Sri Lanka Institute of Information Technology

Report – Victoria’s Secret

IE2062 - Web security

Submitted by:

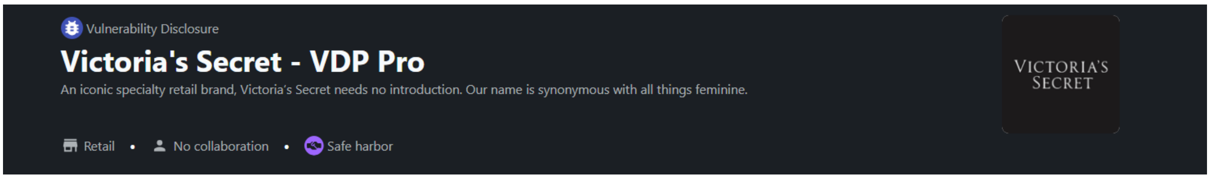
Student Registration Number	Student Name
IT23253476	Bandara S.M.S.N

Date of submission

05/05/2025

Table of Contents

1. Domain: https://www.victoriassecret.com/us/

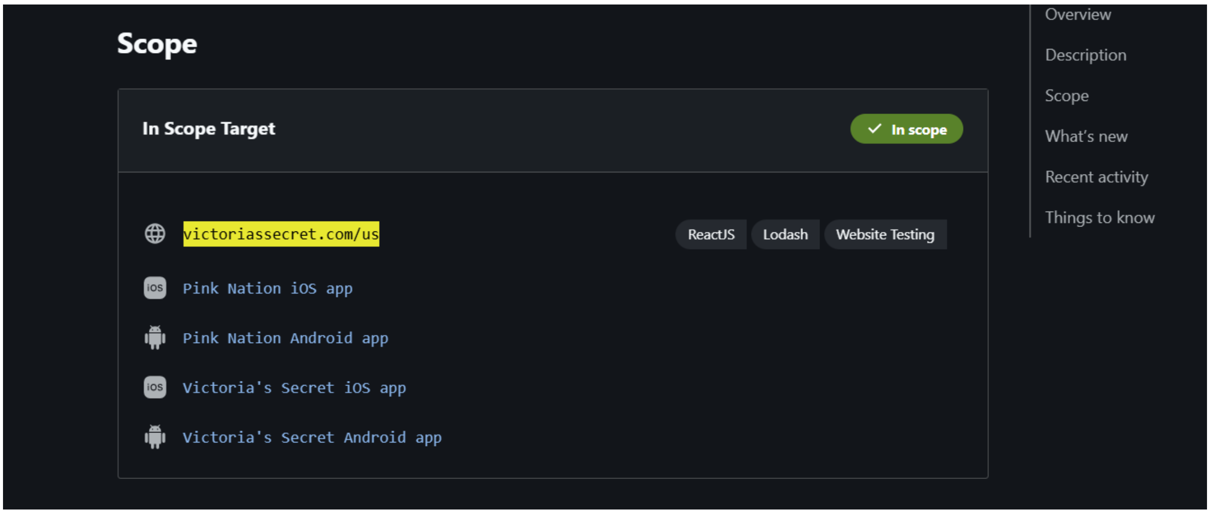


Vulnerability Disclosure

Victoria's Secret - VDP Pro

An iconic specialty retail brand, Victoria's Secret needs no introduction. Our name is synonymous with all things feminine.

Retail • No collaboration • Safe harbor



Scope

In Scope Target ✓ In scope

victoriassecret.com/us ReactJS Lodash Website Testing

Pink Nation iOS app

Pink Nation Android app

Victoria's Secret iOS app

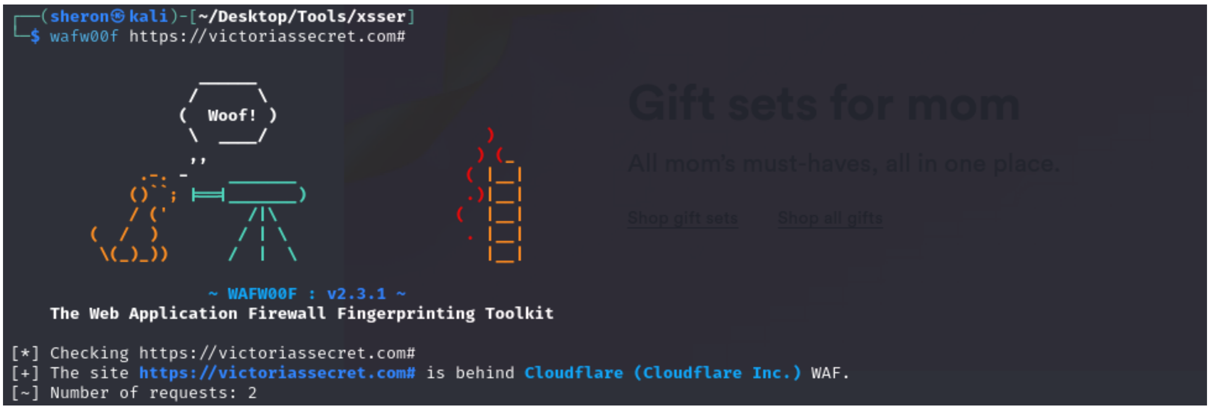
Victoria's Secret Android app

- Link: https://victoriassecret.com#
- Type: Vulnerability Disclosure Program (VDP)
- Category: Retail Store

2. Scanning

2.1. Wafw00f

Before using any tool lets find out if the web application is behind any firewall. By finding the firewall attackers can try to bypass it with the use of known vulnerabilities in this web application it uses,



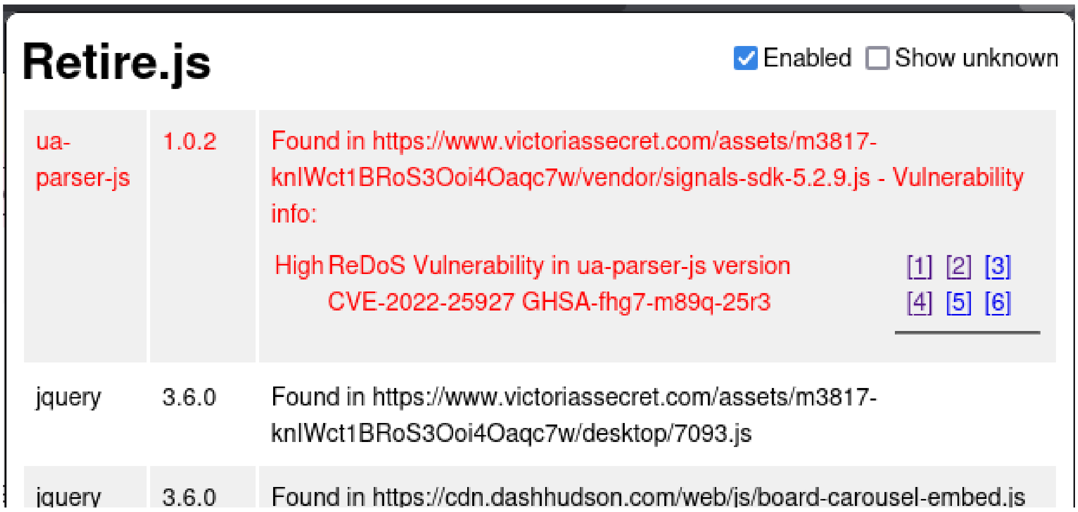
```
┌──(sheron㉿kali)-[~/Desktop/Tools/xsser]
└─$ wafw00f https://victoriassecret.com#

                ~ WAFW00F : v2.3.1 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://victoriassecret.com#
[+] The site https://victoriassecret.com# is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

2.2. Retire.js

Retire.js is web page extension which can find vulnerabilities in java script libraries used. It will also give a description of the vulnerability along with links to the full vulnerability details. Scanning the https://www.victoriassecret.com/us/ domain the following was discovered.



Retire.js

☑ Enabled ☐ Show unknown

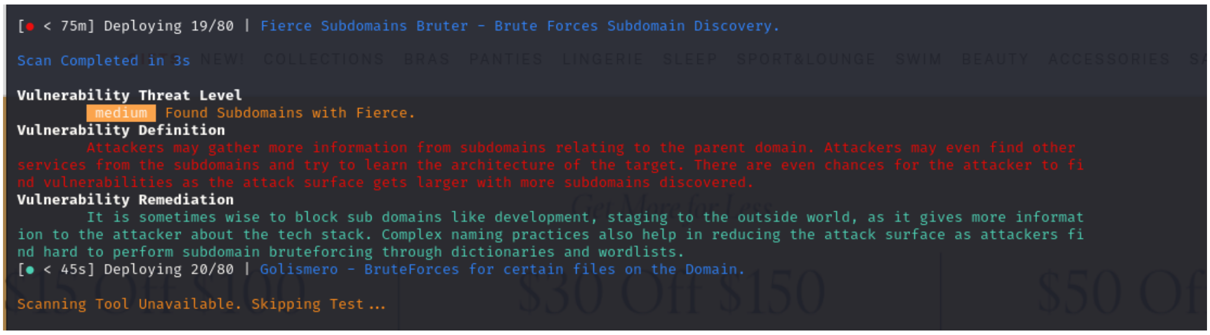
ua-parser-js	1.0.2	Found in https://www.victoriassecret.com/assets/m3817-knlWct1BRoS3Ooi4Oaqc7w/vendor/signals-sdk-5.2.9.js - Vulnerability info: High ReDoS Vulnerability in ua-parser-js version CVE-2022-25927 GHSA-fhg7-m89q-25r3 [1] [2] [3] [4] [5] [6]
jquery	3.6.0	Found in https://www.victoriassecret.com/assets/m3817-knlWct1BRoS3Ooi4Oaqc7w/desktop/7093.js
jquery	3.6.0	Found in https://cdn.dashhudson.com/web/js/board-carousel-embed.js

The vulnerability found was a high severity Regular Expression Denial of Service (ReDos) identified as CVE-2022-25927. What this vulnerability can do will be covered later.

2.3. Rapid Scanner

Rapid Scanner is a valuable tool for bug bounty hunters and a CTF players to find vulnerabilities in web applications. It uses 82 tools to look for vulnerabilities. It provides the vulnerability and its description and a fix to the vulnerability. The scan revealed the following information.

First vulnerability – The scanner was able find details about **subdomain enumeration** with a tool called firerce.



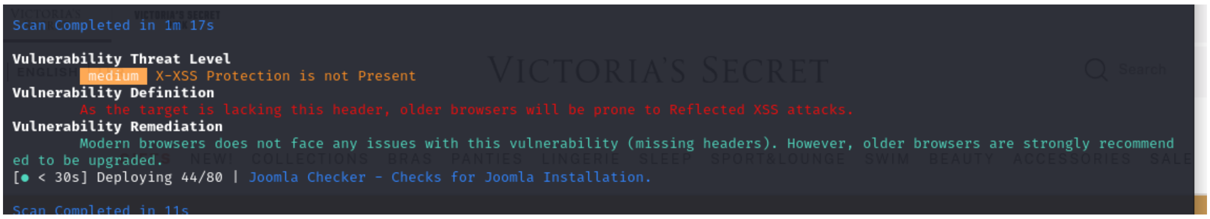
```
[● < 75m] Deploying 19/80 | Fierce Subdomains Bruter - Brute Forces Subdomain Discovery.

Scan Completed in 3s

Vulnerability Threat Level
         medium  Found Subdomains with Fierce.
Vulnerability Definition
         Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other
services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to fi
nd vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
         It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more informat
ion to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers fi
nd hard to perform subdomain bruteforcing through dictionaries and wordlists.
[● < 45s] Deploying 20/80 | Golismero - BruteForces for certain files on the Domain.

Scanning Tool Unavailable. Skipping Test ...
```

Second vulnerability – Has discovered a vulnerability due to a missing header. Due to the absence of this header XSS attacks can be exploited.

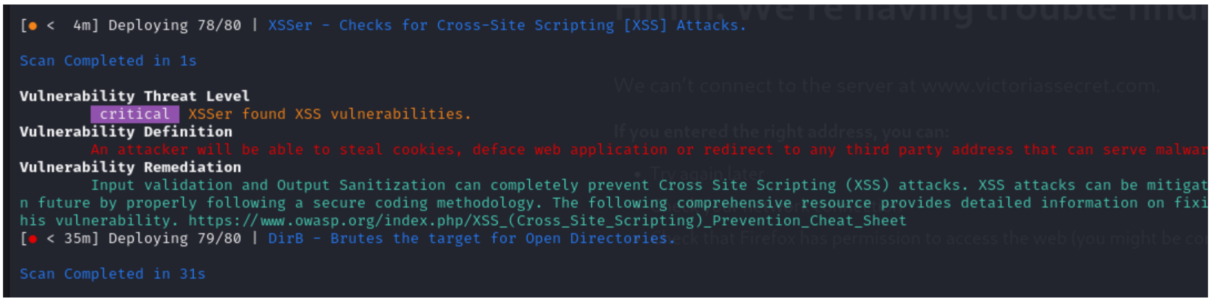


```
Scan Completed in 1m 17s

Vulnerability Threat Level
         medium  X-XSS Protection is not Present
Vulnerability Definition
         As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
         Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommend
ed to be upgraded.
[● < 30s] Deploying 44/80 | Joomla Checker - Checks for Joomla Installation.

Scan Completed in 11s
```

Third vulnerability – A tool named xsser as found vulnerabilities, So that the attacker can steal cookies, deface the website or to redirect to a different malicious web page.



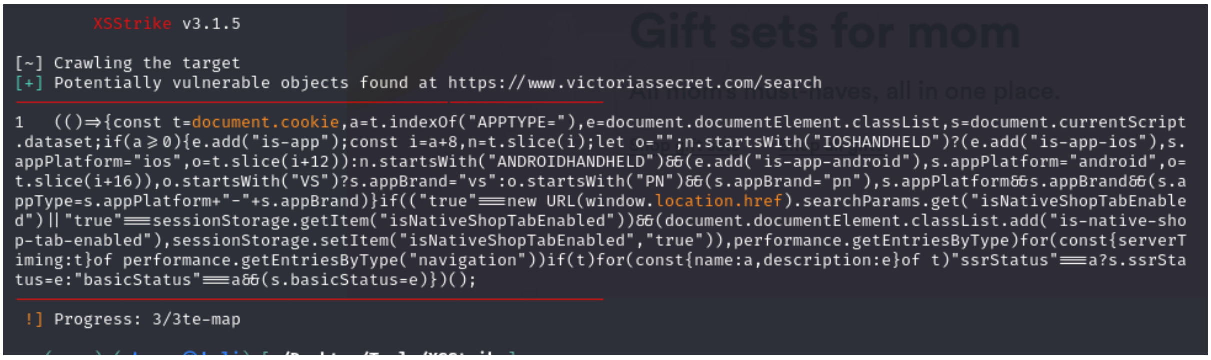
```
[● <  4m] Deploying 78/80 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks.

Scan Completed in 1s

Vulnerability Threat Level
         critical  XSSer found XSS vulnerabilities.
Vulnerability Definition
         An attacker will be able to steal cookies, deface web application or redirect to any third party address that can serve malwar
Vulnerability Remediation
         Input validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks can be mitigat
n future by properly following a secure coding methodology. The following comprehensive resource provides detailed information on fixi
his vulnerability. https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
[● < 35m] Deploying 79/80 | DirB - Brutes the target for Open Directories.

Scan Completed in 31s
```

After using the **XSSer** tool we can confirm the availability of the xss vulnerability as it can find the potentially infected components.

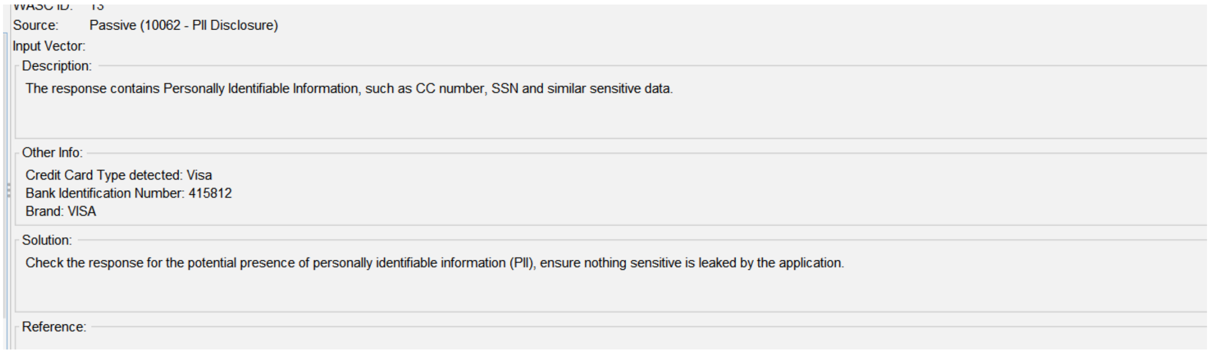


```
        XSStrike v3.1.5

[~] Crawling the target
[+] Potentially vulnerable objects found at https://www.victoriassecret.com/search
------------------------------------------------------------
1   (()=>{const t=document.cookie,a=t.indexOf("APPTYPE="),e=document.documentElement.classList,s=document.currentScript
.dataset;if(a>=0){e.add("is-app");const i=a+8,n=t.slice(i);let o="";n.startsWith("IOSHANDHELD")?(e.add("is-app-ios"),s.
appPlatform="ios",o=t.slice(i+12)):n.startsWith("ANDROIDHANDHELD")&&(e.add("is-app-android"),s.appPlatform="android",o=
t.slice(i+16)),o.startsWith("VS")?s.appBrand="vs":o.startsWith("PN")&&(s.appBrand="pn"),s.appPlatform&&s.appBrand&&(s.a
ppType=s.appPlatform+"-"+s.appBrand)}if(("true"===new URL(window.location.href).searchParams.get("isNativeShopTabEnable
d")||"true"===sessionStorage.getItem("isNativeShopTabEnabled"))&&(document.documentElement.classList.add("is-native-sho
p-tab-enabled"),sessionStorage.setItem("isNativeShopTabEnabled","true")),performance.getEntriesByType)for(const{serverT
iming:t}of performance.getEntriesByType("navigation"))if(t)for(const{name:a,description:e}of t)"ssrStatus"===a?s.ssrSta
tus=e:"basicStatus"===a&&(s.basicStatus=e)}})();
------------------------------------------------------------
 !] Progress: 3/3te-map
```

2.4. OWSAP ZAP

Zap is a powerful tool offered by OWSAP. It can scan for vulnerabilities in a web application. This is a very powerful tool as it can give the correct with proof of exploit to confirm the vulnerability is present. ZAP scan has discovered the following vulnerability in the web application.



WASC ID: 13
Source: Passive (10062 - PII Disclosure)
Input Vector:
Description:
The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

Other Info:
Credit Card Type detected: Visa
Bank Identification Number: 415812
Brand: VISA

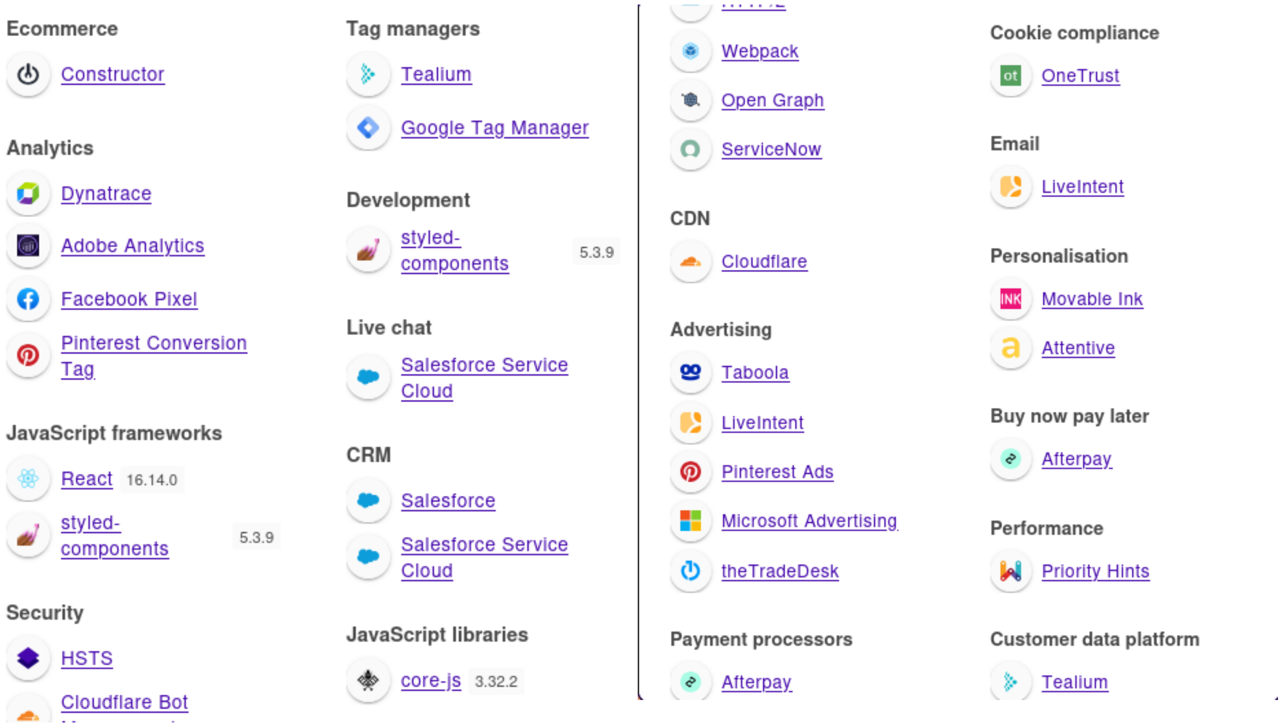
Solution:
Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

Reference:

The above vulnerability is regarding personally identifiable information (PII). It can detect personal information in plain text such as ssn, phone number, credit card number, address and ect…

2.5. Wappalyzer

Wappalyzer is a web browser extension which can be used to look up the web technologies that have been used in a web application. The attacker can look for any potentially vulnerability and exploit any vulnerabilities associated with the old version.



Ecommerce

- Constructor

Analytics

- Dynatrace
- Adobe Analytics
- Facebook Pixel
- Pinterest Conversion Tag

JavaScript frameworks

- React 16.14.0
- styled-components 5.3.9

Security

- HSTS
- Cloudflare Bot

Tag managers

- Tealium
- Google Tag Manager

Development

- styled-components 5.3.9

Live chat

- Salesforce Service Cloud

CRM

- Salesforce
- Salesforce Service Cloud

JavaScript libraries

- core-js 3.32.2

- Webpack
- Open Graph
- ServiceNow

CDN

- Cloudflare

Advertising

- Taboola
- LiveIntent
- Pinterest Ads
- Microsoft Advertising
- theTradeDesk

Payment processors

- Afterpay

Cookie compliance

- OneTrust

Email

- LiveIntent

Personalisation

- Movable Ink
- Attentive

Buy now pay later

- Afterpay

Performance

- Priority Hints

Customer data platform

- Tealium

The following vulnerabilities were found on the technologies that were used.

CVE ID	Vulnerability Name	Technology Name
CVE-2025-2009	WordPress Newsletters Stored Cross-Site Scripting	WordPress
CVE-2025-2167	WordPress Event Post Stored Cross-Site Scripting	WordPress
CVE-2025-2257	BoldGrid WordPress Backup Plugin Remote Code Execution	BoldGrid (WordPress Plugin)
CVE-2024-13801	WordPress BWL Advanced FAQ Manager Unauthorized Data Modification	BWL Advanced FAQ Manager (WordPress Plugin)

3. Vulnerabilities

3.1. Regular Expression Denial of Service (ReDos)

The reason for this vulnerability is the usage of ua-parser-js library. This is also a form of a denial-of-service attack. But a bit more destructive. Here the vulnerability bypasses the library's MAX_LENGTH input limit prevention. By crafting a long string with a specific pattern. The attacker can turn the script to get stuck processing for a very long time which results in a DOS condition.

3.2. Sub domain enumeration with fierce

Understanding the structure of the web site. Such as gaining an idea of the subdomains will greatly elevate the chances of a successful attack. When done correctly the attacker may even find classified data within the subdomains.

3.3. XSS

The rapid scanner has found two vulnerabilities regarding xss attacks. First one being, missing header to prevent xss attacks. This vulnerability might not be affected to modern browsers. How ever old browsers are vulnerabilities.

Also xxsser tool has found a way to perform a xss which is critical vulnerability. The xss vulnerability can run malicious scripts to perform malicious acts. There are many types of xss attacks such as, reflected xss, stored xss and DOM xss.

3.4. PII (personally identifiable information)

Availability of such vulnerabilities can pose a serious threat. Personal information such as name, email, phone numbers, SSN and card details can be gained without the knowledge of the user. Discovery of such details can help the attacker to fine tune his attack for the maximum damage

4. Components Affected

The following table represents the summary of the affected components. It contains details such as the component name, version, CVE and the impact.

Component	Type	Vulnerability	CVE Code	Severity	Impact
ua-parser-js	JavaScript Library	Regular Expression Denial of Service (**ReDoS**)	CVE-2022-25927	High	Allows an attacker to craft long strings that cause excessive processing time, leading to a **Denial-of-Service (DoS)** condition
WordPress	Web CMS	Stored Cross-Site Scripting (**XSS**)	CVE-2025-2009, CVE-2025-2167	High	Enables attackers to inject malicious scripts, potentially leading to **website defacement or session hijacking**
BoldGrid (WordPress Plugin)	Plugin	Remote Code Execution (**RCE**)	CVE-2025-2257	Critical	Attackers can execute arbitrary code remotely, leading to **server compromise**
BWL Advanced FAQ Manager (WordPress Plugin)	Plugin	Unauthorized Data Modification	CVE-2024-13801	High	Allows unauthorized modification of stored data, potentially leading to **information tampering**
Subdomain Enumeration	Reconnaissance	Subdomain Exposure	-	Medium	Attackers can identify hidden subdomains, increasing the likelihood of **classified data leaks**
Missing Security Header	Security Configuration	Increased XSS Risk	-	High	Without this header, older browsers are more susceptible to **XSS attacks**, allowing **cookie theft or unauthorized redirects**
Personally Identifiable Information (PII) Exposure	Data Security	PII Disclosure	-	Critical	Attackers can extract sensitive user details like **SSNs, phone numbers, and card details**, increasing risks of **identity theft**

5. Mitigation

5.1. Regular Expression Denial of Service (ReDos) - Mitigation

The fix for this vulnerability is simply updating to the latest patches such as 0.7.33 / 1.0.33. Since all the versions prior the above version are vulnerable, highly recommended to move to a better version.

5.2. Sub domain enumeration with fierece

Using firewalls to detect traffic of domain enumeration can help to somewhat stop the attacks from happening. Also make sure hide or delete unwanted domains to minimize unwanted threats

5.3. XSS

XSS can be fixed by taking many actions such as,

- Having a all the security headers which help to block xss attacks
- Sanitize users input from both client and sever
- Adding whitelists
- Have all scripting libraries verified and up to date

5.4. PII (personally identifiable information)

This can be mitigated through encrypting the data without using plain text for user and server communication. And also these types of information should not be stored in plain text as well.

6. Conclusion

In conclusion we can see that Victoria's secrets do have vulnerabilities in there systems but it is not in that critical. Users can have a somewhat trust in the web page. But better to have the vulnerabilities fixed.