Penetration Testing

https://starbannerglobal.com

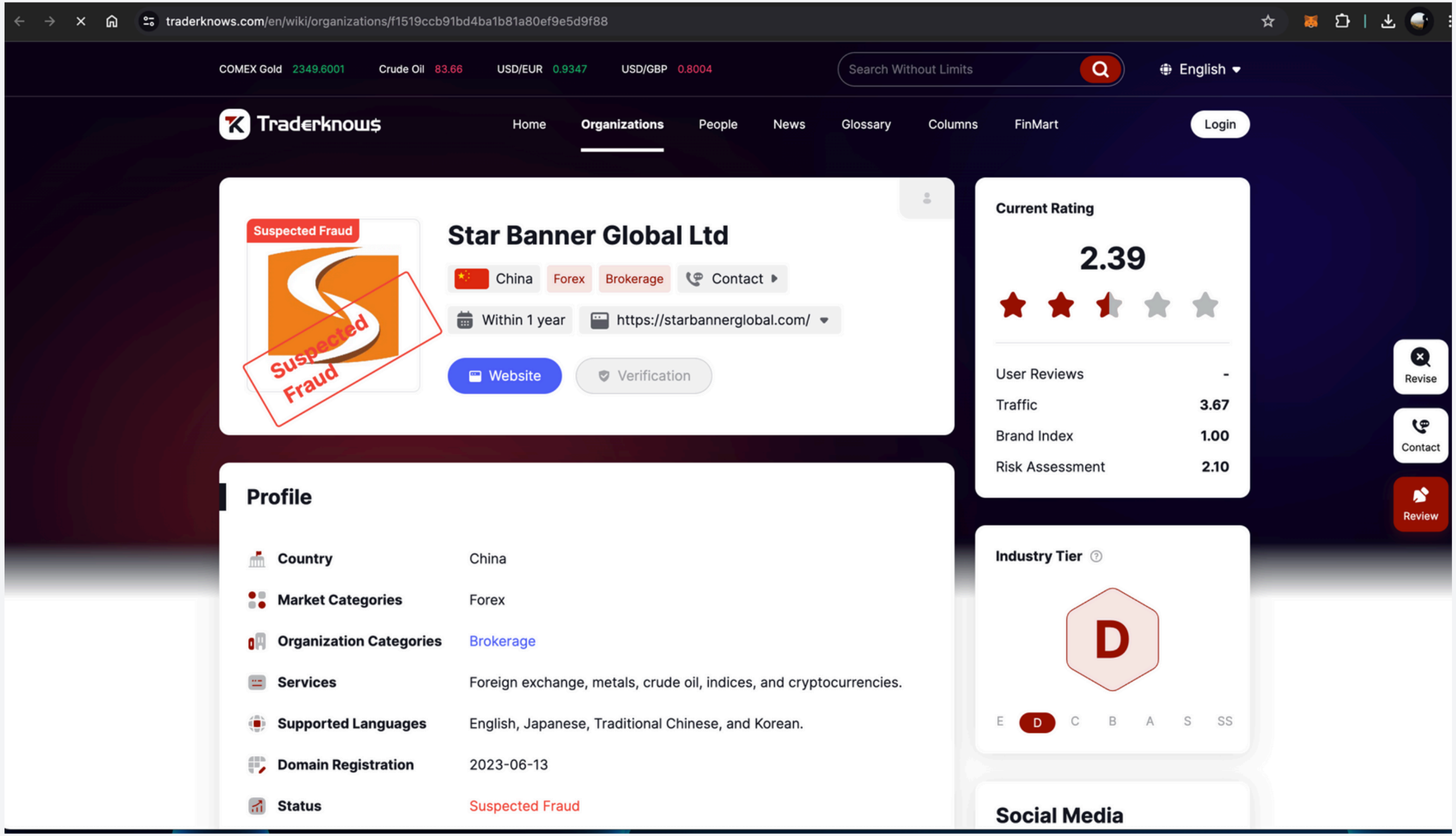
Bhuvan Vijay Kumar(PES1UG21CS140)

Raghav S (PES1UG21CS469)

Rashmi J (PES1UG21CS480)

Shaik Adeeba Saher (PES1UG21CS549)

URL : https://starbannerglobal.com



- Star Banner Global Ltd is an active company incorporated on 13 June 2023 with the registered office located in Cardiff, South Glamorgan.
- Star Banner Global Ltd has been running for 10 months.
- We are testing this website as we have found duplicates and reports have been made against it for fraudulent activities.

Our Setup

Nikto
a Practical Website Vulnerability Scanner

BurpSuite

Nmap

- We performed our testing on **Kali LInux** , **all the three, Nikto, BurpSuite and Nmap** are pre-installed softwares on Kali for **website and server scanning**.

- With these **penetration testing software** we have found **a bunch of vulnerabilities** which have been explained in the following slides.

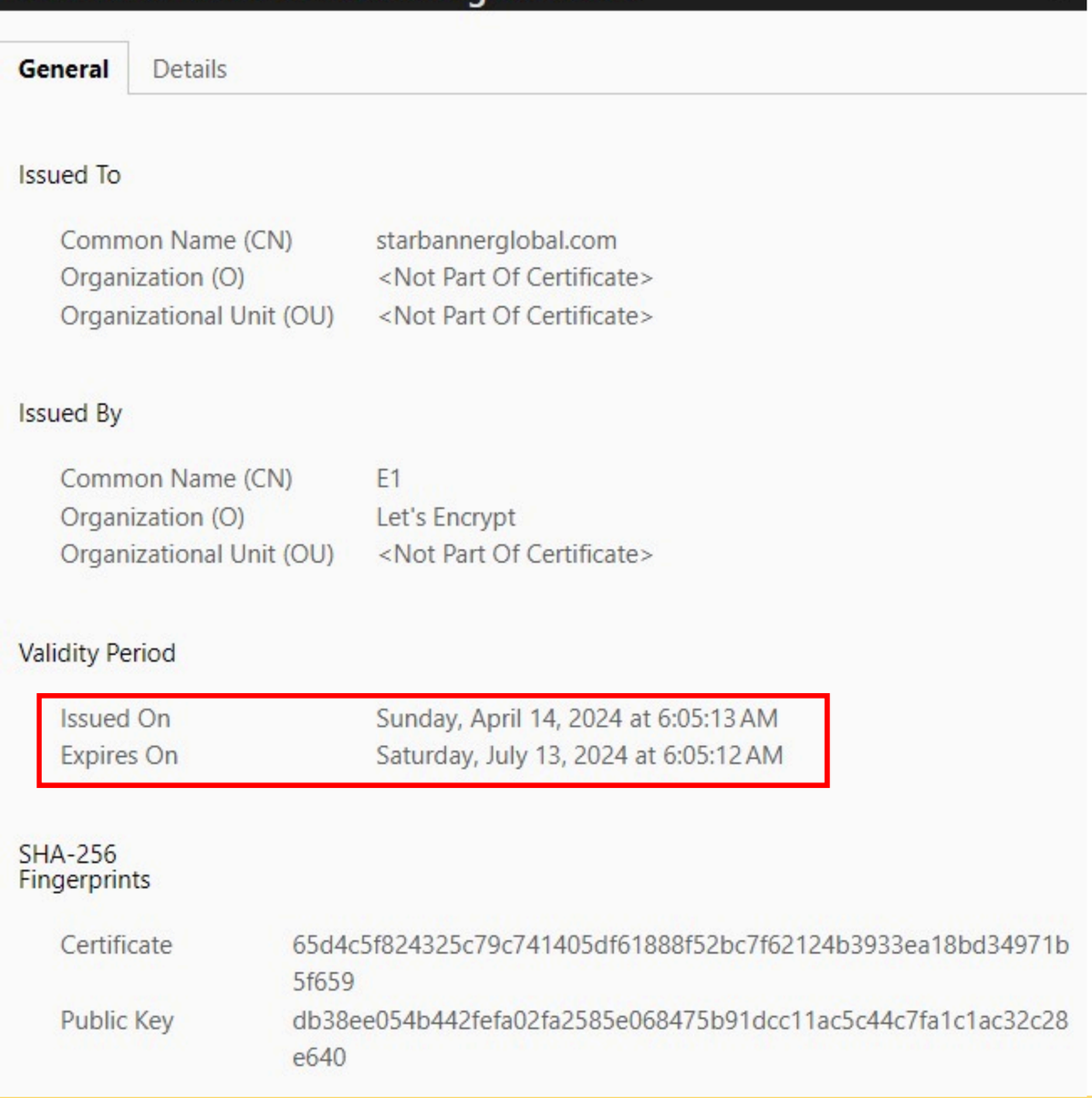
Discovering the ports

```
┌──(raghav㉿raghav)-[~]
└─$ nmap -sV 104.21.25.33
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-24 21:36 IST
Nmap scan report for 104.21.25.33
Host is up (0.0060s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Cloudflare http proxy
443/tcp  open  ssl/https     cloudflare
8080/tcp open  http          Cloudflare http proxy
8443/tcp open  ssl/https-alt cloudflare

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.15 seconds
```

On performing the nmap scanning for the IP address 104.21.25.33,

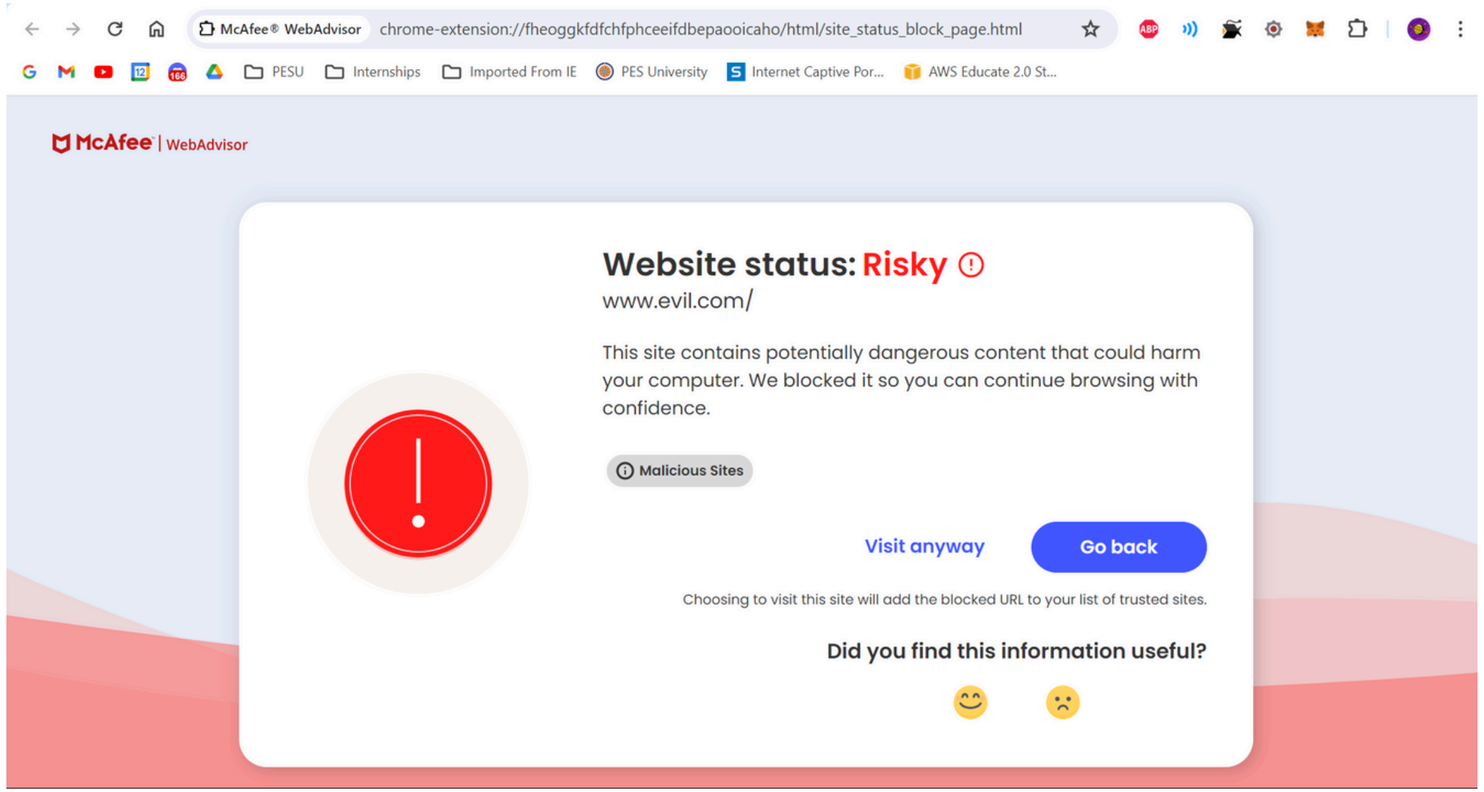
We can conclude that ports 80/tcp, 443/tcp, 8080/tcp and 8443/tcp are the open ports and are running behind a proxy named Cloudflare



Lower Certificate Validity

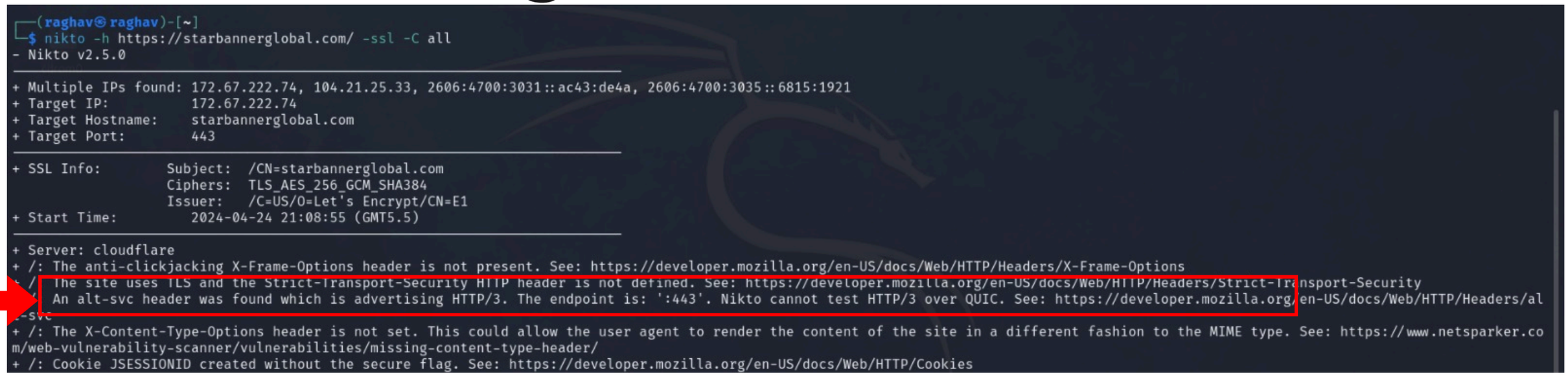
- The SSL certificate issued is a free version which is valid only for 90 days.
- Although this does not prove malicious intent, this does support the fact that this website could be just a **burner website to scam people** and get away after 90 days or sooner.
- This behaviour is consistent with scam websites.

Redirect Attack



- When clicking a button on a website leads to a malicious website, it's typically referred to as a "redirect attack."
- Trial and error on the website led us to evil.com/ when we clicked on sign in and sign up.
- Conclusion: Redirect attack is one of the most common ways to attack as people blindly click on links which leads to malicious websites and hence breaches.

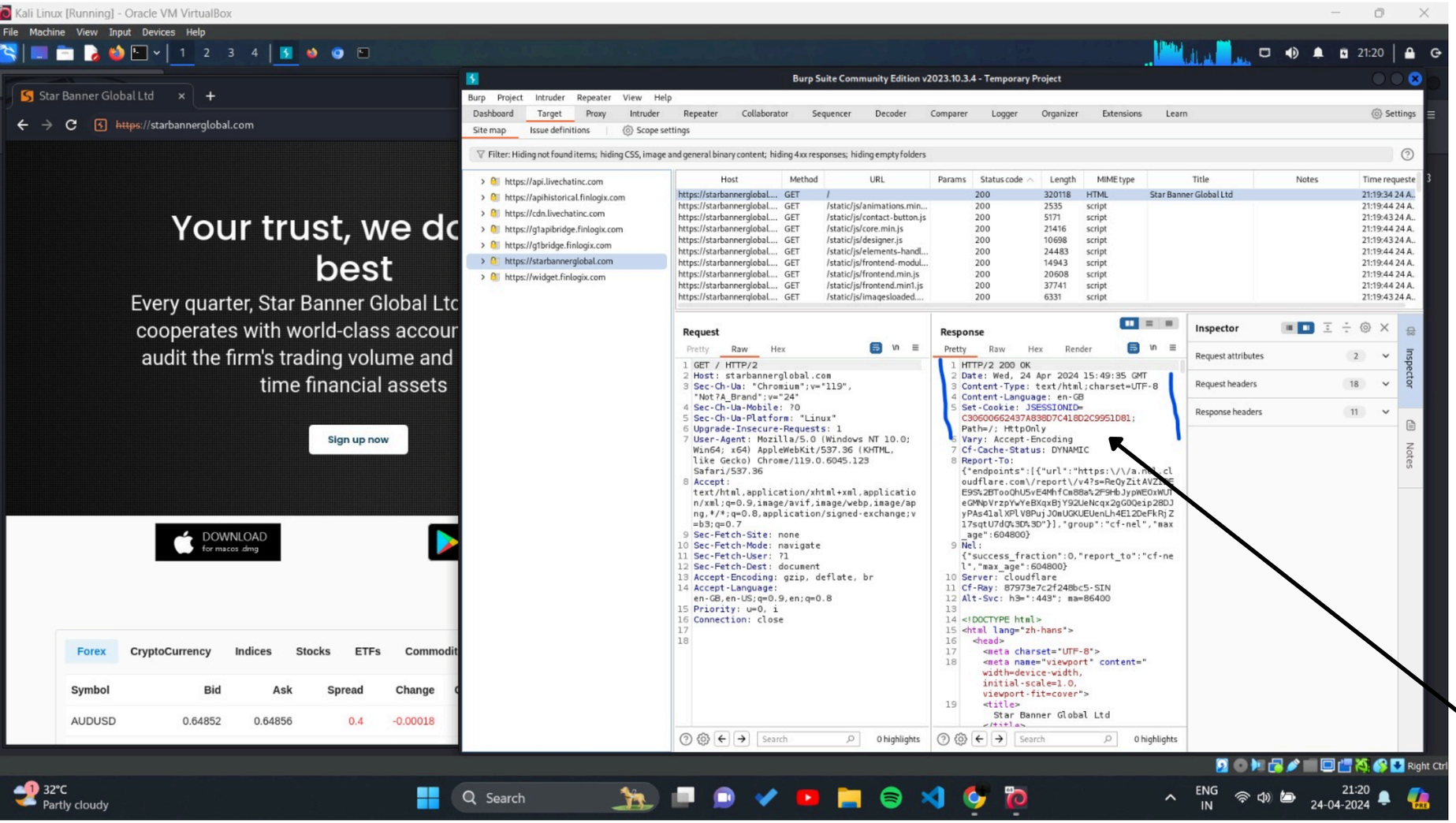
ClickJacking



- Clickjacking involves deceiving users into clicking on something different from what they perceive they are clicking on.
- This is usually achieved by overlaying transparent or opaque elements over legitimate buttons or links on a webpage.
- When the user interacts with what they believe is a harmless element, they are actually interacting with a different, malicious element.
- Clickjacking can be used to hijack clicks to perform unintended actions, such as enabling permissions or initiating downloads without the user's knowledge.

- using the nikto library we have found clickjacking as one moderate vulnerability in this website.

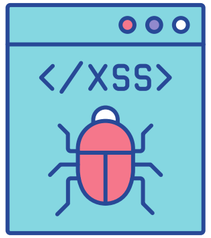
Session Hijacking



Session hijacking occurs when an attacker gains unauthorized access to a user's session by stealing or impersonating their session identifier.

Here, we see the session cookie transferred in plaintext. Attackers could capture this and hijack the session.

XSS

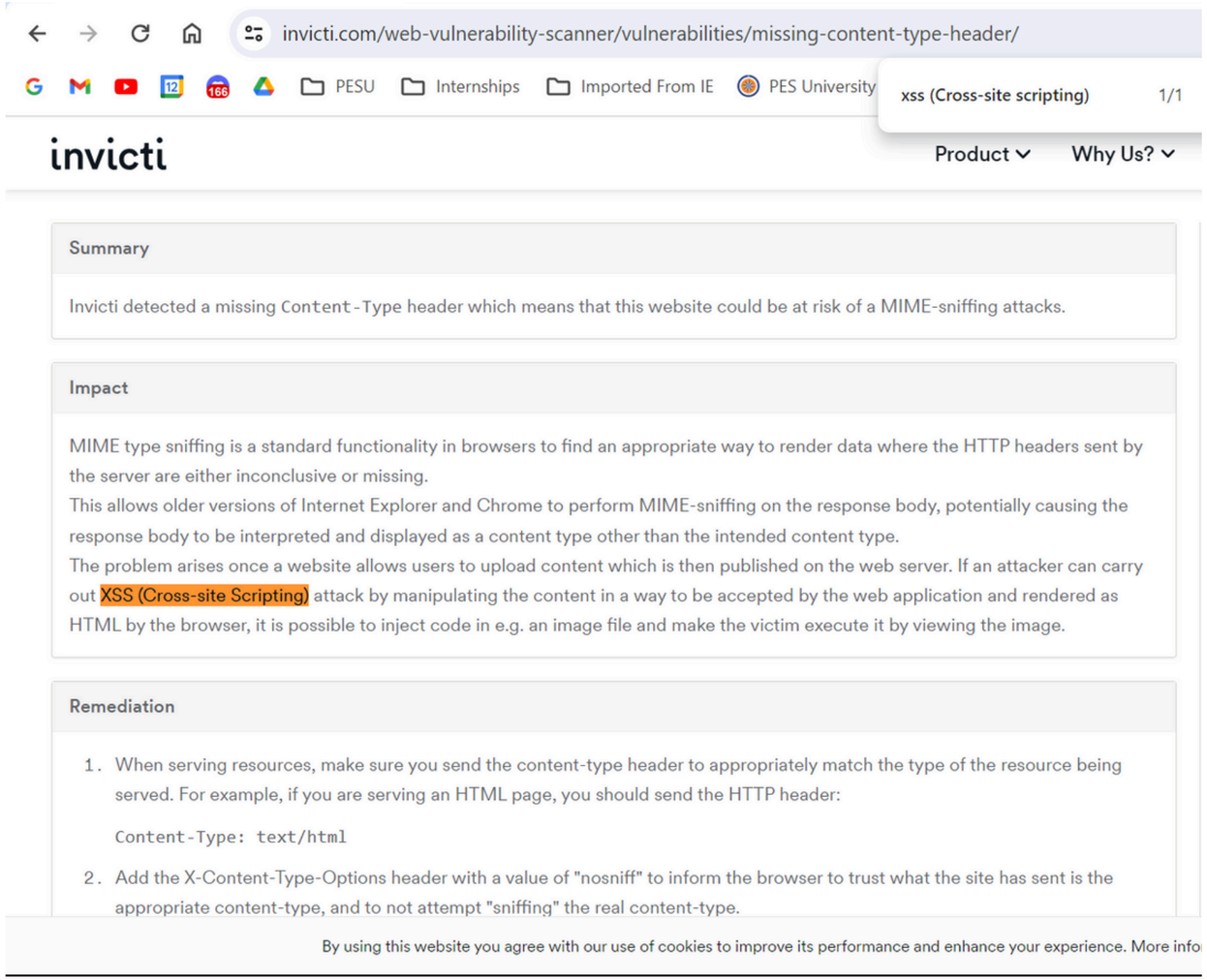



```
┌──(raghav㉿raghav)-[~]
└─$ nikto -h https://starbannerglobal.com/ -ssl -C all
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 172.67.222.74, 104.21.25.33, 2606:4700:3031::ac43:de4a, 2606:4700:3035::6815:1921
+ Target IP:          172.67.222.74
+ Target Hostname:    starbannerglobal.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=starbannerglobal.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=E1
+ Start Time:         2024-04-24 21:08:55 (GMT5.5)
---------------------------------------------------------------------------
+ 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
+ /: 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
+ /: 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/al
+ SVC
+ /: 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.co
n/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie JSESSIONID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
```

XSS: Cross-Site Scripting (XSS) is a vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users.

Found: Using nikto command on kali linux OS

XSS...



Why Vulnerable: Attackers can inject and execute malicious scripts within a website, potentially leading to unauthorized access to

- user sessions
- theft of sensitive information
- the spread of malware to other users

How to prevent:

- Input validation and output encoding
- Use security libraries or frameworks that automatically sanitize input
- Enforce a strict Content Security Policy (CSP)

The Vulnerability Scan was conducted on 24 April 2024, before the websites were taken down. The following exploitable vulnerabilities were found.