

Sri Lanka Institute of Information Technology



**Sri Lanka Institute of
Information Technology**

IE2062 - Web Security

Year 2, Semester 2

(Assignment-Individual)-2023

Bug Bounty Vulnerabilities Scanning Report 9

Student Register Number	Student Name
IT2117096	DE ZOYSA A.S.

Canva

With the help of the tool Canva, you may create anything and share it online. The creation of everything was done using web and mobile apps. Anywhere you post, there are connections between your online and offline personas. As a result, you have a variety of places to look into. People entrust us with all kinds of information, including media assets, commercial adverts, product information, and private information. Despite the fact that Canva is free to use, users must pay to access premium media resources like photo libraries or for corporate subscriptions that include specialized tools, capabilities for workflow management, and team management. We value the community of security researchers and are committed about the safety of our systems. We can safeguard our users' security and privacy thanks to your ethical reporting of security holes found by security researchers.












Assessment of Scope

Scope of the security audit according to <https://bugcrowd.com/canva> is as follows,

In Scope,

- ✓ *.canva.com
- ✓ *.canva.cn
- ✓ *.canva.tech
- ✓ Canva Developer Platform
- ✓ *.canva-apps.com
- ✓ *.canva-apps.cn


In Scope		✓ In scope	
P4	P3	P2	P1
\$100	\$850	\$2500	\$10000
 *.canva.com		Java MySQL Recon +3	
 Canva (Android)		Java Android Mobile Applicati... +2	
 Canva (iOS)		Objective-C SwiftUI Swift +3	
 Canva (Chrome Extension)		Browser Extension Javascript	
 *.canva.cn		Recon Website Testing DNS	
 *.canva.tech		Recon Website Testing DNS	
 Canva Developer Platform			
 *.canva-apps.com			
 *.canva-apps.cn			

Out Scope,


- ✓ *.0.canva.cn
- ✓ *.0.canva-apps.cn

Out of Scope

✕ Out of scope

 *.0.canva.cn

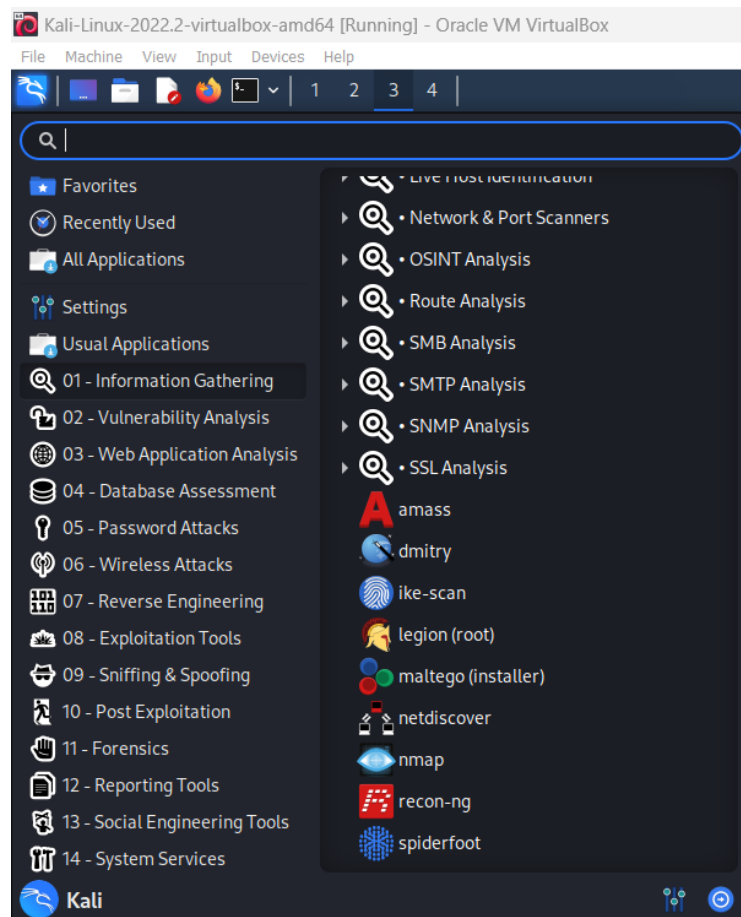
Website TestingDNS

 *.0.canva-apps.cn

Website TestingDNS

Information Gathering

It is the process of collecting data from many sources for a range of purposes. Learning to create efficient information-gathering techniques will benefit studying in a variety of ways. Effective information collecting involves making better use of time, fostering critical thinking through the use of shifting/sorting strategies, and enlarging one's perspective and topic knowledge through the investigation of new sources. Additionally, obtaining knowledge may be useful for a number of purposes, but the major advantage in terms of academic studies is that one will become aware of more varied sources, viewpoints, and techniques that can improve one's academic work.



Focus Areas

- ✚ The main www.canva.com and www.canva.cn assets
- ✚ The Canva iOS and Android apps
- ✚ The Canva Developer Platform www.canva.com/developers

Subdomain for Hunting

Sub-domain enumeration is the process of listing sub-domains for one or more domains. In the process of reconnaissance, it's a crucial phase. Sub-domain enumeration can reveal several domains and sub-domains that are included in a security assessment, which increases the chance of finding vulnerabilities.

Finding applications using cryptic, abandoned sub-domains may reveal serious bugs.

Within a single company, the same vulnerabilities are routinely discovered across many domains and applications.

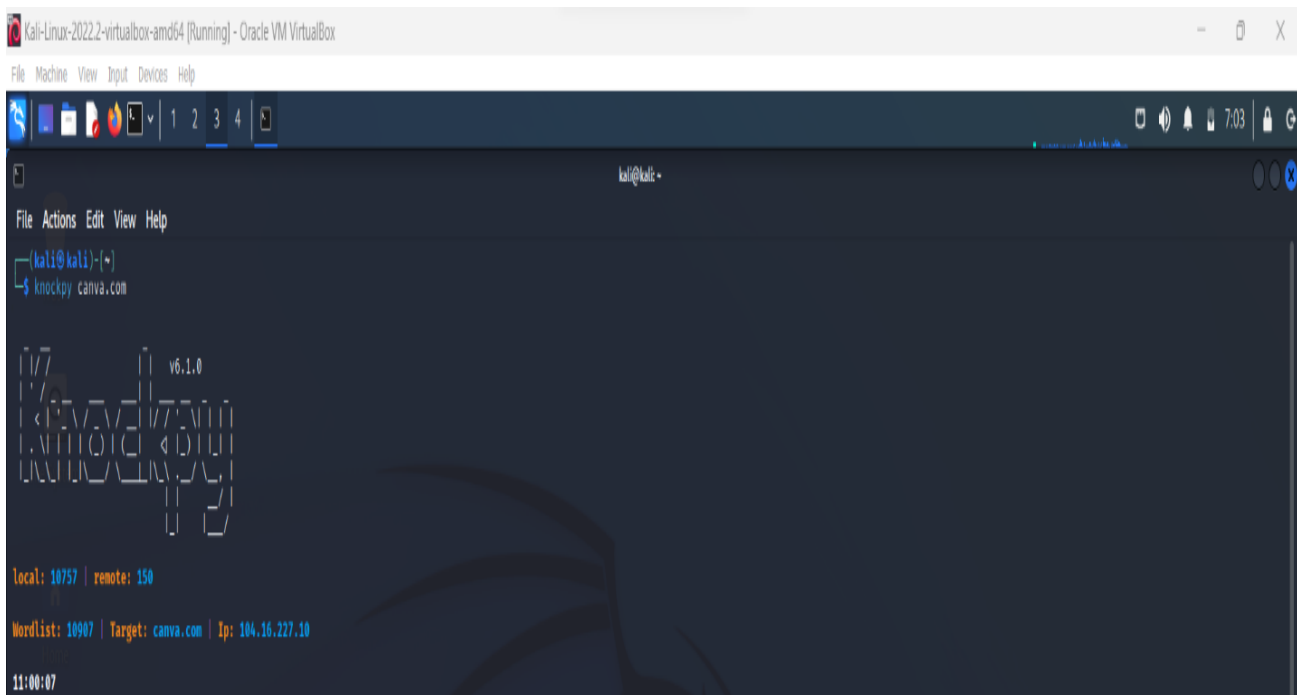
- What is Knockpy?

With only a few lines of code, knockpy's python version of the knockoffs framework makes it simple to use knockoff-based inference. The modular design of Knockpy makes it simple for researchers and analysts to add features on top of it.

searching subdomain by knockpy,

Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.

How to Find Subdomain in Knockpy: `knockpy <Domain Name>`



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ knockpy canva.com
v6.1.0
local: 10757 | remote: 150
WordList: 10907 | Target: canva.com | Ip: 104.16.227.10
11:00:07
```

```
[~]
File Actions Edit View Help
(kali@kali)-[~]
$ knockpy canva.com

[1/7] [KNOCKING] v6.1.0

Local: 19757 | Remote: 141
Wordlist: 10098 | Target: canva.com | Ip: 104.16.226.10
11:21:46
```

Ip address	Code	Subdomain	Server	Real hostname
34.83.150.148	200	ip-sc.canva.com		
104.16.226.10	200	about.canva.com	cloudflare	
104.16.226.10	400	album.canva.com	cloudflare	
104.16.227.10	403	api.canva.com	cloudflare	
54.187.15.122	204	advocates.canva.com		appia.outrch.com
104.16.227.10	403	audio-public.canva.com	cloudflare	
104.16.227.10	403	audio-private.canva.com	cloudflare	
104.16.226.10	403	avatar.canva.com	cloudflare	
104.16.226.10	403	banner-static.canva.com	cloudflare	
104.16.227.10	200	ar-eg.about.canva.com	cloudflare	
104.16.226.10	200	apps.canva.com	cloudflare	
104.16.227.10	200	button-demo.canva.com	cloudflare	
104.16.226.10	403	category-public.canva.com	cloudflare	
35.161.79.191	200	affiliates.canva.com	cloudflare	canva.ip04.com
104.16.226.10	404	cli.canva.com	cloudflare	
52.1.182.132	402	capitalise.canva.com		
104.16.227.10	402	content-management-files.canva.com	cloudflare	
104.16.227.10	404	csp.canva.com	cloudflare	
34.117.119.56	404	creator.canva.com		creator-canva-com.ct.impacetradius.com
216.239.36.21	400	ct.canva.com		
104.16.227.10	200	de-de.learn.canva.com	cloudflare	
104.16.226.10	403	deploy.canva.com	cloudflare	
104.16.227.10	400	dk-dk.about.canva.com	cloudflare	
104.16.227.10	403	design-automation-font-recommendations.canva.com	cloudflare	
104.16.227.10	200	de-de.about.canva.com	cloudflare	
104.16.227.10	403	document-export.canva.com	cloudflare	
104.16.226.10	403	desktop-release.canva.com	cloudflare	
104.16.227.10	200	developers.canva.com	cloudflare	
104.16.226.10	200	developer.canva.com	cloudflare	
104.16.227.10	200	designschool.canva.com	cloudflare	
104.16.226.10	403	email-design-template.canva.com	cloudflare	
104.16.226.10	200	Careers.Canva.Com		
104.16.226.10		email-public.canva.com		
104.16.226.10		en-in.about.canva.com		
104.16.226.10		es-us.about.canva.com		
104.16.227.10		es-es.about.canva.com		
104.16.227.10		es-mx.about.canva.com		
104.16.226.10		docs.developer.canva.com		
104.16.227.10		es-mx.learn.canva.com		
104.16.226.10		es-ar.about.canva.com		
104.16.227.10		events.canva.com		
104.16.226.10		es-co.about.canva.com		
104.16.226.10		engineering.canva.com		
52.216.36.117		cse.canva.com		
104.16.227.10	400	image.canva.com	cloudflare	
104.16.226.10	403	Image-manipulation.canva.com	cloudflare	
104.16.226.10	403	image.canva.com	cloudflare	
104.16.227.10	200	ID-ID.Learn.Canva.Com	cloudflare	
104.16.227.10	403	import.canva.com	cloudflare	
104.16.227.10	403	Import-contributor-upload.canva.com	cloudflare	

Amass – Hunting for Subdomains.

The OWASP Amass Project uses open-source information gathering and active reconnaissance techniques to accomplish network mapping of attack surfaces and external asset discovery.

```

kali@kali: ~
File Actions Edit View Help

(kali㉿kali)-[~]
$ sudo amass enum -h
[sudo] password for kali:

      .+++!,:
+WWwwwwwWwW    :   o8WS:    +WwwwwwWwW+.  oWwwwwwWwW+
SwwW+.  .oW##.  .wwwwwwW.oWWW    :wwW#SWWo  .W#:  .:oW+  .W#+++SwSw
+Ws  Sww  #W  +WwwSwSw+  :wW.  +WS  +W:  .WS  .WS
Sww  Sww  Ww  SwW  .wW  Ww+  .wW.  oWw.  oWw.  oWw:
WW  SwW  SwW:  oW+  oW+  #W.  SwW  +WwW+.  +WwW:
#W  :wW  Sw+  Sw+  WS  :Ww  oWw  oWwwWw+  oWwW
oW+  Wws  Sw+  Sw+  #W  Sw.  .WwW  .+Ww  oWw.
WW  +WwwW,  Sw+  :S  oW+  #W  :WwSwSw  Sw:  ..  :Ww
:wW:  oW#  +Ww  Sw+  :W:  +WwSw++SwW.  SwSw  SwW#o+WwW.  #W:  oW+
:WwwwwwWwwWwW  +  :SwwwwSwW  Sw  .oSwwSw.  :WwwwwwWwW
Ww+oSwSwSw+,  +oooo.

                                     v3.23.2
                               OWASP Amass Project - @owaspamass
                        In-depth Attack Surface Mapping and Asset Discovery

Usage: amass enum [options] -d DOMAIN

-active
    Attempt zone transfers and certificate name grabs
-addr value
    IPs and ranges (192.168.1.1-254) separated by commas
-alts
    Enable generation of altered names
-asn value
    ASNs separated by commas (can be used multiple times)
-aw value
    Path to a different wordlist file for alterations
-awm value
    "hashcat-style" wordlist masks for name alterations
-bl value
    Blacklist of subdomain names that will not be investigated
-blf string
    Path to a file providing blacklisted subdomains
-brute
    Execute brute forcing after searches
-cidr value
    CIDRs separated by commas (can be used multiple times)
-config string
    Path to the INI configuration file. Additional details below
-d value
    Domain names separated by commas (can be used multiple times)
-demo
    Censor output to make it suitable for demonstrations
-df value
    Path to a file providing root domain names
```



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo amass enum -src -brute -d canva.com
[Brute Forcing] apps.canva.com
[AnubisDB] mailer2.canva.com
[DNSHistory] about.canva.com
[DNSDumpster] document-export.canva.com
[HackerTarget] export-download.canva.com
[HackerTarget] o1007.e.engage.canva.com
[RapidDNS] share.canva.com
[HackerTarget] ja-jp.learn.canva.com
[HackerTarget] profile.canva.com
[RapidDNS] pt-pt.about.canva.com
[DNSDumpster] zh-dotcn.about.canva.com
[HackerTarget] cse.canva.com
[DNSDumpster] status.canva.com
[HackerTarget] video-upload.canva.com
[HackerTarget] font-public.canva.com
[DNSDumpster] ar-eg.about.canva.com
[LeakIX] support.canva.com
[HackerTarget] email-public.canva.com
[HackerTarget] de-de.learn.canva.com
[Maltiverse] template-frame.canva.com
[AbuseIPDB] designschool.canva.com
[HackerTarget] media-public.canva.com
[DNS] canva.com
[HackerTarget] static-cse.canva.com
[HackerTarget] o682.engage.canva.com
[DNSDumpster] ru-ru.learn.canva.com
[DNSDumpster] id-id.about.canva.com
[Bing] www.canva.com
[DNS] ns2.canva.com
[DNSDumpster] es-us.about.canva.com
[AbuseIPDB] media-private-assets.canva.com
[AbuseIPDB] us-west-1.newftp.canva.com
[HackerTarget] banner-static.canva.com
[AbuseIPDB] o4226.e.engage.canva.com
[DNSSpy] upload.canva.com
[RapidDNS] help-public.canva.com
[AbuseIPDB] print-thumbnail.canva.com
[AbuseIPDB] ms-my.about.canva.com
[AbuseIPDB] renderer.cse.canva.com
[HackerTarget] it-it.about.canva.com
```

- Open Ports Enumeration applying with nmap

A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and cannot be used for anything else if a service uses it. Open ports offer a security risk if the services operating on them are improperly configured, unsecure, or unpatched.

Using Nmap to List Open Ports

The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool.

```
(kali@kali)-[~]
$ sudo nmap -sS canva.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 08:14 EDT
Nmap scan report for canva.com (104.16.226.10)
Host is up (0.013s latency).
Other addresses for canva.com (not scanned): 104.16.227.10 2606:4700::6810:e30a 2606:4700::6810:e20a
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 5.24 seconds
```

Open Ports are,

PORT	STATE	SERVICE
25/tcp	open	smtp
80/tcp	open	http
443/tcp	open	https
8080/tcp	open	http-proxy

```
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
```

Checking for Vulnerabilities Using **NIKTO**.

A security program called the Nikto web server scanner scans a website for thousands of possible security holes. This includes malicious files, services that have been set up improperly, vulnerable scripts, and other issues. It was created using plugins and is open source to allow for feature expansion. New security checks are frequently added to these plugins through regular updates. Many penetration testers and security analysts maintain the famous Nikto Web Vulnerability Scanner in their toolkit. It typically unearths valuable data about a web server or website that may be used for subsequent exploitation or vulnerability analysis.

```
(kali@kali)~$ sudo nikto -h canva.com
[sudo] password for kali:
- Nikto v2.5.0

+ Multiple IPs found: 104.16.226.10, 104.16.227.10, 2606:4700::6810:e20a, 2606:4700::6810:e30a
+ Target IP: 104.16.226.10
+ Target Hostname: canva.com
+ Target Port: 80
+ Start Time: 2023-05-25 08:34:04 (GMT-4)

+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ Root page / redirects to: https://www.canva.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /canvacom.egg: 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/missing-content-type-header/
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 7962 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2023-05-25 08:41:11 (GMT-4) (427 seconds)

+ 1 host(s) tested
```

```
(kali@kali)~$ sudo nikto -h 104.16.226.10
[sudo] password for kali:
- Nikto v2.5.0

+ Target IP: 104.16.226.10
+ Target Hostname: 104.16.226.10
+ Target Port: 80
+ Start Time: 2023-05-25 08:39:08 (GMT-4)

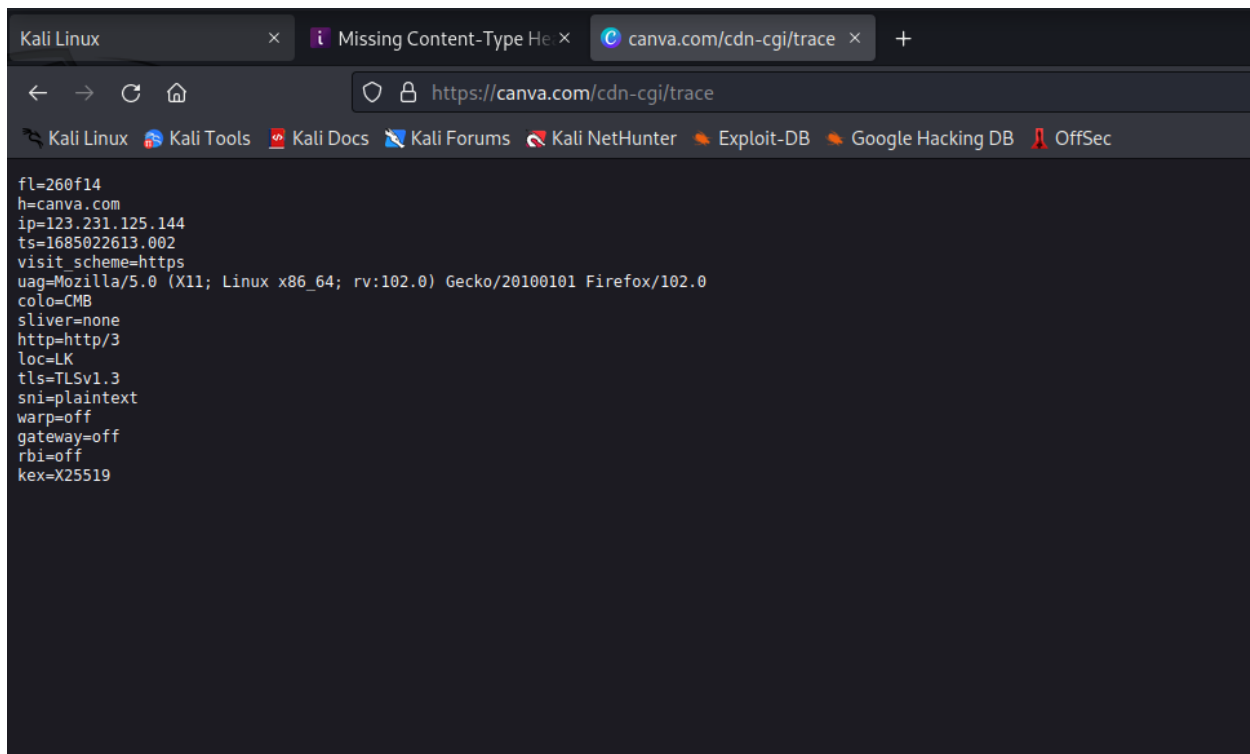
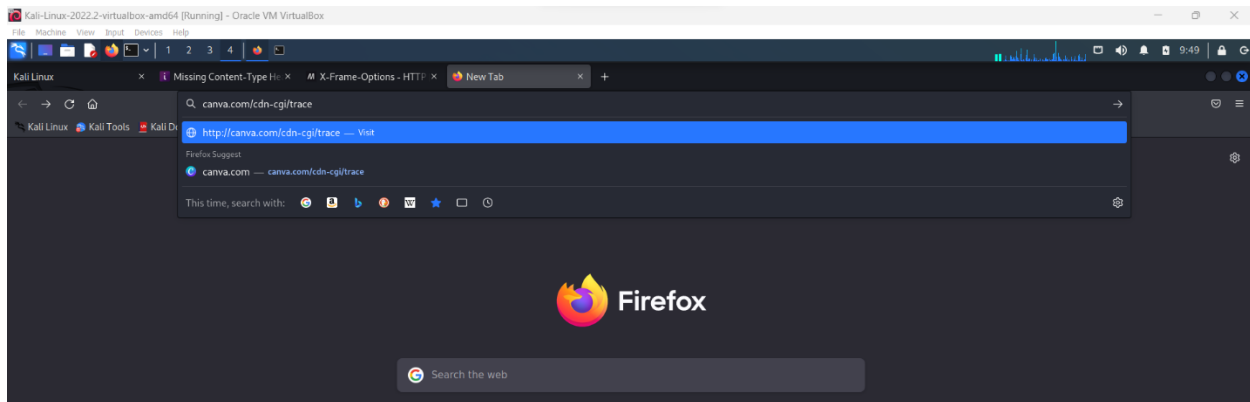
+ Server: cloudflare
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com
+ All CGI Directories 'found', use '-C none' to test none
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 26662 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2023-05-25 09:12:13 (GMT-4) (1985 seconds)

+ 1 host(s) tested
```

Here I found a part of this website where some information is leaking. It can be seen as a vulnerability to the website to some extent.

```
+ /cdn-cgi/trace: Retrieved access control allow origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
```

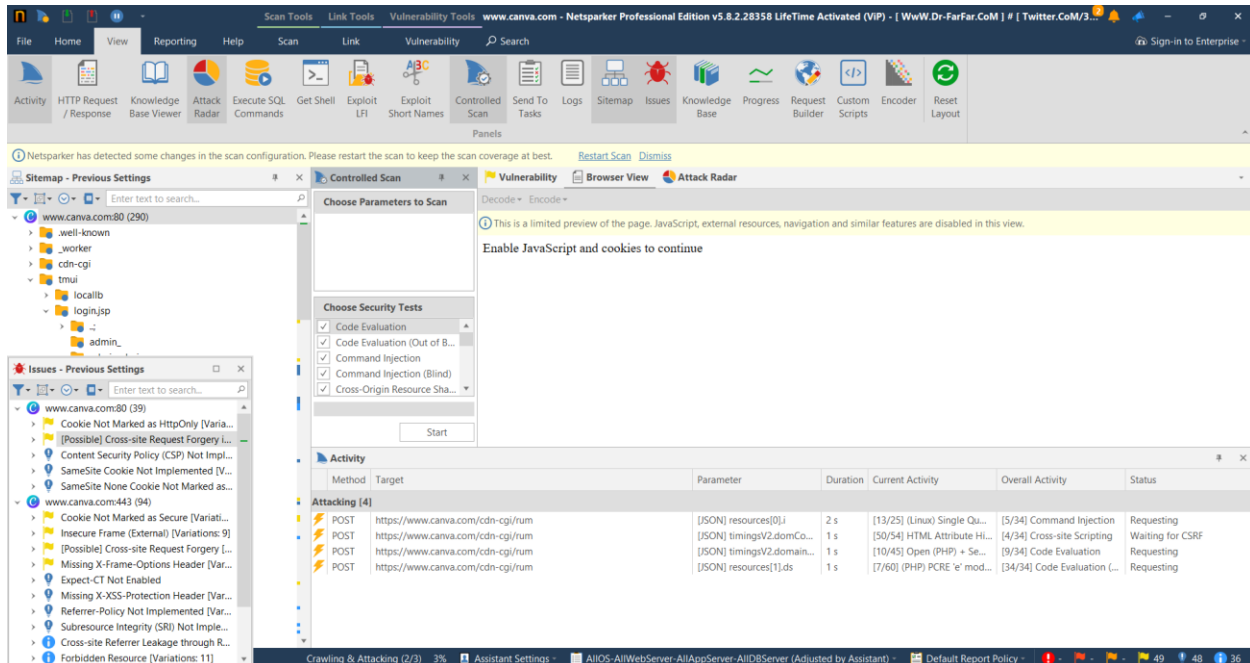
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.



Here we can see some data leakage on the website. As such, this is identified as a vulnerability to the website.

Scanned Vulnerabilities Using Netsparker

- Cross-site Request Forgery



Risk Level : Low

- Vulnerability Details,

Depending on the program, an attacker can perform any of the tasks that a user can perform, such as creating a user, editing material, or deleting data. The attacker has access to all of the functionality provided to the victim. The sole exception to this rule is a page that requires additional information that only the genuine user has access to (for example, the user's password).

- **Impact,**

In this situation, CSRF impacts the login form, which dramatically reduces the effect of this issue. In contrast to standard CSRF vulnerabilities, this will only allow an attacker to exploit specific complicated XSS vulnerabilities; otherwise, it cannot be abused.

As an example,

If a page is unique to each user (for example, "edit my profile") and vulnerable to XSS (Cross-site Scripting), it cannot generally be abused. If the login form is susceptible, an attacker can create a customized profile and compel the victim to login as that person, triggering the XSS exploit. Because there is no ongoing session, the attacker's options with this XSS remain constrained. However, the attacker can exploit this XSS in a variety of ways, including displaying the identical login form but this time collecting and transmitting the entered username/password to the attacker.

In this kind of attack, the attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>
<script>
  document.forms[0].submit();
</script>
```

- **Remedy,**

In each HTTP request, provide extra information that may be used to identify whether the request came from an authorized source. For an attacker who does not already have access to the user's account, this "validation token" should be difficult to guess. If a validation token is absent or does not match the anticipated value, the server should deny the request.

Custom HTTP headers can be used to avoid CSRF when publishing a form in an ajax request since the browser bans sites from sending custom HTTP headers to another site but enables sites to send custom HTTP headers to themselves through XMLHttpRequest.

For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();  
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to

a. individual request

```
$.ajax({  
  url: 'foo/bar',  
  headers: { 'x-my-custom-header': 'some value' }  
});
```

b. every request

```
$.ajaxSetup({  
  headers: { 'x-my-custom-header': 'some value' }  
});  
OR  
$.ajaxSetup({  
  beforeSend: function(xhr) {  
    xhr.setRequestHeader('x-my-custom-header', 'some value');  
  }  
});
```

1) Missing X-Frame-Options Header

- Risk Level : Low

• Vulnerability Details,

The X-Frame Alternatives The HTTP header field defines a policy that determines whether the sent resource should be rendered within a frame or an iframe by the browser. To prevent clickjacking attacks, servers can declare this policy in the header of their HTTP replies, ensuring that their content is not embedded in other sites or frames.

• Impact,

Clickjacking occurs when an attacker employs numerous transparent or opaque layers to deceive a user into clicking on a button or link on a framed website when they intended to click on the top level page. As a result, the attacker is "hijacking" clicks intended for their website and redirecting them to another page, most likely controlled by another application, domain, or both.

Keystrokes can likewise be hijacked using a similar manner. A skillfully prepared mix of stylesheets, iframes, and text boxes can fool a user into thinking they are putting in their email or bank account password, while in fact they are typing into an invisible frame controlled by the attacker.

• Remedy,

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

- X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
- X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
- X-Frame-Options: ALLOW-FROM *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.