Sri Lanka Institute of Information Technology

Individual Assignment

Bug Bounty Report

(PII) disclosure

Web Security - IE2062

BSc Honors in Information Technology Specializing in Cyber Security

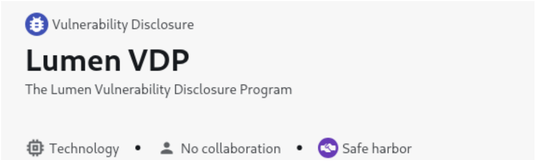
CASE STUDY NAME	BUG BOUNTY Report 01 **-(PII) disclosure**
CAMPUS/CENTER	SLIIT KANDY UNI

Student Details

	Student Registration Number	**Student Name**
1	IT23222854	JAYASINGHE B. I

Table of Contents

Domain – https://www.lumen.com/en-us/home.html

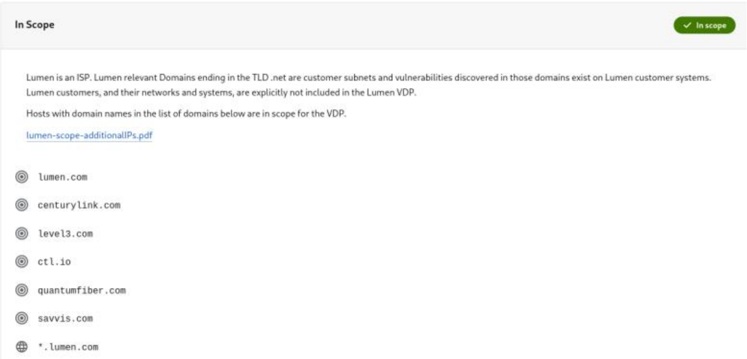


Vulnerability Disclosure

Lumen VDP

The Lumen Vulnerability Disclosure Program

Technology • No collaboration • Safe harbor



In Scope ✓ In scope

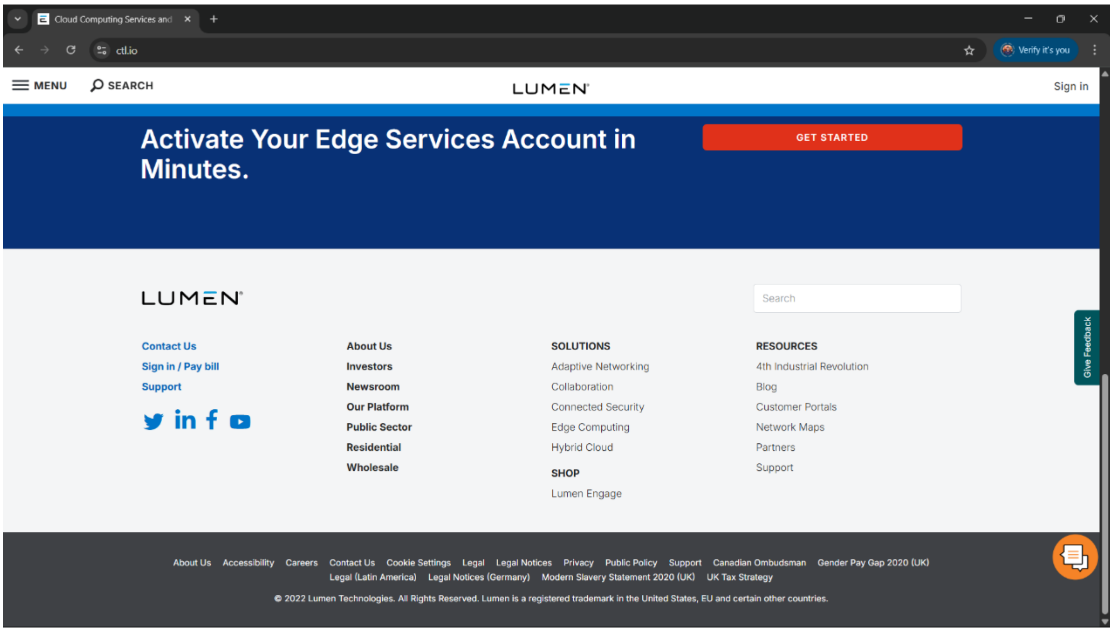
Lumen is an ISP. Lumen relevant Domains ending in the TLD .net are customer subnets and vulnerabilities discovered in those domains exist on Lumen customer systems. Lumen customers, and their networks and systems, are explicitly not included in the Lumen VDP.

Hosts with domain names in the list of domains below are in scope for the VDP.

lumen-scope-additionalIPs.pdf

```
lumen.com
centurylink.com
level3.com
ctl.io
quantumfiber.com
savvis.com
*.lumen.com
```

- Link - https://ctl.io/
- Category – Lumen Technologies provides high-speed internet, cloud solutions, and enterprise-level tech services for both homes and businesses.
- Type - Enterprise-focused platform offering cloud orchestration, application management, and hybrid IT services



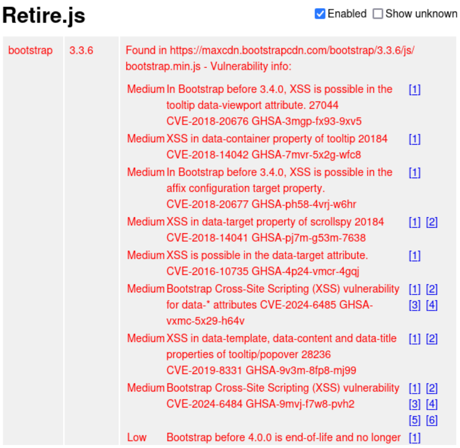
Activate Your Edge Services Account in Minutes.

© 2022 Lumen Technologies. All Rights Reserved. Lumen is a registered trademark in the United States, EU and certain other countries.

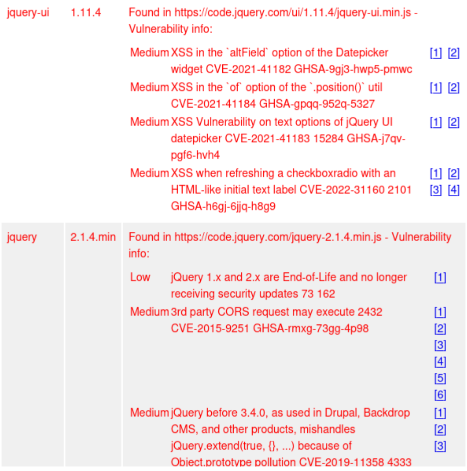
1. JavaScript library scanner.

1.1 Retire.js

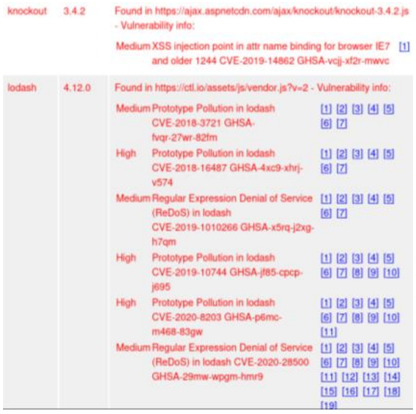
This tool is used to detect the use of JavaScript libraries and Node.js modules with known vulnerabilities.



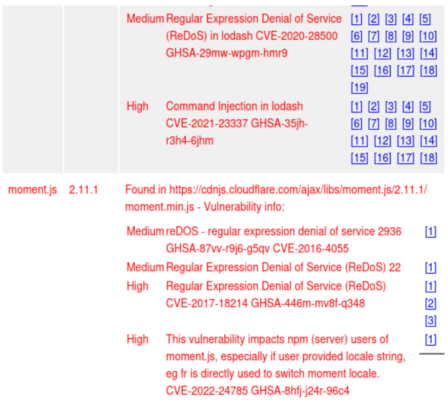
```
Retire.js                                              ☑ Enabled ☐ Show unknown

bootstrap  3.3.6   Found in https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/js/
                   bootstrap.min.js - Vulnerability info:
                   Medium In Bootstrap before 3.4.0, XSS is possible in the      [1]
                          tooltip data-viewport attribute. 27044
                          CVE-2018-20676 GHSA-3mgp-fx93-9xv5
                   Medium XSS in data-container property of tooltip 20184        [1]
                          CVE-2018-14042 GHSA-7mvr-5x2g-wfc8
                   Medium In Bootstrap before 3.4.0, XSS is possible in the      [1]
                          affix configuration target property.
                          CVE-2018-20677 GHSA-ph58-4vrj-w6hr
                   Medium XSS in data-target property of scrollspy 20184         [1] [2]
                          CVE-2018-14041 GHSA-pj7m-g53m-7638
                   Medium XSS is possible in the data-target attribute.          [1]
                          CVE-2016-10735 GHSA-4p24-vmcr-4gqj
                   Medium Bootstrap Cross-Site Scripting (XSS) vulnerability     [1] [2]
                          for data-* attributes CVE-2024-6485 GHSA-              [3] [4]
                          vxmc-5x29-h64v
                   Medium XSS in data-template, data-content and data-title      [1] [2]
                          properties of tooltip/popover 28236
                          CVE-2019-8331 GHSA-9v3m-8fp8-mj99
                   Medium Bootstrap Cross-Site Scripting (XSS) vulnerability     [1] [2]
                          CVE-2024-6484 GHSA-9mvj-f7w8-pvh2                      [3] [4]
                                                                                 [5] [6]
                   Low    Bootstrap before 4.0.0 is end-of-life and no longer   [1]
```



```
jquery-ui  1.11.4      Found in https://code.jquery.com/ui/1.11.4/jquery-ui.min.js -
                       Vulnerability info:
                       Medium XSS in the `altField` option of the Datepicker        [1] [2]
                              widget CVE-2021-41182 GHSA-9gj3-hwp5-pmwc
                       Medium XSS in the `of` option of the `.position()` util      [1] [2]
                              CVE-2021-41184 GHSA-gpqq-952q-5327
                       Medium XSS Vulnerability on text options of jQuery UI        [1] [2]
                              datepicker CVE-2021-41183 15284 GHSA-j7qv-
                              pgf6-hvh4
                       Medium XSS when refreshing a checkboxradio with an           [1] [2]
                              HTML-like initial text label CVE-2022-31160 2101      [3] [4]
                              GHSA-h6gj-6jjq-h8g9

jquery     2.1.4.min   Found in https://code.jquery.com/jquery-2.1.4.min.js - Vulnerability
                       info:
                       Low    jQuery 1.x and 2.x are End-of-Life and no longer      [1]
                              receiving security updates 73 162
                       Medium 3rd party CORS request may execute 2432               [1]
                              CVE-2015-9251 GHSA-rmxg-73gg-4p98                     [2]
                                                                                    [3]
                                                                                    [4]
                                                                                    [5]
                                                                                    [6]
                       Medium jQuery before 3.4.0, as used in Drupal, Backdrop      [1]
                              CMS, and other products, mishandles                   [2]
                              jQuery.extend(true, {}, ...) because of               [3]
                              Object.prototype pollution CVE-2019-11358 4333
```



```
knockout  3.4.2   Found in https://ajax.aspnetcdn.com/ajax/knockout/knockout-3.4.2.js
                  - Vulnerability info:
                  Medium XSS injection point in attr name binding for browser IE7   [1]
                         and older 1244 CVE-2019-14862 GHSA-vcjj-xf2r-mwvc

lodash    4.12.0  Found in https://ctl.io/assets/js/vendor.js?v=2 - Vulnerability info:
                  Medium Prototype Pollution in lodash            [1] [2] [3] [4] [5]
                         CVE-2018-3721 GHSA-                      [6] [7]
                         fvqr-27wr-82fm
                  High   Prototype Pollution in lodash            [1] [2] [3] [4] [5]
                         CVE-2018-16487 GHSA-4xc9-xhrj-           [6] [7]
                         v574
                  Medium Regular Expression Denial of Service     [1] [2] [3] [4] [5]
                         (ReDoS) in lodash                        [6] [7]
                         CVE-2019-1010266 GHSA-x5rq-j2xg-
                         h7qm
                  High   Prototype Pollution in lodash            [1] [2] [3] [4] [5]
                         CVE-2019-10744 GHSA-jf85-cpcp-           [6] [7] [8] [9] [10]
                         j695
                  High   Prototype Pollution in lodash            [1] [2] [3] [4] [5]
                         CVE-2020-8203 GHSA-p6mc-                 [6] [7] [8] [9] [10]
                         m468-83gw                                [11]
                  Medium Regular Expression Denial of Service     [1] [2] [3] [4] [5]
                         (ReDoS) in lodash CVE-2020-28500         [6] [7] [8] [9] [10]
                         GHSA-29mw-wpgm-hmr9                      [11] [12] [13] [14]
                                                                  [15] [16] [17] [18]
                                                                  [19]
```



```
                   Medium Regular Expression Denial of Service     [1] [2] [3] [4] [5]
                          (ReDoS) in lodash CVE-2020-28500         [6] [7] [8] [9] [10]
                          GHSA-29mw-wpgm-hmr9                      [11] [12] [13] [14]
                                                                   [15] [16] [17] [18]
                                                                   [19]
                   High   Command Injection in lodash              [1] [2] [3] [4] [5]
                          CVE-2021-23337 GHSA-35jh-                [6] [7] [8] [9] [10]
                          r3h4-6jhm                                [11] [12] [13] [14]
                                                                   [15] [16] [17] [18]

moment.js  2.11.1  Found in https://cdnjs.cloudflare.com/ajax/libs/moment.js/2.11.1/
                   moment.min.js - Vulnerability info:
                   Medium reDOS - regular expression denial of service 2936    [1]
                          GHSA-87vv-r9j6-g5qv CVE-2016-4055
                   Medium Regular Expression Denial of Service (ReDoS) 22      [1]
                   High   Regular Expression Denial of Service (ReDoS)         [1]
                          CVE-2017-18214 GHSA-446m-mv8f-q348                   [2]
                                                                               [3]
                   High   This vulnerability impacts npm (server) users of     [1]
                          moment.js, especially if user provided locale string,
                          eg fr is directly used to switch moment locale.
                          CVE-2022-24785 GHSA-8hfj-j24r-96c4
```

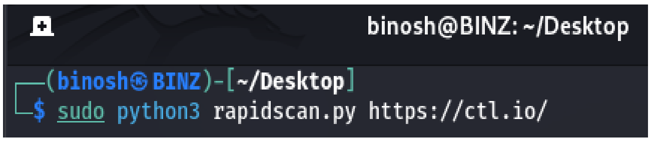
Summary of the above vulnerabilities

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)	Mitigation Strategy
Bootstrap	3.3.6	XSS possible in tooltip data-viewport attribute	Medium	CVE-2019-8331, GHSA-5mp9-3jx9-fv5v	Upgrade to **Bootstrap 3.4.0 or later**; sanitize attributes.
		XSS via data-container property of tooltip	Medium	CVE-2018-14042, GHSA-g7g5-5f72-h6xh	Upgrade Bootstrap and sanitize input before rendering tooltips.
		XSS via data-template attribute of tooltip	Medium	CVE-2018-14041, GHSA-g7g5-5f72-h6xh	Ensure secure attribute parsing; upgrade to patched version.
		General Bootstrap Cross-Site Scripting (XSS) vulnerability	Medium	CVE-2018-14042, GHSA-g7g5-5f72-h6xh	Implement **Content Security Policy (CSP)** to block injections.

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)
jQuery-ui	1.11.4	XSS in altField option of Datepicker widget	Medium	CVE-2021-41182, GHSA-hq93-hxq5-pmv6
		XSS in content of positions utility	Medium	CVE-2021-41184, GHSA-p6gp-7mj3-hmvq
		XSS in text option of Autocomplete widget	Medium	CVE-2021-41183, GHSA-7p4p-g9h6-hmh4
		XSS when refreshing a checkbox with HTML-like initial text	Medium	CVE-2020-28168, GHSA-h6qj-gja9-h8q8
jQuery	2.1.4.min	End-of-Life—no longer receiving security updates	Low	-
		jQuery CORS requests may execute unintended scripts	Medium	CVE-2015-9251, GHSA-mrq9-r7gp-5fj8
		XSS via crafted href attribute	Medium	CVE-2019-11358, GHSA-gxr4-xjj5-4x2g
Knockout	3.4.2	XSS injection point in attr name binding for IE7 & older	Medium	CVE-2019-14862, GHSA-vjjx-rf2v-mxvc
Lodash	4.17.20	Prototype Pollution	Medium/High	CVE-2018-3721, CVE-2019-10744, CVE-2020-8203, CVE-2020-28500
		Regular Expression Denial of Service (ReDoS)	High	CVE-2018-20843, CVE-2020-28550
lodash	-	Regular Expression Denial of Service (ReDoS)	Medium	CVE-2020-28500, GHSA-2mw4-v99m-hm9r
lodash	-	Command Injection	High	CVE-2021-23337, GHSA-35jh-r3h4-6jhm
Moment.js	2.11.1	Regular Expression Denial of Service (ReDoS)	Medium	CVE-2020-28506, GHSA-wvhm-4x4m-9g3q
Moment.js	2.11.1	Regular Expression Denial of Service (ReDoS)	Medium	CVE-2017-18214, GHSA-46r3-8ww4-7h4q
Moment.js	2.11.1	Locale string manipulation vulnerability	High	CVE-2022-31129, GHSA-6h4h-4qp6-9w7p

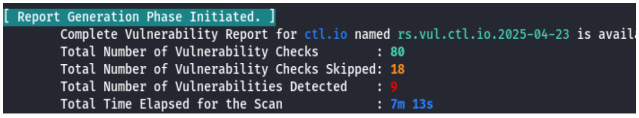
2. Multi Tool Web Vulnerability Scanning

2.1 Rapidscan

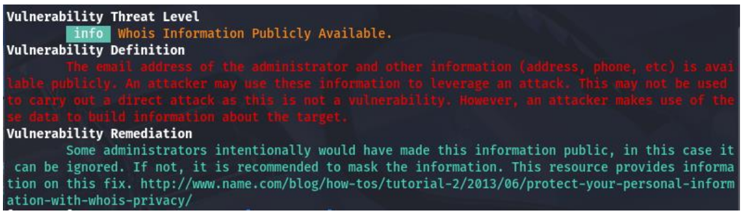


```
binosh@BINZ: ~/Desktop
┌──(binosh㉿BINZ)-[~/Desktop]
└─$ sudo python3 rapidscan.py https://ctl.io/
```

Out of 80 vulnerabilities checked for https://ctl.io/ 9 vulnerabilities were detected



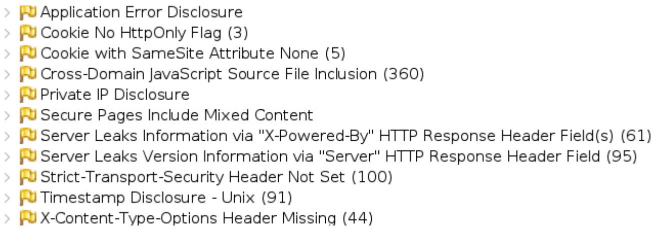
```
[ Report Generation Phase Initiated. ]
        Complete Vulnerability Report for ctl.io named rs.vul.ctl.io.2025-04-23 is avail
        Total Number of Vulnerability Checks        : 80
        Total Number of Vulnerability Checks Skipped: 18
        Total Number of Vulnerabilities Detected    : 9
        Total Time Elapsed for the Scan             : 7m 13s
```



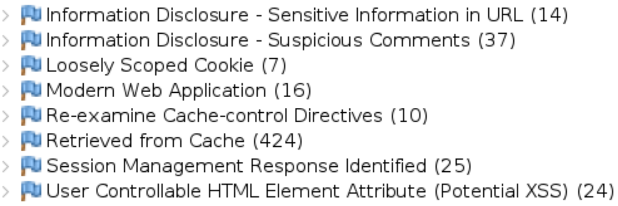
```
Vulnerability Threat Level
        info  Whois Information Publicly Available.
Vulnerability Definition
        The email address of the administrator and other information (address, phone, etc) is avai
lable publicly. An attacker may use these information to leverage an attack. This may not be used
to carry out a direct attack as this is not a vulnerability. However, an attacker makes use of the
se data to build information about the target.
Vulnerability Remediation
        Some administrators intentionally would have made this information public, in this case it
 can be ignored. If not, it is recommended to mask the information. This resource provides informa
tion on this fix. http://www.name.com/blog/how-tos/tutorial-2/2013/06/protect-your-personal-inform
ation-with-whois-privacy/
```

3. Using Components with Known Vulnerabilities

3.1 OWASP ZAP

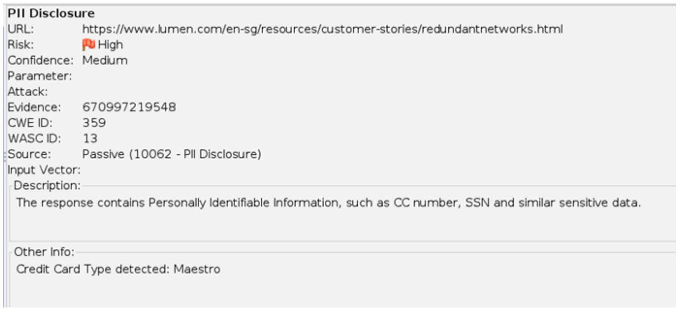


- Application Error Disclosure
- Cookie No HttpOnly Flag (3)
- Cookie with SameSite Attribute None (5)
- Cross-Domain JavaScript Source File Inclusion (360)
- Private IP Disclosure
- Secure Pages Include Mixed Content
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (61)
- Server Leaks Version Information via "Server" HTTP Response Header Field (95)
- Strict-Transport-Security Header Not Set (100)
- Timestamp Disclosure - Unix (91)
- X-Content-Type-Options Header Missing (44)



- Information Disclosure - Sensitive Information in URL (14)
- Information Disclosure - Suspicious Comments (37)
- Loosely Scoped Cookie (7)
- Modern Web Application (16)
- Re-examine Cache-control Directives (10)
- Retrieved from Cache (424)
- Session Management Response Identified (25)
- User Controllable HTML Element Attribute (Potential XSS) (24)

2 High severity and 5 Medium severity and 11 Low severity vulnerabilities were detected from OWASP ZAP vulnerability scanning tool.



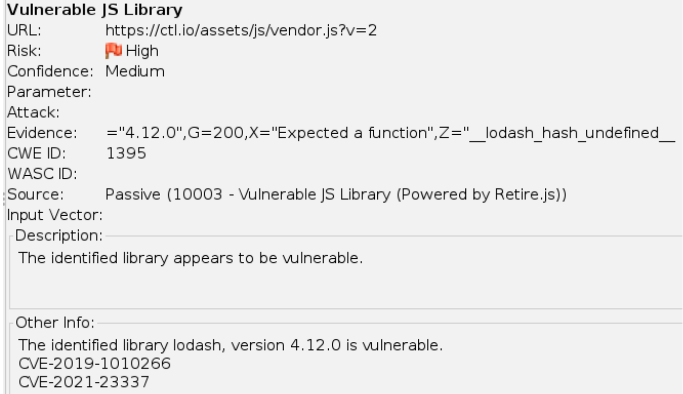
PII Disclosure

URL: https://www.lumen.com/en-sg/resources/customer-stories/redundantnetworks.html
Risk: High
Confidence: Medium
Parameter:
Attack:
Evidence: 670997219548
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.

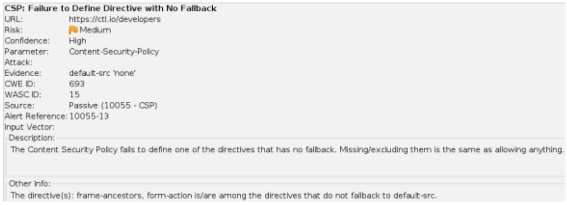
Other Info:
Credit Card Type detected: Maestro

When sensitive personal information, such credit card numbers or Social Security numbers, is accidentally made public on a website, it is usually referred to as personally identifiable information (PII) disclosure. There are serious hazards associated with this vulnerability, such as financial fraud and identity theft. In this case, passive scanning identified a Maestro credit card type. Organizations should employ stringent data sanitization procedures, store sensitive data using encryption or tokenization, and use access control measures to restrict exposure to reduce the dangers. To guarantee data privacy and shield consumers against any misuse, prompt repair is crucial.

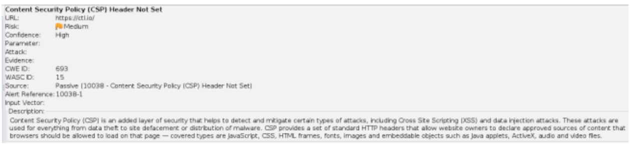


```
Vulnerable JS Library
URL:          https://ctl.io/assets/js/vendor.js?v=2
Risk:         🚩 High
Confidence:   Medium
Parameter:
Attack:
Evidence:     ="4.12.0",G=200,X="Expected a function",Z="__lodash_hash_undefined__
CWE ID:       1395
WASC ID:
Source:       Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
 The identified library appears to be vulnerable.

Other Info:
 The identified library lodash, version 4.12.0 is vulnerable.
 CVE-2019-1010266
 CVE-2021-23337
```

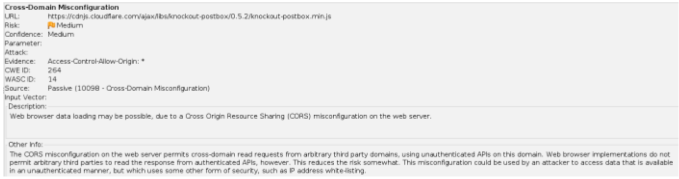
The security report identifies vulnerabilities related to the use of an out-of date JavaScript library called lodash v4.12.0.
Prototype pollution is one of the reported security holes in this version that might allow attackers to control how the application behaves.
The vulnerabilities that have been found are associated with CVE-2019-1010266 and CVE-2021-23337, which raise the possibility of unwanted access or malicious code execution.
This scan's detection methodology was passive, which means it detected risks without direct interaction by analyzing site reactions.



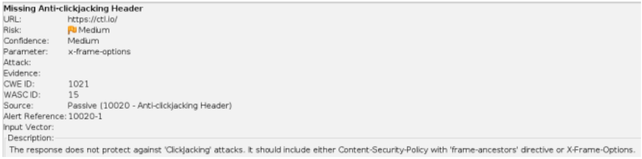
```
CSP: Failure to Define Directive with No Fallback
URL:             https://ctl.io/developers
Risk:            🚩 Medium
Confidence:      High
Parameter:       Content-Security-Policy
Attack:
Evidence:        default-src 'none'
CWE ID:          693
WASC ID:         15
Source:          Passive (10055 - 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.
```



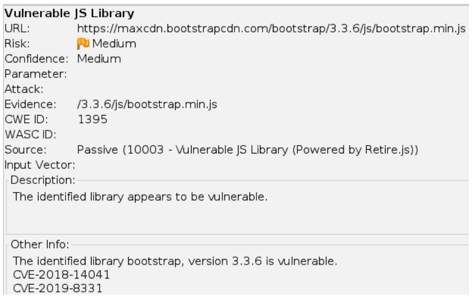
```
Content Security Policy (CSP) Header Not Set
URL:             https://ctl.io/
Risk:            🚩 Medium
Confidence:      High
Parameter:
Attack:
Evidence:
CWE ID:          693
WASC ID:         15
Source:          Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
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, ActiveX, audio and video files.
```



```
Cross-Domain Misconfiguration
URL:        https://cdnjs.cloudflare.com/ajax/libs/knockout-postbox/0.5.2/knockout-postbox.min.js
Risk:       🚩 Medium
Confidence: Medium
Parameter:
Attack:
Evidence:   Access-Control-Allow-Origin: *
CWE ID:     264
WASC ID:    14
Source:     Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:
Description:
 Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Other Info:
 The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not
 permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available
 in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
```

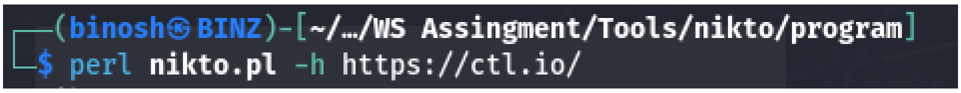


```
Missing Anti-clickjacking Header
URL:             https://ctl.io/
Risk:            🚩 Medium
Confidence:      Medium
Parameter:       x-frame-options
Attack:
Evidence:
CWE ID:          1021
WASC ID:         15
Source:          Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input 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.
```

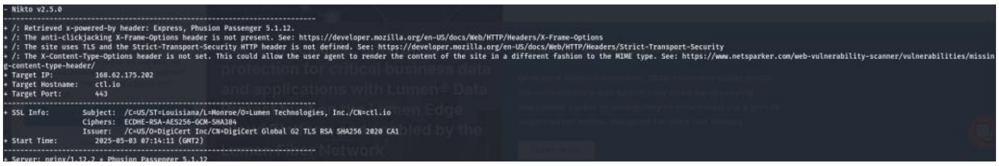


```
Vulnerable JS Library
URL:          https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/js/bootstrap.min.js
Risk:         🚩 Medium
Confidence:   Medium
Parameter:
Attack:
Evidence:     /3.3.6/js/bootstrap.min.js
CWE ID:       1395
WASC ID:
Source:       Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
 The identified library appears to be vulnerable.

Other Info:
 The identified library bootstrap, version 3.3.6 is vulnerable.
 CVE-2018-14041
 CVE-2019-8331
```

3.2 Nikto



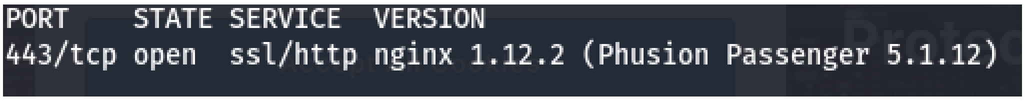
```
┌──(binosh㉿BINZ)-[~/…/WS Assingment/Tools/nikto/program]
└─$ perl nikto.pl -h https://ctl.io/
```



```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ /: Retrieved x-powered-by header: Express, Phusion Passenger 5.1.12.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missin
g-content-type-header/
+ Target IP:          168.62.175.202
+ Target Hostname:    ctl.io
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=Louisiana/L=Monroe/O=Lumen Technologies, Inc./CN=ctl.io
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
+ Start Time:         2025-05-03 07:14:11 (GMT2)
---------------------------------------------------------------------------
+ Server: nginx/1.12.2 + Phusion Passenger 5.1.12
```

The summarization of the above result is that IP address 168.62.175.202's hostname ctl.io on port 443 is missing important security headers including X-Frame-Options, X-Content-Type-Options, and Strict-Transport-Security. The server employs the ECDHE-RSA-AES256-GCM-SHA384 cypher suite and the DigiCert Global G2 TLS RSA SHA256 2020 CA1 certificate. The attack surface is increased by exposing the server stack, which includes nginx/1.12.2 and Phusion Passenger 5.1.12, and by exposing backend technologies like Express and Passenger through the X-Powered-By header. To improve security posture, it is advised to make improvements to server hardening, header configurations, and encryption procedures.

3.3 Nmap

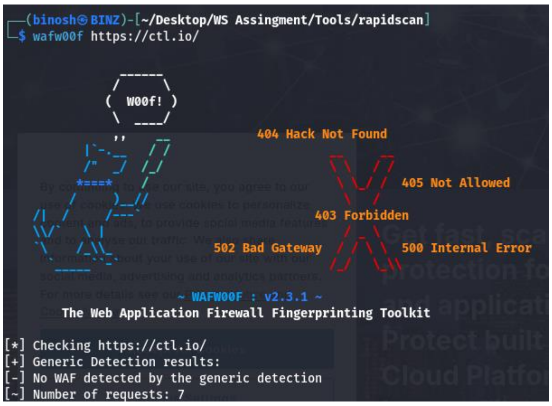


```
PORT     STATE SERVICE  VERSION
443/tcp open  ssl/http nginx 1.12.2 (Phusion Passenger 5.1.12)
```

This nmap scan was done to disclose the open ports and their service versions.

4. Firewall Detection

4.1 Wafw00f



```
┌──(binosh㉿BINZ)-[~/Desktop/WS Assingment/Tools/rapidscan]
└─$ wafw00f https://ctl.io/

                ( W00f! )
                                    404 Hack Not Found
                                                   405 Not Allowed
                                         403 Forbidden
                               502 Bad Gateway        500 Internal Error

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

[*] Checking https://ctl.io/
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

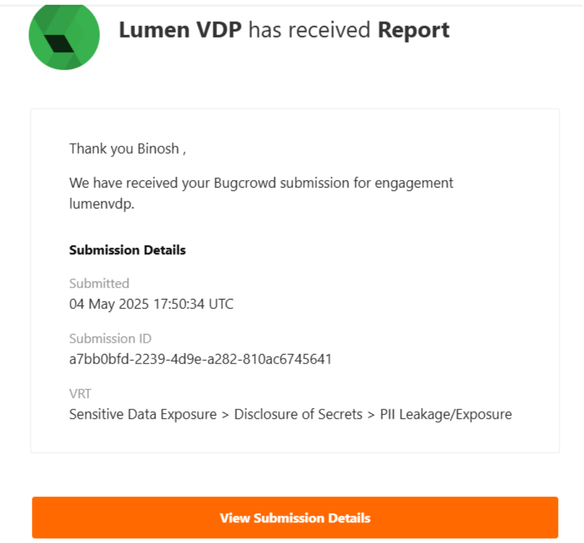
SQL Injection

The website appears to have a high-risk SQL Injection attack vulnerability. Because of this vulnerability, attackers can use input fields to insert malicious SQL queries into the database, which could result in sensitive data being accessed without authorization, database alteration, or even the loss of important records.

Mitigation Strategy we can use

- Update Lodash to 4.17.21 or later to address ReDoS vulnerabilities and prototype pollution.
- Update Moment.js to 2.29.4 or above to minimize security issues with regex.
- To reduce XSS vulnerabilities, update Knockout to 3.5.0 or later.
- Because previous versions of jQuery are vulnerable and deprecated, update to 3.6.0 or later.
- To fix known XSS vulnerabilities, update jQuery UI to version 1.13.2 or higher.
- To fix XSS vulnerabilities, update Bootstrap to 3.4.0 or later.
- To stop script injections, clean up the Bootstrap tooltip properties (data-container, data-viewport, and data-template).
- To prevent unwanted script execution, use robust Content Security Policy (CSP) headers.
- Implement stringent input validation and sanitization, particularly for locale changes and user-generated information.
- Limit input processing to reduce the attack surface for assaults that rely on regular expressions.

Proof of report Submission



Lumen VDP has received **Report**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement lumenvdp.

Submission Details

Submitted
04 May 2025 17:50:34 UTC

Submission ID
a7bb0bfd-2239-4d9e-a282-810ac6745641

VRT
Sensitive Data Exposure > Disclosure of Secrets > PII Leakage/Exposure