Sri Lanka Institute of Information Technology

Bug Bounty - Report 04

Vulnerable JS Library

jQuery UI - v1.13.1

Student Name – Wanasinghe N.K

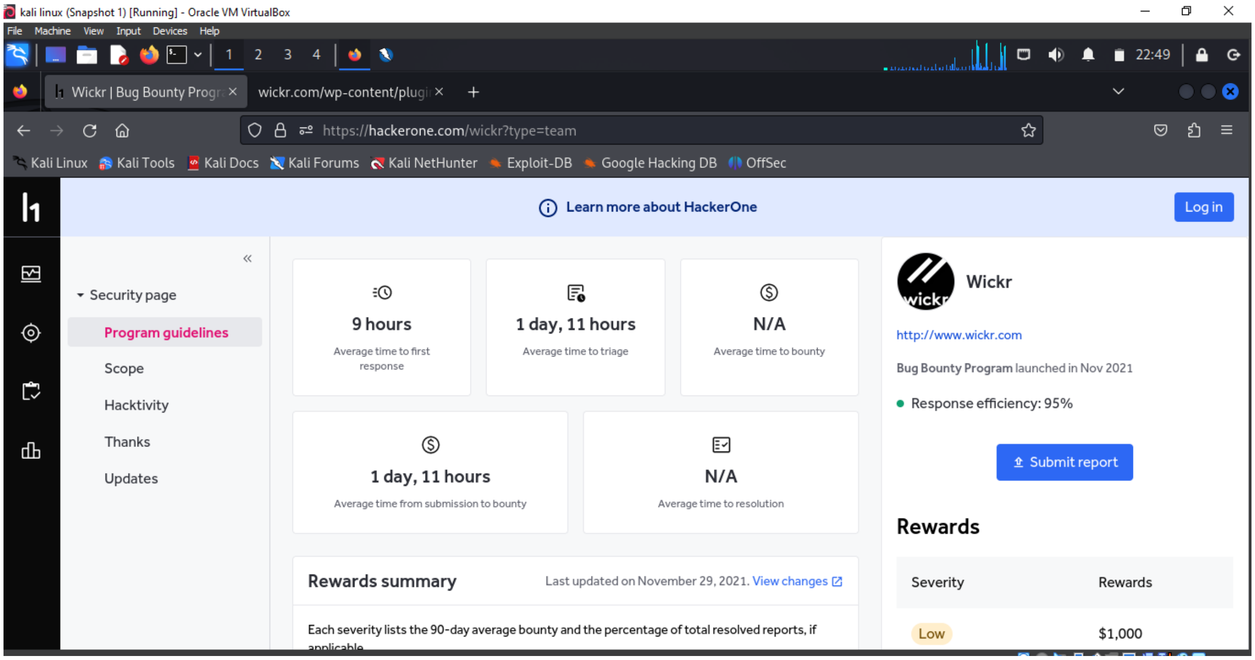
Student ID – IT23221000

IE2062 - Web Security

B.Sc. (Hons) in information Technology Specializing in Cyber Security

Report 04 – wickr.com (Hackerone)

Main domain – www.wickr.com/



9 hours
Average time to first response

1 day, 11 hours
Average time to triage

N/A
Average time to bounty

1 day, 11 hours
Average time from submission to bounty

N/A
Average time to resolution

Rewards summary

Last updated on November 29, 2021. View changes

Each severity lists the 90-day average bounty and the percentage of total resolved reports, if applicable

Wickr

http://www.wickr.com

Bug Bounty Program launched in Nov 2021

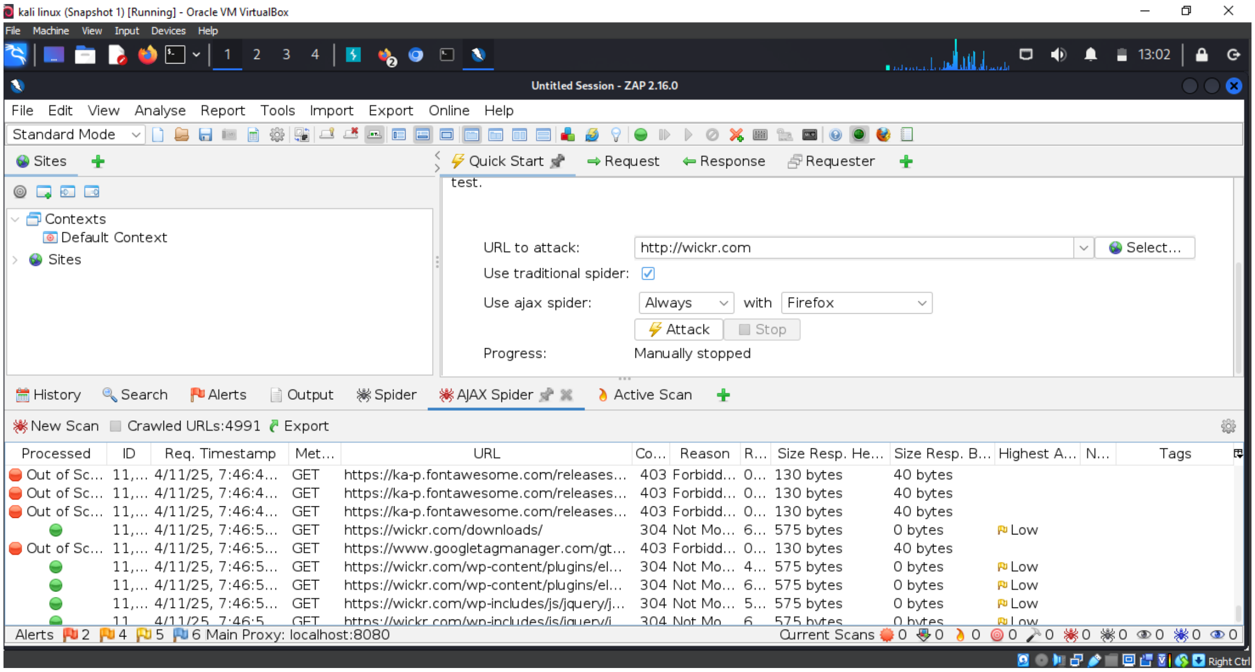
Response efficiency: 95%

Rewards

Severity	Rewards
Low	$1,000

I used OWASP ZAP tool to scan the website.

All the in scope and out of scope domains were found through running a AJAX spider attack.


kali linux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
13:02
Untitled Session - ZAP 2.16.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
New Scan
Export

test.

URL to attack: http://wickr.com

Use traditional spider: ☑

Use ajax spider: Always with Firefox

Attack Stop

Progress: Manually stopped

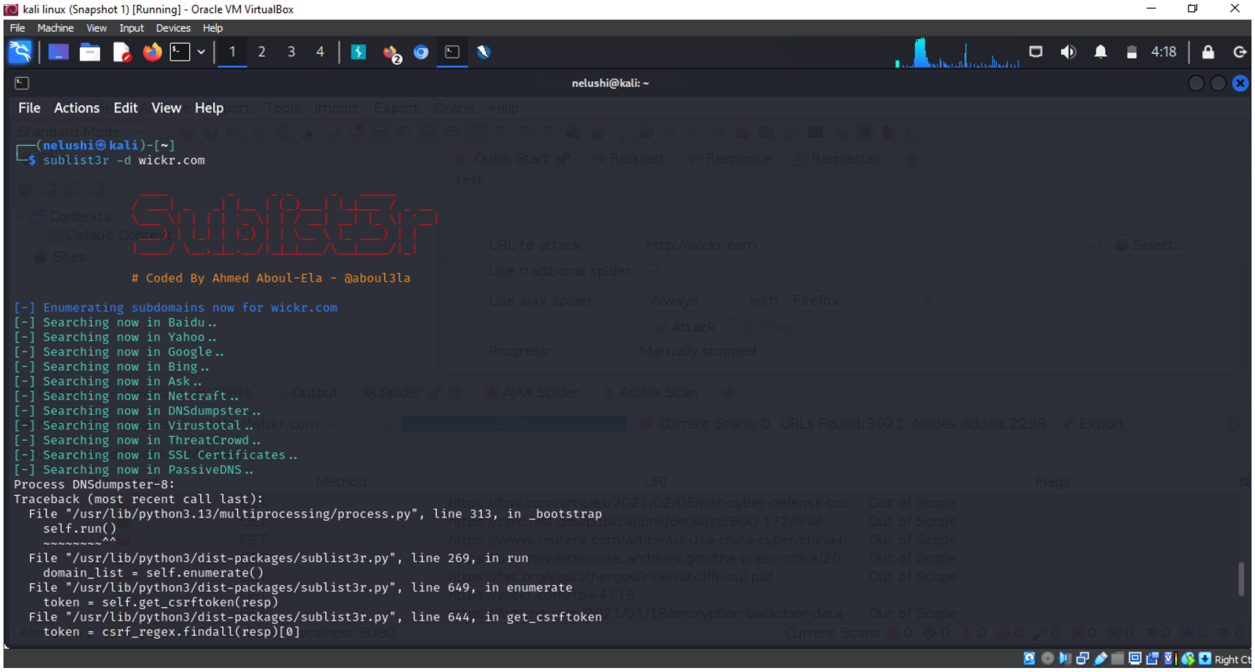
Crawled URLs:4991

Processed	ID	Req. Timestamp	Met...	URL	Co...	Reason	R...	Size Resp. He...	Size Resp. B...	Highest A...	N...	Tags
Out of Sc...	11,...	4/11/25, 7:46:4...	GET	https://ka-p.fontawesome.com/releases...	403	Forbidd...	0...	130 bytes	40 bytes			
Out of Sc...	11,...	4/11/25, 7:46:4...	GET	https://ka-p.fontawesome.com/releases...	403	Forbidd...	0...	130 bytes	40 bytes			
Out of Sc...	11,...	4/11/25, 7:46:4...	GET	https://ka-p.fontawesome.com/releases...	403	Forbidd...	0...	130 bytes	40 bytes			
●	11,...	4/11/25, 7:46:5...	GET	https://wickr.com/downloads/	304	Not Mo...	6...	575 bytes	0 bytes	Low		
Out of Sc...	11,...	4/11/25, 7:46:5...	GET	https://www.googletagmanager.com/gt...	403	Forbidd...	0...	130 bytes	40 bytes			
●	11,...	4/11/25, 7:46:5...	GET	https://wickr.com/wp-content/plugins/el...	304	Not Mo...	4...	575 bytes	0 bytes	Low		
●	11,...	4/11/25, 7:46:5...	GET	https://wickr.com/wp-content/plugins/el...	304	Not Mo...	6...	575 bytes	0 bytes	Low		
●	11,...	4/11/25, 7:46:5...	GET	https://wickr.com/wp-includes/js/jquery/j...	304	Not Mo...	5...	575 bytes	0 bytes	Low		
●	11	4/11/25 7:46:5	GET	https://wickr.com/wp-includes/js/jquery/j	304	Not Mo	6	575 bytes	0 bytes	Low		

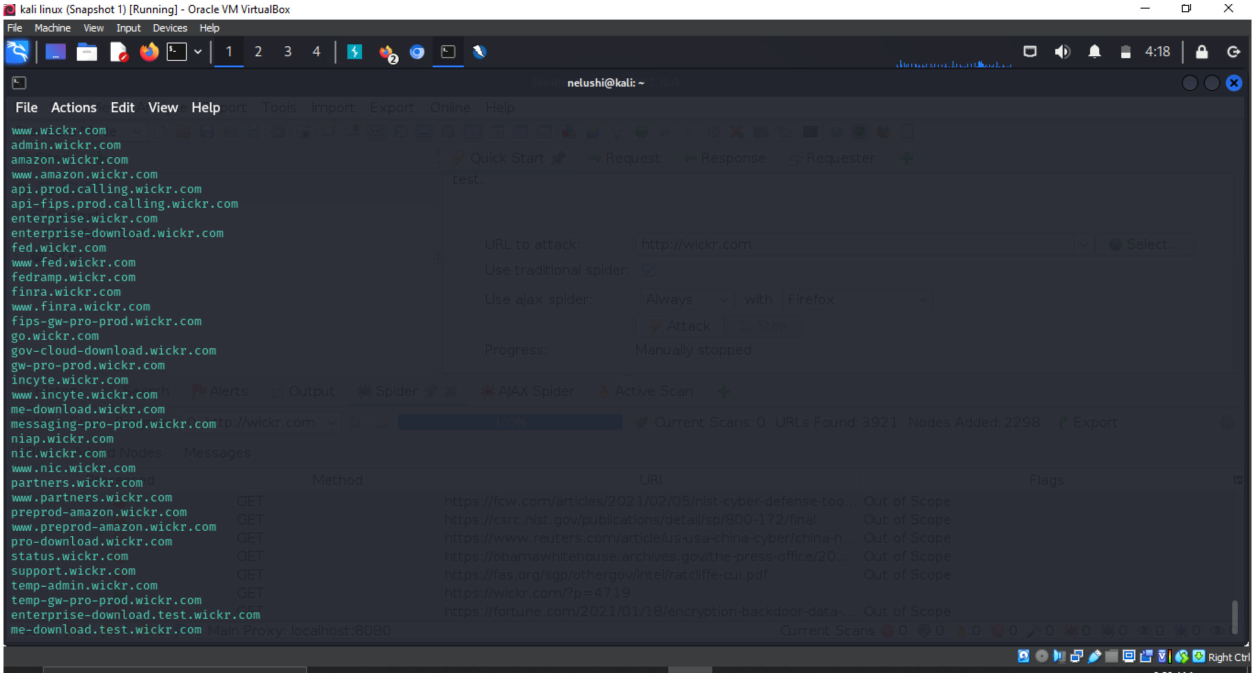
Alerts 2 4 5 6 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

Reconnaissance: Gather information about the target.

I found all the subdomains of the wickr website using the **sublist3r** tool.


kali linux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nelushi@kali: ~
File Actions Edit View Help
4:18

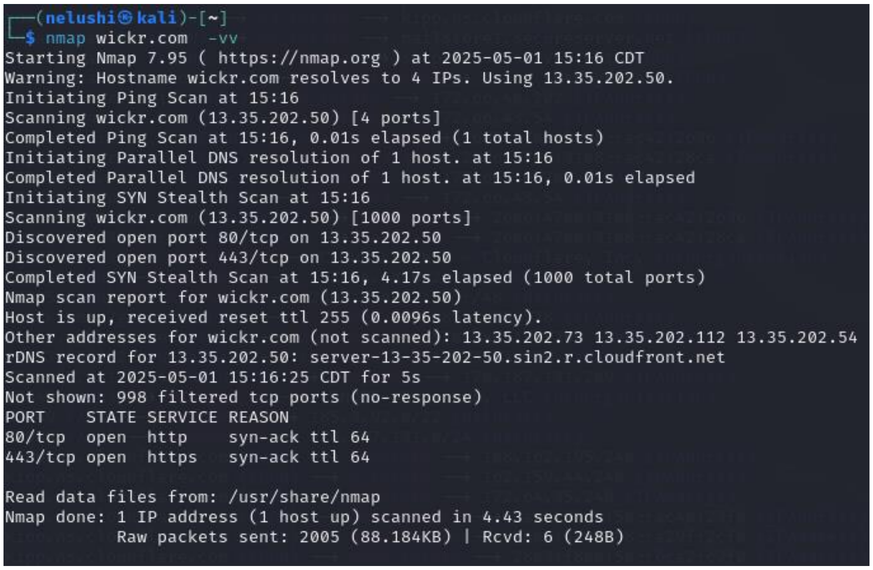
```
┌──(nelushi㉿kali)-[~]
└─$ sublist3r -d wickr.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for wickr.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~~~~^^
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrftoken(resp)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
```


kali linux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nelushi@kali: ~
File Actions Edit View Help
4:18

```
www.wickr.com
admin.wickr.com
amazon.wickr.com
www.amazon.wickr.com
api.prod.calling.wickr.com
api-fips.prod.calling.wickr.com
enterprise.wickr.com
enterprise-download.wickr.com
fed.wickr.com
www.fed.wickr.com
fedramp.wickr.com
finra.wickr.com
www.finra.wickr.com
fips-gw-pro-prod.wickr.com
go.wickr.com
gov-cloud-download.wickr.com
gw-pro-prod.wickr.com
incyte.wickr.com
www.incyte.wickr.com
me-download.wickr.com
messaging-pro-prod.wickr.com
niap.wickr.com
nic.wickr.com
www.nic.wickr.com
partners.wickr.com
www.partners.wickr.com
preprod-amazon.wickr.com
www.preprod-amazon.wickr.com
pro-download.wickr.com
status.wickr.com
support.wickr.com
temp-admin.wickr.com
temp-gw-pro-prod.wickr.com
enterprise-download.test.wickr.com
me-download.test.wickr.com
```

Nmap – Network scanning and enumeration

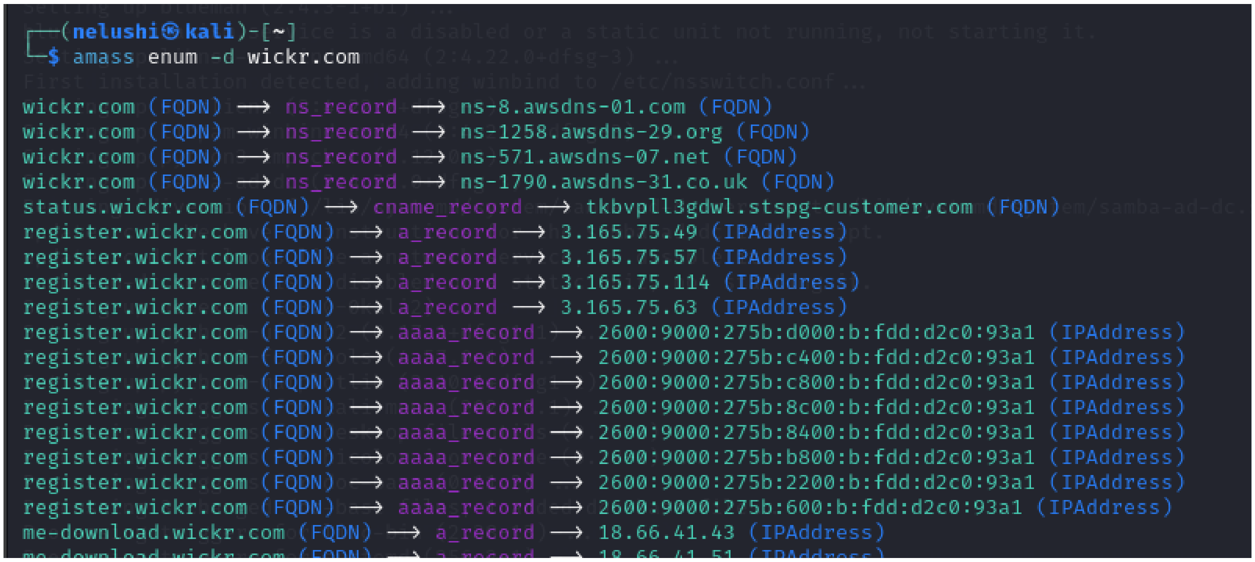
I found all the open ports and detected the running services on the target server using Nmap



```
┌──(nelushi㉿kali)-[~]
└─$ nmap wickr.com  -vv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 15:16 CDT
Warning: Hostname wickr.com resolves to 4 IPs. Using 13.35.202.50.
Initiating Ping Scan at 15:16
Scanning wickr.com (13.35.202.50) [4 ports]
Completed Ping Scan at 15:16, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:16
Completed Parallel DNS resolution of 1 host. at 15:16, 0.01s elapsed
Initiating SYN Stealth Scan at 15:16
Scanning wickr.com (13.35.202.50) [1000 ports]
Discovered open port 80/tcp on 13.35.202.50
Discovered open port 443/tcp on 13.35.202.50
Completed SYN Stealth Scan at 15:16, 4.17s elapsed (1000 total ports)
Nmap scan report for wickr.com (13.35.202.50)
Host is up, received reset ttl 255 (0.0096s latency).
Other addresses for wickr.com (not scanned): 13.35.202.73 13.35.202.112 13.35.202.54
rDNS record for 13.35.202.50: server-13-35-202-50.sin2.r.cloudfront.net
Scanned at 2025-05-01 15:16:25 CDT for 5s
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE REASON
80/tcp  open  http    syn-ack ttl 64
443/tcp open  https   syn-ack ttl 64

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.43 seconds
           Raw packets sent: 2005 (88.184KB) | Rcvd: 6 (248B)
```

Amass – Subdomain and DNS mapping

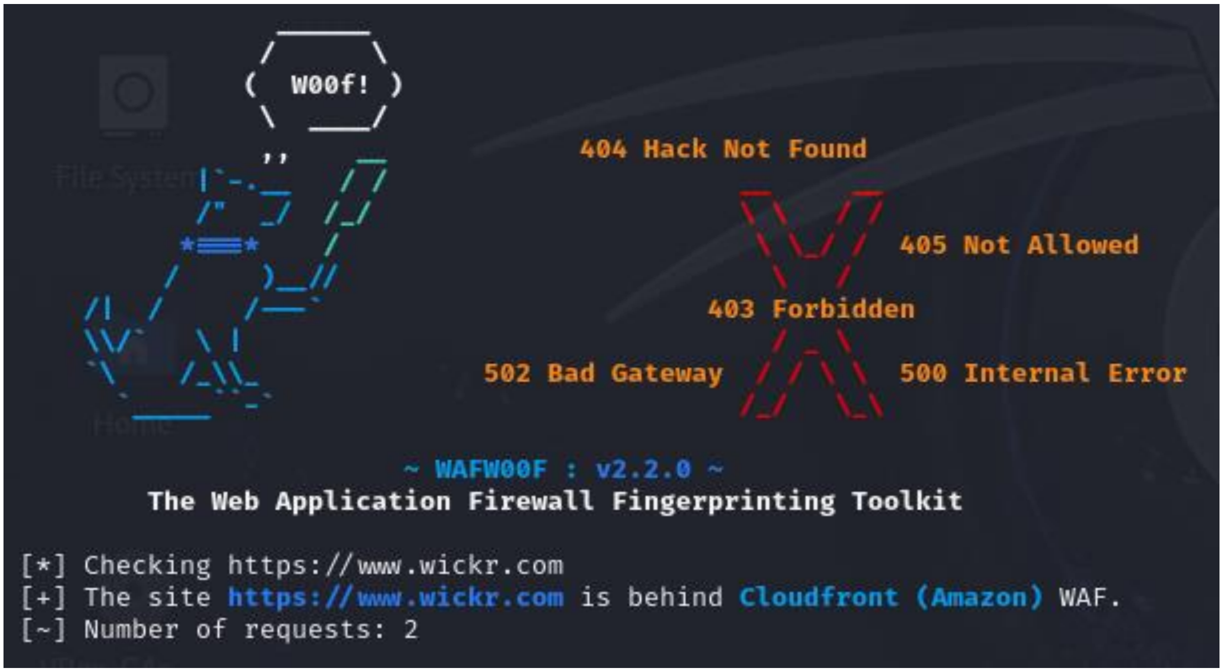
I found all the subdomains related to the target domain using Amass.



```
┌──(nelushi㉿kali)-[~]
└─$ amass enum -d wickr.com

wickr.com (FQDN) ⟶ ns_record ⟶ ns-8.awsdns-01.com (FQDN)
wickr.com (FQDN) ⟶ ns_record ⟶ ns-1258.awsdns-29.org (FQDN)
wickr.com (FQDN) ⟶ ns_record ⟶ ns-571.awsdns-07.net (FQDN)
wickr.com (FQDN) ⟶ ns_record ⟶ ns-1790.awsdns-31.co.uk (FQDN)
status.wickr.com (FQDN) ⟶ cname_record ⟶ tkbvpll3gdwl.stspg-customer.com (FQDN)
register.wickr.com (FQDN) ⟶ a_record ⟶ 3.165.75.49 (IPAddress)
register.wickr.com (FQDN) ⟶ a_record ⟶ 3.165.75.57 (IPAddress)
register.wickr.com (FQDN) ⟶ a_record ⟶ 3.165.75.114 (IPAddress)
register.wickr.com (FQDN) ⟶ a_record ⟶ 3.165.75.63 (IPAddress)
register.wickr.com (FQDN) ⟶ aaaa_record ⟶ 2600:9000:275b:d000:b:fdd:d2c0:93a1 (IPAddress)
register.wickr.com (FQDN) ⟶ aaaa_record ⟶ 2600:9000:275b:c400:b:fdd:d2c0:93a1 (IPAddress)
register.wickr.com (FQDN) ⟶ aaaa_record ⟶ 2600:9000:275b:c800:b:fdd:d2c0:93a1 (IPAddress)
register.wickr.com (FQDN) ⟶ aaaa_record ⟶ 2600:9000:275b:8c00:b:fdd:d2c0:93a1 (IPAddress)
register.wickr.com (FQDN) ⟶ aaaa_record ⟶ 2600:9000:275b:8400:b:fdd:d2c0:93a1 (IPAddress)
register.wickr.com (FQDN) ⟶ aaaa_record ⟶ 2600:9000:275b:b800:b:fdd:d2c0:93a1 (IPAddress)
register.wickr.com (FQDN) ⟶ aaaa_record ⟶ 2600:9000:275b:2200:b:fdd:d2c0:93a1 (IPAddress)
register.wickr.com (FQDN) ⟶ aaaa_record ⟶ 2600:9000:275b:600:b:fdd:d2c0:93a1 (IPAddress)
me-download.wickr.com (FQDN) ⟶ a_record ⟶ 18.66.41.43 (IPAddress)
me-download.wickr.com (FQDN) ⟶ a_record ⟶ 18.66.41.51 (IPAddress)
```

Wafw00f – Firewall Detection

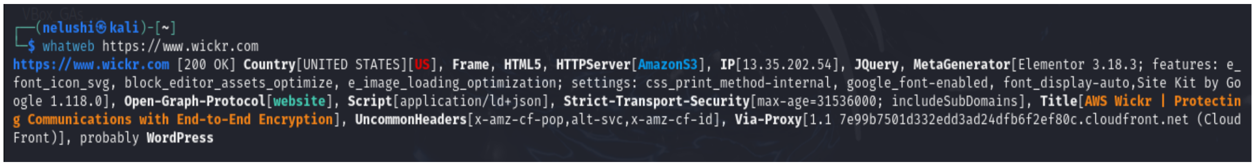
Command used – wafw00f https://www.wickr.com



```
                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.wickr.com
[+] The site https://www.wickr.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

Whatweb – to identify the technologies used by the site.

Commans used – whatweb https://www.wickr.com



```
┌──(nelushi㉿kali)-[~]
└─$ whatweb https://www.wickr.com
https://www.wickr.com [200 OK] Country[UNITED STATES][US], Frame, HTML5, HTTPServer[AmazonS3], IP[13.35.202.54], JQuery, MetaGenerator[Elementor 3.18.3; features: e_
font_icon_svg, block_editor_assets_optimize, e_image_loading_optimization; settings: css_print_method-internal, google_font-enabled, font_display-auto,Site Kit by Go
ogle 1.118.0], Open-Graph-Protocol[website], Script[application/ld+json], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[AWS Wickr | Protectin
g Communications with End-to-End Encryption], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 7e99b7501d332edd3ad24dfb6f2ef80c.cloudfront.net (Cloud
Front)], probably WordPress
```

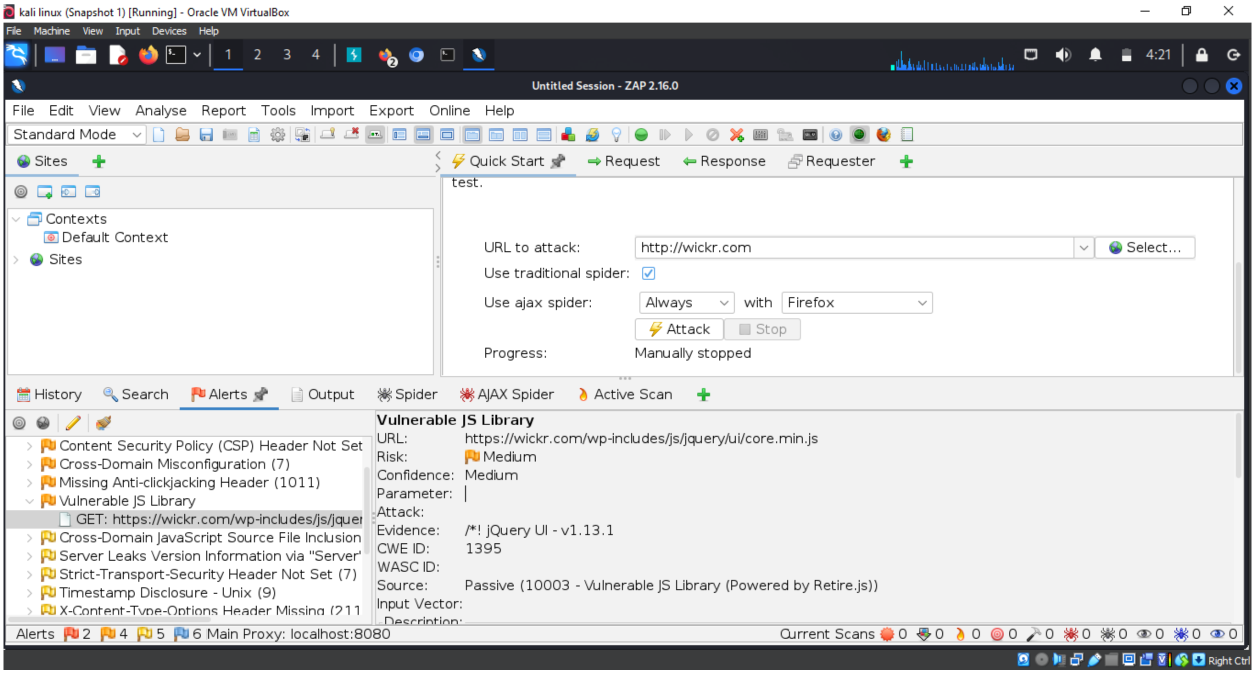
Vulnerability 01

Domain

https://wickr.com/wp-includes/js/jquery/ui/core.min.js

Vulnerability title

Vulnerable JS Library - jQuery UI - v1.13.


kali linux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
4:21
Untitled Session - ZAP 2.16.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Right Ctrl

test.

URL to attack: http://wickr.com
Select...
Use traditional spider: ☑
Use ajax spider: Always with Firefox
Attack Stop
Progress: Manually stopped

Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (7)
Missing Anti-clickjacking Header (1011)
Vulnerable JS Library
GET: https://wickr.com/wp-includes/js/jquer
Cross-Domain JavaScript Source File Inclusion
Server Leaks Version Information via "Server"
Strict-Transport-Security Header Not Set (7)
Timestamp Disclosure - Unix (9)
X-Content-Type-Options Header Missing (211

Vulnerable JS Library
URL: https://wickr.com/wp-includes/js/jquery/ui/core.min.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: /*! jQuery UI - v1.13.1
CWE ID: 1395
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:

Alerts 2 4 5 6 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

Vulnerability description

Vulnerable JavaScript Libraries - A Summary

Web applications often use JavaScript libraries for adding any dynamic or interactive features and saving development time.

A vulnerable javascript library is actually a third-party JavaScript library that has been used in an old version which does not have security patches or an insecure version that comes with typical security bug.

These bugs could lead to attacks such as Cross-Site Scripting (XSS), code injection, or even data manipulation.

Therefore, keeping libraries up to date becomes important for an overall security model of web applications.

Specific Case: jquery-ui v1.13.1

The library that was used in this case is: jquery-ui, in version 1.13.1.

It is a known vulnerability for this version, related to the following security issue:

CVE-2022-31160 - Stored XSS vulnerability in the checkboxradio module.

Attackers could take advantage of this by inserting harmful JavaScript in UI elements that could then be stored and executed later.

Version 1.13.2 addresses this vulnerability.

Therefore, an upgrade is strongly recommended.

Affected components

The **checkboxradio module** allows injection of malicious scripts via **dynamic labels** and **tooltips**, due to improper input sanitization.

Impact assessment

Severity – Medium

- Stored XSS Attacks

These are the types of attacks when a malicious script is injected into the application and is executed whenever the UI component is loaded.

- Session Hijacking and Credential Theft

This results in cookie theft or sensitive form data theft by executing malicious scripts.

- Privilege Escalation

The attacker may act with elevated privileges by injecting malicious scripts into an admin panel.

- Defacement or UI Manipulation

The injected script can modify the appearance or behavior of the interface.

- Redirects To Malicious Sites

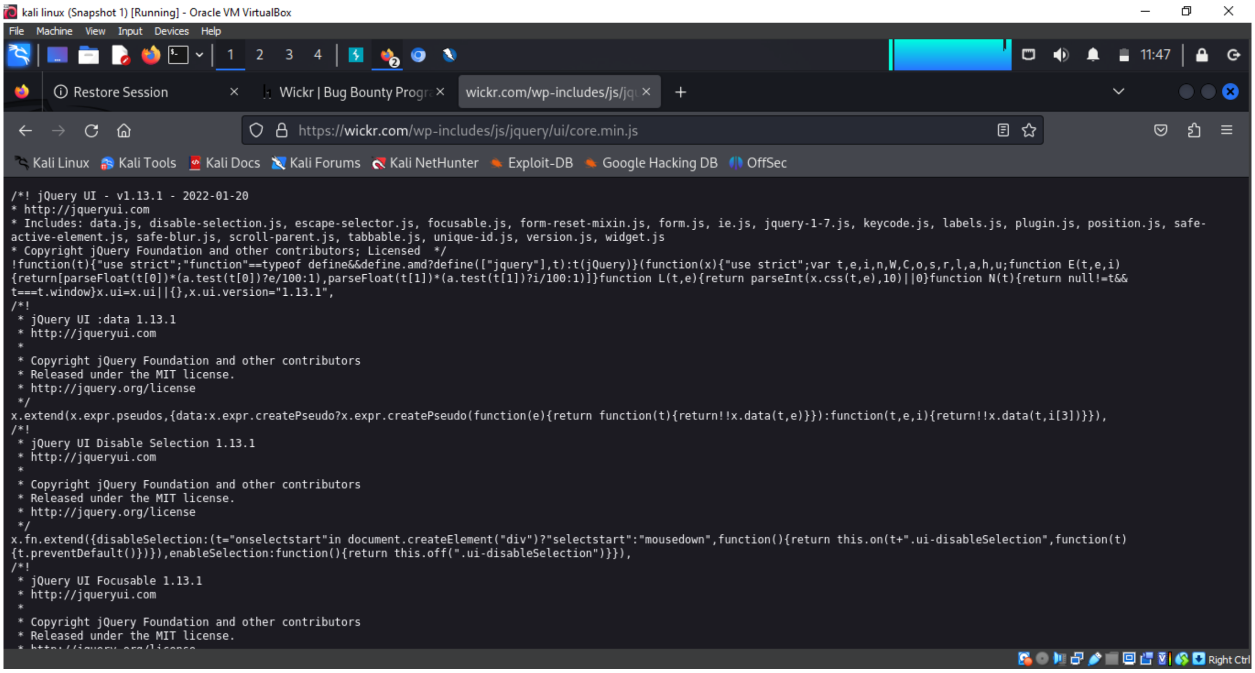
The victim is silently redirected to phishing or malware sites.

- Loss of user trust

Intrusive pop-ups, altered UI, or errors caused by JavaScripts will reduce the user trust level over a site.

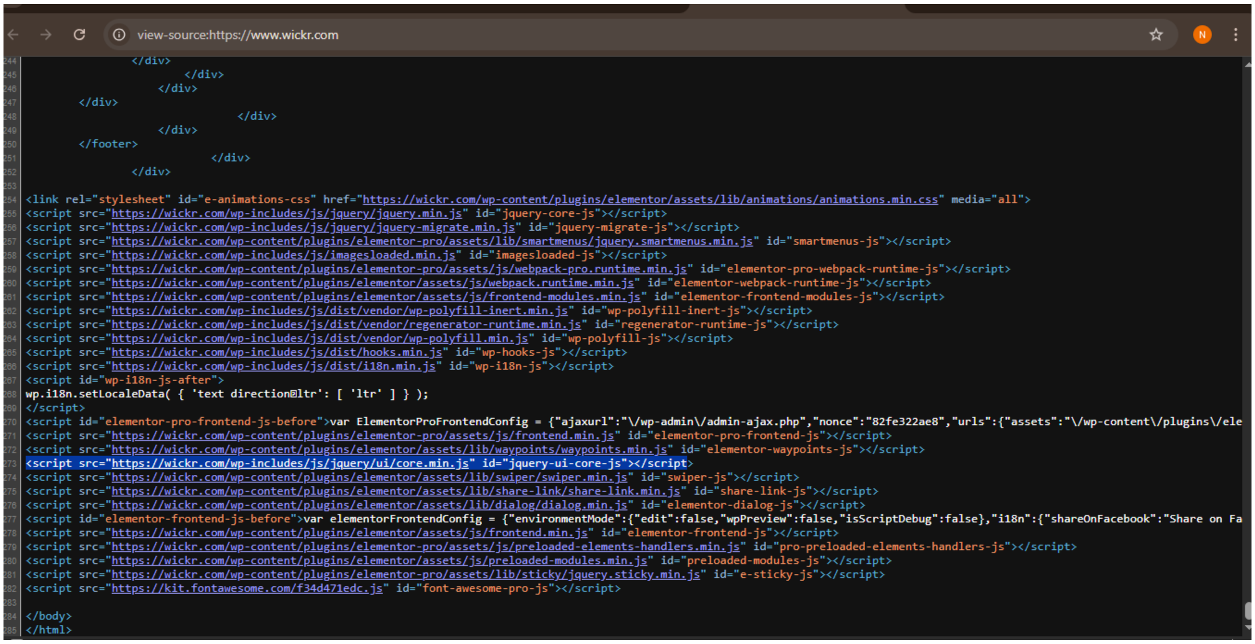
Steps to reproduce with Proof of Concept (poc)

1. First, I navigated the vulnerable JS link and observed it.


kali linux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:47
Restore Session
Wickr | Bug Bounty Progr
wickr.com/wp-includes/js/jq
https://wickr.com/wp-includes/js/jquery/ui/core.min.js
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Right Ctrl

```
/*! jQuery UI - v1.13.1 - 2022-01-20
* http://jqueryui.com
* Includes: data.js, disable-selection.js, escape-selector.js, focusable.js, form-reset-mixin.js, form.js, ie.js, jquery-1-7.js, keycode.js, labels.js, plugin.js, position.js, safe-active-element.js, safe-blur.js, scroll-parent.js, tabbable.js, unique-id.js, version.js, widget.js
* Copyright jQuery Foundation and other contributors; Licensed  */
!function(t){"use strict";"function"==typeof define&&define.amd?define(["jquery"],t):t(jQuery)}(function(x){"use strict";var t,e,i,n,W,C,o,s,r,l,a,h,u;function E(t,e,i)
{return[parseFloat(t[0])*(a.test(t[0])?e/100:1),parseFloat(t[1])*(a.test(t[1])?i/100:1)]}function L(t,e){return parseInt(x.css(t,e),10)||0}function N(t){return null!=t&&
t===t.window}x.ui=x.ui||{},x.ui.version="1.13.1",
/*!
 * jQuery UI :data 1.13.1
 * http://jqueryui.com
 *
 * Copyright jQuery Foundation and other contributors
 * Released under the MIT license.
 * http://jquery.org/license
 */
x.extend(x.expr.pseudos,{data:x.expr.createPseudo?x.expr.createPseudo(function(e){return function(t){return!!x.data(t,e)}}):function(t,e,i){return!!x.data(t,i[3])}}),
/*!
 * jQuery UI Disable Selection 1.13.1
 * http://jqueryui.com
 *
 * Copyright jQuery Foundation and other contributors
 * Released under the MIT license.
 * http://jquery.org/license
 */
x.fn.extend({disableSelection:(t="onselectstart"in document.createElement("div")?"selectstart":"mousedown",function(){return this.on(t+".ui-disableSelection",function(t)
{t.preventDefault()})}),enableSelection:function(){return this.off(".ui-disableSelection")}}),
/*!
 * jQuery UI Focusable 1.13.1
 * http://jqueryui.com
 *
 * Copyright jQuery Foundation and other contributors
 * Released under the MIT license.
 * http://jquery.org/license
```

2. Next, I searched whether this js file is included in the source code of the wickr.com site.



```
                </div>
                        </div>
                    </div>
        </div>
                                </div>
                    </div>
        </footer>
                            </div>
                </div>

<link rel="stylesheet" id="e-animations-css" href="https://wickr.com/wp-content/plugins/elementor/assets/lib/animations/animations.min.css" media="all">
<script src="https://wickr.com/wp-includes/js/jquery/jquery.min.js" id="jquery-core-js"></script>
<script src="https://wickr.com/wp-includes/js/jquery/jquery-migrate.min.js" id="jquery-migrate-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor-pro/assets/lib/smartmenus/jquery.smartmenus.min.js" id="smartmenus-js"></script>
<script src="https://wickr.com/wp-includes/js/imagesloaded.min.js" id="imagesloaded-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor-pro/assets/js/webpack-pro.runtime.min.js" id="elementor-pro-webpack-runtime-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js" id="elementor-webpack-runtime-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor/assets/js/frontend-modules.min.js" id="elementor-frontend-modules-js"></script>
<script src="https://wickr.com/wp-includes/js/dist/vendor/wp-polyfill-inert.min.js" id="wp-polyfill-inert-js"></script>
<script src="https://wickr.com/wp-includes/js/dist/vendor/regenerator-runtime.min.js" id="regenerator-runtime-js"></script>
<script src="https://wickr.com/wp-includes/js/dist/vendor/wp-polyfill.min.js" id="wp-polyfill-js"></script>
<script src="https://wickr.com/wp-includes/js/dist/hooks.min.js" id="wp-hooks-js"></script>
<script src="https://wickr.com/wp-includes/js/dist/i18n.min.js" id="wp-i18n-js"></script>
<script id="wp-i18n-js-after">
wp.i18n.setLocaleData( { 'text direction␂ltr': [ 'ltr' ] } );
</script>
<script id="elementor-pro-frontend-js-before">var ElementorProFrontendConfig = {"ajaxurl":"\/wp-admin\/admin-ajax.php","nonce":"82fe322ae8","urls":{"assets":"\/wp-content\/plugins\/ele
<script src="https://wickr.com/wp-content/plugins/elementor-pro/assets/js/frontend.min.js" id="elementor-pro-frontend-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js" id="elementor-waypoints-js"></script>
<script src="https://wickr.com/wp-includes/js/jquery/ui/core.min.js" id="jquery-ui-core-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js" id="swiper-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js" id="share-link-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js" id="elementor-dialog-js"></script>
<script id="elementor-frontend-js-before">var elementorFrontendConfig = {"environmentMode":{"edit":false,"wpPreview":false,"isScriptDebug":false},"i18n":{"shareOnFacebook":"Share on Fa
<script src="https://wickr.com/wp-content/plugins/elementor/assets/js/frontend.min.js" id="elementor-frontend-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor-pro/assets/js/preloaded-elements-handlers.min.js" id="pro-preloaded-elements-handlers-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor/assets/js/preloaded-modules.min.js" id="preloaded-modules-js"></script>
<script src="https://wickr.com/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js" id="e-sticky-js"></script>
<script src="https://kit.fontawesome.com/f34d471edc.js" id="font-awesome-pro-js"></script>

</body>
</html>
```

It is included in the source code of the site.

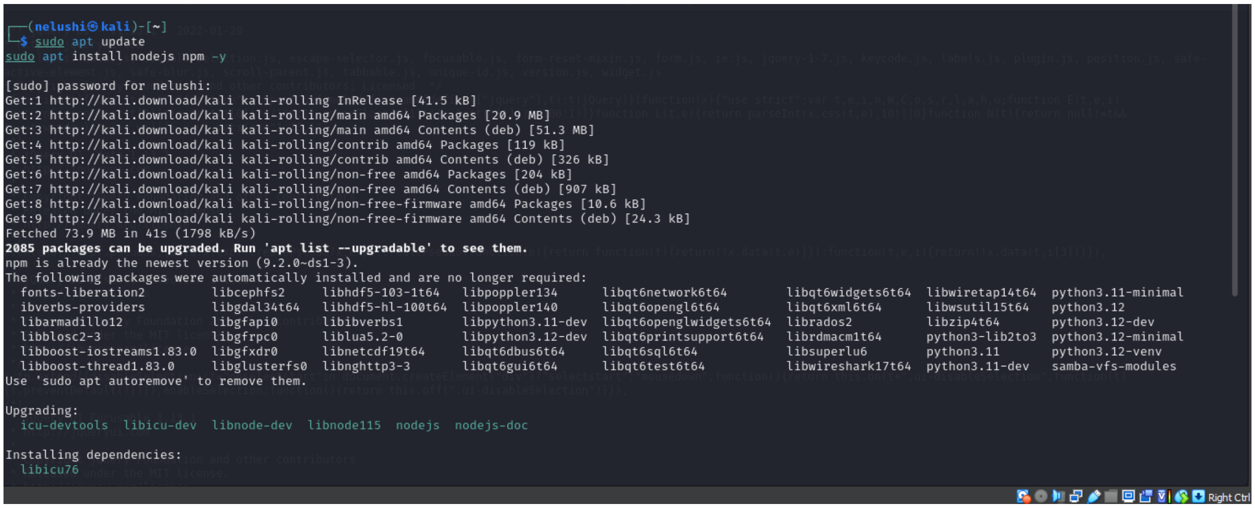
3. Next, I used a tool called **Retire.js** to detect known vulnerabilities in js libraries used in this site, and their CVE numbers.

What is the purpose of Retire.js?

It checks if a site is using javascript libraries with known vulnerabilities by comparing versions to vulnerability databases like CVE.

It provides a link to the specific vulnerability and we can read more about the issue by navigating the link.

✓ First, I installed Retire.js using the commands,
sudo apt install nodejs npm -y

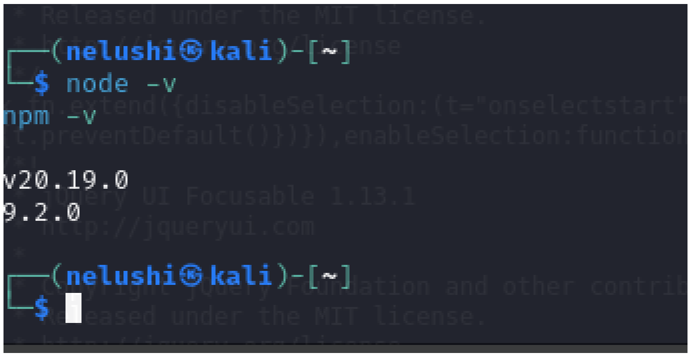


```
┌──(nelushi㉿kali)-[~]
└─$ sudo apt update
sudo apt install nodejs npm -y

[sudo] password for nelushi:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.3 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [326 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [907 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 73.9 MB in 41s (1798 kB/s)
2085 packages can be upgraded. Run 'apt list --upgradable' to see them.
npm is already the newest version (9.2.0~ds1-3).
The following packages were automatically installed and are no longer required:
  fonts-liberation2         libcephfs2     libhdf5-103-1t64   libpoppler134      libqt6network6t64        libqt6widgets6t64  libwiretap14t64  python3.11-minimal
  ibverbs-providers         libgdal34t64   libhdf5-hl-100t64  libpoppler140      libqt6opengl6t64         libqt6xml6t64      libwsutil15t64   python3.12
  libarmadillo12            libgfapi0      libibverbs1        libpython3.11-dev  libqt6openglwidgets6t64  librados2          libzip4t64       python3.12-dev
  libblosc2-3               libgfrpc0      liblua5.2-0        libpython3.12-dev  libqt6printsupport6t64   librdmacm1t64      python3-lib2to3  python3.12-minimal
  libboost-iostreams1.83.0  libgfxdr0      libnetcdf19t64     libqt6dbus6t64     libqt6sql6t64            libsuperlu6        python3.11       python3.12-venv
  libboost-thread1.83.0     libglusterfs0  libnghttp3-3       libqt6gui6t64      libqt6test6t64           libwireshark17t64  python3.11-dev   samba-vfs-modules
Use 'sudo apt autoremove' to remove them.

Upgrading:
  icu-devtools  libicu-dev  libnode-dev  libnode115  nodejs  nodejs-doc

Installing dependencies:
  libicu76
```

✓ I checked the versions using the commands,

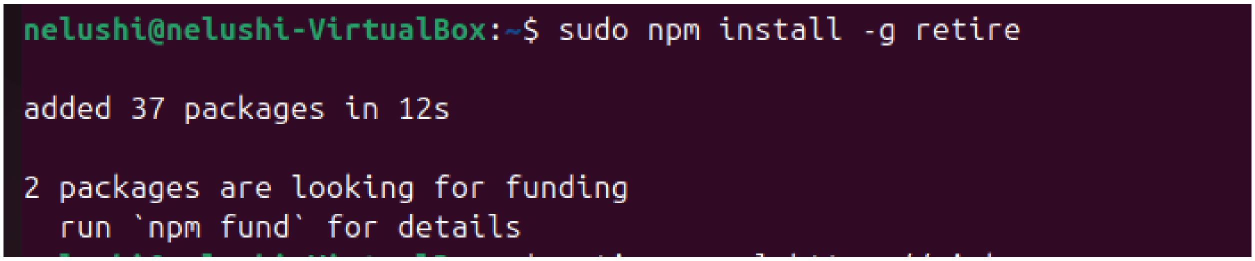
node -v

npm -v



```
┌──(nelushi㉿kali)-[~]
└─$ node -v
npm -v
v20.19.0
9.2.0

┌──(nelushi㉿kali)-[~]
└─$ 
```

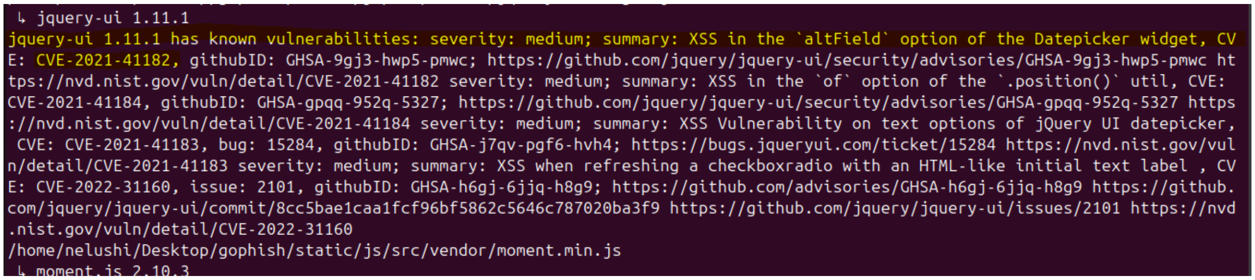
✓ I installed Retire.js globally using the command,
sudo npm install -g retire



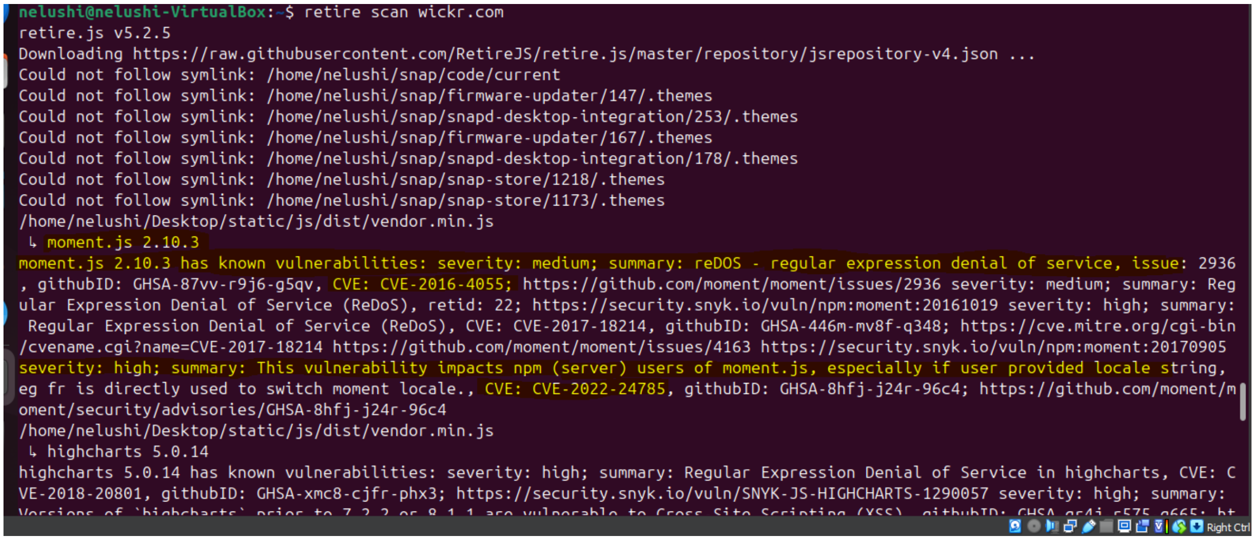
```
nelushi@nelushi-VirtualBox:~$ sudo npm install -g retire

added 37 packages in 12s

2 packages are looking for funding
  run `npm fund` for details
```

✓ I scanned the website using **retire** command.

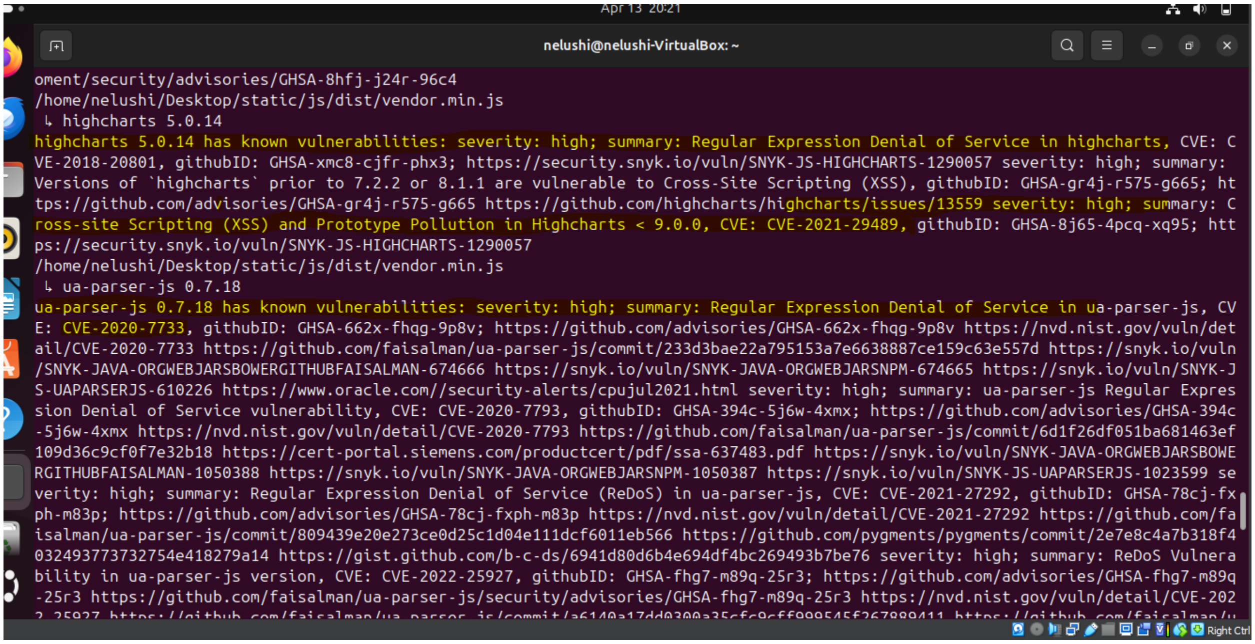
Retire scan wickr.com



```
 ↳ jquery-ui 1.11.1
jquery-ui 1.11.1 has known vulnerabilities: severity: medium; summary: XSS in the `altField` option of the Datepicker widget, CV
E: CVE-2021-41182, githubID: GHSA-9gj3-hwp5-pmwc; https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc ht
tps://nvd.nist.gov/vuln/detail/CVE-2021-41182 severity: medium; summary: XSS in the `of` option of the `.position()` util, CVE:
CVE-2021-41184, githubID: GHSA-gpqq-952q-5327; https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327 https
://nvd.nist.gov/vuln/detail/CVE-2021-41184 severity: medium; summary: XSS Vulnerability on text options of jQuery UI datepicker,
 CVE: CVE-2021-41183, bug: 15284, githubID: GHSA-j7qv-pgf6-hvh4; https://bugs.jqueryui.com/ticket/15284 https://nvd.nist.gov/vul
n/detail/CVE-2021-41183 severity: medium; summary: XSS when refreshing a checkboxradio with an HTML-like initial text label , CV
E: CVE-2022-31160, issue: 2101, githubID: GHSA-h6gj-6jjq-h8g9; https://github.com/advisories/GHSA-h6gj-6jjq-h8g9 https://github.
com/jquery/jquery-ui/commit/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9 https://github.com/jquery/jquery-ui/issues/2101 https://nvd
.nist.gov/vuln/detail/CVE-2022-31160
/home/nelushi/Desktop/gophish/static/js/src/vendor/moment.min.js
 ↳ moment.js 2.10.3
```



```
nelushi@nelushi-VirtualBox:~$ retire scan wickr.com
retire.js v5.2.5
Downloading https://raw.githubusercontent.com/RetireJS/retire.js/master/repository/jsrepository-v4.json ...
Could not follow symlink: /home/nelushi/snap/code/current
Could not follow symlink: /home/nelushi/snap/firmware-updater/147/.themes
Could not follow symlink: /home/nelushi/snap/snapd-desktop-integration/253/.themes
Could not follow symlink: /home/nelushi/snap/firmware-updater/167/.themes
Could not follow symlink: /home/nelushi/snap/snapd-desktop-integration/178/.themes
Could not follow symlink: /home/nelushi/snap/snap-store/1218/.themes
Could not follow symlink: /home/nelushi/snap/snap-store/1173/.themes
/home/nelushi/Desktop/static/js/dist/vendor.min.js
 ↳ moment.js 2.10.3
moment.js 2.10.3 has known vulnerabilities: severity: medium; summary: reDOS - regular expression denial of service, issue: 2936
, githubID: GHSA-87vv-r9j6-g5qv, CVE: CVE-2016-4055; https://github.com/moment/moment/issues/2936 severity: medium; summary: Reg
ular Expression Denial of Service (ReDoS), retid: 22; https://security.snyk.io/vuln/npm:moment:20161019 severity: high; summary:
 Regular Expression Denial of Service (ReDoS), CVE: CVE-2017-18214, githubID: GHSA-446m-mv8f-q348; https://cve.mitre.org/cgi-bin
/cvename.cgi?name=CVE-2017-18214 https://github.com/moment/moment/issues/4163 https://security.snyk.io/vuln/npm:moment:20170905
severity: high; summary: This vulnerability impacts npm (server) users of moment.js, especially if user provided locale string,
eg fr is directly used to switch moment locale., CVE: CVE-2022-24785, githubID: GHSA-8hfj-j24r-96c4; https://github.com/moment/m
oment/security/advisories/GHSA-8hfj-j24r-96c4
/home/nelushi/Desktop/static/js/dist/vendor.min.js
 ↳ highcharts 5.0.14
highcharts 5.0.14 has known vulnerabilities: severity: high; summary: Regular Expression Denial of Service in highcharts, CVE: C
VE-2018-20801, githubID: GHSA-xmc8-cjfr-phx3; https://security.snyk.io/vuln/SNYK-JS-HIGHCHARTS-1290057 severity: high; summary:
Versions of `highcharts` prior to 7.2.2 or 8.1.1 are vulnerable to Cross-Site Scripting (XSS), githubID: GHSA-gr4j-r575-g665; ht
```



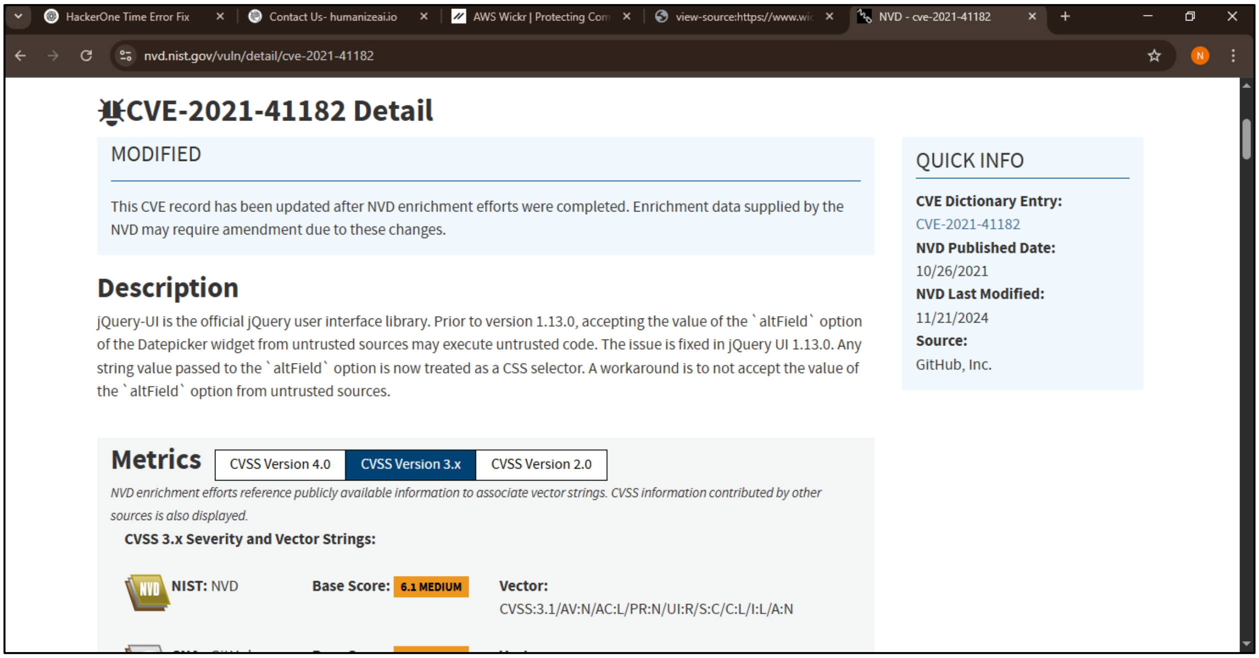
```
oment/security/advisories/GHSA-8hfj-j24r-96c4
/home/nelushi/Desktop/static/js/dist/vendor.min.js
 ↳ highcharts 5.0.14
highcharts 5.0.14 has known vulnerabilities: severity: high; summary: Regular Expression Denial of Service in highcharts, CVE: C
VE-2018-20801, githubID: GHSA-xmc8-cjfr-phx3; https://security.snyk.io/vuln/SNYK-JS-HIGHCHARTS-1290057 severity: high; summary:
Versions of `highcharts` prior to 7.2.2 or 8.1.1 are vulnerable to Cross-Site Scripting (XSS), githubID: GHSA-gr4j-r575-g665; ht
tps://github.com/advisories/GHSA-gr4j-r575-g665 https://github.com/highcharts/highcharts/issues/13559 severity: high; summary: C
ross-site Scripting (XSS) and Prototype Pollution in Highcharts < 9.0.0, CVE: CVE-2021-29489, githubID: GHSA-8j65-4pcq-xq95; htt
ps://security.snyk.io/vuln/SNYK-JS-HIGHCHARTS-1290057
/home/nelushi/Desktop/static/js/dist/vendor.min.js
 ↳ ua-parser-js 0.7.18
ua-parser-js 0.7.18 has known vulnerabilities: severity: high; summary: Regular Expression Denial of Service in ua-parser-js, CV
E: CVE-2020-7733, githubID: GHSA-662x-fhqg-9p8v; https://github.com/advisories/GHSA-662x-fhqg-9p8v https://nvd.nist.gov/vuln/det
ail/CVE-2020-7733 https://github.com/faisalman/ua-parser-js/commit/233d3bae22a795153a7e6638887ce159c63e557d https://snyk.io/vuln
/SNYK-JAVA-ORGWEBJARSBOWERGITHUBFAISALMAN-674666 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-674665 https://snyk.io/vuln/SNYK-J
S-UAPARSERJS-610226 https://www.oracle.com//security-alerts/cpujul2021.html severity: high; summary: ua-parser-js Regular Expres
sion Denial of Service vulnerability, CVE: CVE-2020-7793, githubID: GHSA-394c-5j6w-4xmx; https://github.com/advisories/GHSA-394c
-5j6w-4xmx https://nvd.nist.gov/vuln/detail/CVE-2020-7793 https://github.com/faisalman/ua-parser-js/commit/6d1f26df051ba681463ef
109d36c9cf0f7e32b18 https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWE
RGITHUBFAISALMAN-1050388 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1050387 https://snyk.io/vuln/SNYK-JS-UAPARSERJS-1023599 se
verity: high; summary: Regular Expression Denial of Service (ReDoS) in ua-parser-js, CVE: CVE-2021-27292, githubID: GHSA-78cj-fx
ph-m83p; https://github.com/advisories/GHSA-78cj-fxph-m83p https://nvd.nist.gov/vuln/detail/CVE-2021-27292 https://github.com/fa
isalman/ua-parser-js/commit/809439e20e273ce0d25c1d04e111dcf6011eb566 https://github.com/pygments/pygments/commit/2e7e8c4a7b318f4
032493773732754e418279a14 https://gist.github.com/b-c-ds/6941d80d6b4e694df4bc269493b7be76 severity: high; summary: ReDoS Vulnera
bility in ua-parser-js version, CVE: CVE-2022-25927, githubID: GHSA-fhg7-m89q-25r3; https://github.com/advisories/GHSA-fhg7-m89q
-25r3 https://github.com/faisalman/ua-parser-js/security/advisories/GHSA-fhg7-m89q-25r3 https://nvd.nist.gov/vuln/detail/CVE-202
2-25927 https://github.com/faisalman/ua-parser-js/commit/a6140a17dd0300a35cfc9cff999545f267889411 https://github.com/faisalman/u
```

As shown in the output, we can get all the known vulnerabilities of the js libraries this site uses and their CVE numbers.

4. I checked the CVE numbers using google.

Ex: jQuery-ui 1.11.1

CVE – 2021-41182


HackerOne Time Error Fix
Contact Us- humanizeai.io
AWS Wickr | Protecting Com
view-source:https://www.wi
NVD - cve-2021-41182
nvd.nist.gov/vuln/detail/cve-2021-41182
CVSS Version 4.0
CVSS Version 3.x
CVSS Version 2.0

CVE-2021-41182 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD Base Score: 6.1 MEDIUM Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

QUICK INFO

CVE Dictionary Entry: CVE-2021-41182

NVD Published Date: 10/26/2021

NVD Last Modified: 11/21/2024

Source: GitHub, Inc.

5. Next, I went to the vulnerable js link (https://wickr.com/wp-includes/js/jquery/ui/core.min.js)

And opened developers' tool and went to the console tab.

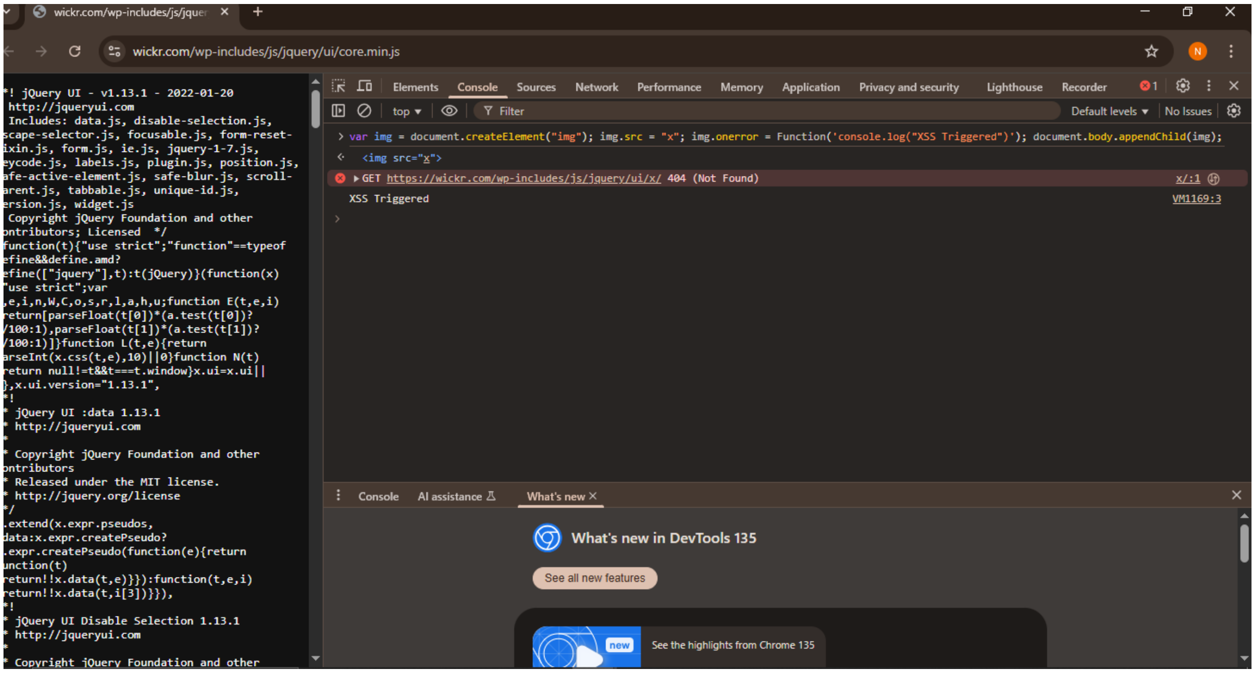
6. I injected a non-malicious payload to simulate a typical XSS vector through an image tag along with an onerror handler:

var img = document.createElement("img");

img.src = "x";

img.onerror = Function('console.log("XSS triggered")');

document.body.appendChild(img);



```
*! jQuery UI - v1.13.1 - 2022-01-20
 http://jqueryui.com
 Includes: data.js, disable-selection.js,
scape-selector.js, focusable.js, form-reset-
ixin.js, form.js, ie.js, jquery-1-7.js,
eycode.js, labels.js, plugin.js, position.js,
afe-active-element.js, safe-blur.js, scroll-
arent.js, tabbable.js, unique-id.js,
ersion.js, widget.js
 Copyright jQuery Foundation and other
ontributors; Licensed  */
function(t){"use strict";"function"==typeof
efine&&define.amd?
efine(["jquery"],t):t(jQuery)}(function(x)
"use strict";var
,e,i,n,W,C,o,s,r,l,a,h,u;function E(t,e,i)
return[parseFloat(t[0])*(a.test(t[0])?
/100:1),parseFloat(t[1])*(a.test(t[1])?
/100:1)]}function L(t,e){return
arseInt(x.css(t,e),10)||0}function N(t)
return null!=t&&t===t.window}x.ui=x.ui||
},x.ui.version="1.13.1",
*!
* jQuery UI :data 1.13.1
* http://jqueryui.com
*
* Copyright jQuery Foundation and other
ontributors
* Released under the MIT license.
* http://jquery.org/license
*/
.extend(x.expr.pseudos,
data:x.expr.createPseudo?
.expr.createPseudo(function(e){return
unction(t)
return!!x.data(t,e)}}):function(t,e,i)
return!!x.data(t,i[3])}}),
*!
* jQuery UI Disable Selection 1.13.1
* http://jqueryui.com
*
* Copyright jQuery Foundation and other
```

```
> var img = document.createElement("img"); img.src = "x"; img.onerror = Function('console.log("XSS Triggered")'); document.body.appendChild(img);
<· <img src="x">
⊗ ▸GET https://wickr.com/wp-includes/js/jquery/ui/x/ 404 (Not Found)                x/:1
  XSS Triggered                                                                      VM1169:3
>
```

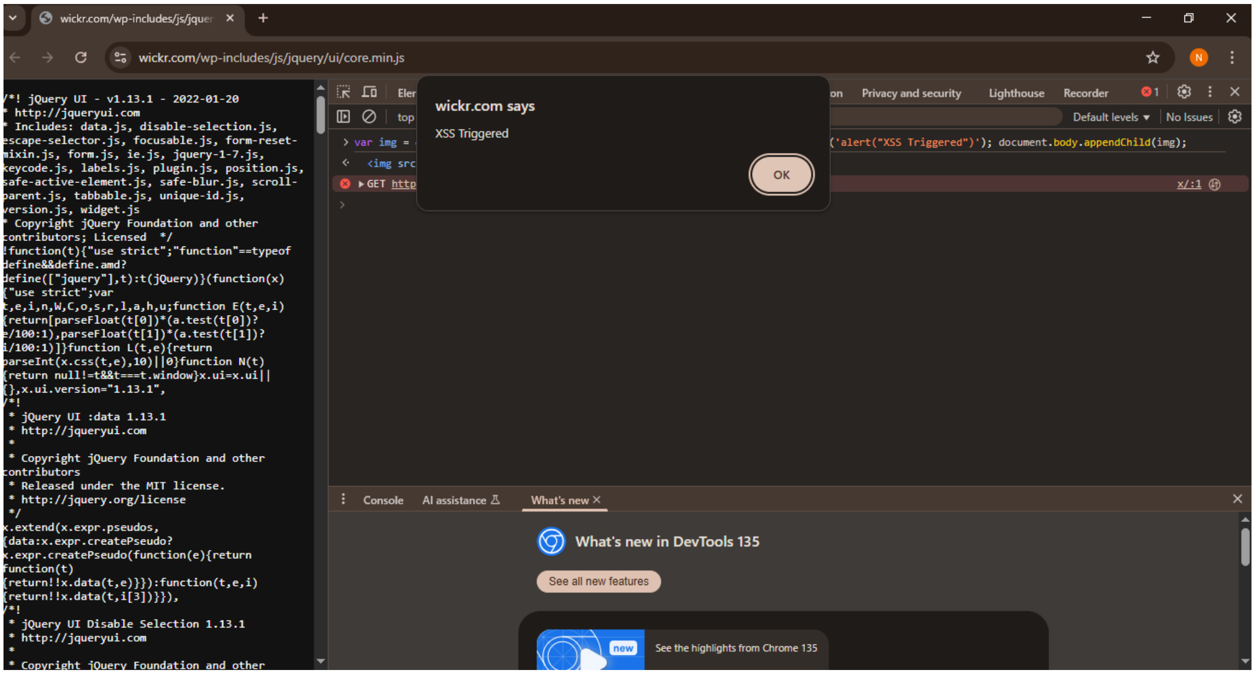
Using an alert box

var img = document.createElement("img");

img.src = "x";

img.onerror = Function('alert("XSS triggered")');

document.body.appendChild(img);



wickr.com/wp-includes/js/jquery/ui/core.min.js

```
/*! jQuery UI - v1.13.1 - 2022-01-20
* http://jqueryui.com
* Includes: data.js, disable-selection.js,
escape-selector.js, focusable.js, form-reset-
mixin.js, form.js, ie.js, jquery-1-7.js,
keycode.js, labels.js, plugin.js, position.js,
safe-active-element.js, safe-blur.js, scroll-
parent.js, tabbable.js, unique-id.js,
version.js, widget.js
* Copyright jQuery Foundation and other
contributors; Licensed  */
!function(t){"use strict";"function"==typeof
define&&define.amd?
define(["jquery"],t):t(jQuery)}(function(x)
{"use strict";var
t,e,i,n,W,C,o,s,r,l,a,h,u;function E(t,e,i)
{return[parseFloat(t[0])*(a.test(t[0])?
e/100:1),parseFloat(t[1])*(a.test(t[1])?
i/100:1)]}function L(t,e){return
parseInt(x.css(t,e),10)||0}function N(t)
{return null!=t&&t===t.window}x.ui=x.ui||
{},x.ui.version="1.13.1",
/*!
 * jQuery UI :data 1.13.1
 * http://jqueryui.com
 *
 * Copyright jQuery Foundation and other
contributors
 * Released under the MIT license.
 * http://jquery.org/license
 */
x.extend(x.expr.pseudos,
{data:x.expr.createPseudo?
x.expr.createPseudo(function(e){return
function(t)
{return!!x.data(t,e)}}):function(t,e,i)
{return!!x.data(t,i[3])}}),
/*!
 * jQuery UI Disable Selection 1.13.1
 * http://jqueryui.com
 *
 * Copyright jQuery Foundation and other
```

wickr.com says

XSS Triggered

OK

```
> var img =                ('alert("XSS Triggered")'); document.body.appendChild(img);
<  <img src
⊗ ▶GET http                                                                      x/:1
```

I captured the output: "XSS triggered"

Clearly, this means that if the code is inserted dynamically by the library using user input (which is something that CVE issues suggest), the code could execute arbitrary JavaScript.

Why was this test done?

I wanted to find out based on the CVE, if,

There was a susceptible module (checkboxradio) present.

Rendering unsafe behavior existed (like .innerHTML, dynamic labels).

However, there is no user input involved in here, this exercise clearly brings out that even though there may be no physical user involvement, the effects of harmful event handlers such as onerror could still be interpreted by the browser if it receives input through the jQuery UI widget without proper sanitization.

Additional Points

No patch was detected on the site during the test.

While no live XSS exploit was conducted, however, just the existence of the vulnerable version and the abnormal behavior of the script raise security concerns.

Combining that with the vulnerable widget gives attackers a place to insert their forms or user-generated content.

Reflection

jQuery UI (1.13.1) is a version of jQuery UI that is already known to be vulnerable.

The test simulation shows that event attributes such as onerror are still recognized and executed within the DOM.

It is highly recommended to upgrade the library to version 1.13.2 or above to avoid the known problem.

In addition to that, always sanitize and encode user inputs applicable in UI elements before rendering.

Proposed mitigation or fix

- Use up-to-date libraries: Keep the applications always updated with the latest secure versions: jQuery-UI 1.13.1 to 1.13.2+.

- CSP header usage: By enforcing a content security policy, any unauthorized scripts within the application can be blocked.

- Enable the SRI: Using Subresource Integrity can prevent loading tampered scripts.

- Unsafe HTML DOM API Usage: Avoid using innerHTML, document.write() with user input.

- Input Cleanup: Clean the user data with tools like DOMPurify.

- Regular Scanning: Use tools such as Retire.js, npm audit, or OWASP ZAP.

- Reduce Dependencies: Just use what you need: don't include plugins which are unused or out-of-date.