Sri Lanka Institute of Information Technology

Report – Ulta Beauty

IE2062 - Web security

Submitted by:

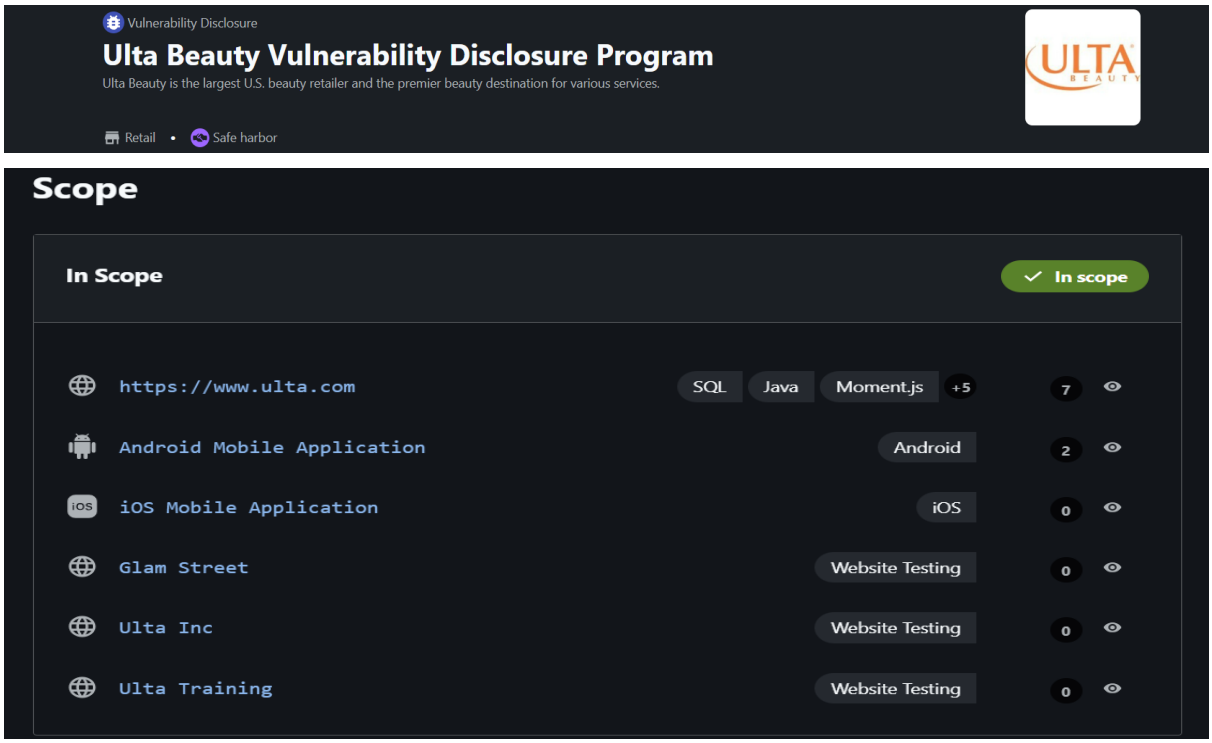
Student Registration Number	Student Name
IT23253476	Bandara S.M.S.N

Date of submission

05/05/2025

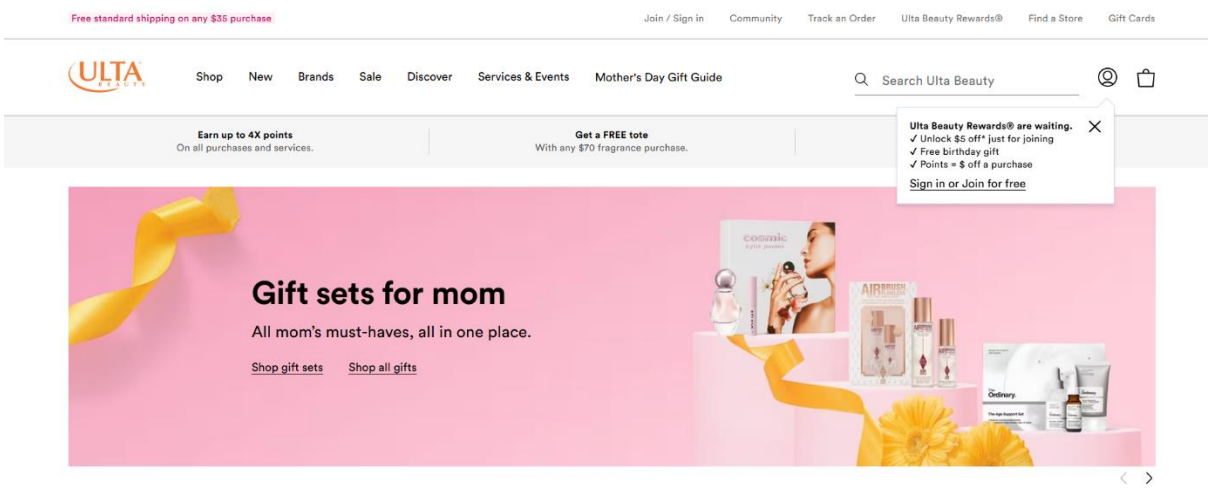
Table of Contents

1. Domain: https://www.ulta.com/



- Link: https://www.ulta.com/
- Category: Vulnerability Disclosure Program (VDP)
- Type: Retail

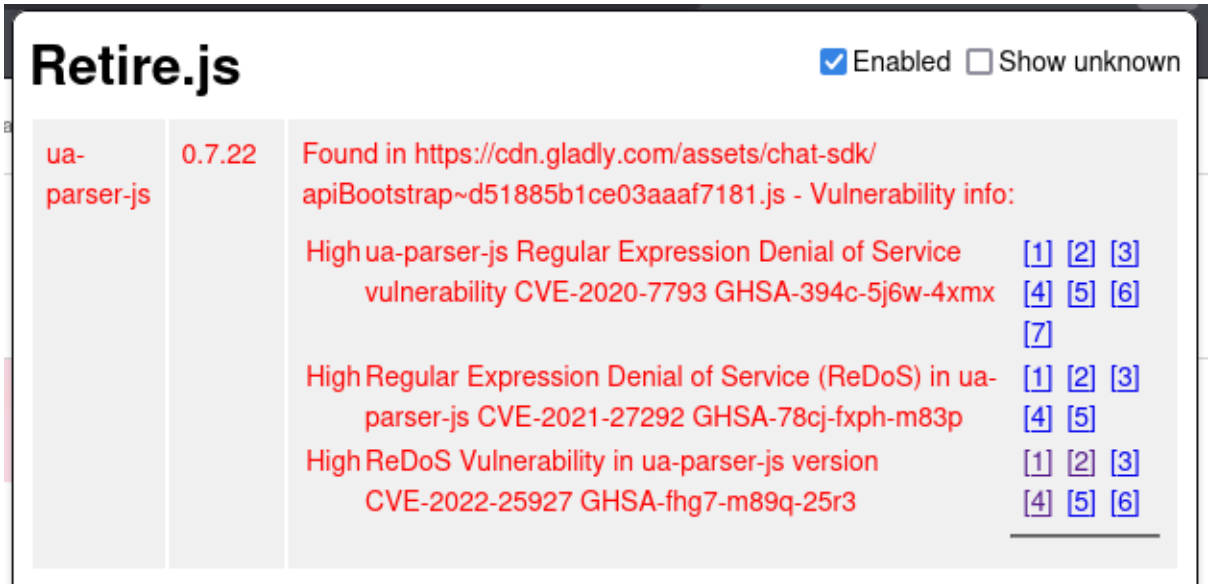
UI of the website is as follows



2. Vulnerability Scanning

2.1. Retire.js

Retire.js is browser extension which aids to find vulnerable java script libraries and their versions. Retire.js also provides a description of the vulnerability found. It also provides links to articles from popular sources about the vulnerability.

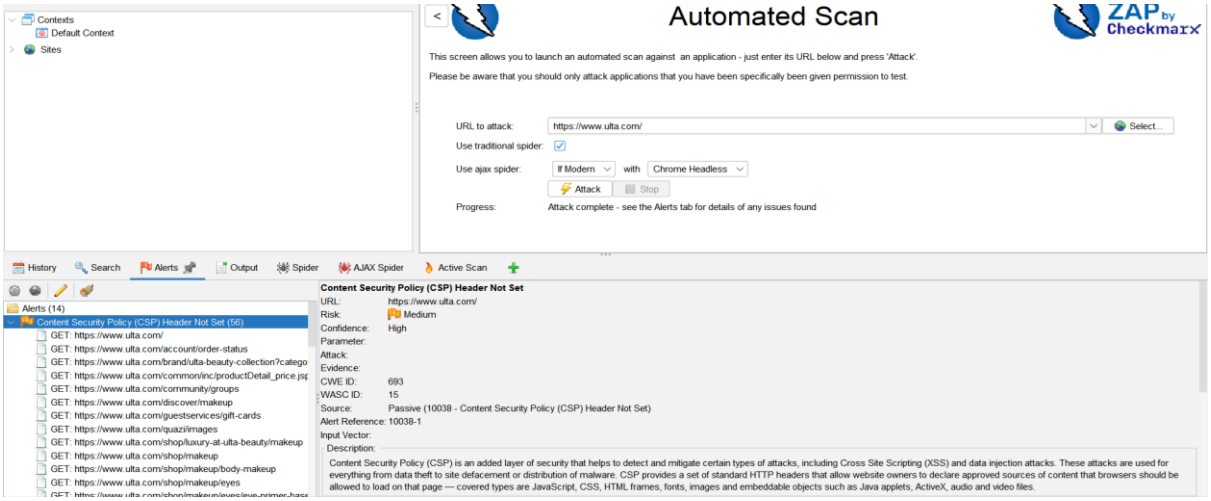


This scan indicates that there is a vulnerability in ua-parser-js which is a form of denial-of-service attack.

To test this tool like **HULK** can be used to send continuous requests to the webserver. After performing HULK on this web application, it gives us response code 500. Which might be a result of firewall blocking the attack.

2.2. OWSAP ZAP

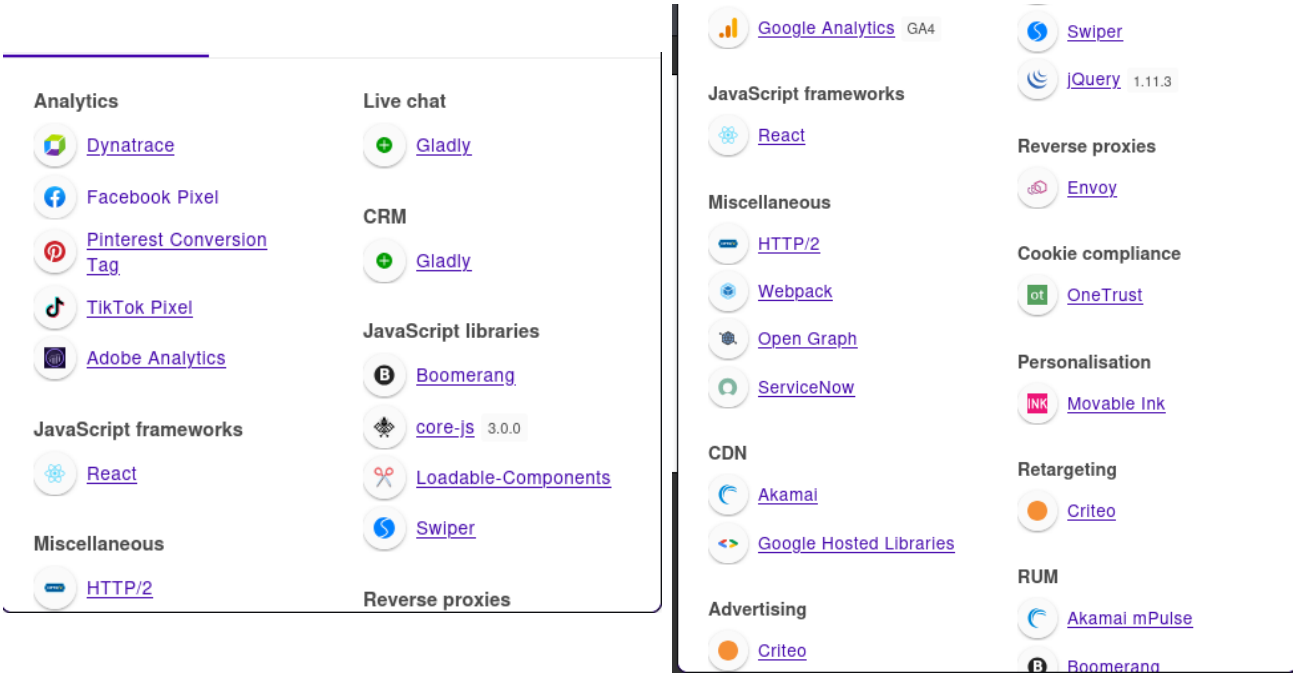
OWSAP ZAP is vulnerability scanner that allows the user to scan the website by crawling through the website. After doing the scan the following vulnerability is shown



It indicates that the website has a **missing content security header** which is used to block cross site scripting attacks and injection attacks.

2.3. Wappalyzer

This tool will give the technologies used and their version numbers. This could be essential for finding bugs with outdated versions



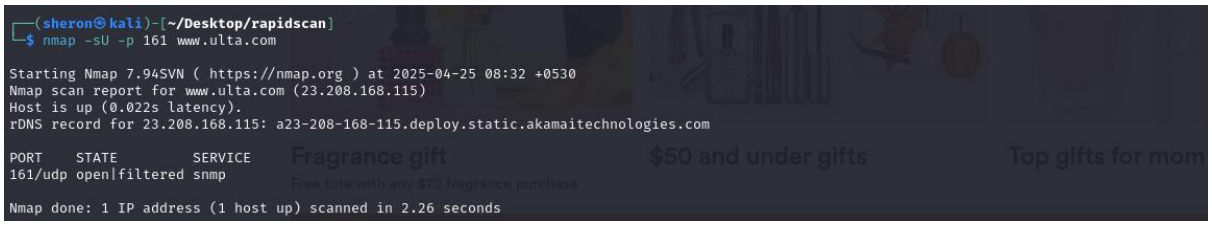
After inspection it is found out that the JavaScript library jQuery 1.11.3 is related to cross site scripting attacks as well as prone to prototype pollution. The other library which is core-js 3.0.0 is an older version that could be potentially vulnerable to prototype pollution. It was also found that HTTP/2 is vulnerable to CVE-2023-44487 which is a denial-of-service attack.

2.4. Rapid Scan

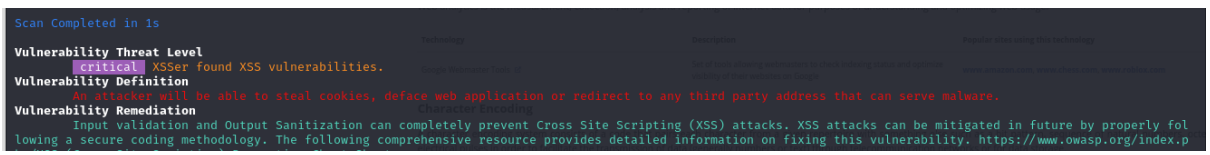
Rapid scan in a multi vulnerability scanner. It allows a combination of 82 scanners to look for vulnerabilities. And the scan gave this vulnerability it indicates a medium level threat in SNMP service. This can expose community strings to unauthorized access, allowing hackers to extract sensitive information from the user.

First vulnerability - The scanner has found a vulnerability regarding a open SNMP service which help the attacker to gather information from headers

This can be further validated by a **nmap** scan looking for the snmp service specifically



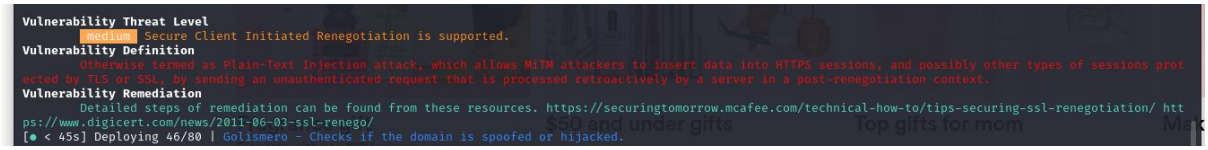
Second Vulnerability - vulnerability regarding a **cross-site scripting** attack. It used XSSer which is tool to exploit xss related vulnerabilities. It indicates that the vulnerability in a critical level



Let's use **XSStrike** to see if the page has vulnerabilities in XSS.

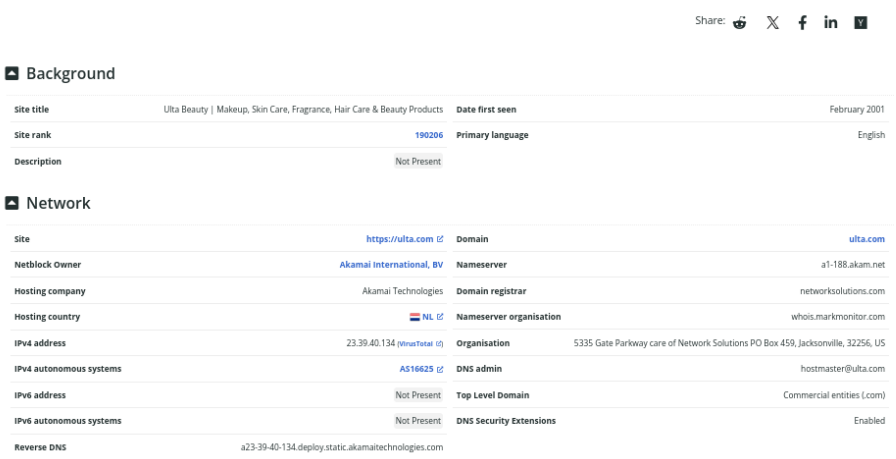
The scan was stopped by the firewall. Therefore, cannot determine if xss can or cannot be done. Further testing is required.

Third Vulnerability - Another vulnerability discovered by rapid scanner. This is medium level threat. Which is a **TSL/SSL renegotiation** vulnerability. Also known as a plain text injection attack. This vulnerability allows man in the middle attacker to inject data into an https session. Specially during an SSL or TSL session, renegotiation is a process where either client or server can request to reset the encryption parameters



2.5. Netcraft

The Netcraft Site Report tool can be utilized for site mining purposes. Following its analysis, the information below was gathered regarding the site



Site Technology (fetched yesterday)

HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Envoy	Open source proxy	www.bbc.com, www.ebay.co.uk, www.nytimes.com

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Java Servlet	A server-side Java programming language class	www.ixl.com, www.arco.co.uk, www.alibaba.com
SSL	A cryptographic protocol providing communication security over the Internet	www.linkedin.com, www.microsoft.com, www.deepl.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Session Storage	*No description*	www.ironfx.com, www.bankofamerica.com, www.icloud.com
Local Storage	*No description*	www.amazon.ca, www.amazon.it, www.aliexpress.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	

Web Stats

Web analytics is the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimizing web usage.

Technology	Description	Popular sites using this technology
Google Webmaster Tools	Set of tools allowing webmasters to check indexing status and optimize visibility of their websites on Google	www.amazon.com, www.chess.com, www.roblox.com

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	www.tiktok.com, www.twitch.tv, www.amazon.de

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.amazon.com.mx, www.expedia.com, www.novasports.gr

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
X-Frame-Options Deny	Prevents the web page being embedded in a frame	www.bbc.co.uk, mytime-lite.aka.corp.amazon.com, app.powerbi.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	erp.fxpro.com, chat.deepseek.com

2.6. Nmap scan

By using the nmap scan we can see what ports are open and what services are running on each port. Understanding what the target is doing is crucial when conducting attacks. Following are the ports and the services running on them.

3. Vulnerabilities Found

The following are the most severe vulnerabilities found in the web application.

3.1. ReDos vulnerability

Form the retire.js scan that we did, we discovered a vulnerability regarding a Regular Expression Denial of Service (ReDos) vulnerability. This vulnerability belongs to the family of the DoS attacks. DoS make the systems unusable for legitimate users. This could happen due to many reasons.

The ReDos that is in the web site is caused by the ua-parser-js package. According to the snyk security it has severity of 7.5 which is high. The following is a proof of concept extracted from the snyk security web site.

Proof of Concept by Miguel de Moura

```
 jsconst ua_parser = require('ua-parser-js');const N_SIZE =
5000;const MALICIOUS_UA = `android;;Trio${' '.repeat(N_SIZE)}
buil`;// Trigger ReDoSua_parser(MALICIOUS_UA);
```

If the above code is saved as script and executed in a controlled environment after installing the vulnerable version. You can see the increase in resource usage.

4. Mitigation methods

4.1. ReDoS

This has an easy fix. You simply need to upgrade to the latest version the js library using. Also, you can use fire walls to detect the ReDoS attacks.

4.2. Snmp service vulnerability

This vulnerability can be removed by many ways. First, you can use a fire wall to block suspicious traffic and eliminate the risk of being attacked. Furthermore, if you don't use the service you can close the service entirely making it much safer.

5. Vulnerable Components

The following table is a summarization of the components that were found vulnerabille

Component	Type	Vulnerability	Severity	Impact
ua-parser-js	JavaScript Library	Regular Expression Denial of Service (**ReDoS**)	High (7.5)	Can cause excessive resource consumption, leading to denial of service
jQuery 1.11.3	JavaScript Library	**Cross-Site Scripting (XSS)** & **Prototype Pollution**	Medium to High	Allows attackers to inject malicious scripts & manipulate object properties
core-js 3.0.0	JavaScript Library	**Prototype Pollution**	Medium	Can enable modification of global JavaScript properties, leading to unexpected behavior
HTTP/2	Network Protocol	**CVE-2023-44487 - Rapid Reset Attack (DoS)**	High	Can overwhelm the target server, causing denial of service
SNMP Service	Network Service	**Exposure of community strings to unauthorized access**	Medium	Attackers can extract sensitive information from network devices
TLS/SSL Renegotiation	Encryption Protocol	**Man-in-the-Middle (MITM) / Plaintext Injection Attack**	Medium	Allows an attacker to insert data into encrypted sessions
Missing CSP Header	Security Configuration	**Increased risk of XSS & injection attacks**	High	Allows script injection that can compromise users

6. Conclusion

In the domain www.ultas.com we can observe some vulnerabilities. Even though they are not critical they must be addressed. And the cause for the vulnerability is simply negligence of the site maintainers to upgrade to new versions.