

Sri Lanka Institute of Information Technology



Individual Assignment

Bug Bounty Report

Web Security - IE2062


BSc Honors in Information Technology Specializing in Cyber Security

CASE STUDY NAME	BUG BOUNTY Report 08
CAMPUS/CENTER	SLIIT KANDY UNI


Student Details




	Student Registration Number	Student Name
1	IT23222854	JAYASINGHE B. I

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 Targets ✓ In scope

www.insigniafinancial.com.au	Website Testing
www.mlc.com.au	Website Testing
www.bridges.com.au	Java jQuery Website Testing
www.sfg.com.au	Website Testing
www.mlc.com.au	Website Testing
www.antaescapital.com.au	Website Testing
hub.anzsmartchoice.com.au	Website Testing
dataservices.ioof.com.au	Website Testing
ddo.ioof.com.au	RequireJS ReactJS Website Testing
www.ioof.com.au	Moment.js Backbone ASP.NET +3

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://www.victoriassecret.com/us/>
- Category – Vulnerability Disclosure Program (VDP)
- Type – Retail Company






Shipping outside United States / U.S. Territory?

You are currently shopping on the United States / U.S. Territory website. Visit your local website for the most relevant promotions and products catered for your region.

[CHOOSE LOCATION](#)
[STAY ON THIS SITE](#)



SIGN UP FOR EMAILS & TEXTS

HELP

[Customer Service](#)
[Live Chat](#)
[About VS Credit Card](#)
[Find a Store](#)
[Careers](#)

ORDERS & RETURNS

[Order Status](#)
[Shipping Information](#)
[Return Policy](#)


SERVICES

[Store Offer & Events](#)
[VS & PINK Creator Program](#)
[Discover](#)
[Get the iOS App](#)
[Get the Android App](#)
[Pay My Bill](#)

© 2025 Victoria's Secret. All Rights Reserved.

[Terms of Use](#) |
 [Privacy & Security](#) |
 [Report a Vulnerability](#) |
 [California Privacy Rights](#) |
 [Do Not Sell or Share My Personal Information](#) |
 [Modern Slavery Transparency Statement](#) |
 [Ad Preferences](#) |
 [Careers](#) |
 [Product Catalog](#) |
 [Site Map](#)

Ready to get rewarded?



1. Sensitive Data Exposure

1.1 Retire.js

Retire.js
☒ Enabled ☐ Show unknown

ua-parser-js	1.0.2	Found in https://www.victoriassecret.com/assets/m3836-0l7aytFSTwKVDImIg7AoUg/vendor/signals-sdk-5.2.9.js - Vulnerability info: High ReDoS Vulnerability in ua-parser-js version CVE-2022-25927 GHSA-fhg7-m89q-25r3
--------------	-------	--

Summary for the above vulnerabilities.

Library	Version	Vulnerability Description	Severity	Mitigation Strategy
ua-parser-js	1.0.2	Regular Expression Denial of Service (ReDoS)	High	Upgrade to ua-parser-js 1.0.35 or later for patched security.
				Limit input complexity for regex processing to prevent excessive load.
				Consider alternative parsing libraries if upgrading is not feasible.

2.1. Netcraft

The Netcraft tool provides information about a website's infrastructure including,

- Web server
- Operating system
- Hosting provider
- SSL certificate details.

Attackers can use this information for reconnaissance purposes to identify potential vulnerabilities and plan targeted attacks. Mitigation strategies include keeping software up to date, using secure hosting providers, and implementing strong SSL/TLS configurations.

Background

Site title	Victoria's Secret: Luxury Bras, Knickers, Lingerie, Sleepwear & Beauty	Date first seen	April 1999
Site rank	12827	Primary language	English
Description	Iconic and glamorous – Victoria's Secret is the world's go-to label for giving women everywhere one-of-a-kind lingerie, sleep, beauty and accessories.		

Network

Site	https://www.victoriassecret.com	Domain	victoriassecret.com
Netblock Owner	Cloudflare, Inc.	Nameserver	lv.ns.cloudflare.com
Hosting company	Cloudflare	Domain registrar	markmonitor.com
Hosting country	US	Nameserver organisation	whois.cloudflare.com
IPv4 address	104.18.43.77	Organisation	Victoria's Secret Stores Brand Management, LLC, United States
IPv4 autonomous systems	AS13335	DNS admin	dns@cloudflare.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled
Reverse DNS	Unknown		

IP delegation

Web Security - IE2062**Year 2 Semester 2 - 2025****SSL/TLS**

Assurance	Organisation validation	Perfect Forward Secrecy	
Common name	*victorlasecret.com	Supported TLS Extensions	RFC8446 key share, RFC8446 supported versions, RFC4366 server name, RFC7301 application-layer protocol negotiation, RFC4366 status request
Organisation	VS Service Company, LLC	Application-Layer Protocol Negotiation	h2
State	Ohio	Next Protocol Negotiation	Not Present
Country		Issuing organisation	Sectigo Limited
Organisational unit	Not Present	Issuer common name	Sectigo RSA Organization Validation Secure Server CA
Subject Alternative Name	*victorlasecret.com, victorlasecret.com	Issuer unit	Not Present
Validity period	From Feb 12 2025 to Feb 12 2026 (12 months)	Issuer location	Salford
Matches hostname		Issuer country	
Server	cloudflare	Issuer state	Greater Manchester
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://cf.sctigo.com/SectigoRSAOrganizationValidationSecureServerCA.crl
Protocol version		Certificate Hash	twexOncLNol2P9aYhY9Wu5efw
Public key length	2048	Public Key Hash	e46b13b29cd8648536b7baa044f733e93c45232e55167e0886d0896b3c4c785
Certificate check		OCSP servers	http://ocsp.sctigo.com
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	Certificate valid
Serial number	0x35c2c7d772dd8dc38d1cda913fcb	OCSP data generated	Apr 27 23:43:05 2025 GMT
Cipher	TLS_AES_256_GCM_SHA384	OCSP data expires	May 4 23:43:04 2025 GMT
Version number	0x02		

Certificate Transparency**Signed Certificate Timestamps (SCTs)**

Source	Log	Timestamp	Signature Verification
Certificate	Unknown 1pdrv1P9Y163394d9uhtC9+wa9X2j9PC2kaKPa/KqCY=	2025-02-12 09:16:52	Unknown
Certificate	Unknown GYbixy1qbu/66A294KX8B8karOLX1xDe70X0BLSVftx90=	2025-02-12 09:16:52	Unknown
Certificate	Unknown yz13FY18NKFEX1v83Fv3zvKalc3KcaFhZDLFRMU0c=	2025-02-12 09:16:52	Unknown

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

[More information about SSL version 3 and the POODLE vulnerability.](#)

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. [More information about Heartbleed detection.](#)

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Strict-Transport-Security (including subdomains)	No description	chatgpt.com , accounts.google.com , docs.google.com
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	teams.microsoft.com
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	chat.deepseek.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	
Content Security Policy	Detect and mitigate attacks in the browser	

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	www.amazon.com , webmail.vincichoteles.com , mail.google.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

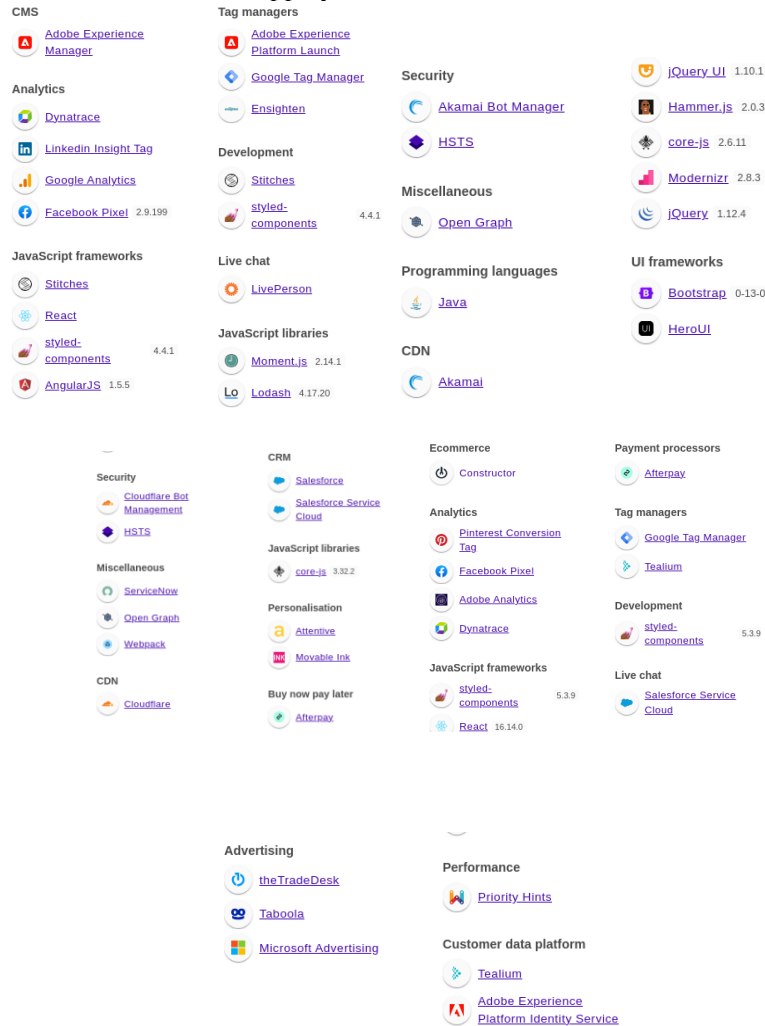
CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	mail.yahoo.com
Embedded	Styles defined within a webpage	www.amazon.it , www.amazon.es , www.amazon.ca

2.2 Wappalyzer

Here are the results of the Wappalyzer detect



2. Multi Tool Web Vulnerability Scanner

2.1 Rapidscan

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools]
$ cd rapidscan/

(binosh@BINZ)-[~/Desktop/WS Assingment/Tools/rapidscan]
$ sudo python3 rapidscan.py https://www.victoriassecret.com/us/
```

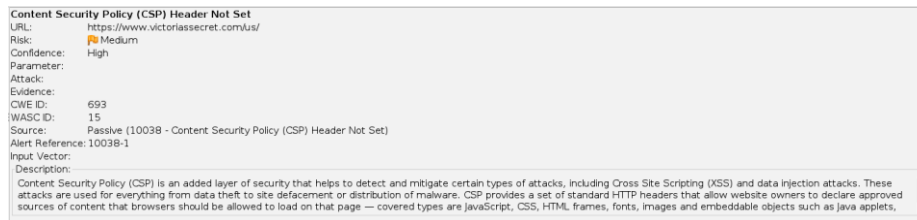
Out of 80 vulnerabilities checked for <https://www.victoriassecret.com/us/> **4 vulnerabilities were detected**

```

Vulnerability Threat Level
[Medium] does not have an IPv6 Address. It is good to have one.
Vulnerability Definition
Not a vulnerability, just an informational alert. The host does not have IPv6 support. IPv6 provides more security as IPsec (responsible for CIA - Confidentiality, Integrity and Availability) is incorporated into this model. So it is good to have IPv6 support.
Vulnerability Remediation
It is recommended to implement IPv6. More information on how to implement IPv6 can be found from this resource, https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implementation_CS.html

```

2.2 OWASP



Detected Vulnerability: CSP Header Not Set

The missing Content-Security-Policy Header introduces a medium security risk, making the application vulnerable to Cross-Site Scripting (XSS) and content injection threats. Immediate implementation of CSP is recommended to enforce security measures and reduce exposure to attacks.

- Risk Level: Medium
- Confidence Level: High
- Vulnerability Type: Missing Content Security Policy Header
- CWE ID: 693 – Protection Mechanism Failure
- WASC ID: 15 – Application Misconfiguration
- Alert Reference: 10038-1

Details of Vulnerability

- Key Parameter Affected: Content-Security-Policy
- Attack Vector: None
- Evidence: CSP missing from HTTP headers
- Source: Passive scan (10038 - CSP Header Not Set)
- Issue Description: The web server lacks a CSP header, increasing risks related to content injection and malicious code execution

Impact Assessment

Potential Risk

- Increased vulnerability to Cross-Site Scripting (XSS) attacks
- Higher risk of Clickjacking and unauthorized content framing
- Possible exposure to data injection attacks

Recommended Remediation


Short-Term Fixes

- Define and set a Content-Security-Policy header to restrict allowed content sources
- Enforce strict policies to block unauthorized JavaScript and iframe embedding

Long-Term Fixes

- Conduct periodic security audits to validate CSP configurations
- Strengthen CSP directives such as default-src 'none' for improved protection
- Implement secure response headers to mitigate common web attacks

Web Security - IE2062**Year 2 Semester 2 - 2025**

Content Security Policy (CSP) Header Not Set
URL: <https://www.victoriassecret.com/us/>
Risk:  Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets.

The missing Content-Security-Policy Header introduces a medium security risk, increasing exposure to Cross-Site Scripting (XSS) and unauthorized resource loading vulnerabilities. Immediate CSP implementation is highly recommended to strengthen security defenses.

Detected Vulnerability: CSP Header Not Set

- **Risk Level:** Medium
- **Confidence Level:** High
- **Vulnerability Type:** Missing Content Security Policy Header
- **CWE ID:** 693 – Protection Mechanism Failure
- **WASC ID:** 15 – Application Misconfiguration
- **Alert Reference:** 10309-3

Details of Vulnerability

- **Key Parameter Affected:** Content-Security-Policy
- **Attack Vector:** Not applicable
- **Evidence:** CSP missing from HTTP headers
- **Source:** Passive scan (10309 - CSP Header Not Set)
- **Issue Description:** CSP is an additional security layer that helps detect and mitigate certain types of attacks, including **Cross-Site Scripting (XSS)** and **data injection attacks**. The absence of this header increases the risk of **malicious content execution and unauthorized resource loading**.

Impact Assessment**Potential Risk**

- Increased vulnerability to **Cross-Site Scripting (XSS)** attacks
- Higher risk of **Clickjacking** and unauthorized content framing
- Possible exposure to **data injection attacks and unauthorized scripts**

Recommended Remediation**Short-Term Fixes:**

- Implement and set a **Content-Security-Policy** header to restrict allowed content sources
- Define explicit directives to block unauthorized script execution
- Use frame ancestors 'none' to prevent Clickjacking risks

Long-Term Fixes

- Conduct periodic **CSP audits** to validate configurations
- Strengthen CSP directives such as default-src 'none' for improved protection
- Implement **secure response headers** to mitigate common web attacks

Web Security - IE2062

Year 2 Semester 2 - 2025

Missing Anti-clickjacking Header	
URL:	https://www.victorlasecret.com/us/vs/insider
Risk:	Medium
Confidence:	Medium
Parameter:	x-frame-options
Attack:	
Evidence:	
CWE ID:	1021
WASC ID:	15
Source:	Passive (10020 - Anti-clickjacking Header)
Alert Reference:	10020-1
Input Vector:	
Description:	The response does not protect against 'Clickjacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Detected Vulnerability: Anti-Clickjacking Header Not Set

The absence of anti-clickjacking headers introduces a medium security risk, potentially allowing malicious UI manipulations that could lead to fraudulent interactions and user deception. Immediate remediation through X-Frame-Options and CSP enhancements is advised to mitigate vulnerability.

- **Risk Level:** Medium
- **Confidence Level:** Medium
- **Vulnerability Type:** Lack of Clickjacking Protection
- **CWE ID:** 1021 – Clickjacking
- **WASC ID:** 15 – Application Misconfiguration
- **Alert Reference:** 10020-1

Details of Vulnerability

- **Key Parameter Affected:** X-Frame-Options
- **Attack Type:** Clickjacking
- **Evidence:** Missing X-Frame-Options or Content-Security-Policy: frame-ancestors directive
- **Source:** Passive scan (10020 - Anti-Clickjacking Header)
- **Issue Description:** The response does not protect against **Clickjacking attacks**, which can allow malicious sites to **embed the page in an iframe** and trick users into interacting with concealed UI elements.

Impact Assessment

Potential Risk

- Unauthorized interaction leading to **account compromise**
- Manipulation of user inputs for **phishing and social engineering attacks**
- Increased risk of **fraudulent transactions** through embedded malicious interfaces

Recommended Remediation

Short-Term Fixes:

- Set **X-Frame-Options** HTTP response header to DENY or SAMEORIGIN
- Implement **Content-Security-Policy (CSP) with frame-ancestors** to restrict embedding

Long-Term Fixes:

- Conduct **regular security audits** to verify correct header configurations
- Strengthen CSP directives for **cross-origin iframe embedding protection**
- Ensure clickjacking defenses align with **OWASP security best practices**

>	Content-Security-Policy (CSP) Header Not Set (9992)
>	Missing Anti-clickjacking Header (292)
>	Cookie No HttpOnly Flag (24000)
>	Cookie Without Secure Flag (23994)
>	Cookie with SameSite Attribute None (3523)
>	Cookie without SameSite Attribute (23997)
>	Cross-Domain JavaScript Source File Inclusion (14500)
>	Timestamp Disclosure - Unix (494)
>	X-Content-Type-Options Header Missing (7399)
>	Information Disclosure - Suspicious Comments (1398)
>	Loosely Scoped Cookie (9728)
>	Modern Web Application (9913)
>	Re-examine Cache-control Directives (7407)
>	Retrieved from Cache (29)
>	User Controllable HTML Element Attribute (Potential XSS) (2038)

3. Injection

3.1. XSSStrike

Need to install requirements before using the xssstrike.py.

Python3 xssstrike.py -u https://www.vicctoriassecret.com/us/ --crawl

```

[www@localhost ~]$ cd /Desktop/NS Assignment/Tools/XSSStrike/
$ python3 xssstrike.py -u https://www.vicctoriassecret.com/us/

XSSStrike v3.1.3

[-] Checking for OW vulnerabilities
[-] Potentially vulnerable objects found

1. [[{"url": "https://www.vicctoriassecret.com/us/", "appType": "is-app", "appPlatform": "ios", "appBrand": "pn", "appVersion": "1.0.0", "appStatus": "active", "appDescription": "A mobile application for iOS devices."}, {"url": "https://www.vicctoriassecret.com/us/", "appType": "is-app", "appPlatform": "android", "appBrand": "pn", "appVersion": "1.0.0", "appStatus": "active", "appDescription": "A mobile application for Android devices."}]]

2. No parameters to test.

[www@localhost ~]$ cd /Desktop/NS Assignment/Tools/XSSStrike/
$ python3 xssstrike.py -u https://www.vicctoriassecret.com/us/ --crawl

XSSStrike v3.1.3

[-] Crawling the target
[-] Potentially vulnerable objects found at https://www.vicctoriassecret.com/us/

1. [[{"url": "https://www.vicctoriassecret.com/us/", "appType": "is-app", "appPlatform": "ios", "appBrand": "pn", "appVersion": "1.0.0", "appStatus": "active", "appDescription": "A mobile application for iOS devices."}, {"url": "https://www.vicctoriassecret.com/us/", "appType": "is-app", "appPlatform": "android", "appBrand": "pn", "appVersion": "1.0.0", "appStatus": "active", "appDescription": "A mobile application for Android devices."}]]

2. Progress: 2/24-map

```

A one potential vulnerability could be found from this tool. The JavaScript code had resulted.

```

({}) => {
  const cookie = document.cookie;
  const index = cookie.indexOf("APPTYPE="); // Finding the index of "APPTYPE=" in the cookie

  // Adding classes to the document element based on the presence of "APPTYPE=" in the cookie
  if (index >= 0) {
    const classes = document.documentElement.classList;
    classes.add("is-app"); // Adding "is-app" class
    const startIndex = index + 8; // Moving to the position after "APPTYPE="
    const substring = cookie.slice(startIndex); // Extracting substring after "APPTYPE="
    let appType = "";

    if (substring.startsWith("IOSHANDHELD")) {
      classes.add("is-app-ios"); // Adding "is-app-ios" class
      dataset.appPlatform = "ios";
    } else if (substring.startsWith("ANDROIDHANDHELD")) {
      classes.add("is-app-android"); // Adding "is-app-android" class
      dataset.appPlatform = "android";
    } else {
      appType = cookie.slice(startIndex + 16); // Slicing the part after "ANDROIDHANDHELD"
    }

    if (appType.startsWith("VS")) {
      dataset.appBrand = "vs";
    } else if (appType.startsWith("PN")) {
      dataset.appBrand = "pn";
    }

    if (dataset.appPlatform && dataset.appBrand) {
      dataset.appType = dataset.appPlatform + "-" + dataset.appBrand; // Constructing appType like "ios-vs" or "android-pn"
    }
  }

  // Checking for "isNativeShopTabEnabled" in URL or sessionStorage and adding class accordingly
  if ("true" === new URL(window.location.href).searchParams.get("isNativeShopTabEnabled") || "true" === sessionStorage.getItem("isNativeShopTabEnabled")) {
    document.documentElement.classList.add("is-native-shop-tab-enabled");
    sessionStorage.setItem("isNativeShopTabEnabled", "true");
  }

  // Parsing server timings from performance entries and setting properties in dataset
  if (performance.getEntriesByType("server-timing")) {
    for (const { name, description } of performance.getEntriesByType("server-timing")) {
      if (name === "isrStatus") {
        dataset.isrStatus = description;
      } else if (name === "basicStatus") {
        dataset.basicStatus = description;
      }
    }
  }
}
})();

```

This JavaScript code is designed to modify the behavior and appearance of a website based on certain conditions, such as the presence of specific cookies or URL parameters, and performance metrics.

3.2 Uniscan

```
root@kali:~/Desktop/Assignment/Tools#
root@kali:~/Desktop/Assignment/Tools# sudo uniscan -u https://www.victoriassecret.com/us/ -d -q -s -r
Unknown option: s
#####
# uniscan project #
# http://uniscan.sourceforge.net/ #
#####
v. 0.3

Scan date: 2-5-2025 1:45:47
#####
Domain: https://www.victoriassecret.com/us/
Server: Cloudflare
IP: 104.18.43.77
#####
Directory check:
[+] Skipped because https://www.victoriassecret.com/us/uniscan337/ did not return the code 404
#####
Crawler Started:
[+] Plugin name: E-mail Detection v.1.1 Loaded.
[+] Plugin name: Upload Form Detect v.1.1 Loaded.
[+] Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
[+] Plugin name: External Host Detect v.1.2 Loaded.
[+] Plugin name: FCKeditor upload test v.1 Loaded.
[+] Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
[+] Plugin name: Code Disclosure v.1.1 Loaded.
[+] Plugin name: phpinfo() Disclosure v.1 Loaded.
[+] [+] Crawling finished, 1 URL's found!

E-mails:

File Upload Forms:
```

uniscan -u https://www.victoriassecret.com/us/ -qd

qd → To enable directory and dynamic checks.

The uniscan results are as below.

```
Crawler Started:
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
[+] Crawling finished, 1 URL's found!
```

The above result is about detected plugins or features that may be vulnerable to exploitation. It is noticeable that older versions of some services are being used in this domain. And, the below potential issues were found suggesting that the website may expose email addresses insecurely, potentially leading to spam or phishing attacks. It also indicates the presence of an upload form that could be exploited to upload malicious files, as well as making requests to external hosts, which could pose a security risk if not properly managed.

4. Firewall Detection

4.1. Wafw00f

```
(binosh@BIN2) ~/Desktop/WS_Assingment/Tools
$ wafw00f https://www.victoriassecret.com/us/
The United States / U.S. Territory
shopping on the United States / U.S. Territory
promotions and products catered for your region.

{
  "Woof!"
}

{
  "O";
  "C";
  "V";
}

{
  "ENGLISH" | USD
}

{
  "PANTIES"
}

{
  "SLEEP"
}

{
  "SWIM"
}

{
  "ACTIVE"
}

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

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

Could be detected that Cloudflare is being used as the firewall in this site. There is a known vulnerability for Cloudflare Firewall. Need to be alert about this and have to update the firewall regularly.

How to mitigate the Vulnerability

- Apply security patches by updating to the most recent version of Angular.
- Verify and clean user input to avoid doing too much backtracking.
- To stop unwanted script execution, use stringent Content Security Policy (CSP) headers.
- Switch to an updated, security-patched version of Angular.
- Update to jQuery UI 1.13.2 or later, as this problem has been fixed.
- Before transferring user input to UI elements, sanitize it.
- Update to at least jQuery 3.5.0.
- For security patches, update to Moment.js 2.29.2 or later.
- Before sending locale inputs to Moment.js routines, clean them up.
- Limit modifications to dynamic locales to trusted values only.
- Before sending user input to DOM manipulation routines, clean it up.
- Use CSP headers to prevent malicious scripts from running.

Proof of report submission.



Victoria's Secret - VDP Pro has received
WS Assingment

Thank you Binosh ,

We have received your Bugcrowd submission for engagement
victoriasecret-vdp.

Submission Details

Submitted
04 May 2025 19:29:51 UTC

Submission ID
208f2f4b-bf98-44c1-bc5d-400c5a54b3e5

VRT
Server Security Misconfiguration > Lack of Security Headers > X-Webkit-
CSP

[View Submission Details](#)