

# Penetration Testing

<https://starbannerglobal.com>

Bhuvan Vijay Kumar(PES1UG21CS140)

Raghav S (PES1UG21CS469)

Rashmi J (PES1UG21CS480)

Shaik Adeeba Saher (PES1UG21CS549)

# URL : <https://starbannerglobal.com>

02

traderknows.com/en/wiki/organizations/f1519ccb91bd4ba1b81a80ef9e5d9f88

COMEX Gold 2349.6001 Crude Oil 83.66 USD/EUR 0.9347 USD/GBP 0.8004

Search Without Limits English

Traderknows Home Organizations People News Glossary Columns FinMart Login

**Star Banner Global Ltd**

Suspected Fraud

China Forex Brokerage Contact

Within 1 year https://starbannerglobal.com/

Website Verification

**Current Rating**

2.39

User Reviews -

Traffic 3.67

Brand Index 1.00

Risk Assessment 2.10

**Profile**

Country China

Market Categories Forex

Organization Categories Brokerage

Services Foreign exchange, metals, crude oil, indices, and cryptocurrencies.

Supported Languages English, Japanese, Traditional Chinese, and Korean.

Domain Registration 2023-06-13

Status Suspected Fraud

**Industry Tier** D

E D C B A S SS

**Social Media**

- 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



- 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        v6.3.10-Cloudflare http proxy
443/tcp   open  ssl/https  120.219.120.41:443 - cloudflare - 412 post
8080/tcp  open  http        46.101.144.134:8080 - 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

## Issued To

Common Name (CN) starbannerglobal.com  
Organization (O) <Not Part Of Certificate>  
Organizational Unit (OU) <Not Part Of Certificate>

## Issued By

Common Name (CN) E1  
Organization (O) Let's Encrypt  
Organizational Unit (OU) <Not Part Of Certificate>

## Validity Period

Issued On	Sunday, April 14, 2024 at 6:05:13 AM
Expires On	Saturday, July 13, 2024 at 6:05:12 AM

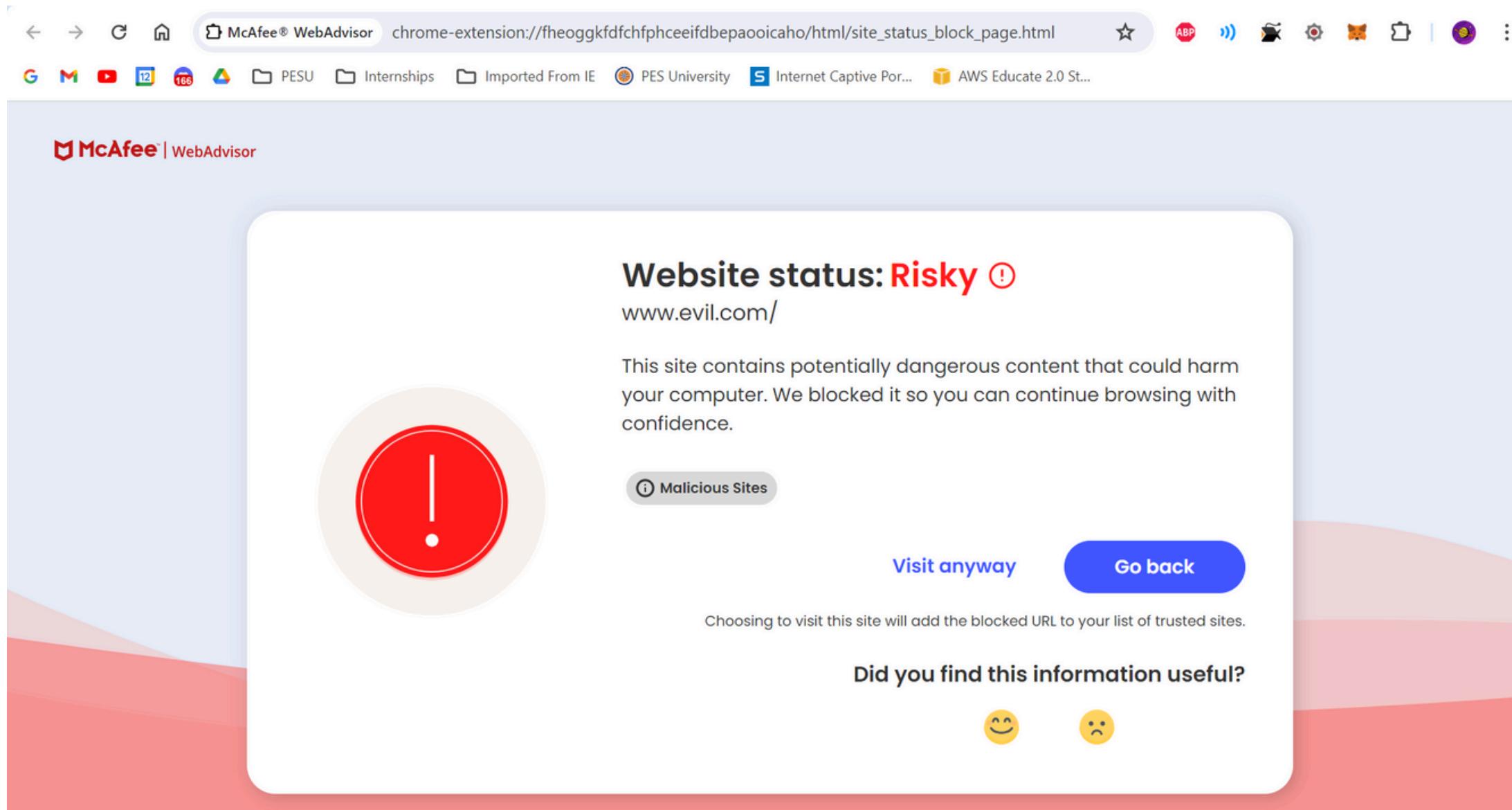
## SHA-256 Fingerprints

Certificate	65d4c5f824325c79c741405df61888f52bc7f62124b3933ea18bd34971b 5f659
Public Key	db38ee054b442fefa02fa2585e068475b91dcc11ac5c44c7fa1c1ac32c28 e640

# 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

```
(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/alt-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.com/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
```

- 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.

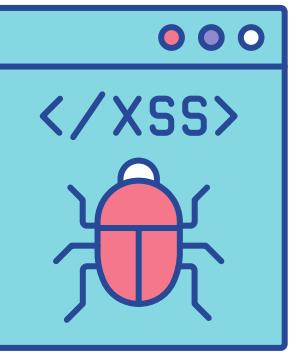
# Session Hijacking

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.

The screenshot shows a Kali Linux desktop environment with several windows open. In the center is the Burp Suite Community Edition v2023.10.3.4 - Temporary Project window. The 'Target' tab is selected. The 'Site map' section shows a tree of URLs for 'Star Banner Global Ltd'. The 'Request' and 'Response' panes show a captured HTTP request and response. The response body contains a session cookie: 'Set-Cookie: JSESSIONID=C3060062437A838D7C418D2C9951D81; Path=/; HttpOnly'. A blue arrow points from this cookie value to the 'Response' pane. Below the Burp Suite window is a web browser displaying the Star Banner Global Ltd website. The site has a dark theme with white text. It features a 'Sign up now' button and download links for macOS and Android. At the bottom, there's a trading interface with tabs like 'Forex', 'CryptoCurrency', 'Indices', etc., and a table for AUDUSD.

# 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/alt-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.com/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...



invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

xss (Cross-site scripting) 1/1

Product ▾ Why Us? ▾

## invicti

**Summary**

Invicti detected a missing Content-Type header which means that this website could be at risk of a MIME-sniffing attacks.

**Impact**

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type. The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

**Remediation**

- When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:  
Content-Type: text/html
- Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

By using this website you agree with our use of cookies to improve its performance and enhance your experience. [More info](#)

**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.