

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 05
CAMPUS/CENTER	SLIIT KANDY UNI

Student Details

	Student Registration Number	Student Name
1	IT23222854	JAYASINGHE B. I

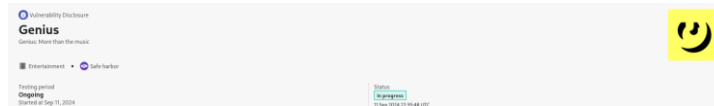
Table of Contents

Domain – https://genius.com/signup	4
1. Sensitive data Exposure	5
1.1 Retire.js	5
Summary fo the above vulnerabilities.	5
1.2 Netcraft	7
1.3 Wappalyzer	9
2. Injection	10
2.1 Uniscan	10
3. Firewall Detection	11
3.1 Wafw00f	11
4. Multi Tool Web Vulnerability Scanning	11
4.1 Rapidscan	11
4.3 OWASP	12
How to mitigate the above Vulnerability	13
Proof of Report Submission	13

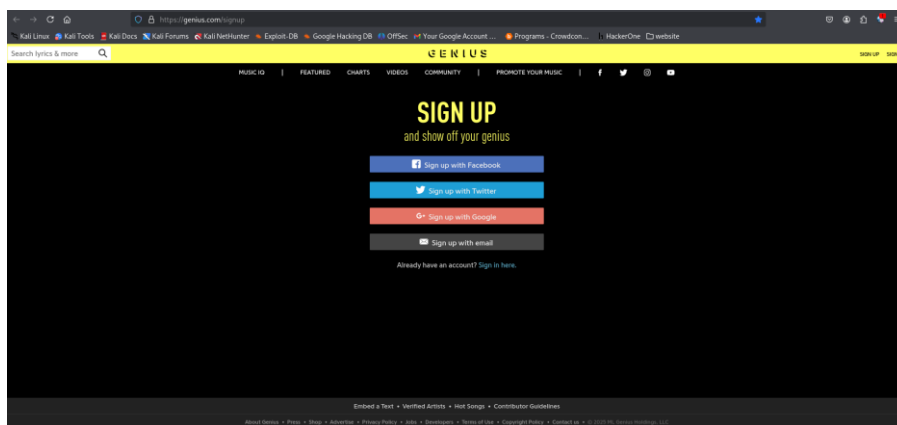
Web Security - IE2062

Year 2 Semester 2 - 2025

Domain – <https://genius.com/signup>



- Link - <https://genius.com/signup>
- Category – Vulnerability Disclosure Program (VDP)
- Type – Music promotes website



1. Sensitive data Exposure

1.1 Retire.js

Retire.js		Enabled <input checked="" type="checkbox"/> Show unknown <input type="checkbox"/>
angularjs	1.6.6	<p>Found in https://assets.genius.com/javascripts/compiled/sprockets-64091e49231fa6ab1ae0a62d2e69dd4.js - Vulnerability info:</p> <p>Low XSS through SVG if enableSvg is set 48 [1] [2]</p> <p>High Prototype pollution 47 GHSA-89mq-4x47-5v83 CVE-2019-10768 [1] [2]</p> <p>Medium XSS via JQLite DOM manipulation functions in AngularJS GHSA-5cp4-mrw2-j8xw [1]</p> <p>Medium XSS may be triggered in AngularJS applications that sanitize user-controlled HTML snippets before passing them to JQLite methods like JQLite.prepend, JQLite.append, JQLite.replaceWith, JQLite.append, new JQLite and angular.element. CVE-2020-7676 GHSA-mhp6-pxh8-675 [1] [2]</p> <p>Medium angular vulnerable to regular expression denial of service via the \$resource service CVE-2023-26117 GHSA-2q3q-w9hr-q5gx [1]</p> <p>Medium angular vulnerable to regular expression denial of service via the angular.copy() utility CVE-2023-26116 GHSA-2vrf-h26j-jp5 [1]</p> <p>Medium Angular (deprecated package) Cross-site Scripting CVE-2022-25869 GHSA-prc3-vjfx-vhm9 [1]</p> <p>Medium angular vulnerable to regular expression denial of [1]</p>
chart.js	1.0.2	<p>Found in https://assets.genius.com/javascripts/compiled/sprockets-64091e49231fa6ab1ae0a62d2e69dd4.js - Vulnerability info:</p> <p>High Prototype pollution in chart.js CVE-2020-7746 GHSA-hb8q-55f-x68w [1]</p>
jquery	1.7.2	<p>Found in https://assets.genius.com/javascripts/compiled/sprockets-64091e49231fa6ab1ae0a62d2e69dd4.js - Vulnerability info:</p> <p>Medium Selector interpreted as HTML CVE-2012-6708 11290 GHSA-2pq-qh3v-pgqw [1] [2] [3]</p> <p>Medium Versions of jquery prior to 1.9.0 are vulnerable to Cross-Site Scripting. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e. "<script> ", which results in the enclosed script logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser.</p> <p>## Recommendation</p> <p>Upgrade to version 1.9.0 or later. CVE-2020-7656 GHSA-q4m3-2j7h-17xw [1]</p> <p>Medium 3rd party CORS request may execute 2432 CVE-2015-9251 GHSA-ixmg-73gg-4p98 [1] [2] [3]</p>
moment.js	2.10.6	<p>Found in https://assets.genius.com/javascripts/compiled/sprockets-64091e49231fa6ab1ae0a62d2e69dd4.js - Vulnerability info:</p> <p>Medium reDOS - regular expression denial of service 2936 GHSA-87vw-r9j6-g5qv CVE-2016-4055 [1]</p> <p>Medium Regular Expression Denial of Service (ReDoS) 22 [1]</p> <p>High Regular Expression Denial of Service (ReDoS) CVE-2017-18214 GHSA-446m-mv8f-q348 [1] [2] [3]</p> <p>High This vulnerability impacts npm (server) users of moment.js, especially if user provided locale string, eg [1]</p>
		<p>Medium angular vulnerable to regular expression denial of service via the angular.copy() utility CVE-2023-26116 GHSA-2vrf-h26j-jp5 [1]</p> <p>Medium Angular (deprecated package) Cross-site Scripting CVE-2022-25869 GHSA-prc3-vjfx-vhm9 [1]</p> <p>Medium angular vulnerable to regular expression denial of service via the <input type="url"> element GHSA-qwqh-hm9m-p5hr CVE-2023-26118 [1]</p> <p>Low AngularJS allows attackers to bypass common image source restrictions CVE-2024-8373 GHSA-mqgm-c95h-x2p6 [1] [2] [3] [4] [5] [6] [7]</p> <p>High angular vulnerable to super-linear runtime due to backtracking CVE-2024-21490 GHSA-4w4v-5hc9-xrr2 [1] [2] [3] [4] [5] [6] [7]</p> <p>Low AngularJS allows attackers to bypass common image source restrictions CVE-2024-8372 GHSA-m9gf-397r-hwpg [1] [2] [3] [4] [5] [6]</p> <p>Low End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 54 [1]</p>
		<p>Low jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates 73 162 [1]</p> <p>Medium jQuery before 3.4.0, as used in Drupal,Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution CVE-2019-11358 4333 GHSA-ec3j-c64m-qhqq [1] [2] [3]</p> <p>Medium passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. html(), append(), and others) may execute untrusted code. CVE-2020-11023 4647 GHSA-jpcq-qgw6-v4j6 [1]</p> <p>Medium Regexp in its jQuery.htmlPrefilter sometimes may introduce XSS CVE-2020-11022 4642 GHSA-gx4-xj5-5px2 [1]</p>

Summary fo the above vulnerabilities.

Severity	Vulnerability	CVE/Advisory
Low	XSS through SVG if enableSvg is set	-
High	Prototype pollution	GHSA-6mj9-4x47-5v63, CVE-2018-16487
Medium	XSS via JQLite DOM manipulation functions	GHSA-5cp4-mrw2-j8xw
Medium	XSS triggered in AngularJS applications via HTML sanitization	GHSA-5cp4-mrw2-j8xw
Medium	JQLite allows parsing of AngularJS template elements, leading to XSS	GHSA-5cp4-mrw2-j8xw
Medium	Regular expression denial of service via \$resource service	CVE-2023-26117, GHSA-v6gp-9f3c-2mpw
Medium	AngularJS allows remote attackers to bypass Strict Contextual Escaping (SCE)	CVE-2015-8861

Web Security - IE2062
Year 2 Semester 2 - 2025

Severity	Vulnerability	CVE/Advisory
Medium	Regular expression denial of service via angular.copy()	CVE-2021-28116, GHSA-2vf4-h2c5-j95
Medium	Cross-site scripting in deprecated Angular package	CVE-2022-25840, GHSA-pc5j-vj8e-vh6m
Medium	Regular expression denial of service via	CVE-2023-26118, GHSA-h6mm-g9tw-6v5c
Low	Bypassing common image source restrictions in AngularJS	CVE-2020-8373, GHSA-4mmq-q5xh-kj2j6
High	Super-linear runtime due to backtracking	CVE-2021-0948, GHSA-6v4h-4w2c
Low	Another instance of image source restriction bypass	CVE-2020-8372, GHSA-3h9h-hagg
Low	End-of-Life: Long-term support for AngularJS discontinued	As of Dec 31, 2021

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)
jQuery	1.x, 2.x	End-of-Life—no longer receiving security updates	Low	-
jQuery	< 3.4.0	Object.prototype pollution in \$.extend(true, ...)	Medium	CVE-2019-11358, GHSA-c6qr-hxjj-8vh3
jQuery	< 3.5.0	XSS via elements from untrusted sources	Medium	CVE-2020-11022, GHSA-gxr4-xjj5-5px2
jQuery	< 3.5.0	DOM manipulation methods vulnerable to XSS	Medium	CVE-2020-11023, GHSA-q6qp-xvpc-9m8c
Moment.js	2.14.1	Regular Expression Denial of Service (ReDoS)	Medium	CVE-2022-31129, GHSA-wvhm-4x4m-9g3q
Moment.js	2.14.1	User-provided locale may lead to unintended execution	High	CVE-2022-43306, GHSA-xpf4-46gq-29qx

Library	Version	Found at URL	Vulnerability Description	Severity	Reference (CVE/GHSA)
Chart.js	1.0.2	Compiled Sprockets	Prototype Pollution in Chart.js	High	CVE-2020-7746, GHSA-h6mp-59jj-8f4r
jQuery	1.7.2	Compiled Sprockets	Selector interpreted as HTML vulnerability	Medium	CVE-2012-6708, GHSA-gxr4-xjjq-h6j6
			XSS via location.hash or location.search	Medium	CVE-2020-7656, GHSA-gxr4-xjjq-h6j6
			CORS misconfiguration enabling XSS	Medium	CVE-2015-9251, GHSA-mh6f-mr8p-5498

Web Security - IE2062**Year 2 Semester 2 - 2025****1.2 Netcraft****Background**

Site title	Genius	Date first seen	March 1996
Site rank	859	Primary language	English
Description	Not Present		

Network

Site	https://genius.com	Domain	genius.com
Netblock Owner	Cloudflare, Inc.	Nameserver	cody.ns.cloudflare.com
Hosting company	Cloudflare	Domain registrar	amazon.com
Hosting country	US	Nameserver organisation	whois.cloudflare.com
IPv4 address	104.18.23.208 (Whois)	Organisation	Identity Protection Service, PO Box 786, Hayes, UB3 9TR, United Kingdom
IPv4 autonomous systems	AS13335	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:0:0:0:0:6812:16d0	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS13335	DNS Security Extensions	Enabled
Reverse DNS	Unknown		

IP delegation**SSL/TLS**

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	genius.com	Supported TLS Extensions	RFC4366 server name , RFC7627 extended master secret , RFC5746 renegotiation info , RFC4492 EC point formats , RFC5077 session ticket , RFC7301 application-layer protocol negotiation , RFC4366 status request
Organisation	Not Present	Application-Layer Protocol Negotiation	h2
		Next Protocol	
Organisation	Not Present	Application-Layer Protocol Negotiation	h2
State	Not Present	Next Protocol Negotiation	h2.http/1.1
Country	Not Present	Issuing organisation	Google Trust Services
Organisational unit	Not Present	Issuer common name	WE1
Subject Alternative Name	genius.com , *genius.com	Issuer unit	Not Present
Validity period	From Mar 26 2025 to Jun 24 2025 (2 months, 4 weeks, 1 day)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	cloudflare	Issuer state	Not Present
Public key algorithm	id-ecPublicKey	Certificate Revocation Lists	http://c.pki.google/we1/ygWPENkxpm.crl
Protocol version	TLSv1.2	Certificate Hash	zUofntbmRrzqjjo3kiK86WBMg4
Public key length	256	Public Key Hash	8d85b31b8c2ec495e562e0caa94bf1f49d94e03bf84bf5ba96057028340dc7d6
Certificate check	OK	OCSP servers	http://c.pki.google/s/we1/6OQ
Signature algorithm	ecdsa-with-SHA256	OCSP stapling response	Certificate valid
Serial number	0xe8e4cd09d8c7790d5dfef64b4dea42	OCSP data generated	Apr 30 14:09:23 2025 GMT
Cipher	ECDHE-ECDSA-AES128-GCM-SHA256	OCSP data expires	May 7 13:09:22 2025 GMT
Version number	0x02		

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

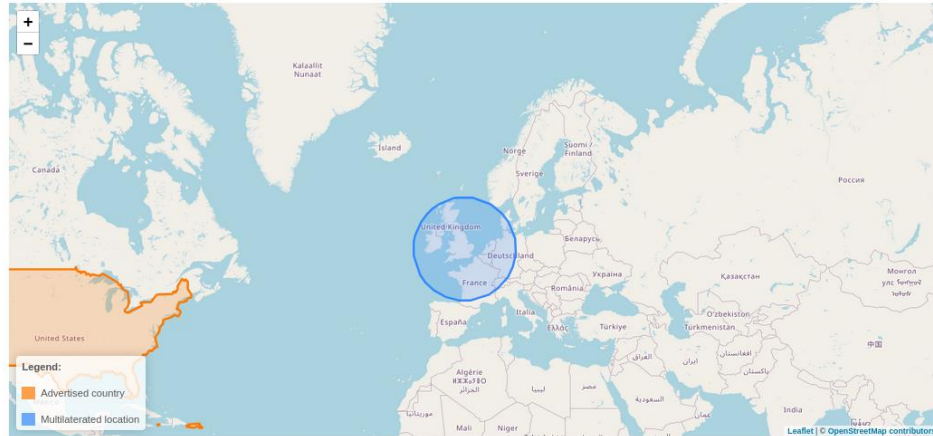
Source	Log	Timestamp	Signature Verification
Certificate	Unknown xsFM7l0u/fK/zhlvZa58b6RpxZ8qul+ysAdJb48790vq=	2025-03-26 08:27:16	Unknown
	Unknown		

Web Security - IE2062

Year 2 Semester 2 - 2025

IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)



SSL/TLS

Assurance	Extended validation	Perfect Forward Secrecy	Yes
Common name	www.bathandbodyworks.com	Supported TLS Extensions	RFC4446 is supported versions, RFC4446 is key share, RFC4366 is server name, RFC7301 is application-layer protocol negotiation, RFC4366 is status request, RFC4446 is early data
Organisation	Bath & Body Works Inc	Application-Layer Protocol Negotiation	n2
State	Ohio	Next Protocol Negotiation	Not Present
Country	US	Issuing organisation	Sectigo Limited
Organisational unit	Not Present	Issuer common name	Sectigo RSA Extended Validation Secure Server CA
Subject Alternative Name	www.bathandbodyworks.com	Issuer unit	Not Present
Validity period	From Aug 30 2024 to Aug 30 2025 (12 months)	Issuer location	Salford
Hosts hostname	Yes	Issuer country	GB
Server	Varnish	Issuer state	Greater Manchester
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://crl.sectigo.com/SectigoRSAExtendedValidationSecureServerCA.crl
Protocol version	TLSv1.3	Certificate Hash	R1685bv+DonKABtp4jWC5enU
Public key length	2048	Public Key Hash	4265er7d3e0a6831dcd8711f756718a0eb1f1a3782dc2d331262525811fa7da2
Certificate check	OK	OCSP servers	http://ocsp.sectigo.com
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	Certificate valid
Serial number	0x110246cd960cebe5a589ac2af9aee3cc	OCSP data generated	Apr 28 10:46:36 2025 GMT
Cipher	TLS_AES_128_GCM_SHA256	OCSP data expires	May 5 10:46:36 2025 GMT
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Unknown 3d0NJC0dR7Y35Yvsef+0ic1Uk/hd0icEnYkKy7yCo=	2024-08-30 13:41:22	Unknown
Certificate	Unknown DahyKcV7c-FAh7J2U0u/EdhFJ00R7vD0aTetH0Qqj0=	2024-08-30 13:41:22	Unknown
Certificate	Unknown EY+P0R_1T7+uV8h+Dj+p95E/(ntM0S)2u19M0E+M6J1oe	2024-08-30 13:41:22	Unknown

Google EV whitelist

Certificate **is not** in Google's EV whitelist

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 offered the Heartbeat TLS extension prior to the Heartbleed disclosure, but is using a new certificate and no longer offers Heartbeat.

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

SSL Certificate Chain

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](#). Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

Warning: It appears that this host does not have an SPF record. There may be an SPF record on bathandbodyworks.com. Check the [site report](#).

Web Security - IE2062

Year 2 Semester 2 - 2025

Site Technology (fetched today)

HTTP Accelerator

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

Technology	Description	Popular sites using this technology
Varnish id	An HTTP accelerator for web applications	www.inopaq.qc.ca , www.mozilla.org , www.bbc.co.uk

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
JavaScript id	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.netflix.com , www.linkedin.com , www.deep1.com

Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Fastly CDN id	Content Delivery Network	

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 id	UCS Transformation Format 8 bit	www.tiktok.com , www.twitch.tv , www.amazon.de

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.

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
Referrer Policy id	Restrict referrer information included in subsequent requests	www.perplexity.ai , www.deep1.com , www.startpage.com
Document Compatibility Mode id	A meta-tag used in Internet Explorer 8 to enable compatibility mode	www.microsoft.com , www.amazon.de , www.netflix.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	www.linkedin.com , www.tiktok.com , www.twitch.tv

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 id	Latest revision of the HTML standard, the main markup language on the web	mail.google.com , docs.google.com , accounts.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.


Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	stackoverflow.com

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
CSS Media Query	No description	www.imdb.com , www.paypal.com , www.aliexpress.com
Embedded id	Styles defined within a webpage	www.amazon.ca , www.amazon.fr , www.amazon.es

1.3 Wappalyzer


Wappalyzer - Techn...

Analytics

- [Pinterest Conversion Tag](#)
- [Adobe Analytics](#)

JavaScript frameworks

- [React](#)
- [Emotion](#)

Video players

- [Brightcove](#)

Security

- [PerimeterX](#)

Live chat

- [Cognigy](#)

CRM

- [Cognigy](#)

JavaScript libraries

- [Swiper](#)
- [lit-html](#) 3.2.1
- [lit-element](#) 4.1.1
- [Loadable-Components](#)
- [core-js](#) 3.23.4

Security

- [PerimeterX](#)
- [HSTS](#)

Miscellaneous

- [PWA](#)
- [ServiceNow](#)

Caching

- [Varnish](#)

CDN

- [jQuery CDN](#)
- [Amazon S3](#)
- [Amazon CloudFront](#)

Maps

WordPress components

- [core-js](#) 3.23.4
- [jQuery](#) 3.7.1

PaaS

- [Amazon Web Services](#)

UI frameworks

- [Chakra UI](#)

Cookie compliance

- [OneTrust](#)

Affiliate programs

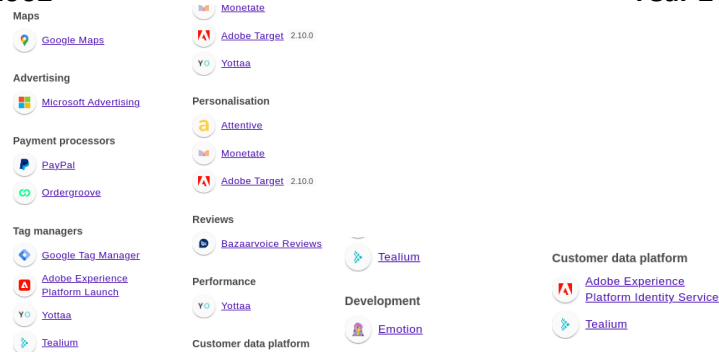
- [Pepperjam](#)

A/B testing

- [Monetate](#)

Web Security - IE2062

Year 2 Semester 2 - 2025



2. Injection

2.1 Uniscan

```
(binosh@BINZ) [~/Desktop/WS_Assingment/Tools]
$ sudo uniscan -u https://genius.com/signup -qweds

[sudo] password for binosh:
[sudo] password for binosh:
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
v. 6.3
```

This uniscan report indicates that a collection of security tests were performed on the website "<https://genius.com/signup>".

- FCKeditor File Upload
- Web Backdoors
- Source Code Disclosure
- PHPinfo() Disclosure
- E-mails
- File Upload Forms
- External Hosts
- Timthumb
- Dynamic Tests

Mitigation Strategies

- Secure File Uploads
- Backdoor Detection
- Source Code Protection
- Email Security
- Timthumb Patching
- Vulnerability Patching

```
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, 2 URL's found!
```

3. Firewall Detection

3.1 Wafw00f

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools]
$ wafw00f https://genius.com/signup

      { Woof! }
    (  )  (  )
   (  )  (  )
  (  )  (  )
 (  )  (  )
(  )  (  )

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

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

It was detected that the Web Application Firewall that is behind the <https://genius.com/signup> site is Cloudfront.

4. Multi Tool Web Vulnerability Scanning

4.1 Rapidscan

```
zsh: corrupt history file /home/binosh/.zsh_history
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools/rapidscan]
$ python3 rapidscan.py https://genius.com/signup
```

```
Vulnerability Threat Level
low Some ports are open. Perform a full-scan manually.
Vulnerability Definition
Open Ports give attackers a hint to exploit the services. Attackers try
to retrieve banner information through the ports and understand what type of ser
vice the host is running
Vulnerability Remediation
It is recommended to close the ports of unused services and use a firewa
ll to filter the ports wherever necessary. This resource may give more insights.
https://security.stackexchange.com/a/145781/6137
```

4.2 Nmap(To validate rapidscan vulnerability)




















2 ports are open


```
PORT      STATE SERVICE
80/tcp    open  http
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp    open  https
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2011-3192:
VULNERABLE:
Apache byterange filter DoS
State: VULNERABLE
IDS: CVE:2011-3192 BID:49303
The Apache web server is vulnerable to a denial of service attack when numerous
overlapping byte ranges are requested.
Disclosure date: 2011-08-19
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
https://www.tenable.com/plugins/nessus/55976
https://www.securityfocus.com/bid/49303
https://seclists.org/fulldisclosure/2011/Aug/175
http-fileupload-exploiter:
```


Web Security - IE2062

Year 2 Semester 2 - 2025

4.3 OWASP

- >  PII Disclosure (2)
- >  CSP: Failure to Define Directive with No Fallback (531)
- >  CSP: Wildcard Directive (531)
- >  CSP: script-src unsafe-inline (531)
- >  CSP: style-src unsafe-inline (531)
- >  Content Security Policy (CSP) Header Not Set (8)
- >  Missing Anti-clickjacking Header
- >  Cookie No HttpOnly Flag (698)
- >  Cookie Without Secure Flag (652)
- >  Cookie without SameSite Attribute (781)
- >  Cross-Domain JavaScript Source File Inclusion (3646)
- >  Secure Pages Include Mixed Content (521)
- >  Strict-Transport-Security Header Not Set (527)
- >  Timestamp Disclosure - Unix (13968)
- >  X-Content-Type-Options Header Missing (502)
- >  Authentication Request Identified (6)
- >  Content Security Policy (CSP) Report-Only Header Found (516)
- >  Information Disclosure - Suspicious Comments (320)
- >  Modern Web Application (523)
- >  Re-examine Cache-control Directives (506)

PII Disclosure	
URL:	https://genius.com/Ellis-presley-cant-help-falling-in-love-lyrics
Risk:	 High
Confidence:	High
Parameter:	
Attack:	
Evidence:	5703277939363
CWE ID:	359
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: Maestro
	Bank Identification Number: 570327
	Brand: MAESTRO
Solution:	Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

CSP: Failure to Define Directive with No Fallback	
URL:	https://genius.com/sitemap.xml
Risk:	 Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	upgrade-insecure-requests
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-13
Input Vector:	
Description:	The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.
Other Info:	
	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Solution:	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

How to mitigate the above Vulnerability

- Upgrade jQuery and Moment.js to the latest versions to mitigate known vulnerabilities.
- Implement strict Content Security Policy (CSP) headers to prevent XSS attacks.
- Sanitize all user-generated content before processing it in the application.
- Upgrade Chart.js to the latest available version to patch prototype pollution vulnerabilities.
- Upgrade jQuery to latest version or later to fix XSS and selector interpretation risks.
- Sanitize user inputs and restrict script execution to prevent cross-site scripting (XSS).
- Implement CSP headers to mitigate XSS and ensure CORS policies are properly configured.

Proof of Report Submission



Genius has received **WS ASSINGMENT**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement Genius-VDP.

Submission Details

Submitted
04 May 2025 19:19:36 UTC

Submission ID
244a3e92-2c54-4da9-b084-2d71ae749021

VRT
Cross-Site Scripting (XSS) > Reflected > Non-Self

[View Submission Details](#)