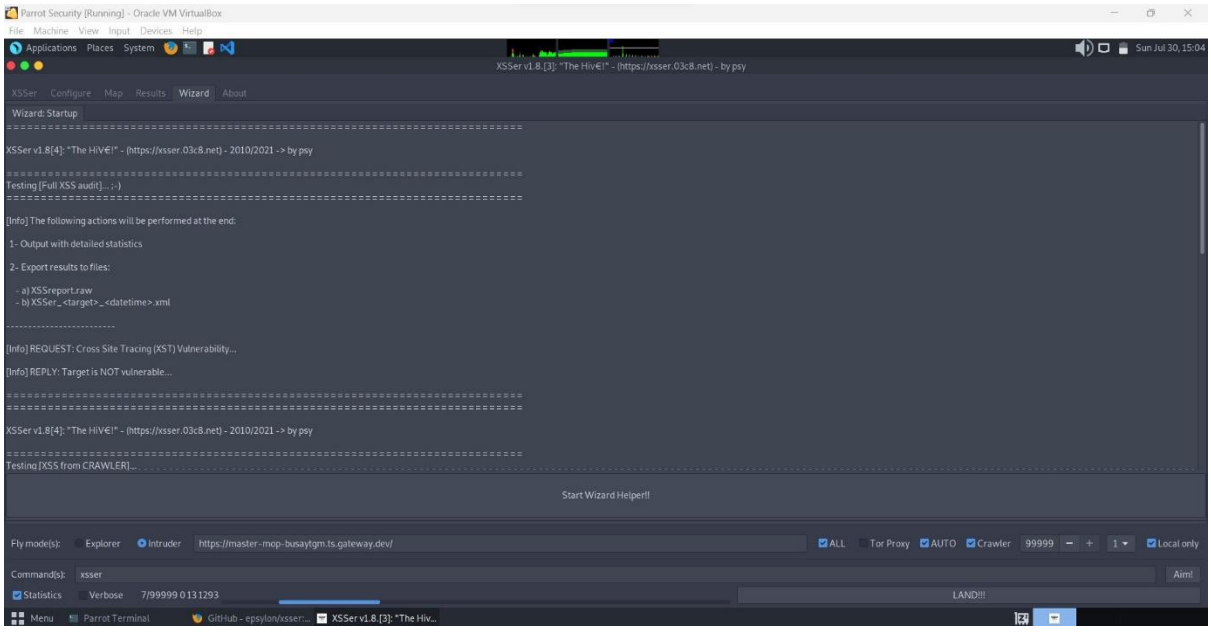

[*] Test: [36/1294] <-> 2023-08-31 04:33:15.862764
[+] Target:
[https://master-mop-busaytgm.ts.gateway.dev/static/styles/base-styles.css/XSS]
[!] Hashing:
[41d62df8f2b9c2a9abfbfc7346047564] : [https://master-mop-busaytgm.ts.gateway.dev/static/styles/base-styles.css/XSS]
[0c9bf1f0b14f9083e58c6d3495612d70] : [XSA]
[5afa84ea04d389d28c4605a6e698a324] : [XSR]
[7f7c3a7af48c624a860e8a2408be1950] : [COO]
[*] Trying: + ['XSA', 'XSR', 'COO']
https://master-mop-busaytgm.ts.gateway.dev/static/styles/base-styles.css/XSS?=60%2C105%2C102%2C114%2C97%2C109%2C101%2C60%2C63%2C112%2C104%2C112%2C32%2C101%2C99%2C104%2C111%2C32%2C99%2C104%2C114%2C40%2C49%2C50%2C41%2C6-3%2C62%2C32%2C111%2C110%2C108%2C111%2C97%2C100%2C61%2C52%2C49%2C100%2C54%2C50%2C100%2C102%2C56%2C102%2C50%2C98%2C57%2C99%2C50%2C97%2C57%2C97%2C98%2C102%2C98%2C102%2C99%2C55%2C51%2C52%2C54%2C48-%2C52%2C55%2C53%2C54%2C52%2C62%2C60%2C47%2C105%2C102%2C114%2C97%2C109%2C101%2C62
Start Wizard Helper!!
Fly mode(s): Explorer Intruder https://master-mop-busaytgm.ts.gateway.dev/about ALL Tor Proxy AUTO Crawler 100 1 Local only
Command(s): xsser Aim!
Statistics Verbose 7/99999 0 131293 LAND!!!
Menu Parrot Terminal XSSer v1.8.[3]: "The Hiv...
12°C ENG 2:34 PM

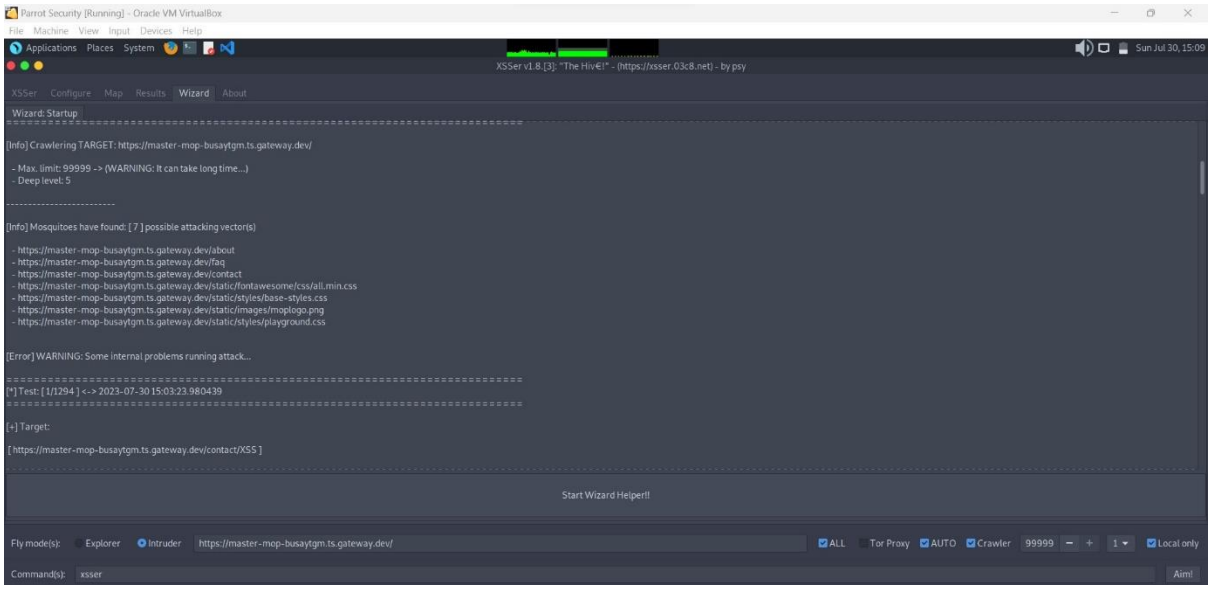
The screenshot below displays the chosen options during the second scan and attack attempt using the Xsser Wizard.

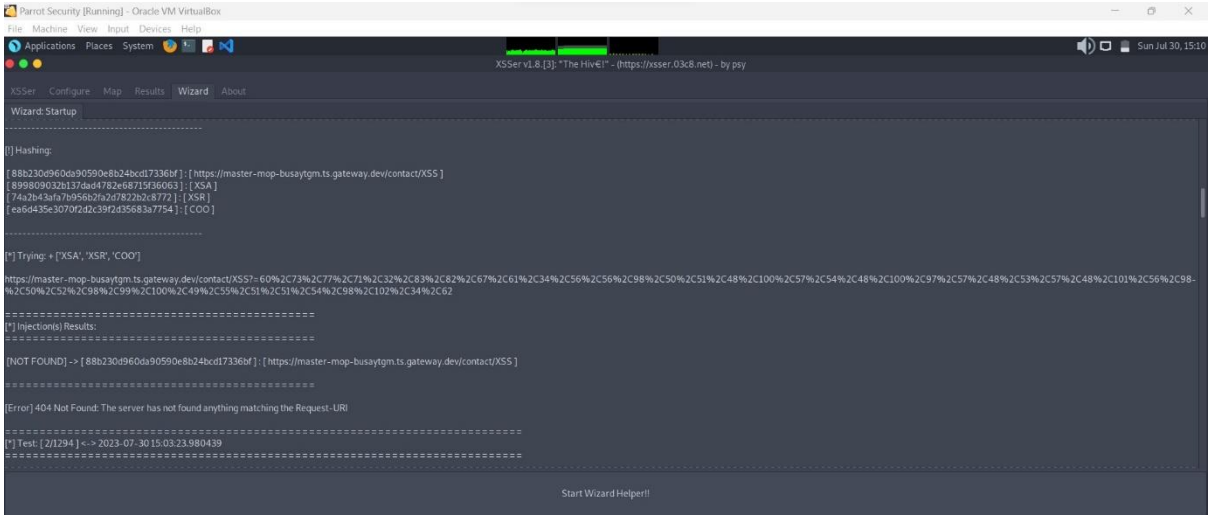


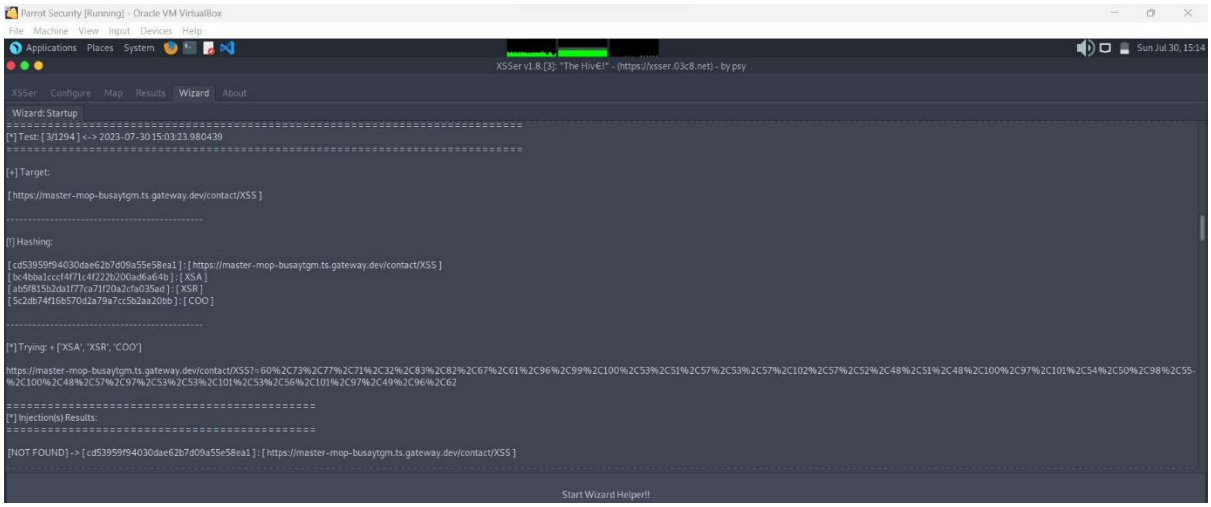
Possible vulnerabilities

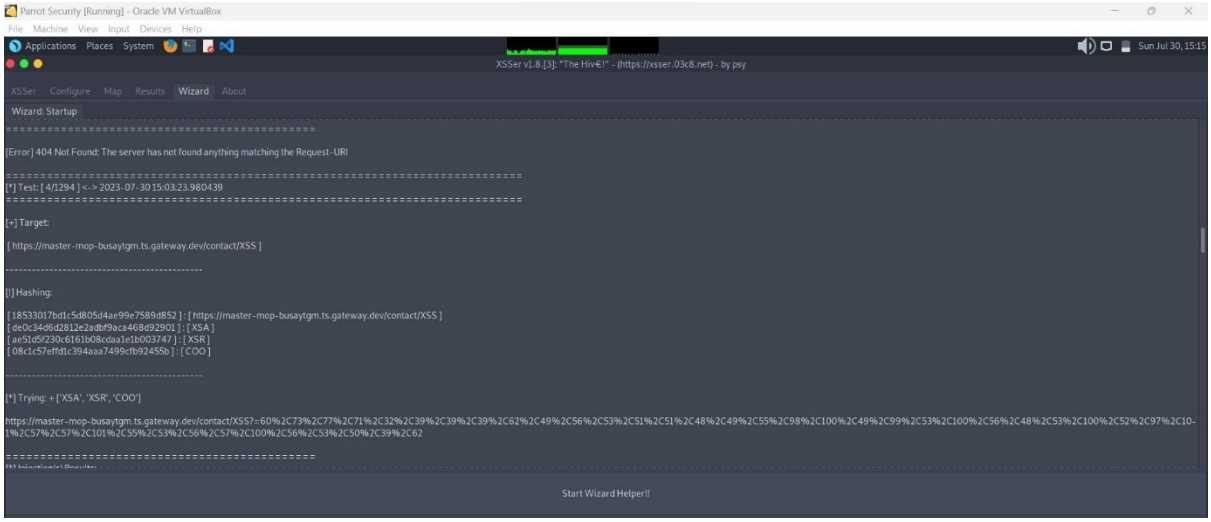
The following screenshots depict the results obtained from the second scan and attack attempt. While the attempt was still unsuccessful, it revealed the highest number of vulnerable pages to date, totalling 8.

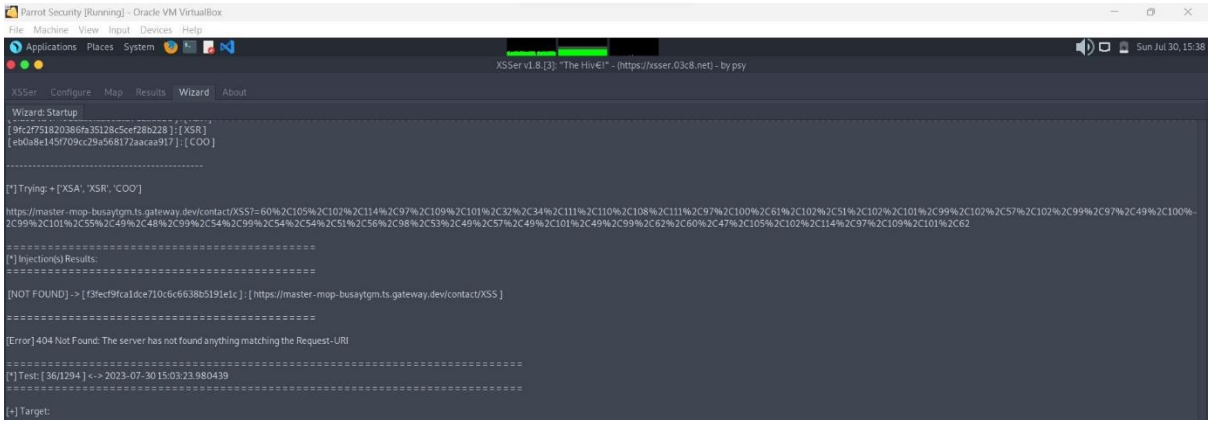



Parrot Security [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Sun Jul 30, 15:09
XSSer v1.8.[3]: "The Hive€!" - (https://xsser.03c8.net) - by psy
XSSer Configure Map Results Wizard About
Wizard: Startup
[Info] Crawlering TARGET: https://master-mop-busaytgm.ts.gateway.dev/
- Max. limit: 99999 -> (WARNING: It can take long time...)
- Deep level: 5
[Info] Mosquitoes have found: [7] possible attacking vector(s)
- https://master-mop-busaytgm.ts.gateway.dev/about
- https://master-mop-busaytgm.ts.gateway.dev/faq
- https://master-mop-busaytgm.ts.gateway.dev/contact
- https://master-mop-busaytgm.ts.gateway.dev/static/fontawesome/css/all.min.css
- https://master-mop-busaytgm.ts.gateway.dev/static/styles/base-styles.css
- https://master-mop-busaytgm.ts.gateway.dev/static/images/moplogo.png
- https://master-mop-busaytgm.ts.gateway.dev/static/styles/playground.css
[Error] WARNING: Some internal problems running attack...
[*] Test: [1/1294] <-> 2023-07-30 15:03:23.980439
[+] Target:
[https://master-mop-busaytgm.ts.gateway.dev/contact/XSS]
Start Wizard Helper!!
Fly mode(s): Explorer Intruder https://master-mop-busaytgm.ts.gateway.dev/ ALL Tor Proxy AUTO Crawler 99999 1 Local only
Command(s): xsser Aim!


Parrot Security [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Sun Jul 30, 15:10
XSSer v1.8.[3]: "The Hive€!" - (https://xsser.03c8.net) - by psy
XSSer Configure Map Results Wizard About
Wizard: Startup
[!] Hashing:
[88b230d960da90590e8b24bcd17336bf] : [https://master-mop-busaytgm.ts.gateway.dev/contact/XSS]
[899809032b137dad4782e68715f36063] : [XSA]
[74a2b43afa7b956b2fa2d7822b2c8772] : [XSR]
[ea6d435e3070f2d2c39f2d35683a7754] : [COO]
[*] Trying: + ['XSA', 'XSR', 'COO']
https://master-mop-busaytgm.ts.gateway.dev/contact/XSS?=60%2C73%2C77%2C71%2C32%2C83%2C82%2C67%2C61%2C34%2C56%2C56%2C98%2C50%2C51%2C48%2C100%2C57%2C54%2C48%2C100%2C97%2C57%2C48%2C53%2C57%2C48%2C101%2C56%2C98-%2C50%2C52%2C98%2C99%2C100%2C49%2C55%2C51%2C51%2C54%2C98%2C102%2C34%2C62
[*] Injection(s) Results:
[NOT FOUND] -> [88b230d960da90590e8b24bcd17336bf] : [https://master-mop-busaytgm.ts.gateway.dev/contact/XSS]
[Error] 404 Not Found: The server has not found anything matching the Request-URI
[*] Test: [2/1294] <-> 2023-07-30 15:03:23.980439
Start Wizard Helper!!

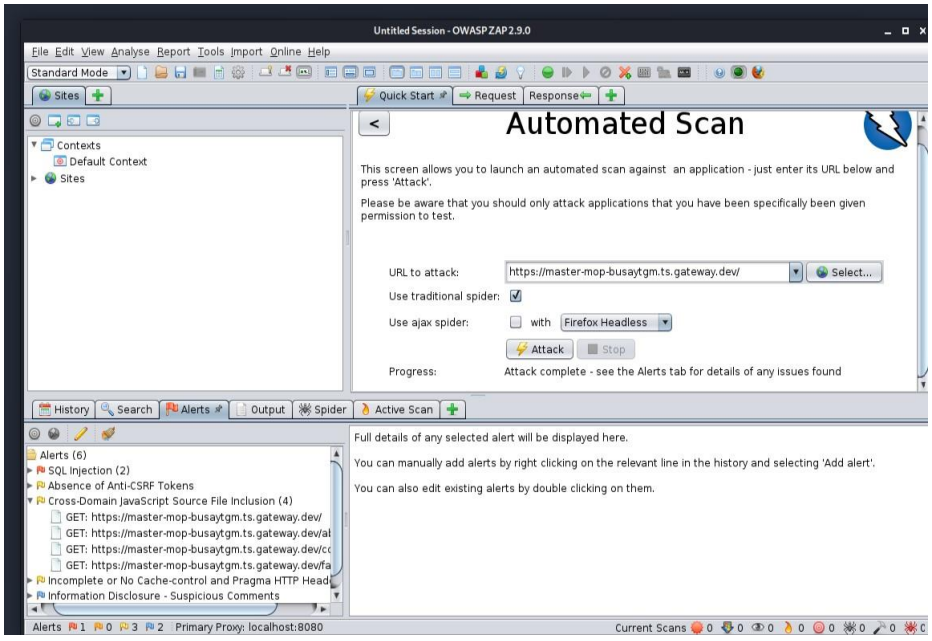

Parrot Security [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Sun Jul 30, 15:14
XSSer v1.8.[3]: "The Hive€!" - (https://xsser.03c8.net) - by psy
XSSer Configure Map Results Wizard About
Wizard: Startup
[*] Test: [3/1294] <-> 2023-07-30 15:03:23.980439
[+] Target:
[https://master-mop-busaytgm.ts.gateway.dev/contact/XSS]
[!] Hashing:
[cd53959f94030dae62b7d09a55e58ea1] : [https://master-mop-busaytgm.ts.gateway.dev/contact/XSS]
[bc4bba1cccf4f71c4f222b200ad6a64b] : [XSA]
[ab5f815b2da1f77ca71f20a2cfa035ad] : [XSR]
[5c2db74f16b570d2a79a7cc5b2aa20bb] : [COO]
[*] Trying: + ['XSA', 'XSR', 'COO']
https://master-mop-busaytgm.ts.gateway.dev/contact/XSS?=60%2C73%2C77%2C71%2C32%2C83%2C82%2C67%2C61%2C96%2C99%2C100%2C53%2C51%2C57%2C53%2C57%2C102%2C57%2C52%2C48%2C51%2C48%2C100%2C97%2C101%2C54%2C50%2C98%2C55-%2C100%2C48%2C57%2C97%2C53%2C53%2C101%2C53%2C56%2C101%2C97%2C49%2C96%2C62
[*] Injection(s) Results:
[NOT FOUND] -> [cd53959f94030dae62b7d09a55e58ea1] : [https://master-mop-busaytgm.ts.gateway.dev/contact/XSS]
Start Wizard Helper!!





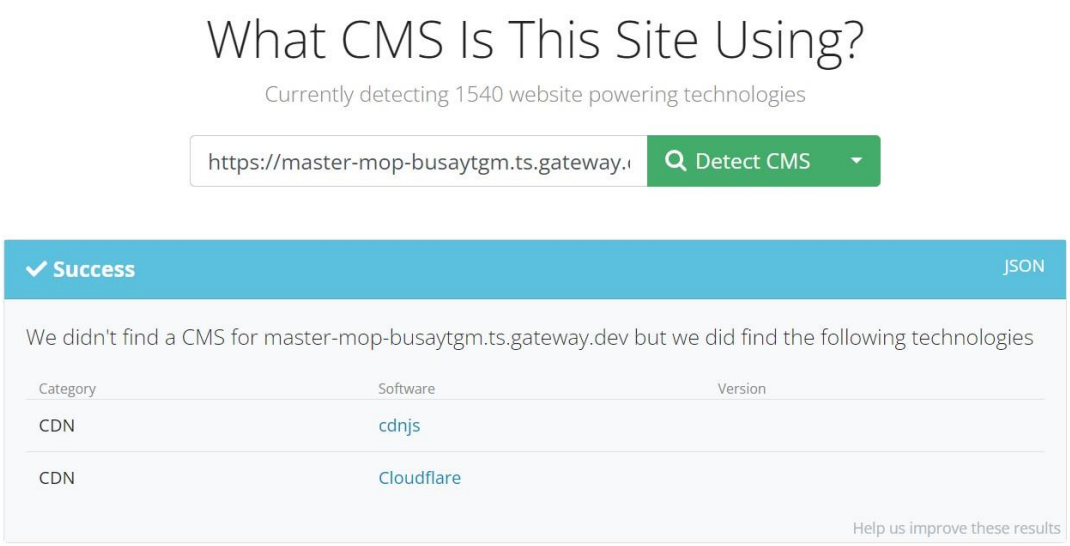
Results of OWASP Scan

The screenshot below provides the results of the OWASP scan, indicating that the website is susceptible to DOM-based XSS attacks.

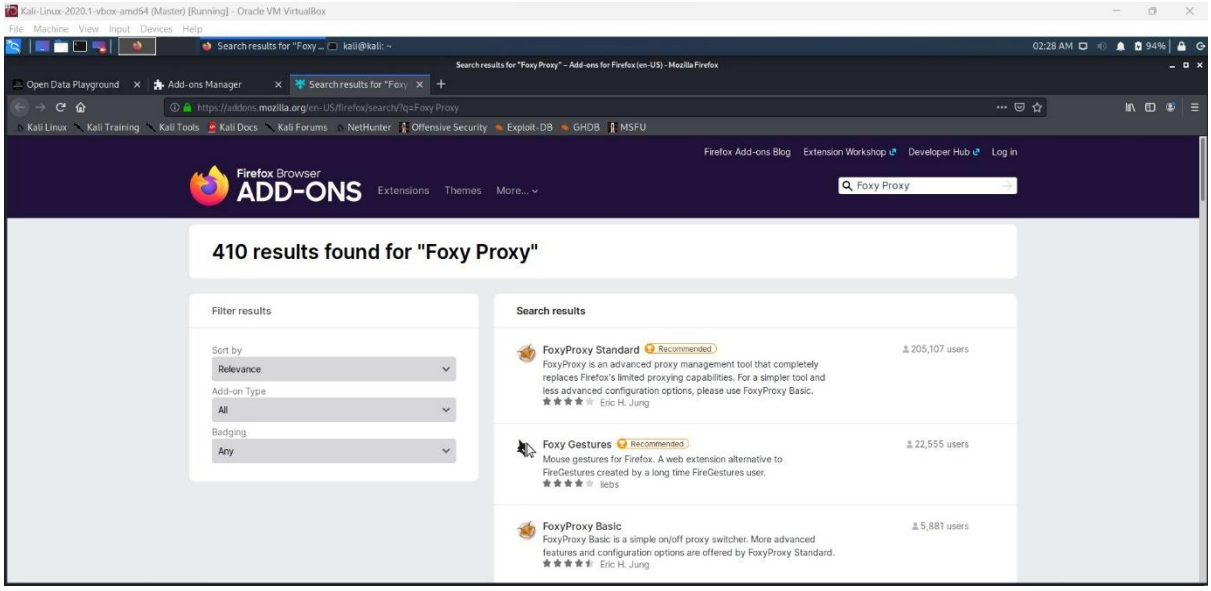


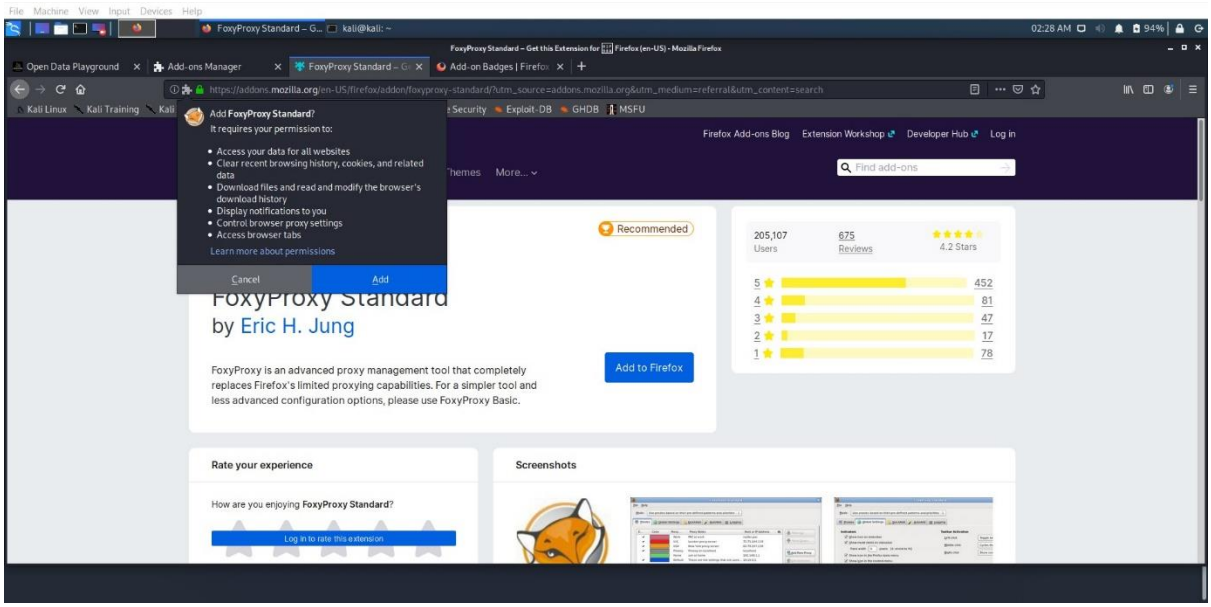
CMS

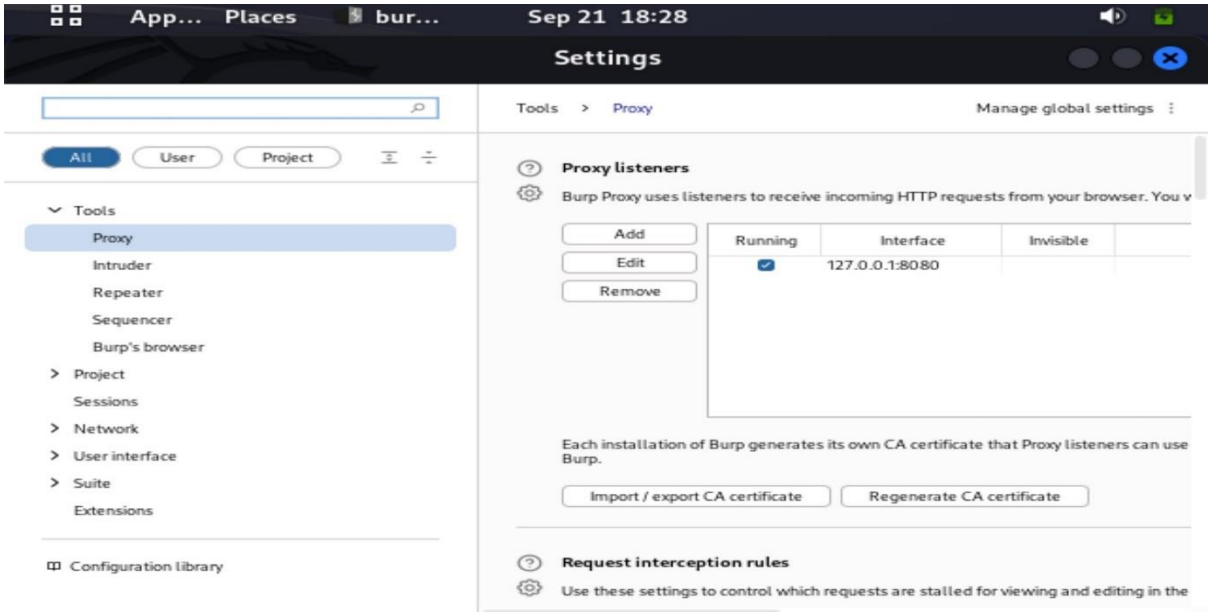
The below screenshot demonstrates that a scan of the website was conducted to gain a better understanding of what CMS it uses to rule out specific CMS scanners such as WPScan which is used to scan WordPress websites for vulnerabilities.

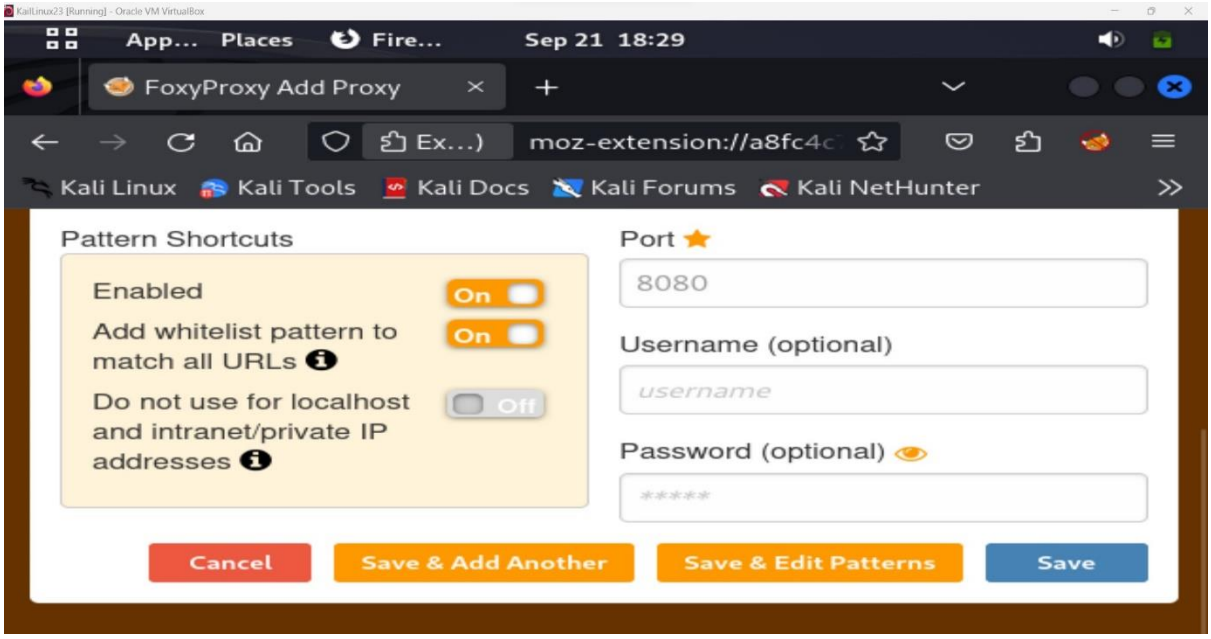


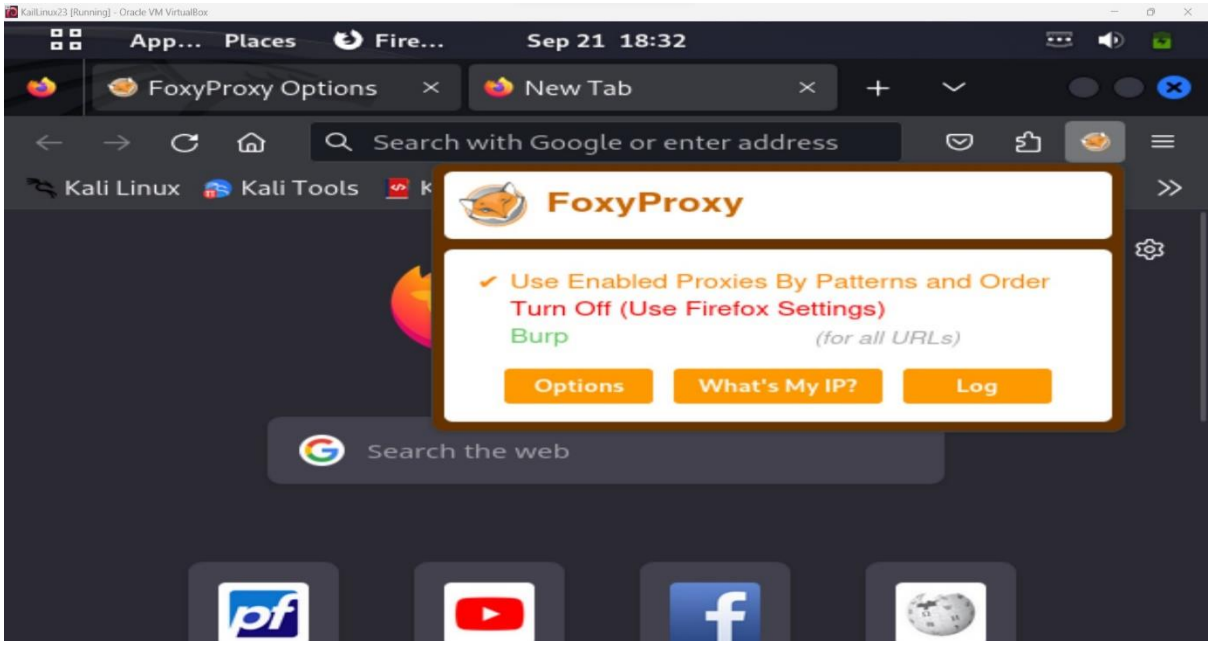
The following screenshots illustrate the process of downloading and connecting FoxyProxy to BurpSuite, facilitating the analysis of the website's HTTP traffic for potential vulnerabilities.



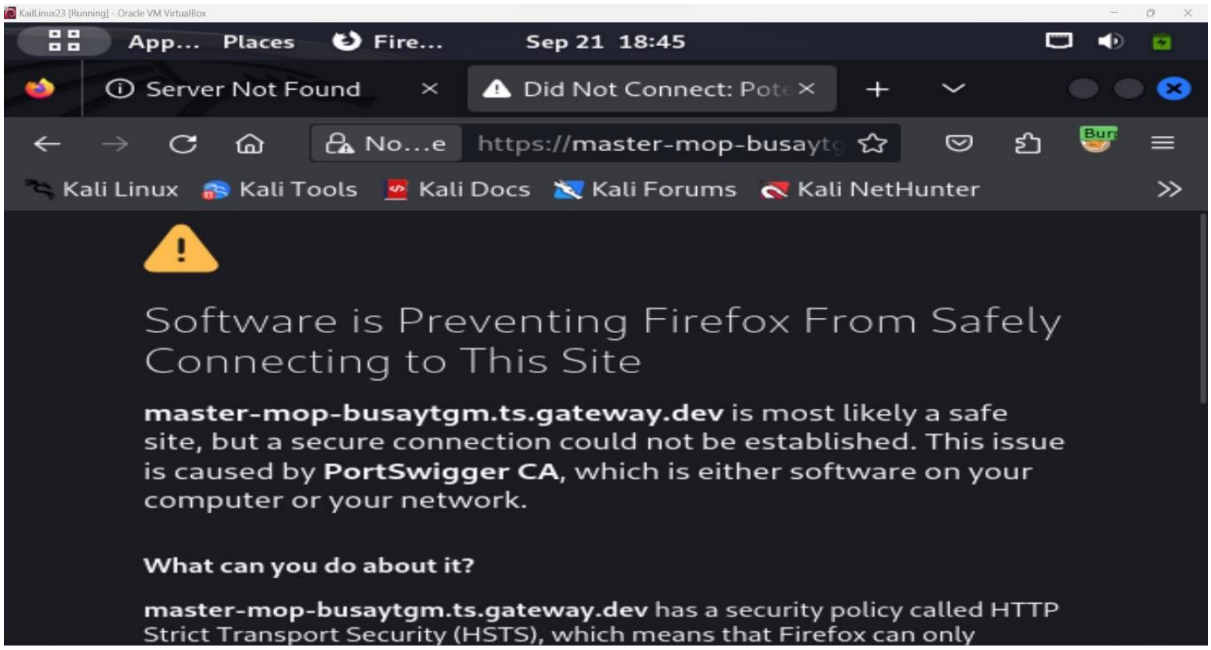

Add FoxyProxy Standard?
It requires your permission to:
Access your data for all websites
Clear recent browsing history, cookies, and related data
Download files and read and modify the browser's download history
Display notifications to you
Control browser proxy settings
Access browser tabs
Learn more about permissions
Cancel
Add
FoxyProxy Standard
by Eric H. Jung
FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.
Add to Firefox
Recommended
205,107 Users
675 Reviews
4.2 Stars
Rate your experience
How are you enjoying FoxyProxy Standard?
Log in to rate this extension
Screenshots


App... Places bur... Sep 21 18:28
Settings
Tools > Proxy
Manage global settings
All
User
Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Suite
Extensions
Configuration library
Proxy listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You v
Add
Edit
Remove
Running
Interface
Invisible
127.0.0.1:8080
Each installation of Burp generates its own CA certificate that Proxy listeners can use
Burp.
Import / export CA certificate
Regenerate CA certificate
Request interception rules
Use these settings to control which requests are stalled for viewing and editing in the


App... Places Fire... Sep 21 18:29
FoxyProxy Add Proxy
Ex...)
moz-extension://a8fc4c
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
Pattern Shortcuts
Enabled On
Add whitelist pattern to match all URLs On
Do not use for localhost and intranet/private IP addresses Off
Port
8080
Username (optional)
username
Password (optional)
*****
Cancel
Save & Add Another
Save & Edit Patterns
Save


App... Places Fire... Sep 21 18:32
FoxyProxy Options
New Tab
Search with Google or enter address
Kali Linux Kali Tools
FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
Burp (for all URLs)
Options
What's My IP?
Log
Search the web

The screenshot below highlights that the website restricts users from connecting through a proxy, thereby preventing the attack from progressing further.



Result Comparison:

Below are the similarities and differences between the two attacks.

Similarities	Differences
- **Toolset**: Both attacks utilized common tools such as Parrot OS, Kali Linux, BurpSuite, Foxy Proxy, OWASP, and Xsser, indicating a consistent methodology. - **Initial Unsuccessful Attempt:** Both scans resulted in an initial unsuccessful attempt, revealing potential vulnerabilities but not achieving the intended exploitation.	- **Scope:** The first attack focused on an initial scan and attack attempt using Xsser, whereas the second attack aimed to enhance the scan's scope, leading to the discovery of a higher number of vulnerable pages. - **Vulnerable Pages:** The second scan uncovered a significantly greater number of vulnerable pages, totalling 8, compared to the first scan. - **OWASP Scan:** The second scan included an OWASP scan, which specifically identified the susceptibility to DOM-based XSS attacks on the website. This crucial finding was absent in the first scan.

Recommendations:

Based on the assessment findings, the following recommendations are proposed:

- **Implement Input Validation:** Implement strong input validation and output encoding to prevent XSS vulnerabilities in the application.
- **Security Education:** Conduct regular security training for developers to ensure they are aware of best practices for secure coding and XSS prevention.
- **Regular Scans:** Continuously perform security scans and assessments on the web application to proactively identify and address emerging vulnerabilities.
- **Content Security Policy (CSP):** Consider implementing a strict Content Security Policy to mitigate the impact of XSS attacks.
- **Update Tools and Methodology:** Ensure that you are using the latest versions of security assessment tools and methodologies. Cybersecurity tools and attack techniques are continually evolving, so staying current is crucial.

Conclusion:

In conclusion, this XSS vulnerability assessment of the City of Melbourne – open data (MOP) website provided valuable insights into potential security risks. While both scan attempts using Xsser initially yielded no successful exploits, the second scan revealed a more extensive list of vulnerable pages, emphasizing the importance of thorough testing.

The OWASP scan results highlighted the susceptibility to DOM-based XSS attacks, a critical finding that necessitates immediate attention. By addressing the identified vulnerabilities and implementing recommended security measures, the website can significantly enhance its resilience against XSS attacks.

Continuous vigilance, regular security assessments, and an emphasis on secure coding practices are essential to maintaining the security and integrity of web applications in today's threat landscape. This assessment serves as a starting point for improving the website's security posture and ensuring the protection of user data and sensitive information.

References:

[1] Pentester Academy TV, "[Attack-Defense] XSS Attack with XSSer," *YouTube*. May 21, 2020. Accessed: Sep. 22, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=HZ2K-Y8fTyc&t=84s

[2] Loi Liang Yang, "Cross-Site Scripting (XSS) Explained And Demonstrated!," *YouTube*. Jan. 24, 2022. Accessed: Sep. 22, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=1Hr4_r2xQXY&t=178s

[3] 0xdf, "Configuring Burp + FoxyProxy + Firefox," *YouTube*. Nov. 30, 2021. Accessed: Sep. 22, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=iTm33Miymdg

[4] "Cross Site Scripting (XSS) | OWASP Foundation," *Owasp.org*, 2023. https://owasp.org/www-community/attacks/xss/ (accessed Sep. 22, 2023).

[5] "What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy," *Portswigger.net*, 2021. https://portswigger.net/web-security/cross-site-scripting (accessed Sep. 22, 2023).

[6] "What is Cross-Site Scripting? XSS Cheat Sheet | Veracode," *Veracode*, 2021. https://www.veracode.com/security/xss (accessed Sep. 22, 2023).

[7] "What is cross-site scripting?," *Cloudflare*, 2023. https://www.cloudflare.com/en-gb/learning/security/threats/cross-site-scripting/ (accessed Sep. 22, 2023).

[8] daxxog, "xsser/gtk/docs/documentation.txt at master · daxxog/xsser," *GitHub*, 2021. https://github.com/daxxog/xsser/blob/master/gtk/docs/documentation.txt (accessed Sep. 22, 2023).