

Sri Lanka Institute of Information Technology



Individual Assignment

## **Bug Bounty Report**

### **Client-side Cross-Site Scripting (XSS)**

**Web Security - IE2062**

BSc Honors in Information Technology Specializing in Cyber Security

<b>CASE STUDY NAME</b>	BUG BOUNTY Report 02 - Client-side Cross-Site Scripting (XSS)
<b>CAMPUS/CENTER</b>	SLIIT KANDY UNI

**Student Details**

	<b>Student Registration Number</b>	<b>Student Name</b>
<b>1</b>	IT23222854	JAYASINGHE B. I

## Table of Contents

<b>Domain – <a href="https://www.dickssportinggoods.com/">https://www.dickssportinggoods.com/</a></b>	<b>4</b>
<b>1. JavaScript library scanner</b>	<b>5</b>
1.1 Retire.js	5
Summary of the above vulnerabilities	5
<b>2. Multi Tool Web Vulnerability Scanning</b>	<b>5</b>
2.1 Rapidscan	5
<b>3. Firewall Detection</b>	<b>6</b>
3.1 Wafw00f	6
<b>4. Using Components with Known Vulnerabilities</b>	<b>6</b>
4.1 Nmap	6
4.2 Netcraft	6
<b>How to mitigate the above Vulnerability</b>	<b>8</b>
<b>Proof of Report Submission</b>	<b>8</b>

Domain – <https://www.dickssportinggoods.com/>

Engagements > DICK'S Sporting Goods

Vulnerability Disclosure • Updated

### DICK'S Sporting Goods

DICK'S Sporting Goods Vulnerability Disclosure Program

Retail • No collaboration • Safe harbor

---

In Scope Targets ✓ In scope

**Targets:**  
NOTE: Any identical issues found between the below domains will be treated as a duplicate. We would very much appreciate explicit callout if something is found on more than one of the domains. Thank you.

**Updated scope**  
The following list of IP CIDR ranges are owned by Dick's Sporting Goods or are part of a shared cloud IP address space.  
ONLY test against systems in the in-scope domains for this program if their IP address is in one of the ranges below.  
Any IP address owned by Microsoft, Google, Amazon or Akamai is in scope.

ADDRESS RANGE	CIDR MASK	CIDR IP Range
4.7.200.160	/27	4.7.200.160 - 4.7.200.191
8.42.209.0	/24	8.42.209.0 - 8.42.209.255
63.161.110.0	/24	63.161.110.0 - 63.161.110.255
71.16.39.0	/24	71.16.39.0 - 71.16.39.255
199.30.192.0	/24	199.30.192.0 - 199.30.192.255
199.30.193.0	/24	199.30.193.0 - 199.30.193.255

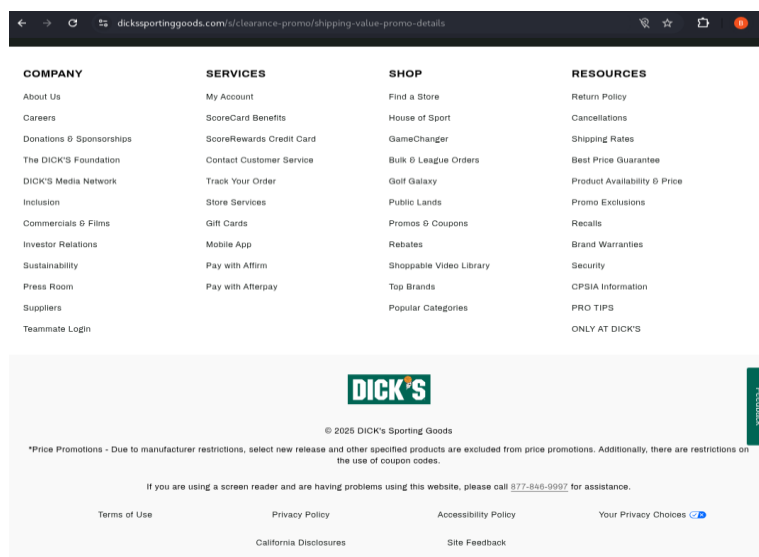
[Show more](#)

\*.dickssportinggoods.com Website Testing

\*.goinggoingnowhere.com TypeScript ReactJS jQuery

\*.publiclands.com Website Testing

- Link - <https://www.dickssportinggoods.com/>
- Category – Vulnerability Disclosure Program (VDP)
- Type - Sporting goods website offering apparel, footwear, equipment, and outdoor gear for athletes and enthusiasts.



Navigation links:

- COMPANY**
  - About Us
  - Careers
  - Donations & Sponsorships
  - The DICK'S Foundation
  - DICK'S Media Network
  - Inclusion
  - Commercials & Films
  - Investor Relations
  - Sustainability
  - Press Room
  - Suppliers
  - Teammate Login
- SERVICES**
  - My Account
  - ScoreCard Benefits
  - ScoreRewards Credit Card
  - Contact Customer Service
  - Track Your Order
  - Store Services
  - Gift Cards
  - Mobile App
  - Pay with Affirm
  - Pay with Afterpay
- SHOP**
  - Find a Store
  - House of Sport
  - GameChanger
  - Bulk & League Orders
  - Golf Galaxy
  - Public Lands
  - Promos & Coupons
  - Rebates
  - Shoppable Video Library
  - Top Brands
  - Popular Categories
- RESOURCES**
  - Return Policy
  - Cancellations
  - Shipping Rates
  - Best Price Guarantee
  - Product Availability & Price
  - Promo Exclusions
  - Recalls
  - Brand Warranties
  - Security
  - CPSIA Information
  - PRO TIPS
  - ONLY AT DICK'S

**DICK'S**

© 2025 DICK'S Sporting Goods

\*Price Promotions - Due to manufacturer restrictions, select new release and other specified products are excluded from price promotions. Additionally, there are restrictions on the use of coupon codes.

If you are using a screen reader and are having problems using this website, please call 877-846-9997 for assistance.

[Terms of Use](#)
[Privacy Policy](#)
[Accessibility Policy](#)
[Your Privacy Choices](#)

[California Disclosures](#)
[Site Feedback](#)

## 1. JavaScript library scanner

### 1.1 Retire.js

This tool is used to detect the use of JavaScript libraries and Node.js modules with known vulnerabilities.

**Retire.js**
☒ Enabled ☐ Show unknown

<b>axios</b>	<b>1.6.2</b>	Found in <a href="https://www.dickssportinggoods.com/etc.clientlibs/dsg/clientlibs/clientlib-site-ic-31ae9b6db08bce376a316f5104e27a4d-ic.min.js">https://www.dickssportinggoods.com/etc.clientlibs/dsg/clientlibs/clientlib-site-ic-31ae9b6db08bce376a316f5104e27a4d-ic.min.js</a> - Vulnerability info: Medium Versions before 1.6.8 depends on follow-redirects before 1.15.6 which could leak the proxy authentication credentials 6300 [1] High Server-Side Request Forgery in axios CVE-2024-39338 GHSA-8hc4-vh64-cxmj [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] High axios Requests Vulnerable To Possible SSRF and Credential Leakage via Absolute URL CVE-2025-27152 GHSA-jf5f-v2jv-69x6 [1] [2] [3] [4] [5] [6] [7]
<b>DOMPurify</b>	<b>3.0.6</b>	Found in <a href="https://www.dickssportinggoods.com/etc.clientlibs/dsg/clientlibs/clientlib-site-ic-31ae9b6db08bce376a316f5104e27a4d-ic.min.js">https://www.dickssportinggoods.com/etc.clientlibs/dsg/clientlibs/clientlib-site-ic-31ae9b6db08bce376a316f5104e27a4d-ic.min.js</a> - Vulnerability info: High DOMPurify has a nesting-based XSS CVE-2024-47875 GHSA-gx9m-whjm-85jf [1] [2] [3] [4] [5] [6] [7] High DOMPurify allows tampering by prototype pollution CVE-2024-45801 GHSA-mmhx-hmjr-r674 [1] [2] [3] [4] [5] [6] Medium DOMPurify allows Cross-site Scripting (XSS) [1] [2] [3]

**jquery**

**1.12.4-aem**

Found in <https://www.dickssportinggoods.com/etc.clientlibs/clientlibs/granite/jquery-ic-f9e8e8c279baf6a1a278042afe4f395a-ic.min.js> - Vulnerability info:  
 Low jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates 73 162 [1]  
 Medium 3rd party CORS request may execute 2432 CVE-2015-9251 GHSA-rmxg-73gg-4p98 [1] [2] [3] [4] [5] [6]  
 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-6c3j-c64m-qhgq [1] [2] [3]  
 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-cgw6-v4j6 [1]  
 Medium Regex in its jQuery.htmlPrefilter sometimes may introduce XSS CVE-2020-11022 4642 GHSA-gxr4-xjjs-5px2 [1]

#### Summary of the above vulnerabilities

Severity	Description	CVE Identifier	GHSA Identifier
Low	jQuery 1.x and 2.x are End-of-Life and no longer receive security updates.	-	-
Medium	Third-party CORS requests may execute improperly.	CVE-2015-9251	GHSA-rmqq-739g-4pg8
Medium	Object PrototypPollution using jQuery.extend(true, ...), due to mishandling object prototypes.	CVE-2019-11358	GHSA-6cj6-c64m-qjhq
Medium	Passing HTML containing elements from untrusted sources may execute untrusted code.	CVE-2020-11023	GHSA-jqcv-gw6v-9f4c
Medium	Regex in jQuery.htmlPrefilter may introduce XSS vulnerabilities.	CVE-2020-11022	GHSA-gxr4-xjjs-5px2
Medium	Regular Expression Denial of Service (ReDOS) exploiting inefficient regex patterns	CVE-2016-4055	GHSA-87vv-r9j6-5qgv
Medium	Regular Expression Denial of Service (ReDOS) vulnerabilities impacting certain patterns	CVE-2017-18214	GHSA-446m-mv8f-q348
High	Unsafe user-provided locale strings triggering vulnerabilities in moment.js.	CVE-2022-24785	GHSA-8fhj-24r4-96c4

## 2. Multi Tool Web Vulnerability Scanning

### 2.1 Rapidscan

```

(binosh@BINZ)~$ python3 rapidscan.py https://www.dickssportinggoods.com/s/clearance-promo/shipping-value-promo-details
  
```

Out of 80 vulnerabilities checked for <https://www.dickssportinggoods.com/s/clearance-promo/shipping-value-promo-details> **4 vulnerabilities were detected**

### 3. Firewall Detection

#### 3.1 Wafw00f

```
(binosh@BINZ)-[~]
$ wafw00f https://www.dickssportinggoods.com/s/clearance-promo/shipping-value-promo-details

      ( Woof! )
    /  |  \
   /   |   \
  /    |    \
 /     |     \
/      |      \
(      |      )
 \     |     /
  \    |    /
   \   |   /
    \  |  /
     ( Woof! )

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

[*] Checking https://www.dickssportinggoods.com/s/clearance-promo/shipping-value-promo-details
[+] The site https://www.dickssportinggoods.com/s/clearance-promo/shipping-value-promo-details is behind Kona SiteDefender (Akamai)
[-] Number of requests: 2
```

### 4. Using Components with Known Vulnerabilities

#### 4.1 Nmap

```
(binosh@BINZ)-[~/WS Assingment /Tools]
$ nmap -Pn www.dickssportinggoods.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 05:14 SAST
```

PORT	STATE	SERVICE
21/tcp	open	ftp
25/tcp	open	smtp
80/tcp	open	http
443/tcp	open	https

From the Nmap scanning results it can be identified that port 21 for FTP service is open. Hence it is verified that there is a critical vulnerability in this domain which is that the FTP port is open.

#### 4.2 Netcraft


The Netcraft Site Report tool can be used to conduct mining on the site.

After analyzing below information regarding the site was gathered.

Background

Site title	Access Forbidden	Date first seen	February 1999
Site rank	8249	Primary language	English
Description	Not Present		

Network

Site	<a href="http://www.dickssportinggoods.com">http://www.dickssportinggoods.com</a>	Domain	<a href="http://dickssportinggoods.com">dickssportinggoods.com</a>
Netblock Owner	Akamai International, BV	Nameserver	<a href="http://dns1.cscdns.net">dns1.cscdns.net</a>
Hosting company	Akamai Technologies	Domain registrar	<a href="http://corporatedomains.com">corporatedomains.com</a>
Hosting country	 NL	Nameserver organisation	<a href="http://whois.corporatedomains.com">whois.corporatedomains.com</a>
IPv4 address	23.39.41.173 ( <a href="http://www.ripe.net">www.ripe.net</a> )	Organisation	American Sports Licensing, Inc., c/o Dick's Sporting Goods, Inc., Coraopolis, 15108, US
IPv4 autonomous systems	<a href="http://AS16625">AS16625</a>	DNS admin	<a href="mailto:hostmaster@cscdns.net">hostmaster@cscdns.net</a>
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled
Reverse DNS	<a href="http://x23-39-41-173.deploy.static.akamaitechnologies.com">x23-39-41-173.deploy.static.akamaitechnologies.com</a>		

IP delegation

### IP Geolocation

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



### SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the [HTTPS site report](#).

### 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 [dickssportinggoods.com](#). Check the [site report](#).

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any [mail-enabled subdomains](#). It is recommended to add an SPF record to any subdomain with an MX record.

### DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see [dmarc.org](#).

This host does not have a DMARC record. There may be a DMARC record on the site report for [dickssportinggoods.com](#). Check the [site report](#).

### Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

No known trackers were identified.

### Site Technology (fetched today)

#### 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
Akamai <a href="#">id</a>	Web Content Delivery service provider	<a href="#">www.ibm.com</a> , <a href="#">www.aliexpress.com</a> , <a href="#">www.dailymail.co.uk</a>

#### 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
Content Security Policy <a href="#">id</a>	Detect and mitigate attacks in the browser	<a href="#">www.tiktok.com</a> , <a href="#">www.deepi.com</a> , <a href="#">mail.google.com</a>

#### 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 <a href="#">id</a>	Latest revision of the HTML standard, the main markup language on the web	<a href="#">www.netflix.com</a> , <a href="#">www.linkedin.com</a> , <a href="#">www.twitch.tv</a>

#### 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
Embedded <a href="#">id</a>	Styles defined within a webpage	<a href="#">www.amazon.de</a> , <a href="#">www.amazon.fr</a> , <a href="#">www.amazon.it</a>

With these gathered information attackers can identify a website's technology stack, pinpoint vulnerabilities, target outdated software, and craft convincing phishing attacks. They can also map out a target's internet infrastructure for planning sophisticated attacks. Regular software updates, strong authentication, and security best practices are essential for mitigation.

### How to mitigate the above Vulnerability

- Upgrade to jQuery 3.x CORS instead of outdated jQuery (1.x/2.x), which lacks security updates. Configurations that are incorrect (like CVE-2015-9251): may reveal information through cross-domain requests; this can be avoided by limiting Allow-Origin-Control-Access to reliable domains  
Unsafe use of \$.extend(true,...) is the cause of prototype pollution (CVE-2019-11358); this can be fixed by verifying inputs or by utilizing safe substitutes.
- Injecting untrusted HTML causes XSS via jQuery (CVE-2020-11023); utilize sanitization tools such as DOMPurify.  
CVE-2016-4055 and CVE-2017-18214 are examples of ReDoS attacks. Using optimized regex can help reduce execution lag caused by poor regex patterns. Moment.js Unsafe locale string handling is the vulnerability (CVE-2022-24785); clean up and limit locale inputs.
- Developers should use tools like Retire.js and npm audit, deploy security fixes, and audit dependencies on a regular basis to avoid these vulnerabilities. Developing secure online apps requires implementing robust validation and sanitization procedures.

### Proof of Report Submission



**DICK'S Sporting Goods** has received **WS Assignment**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement dickssportinggoods.

**Submission Details**

Submitted

04 May 2025 18:55:14 UTC

Submission ID

fda53838-a041-4937-a2a1-86c5deaf4652

VRT

Server Security Misconfiguration > Lack of Security Headers > X-XSS-Protection

[View Submission Details](#)