



**BSc. (Hons) Degree in IT  
(Sp. Cyber Security) – 2<sup>nd</sup> Year 2<sup>nd</sup> Semester**

**Web Security – IE2062**

**Title:  
Web Audit Assignment – Final Report**

**IT19127910**

**R.P.A. Ranasinghe**

<b>Content</b>	<b>Page</b>
<b>Introduction</b>	<b>03</b>
<b>Steps of Web Audit</b>	<b>05</b>
<b>Netspaker</b>	<b>08</b>
<b>Nikto</b>	<b>26</b>
<b>References</b>	<b>44</b>

## **Introduction**

This is my final report based on web security web audit assignment. To do this assignment I had to select a domain and scan that domain to check whether our selected domain has top 10 vulnerabilities listed by OWASP.

### **OWASP Top 10 Web Application Security Risks**

#### **Injection:**

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

#### **Broken Authentication:**

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

#### **Sensitive Data Exposure:**

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

#### **XML External Entities (XXE):**

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

#### **Broken Access Control:**

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

#### **Security Misconfiguration:**

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

#### **Cross-Site Scripting XSS:**

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which

can hijack user sessions, deface web sites, or redirect the user to malicious sites.

### **Insecure Deserialization:**

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

### **Using Components with Known Vulnerabilities:**

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

### **Insufficient Logging & Monitoring:**

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Do that scanning processes I used different tools. They are

- Netsparker
- Nikto

## Steps of Web Audit

Before these scans I created an account in hackerone and searched domains.

The screenshot shows the HackerOne dashboard with the URL [hackerone.com/hacker\\_dashboard/overview](https://hackerone.com/hacker_dashboard/overview). The main navigation bar includes 'Overview', 'My Programs', 'Retesting', 'Followed Hackers', and 'Pending Invitations'. On the left, there's a profile section for 'Aloka Ranasinghe (@lokaranasinghe)' with a placeholder profile picture. It shows 'Resolved 0% reports' and a breakdown of severity: Low (0), Medium (0), High (0), and Critical (0). Below that is a 'My stats' box showing 9 items. A large callout box on the right encourages users to update their profile settings, mentioning features like ranking against other hackers. Below this, there are two main sections: 'About HackerOne' (with a circular icon containing a stylized '1') and 'Learn how to hack' (with a circular icon containing a graduation cap).

Then I selected 3 domains to scan scope of sub domains. They are

**playstaion.com**

The screenshot shows the 'Directory' tab of the HackerOne dashboard. It lists several programs under the heading 'These programs are professionally managed by HackerOne, and have a higher overall success rate.' The programs listed are: UpGuard (Managed), Wells Fargo (Managed), PlayStation (Managed), Courier (Managed), Magisto (Managed), and Bitwala (Managed). Each entry includes the program name, status, last updated date (06/2020), number of reports (ranging from 6 to 134), reward amount (\$50 to \$400), and a star icon for favoriting.

## paypal.com

	OpenVPN	09 / 2018	4	\$100	-	☆
	VeraCrypt	09 / 2018	0	\$500	-	☆
	PayPal	08 / 2018	956	-	\$1k-\$2k	☆
	MariaDB	07 / 2018	28	-	-	☆

## monolith.com

	Endless Hosting	02 / 2020	50	-	-	☆
	Koho	02 / 2020	19	-	-	☆
	Monolith	02 / 2020	6	\$50	\$1k-\$1k	☆
	Marriott Vulnerability Disclosure Program	02 / 2020	160	-	-	☆
	Monolith	02 / 2020	67	100	1000-2000	☆

After that I had to install sublist3r in my kali virtual machine. To perform that firstly I searched sublist3r in google and then I got a GitHub link. By using that GitHub link, I got gitclone command. Then copy that command and paste it in my Kali machine terminal. After cloned I installed python3.pip and python.pip.

Then went to sublist3r directory and run this **sudo pip install -r requirements.txt command**. After that I had to install python setup. But when I tried to do that, I got an error So, I searched that error in google and I had to install python setup tools before install python setup. After complete above steps successfully I run the sublist3r.py.

```

shin@kali:~/Sublist3r$ git clone https://github.com/aboul3la/Sublist3r.git
shin@kali:~/Sublist3r$ cd Sublist3r
shin@kali:~/Sublist3r$ sudo pip install -r requirements.txt
Adding argparse 1.2.1 to easy-install.pth file
Using /usr/lib/python2.7
Searching for requests==2.22.0
Best match: requests 2.22.0
Adding requests 2.22.0 to easy-install.pth file
Using /usr/lib/python2.7/dist-packages
Searching for dnspython==1.16.0
Best match: dnspython 1.16.0
Adding dnspython 1.16.0 to easy-install.pth file
Using /usr/lib/python2.7/dist-packages
Finished processing dependencies for Sublist3r==1.0
shin@kali:~/Sublist3r$ python sublist3r.py

[REDACTED]
# Coded By Ahmed Aboul-Ela - @aboul3la

Usage: python sublist3r.py [Options] use -h for help
Error: argument -d/-domain is required
shin@kali:~/Sublist3r$ [REDACTED]

• The recommended version for Python 3 is 3.4.x

```

Firstly, I scanned playstation.com. Then I scanned paypal.com and monolith.com. After those scanning, I had to select a domain among them. So, I decided to select paypal.com.

All of the above-mentioned steps are in this video:

[https://drive.google.com/file/d/1jHEWSci\\_XdoQqaQOizJM\\_8Lj6ZCIkDCS/view?usp=sharing](https://drive.google.com/file/d/1jHEWSci_XdoQqaQOizJM_8Lj6ZCIkDCS/view?usp=sharing)

Then I started scanning process of my selected domain paypal.com. I selected these sub domains to scan:

- paypal.com
- xoom.com
- braintreegateway.com
- braintreepayments.com
- paypal.me
- paydiant.com
- paypalobjects.com
- prequal.swiftfinancial.com
- partner.swiftfinancial.com
- decision.swiftfinancial.com
- swiftcapital.com
- loanbuilder.com
- swiftfinancial.com
- api.swiftfinancial.com
- my.swiftfinancial.com
- api.loanbuilder.com
- my.loanbuilder.com

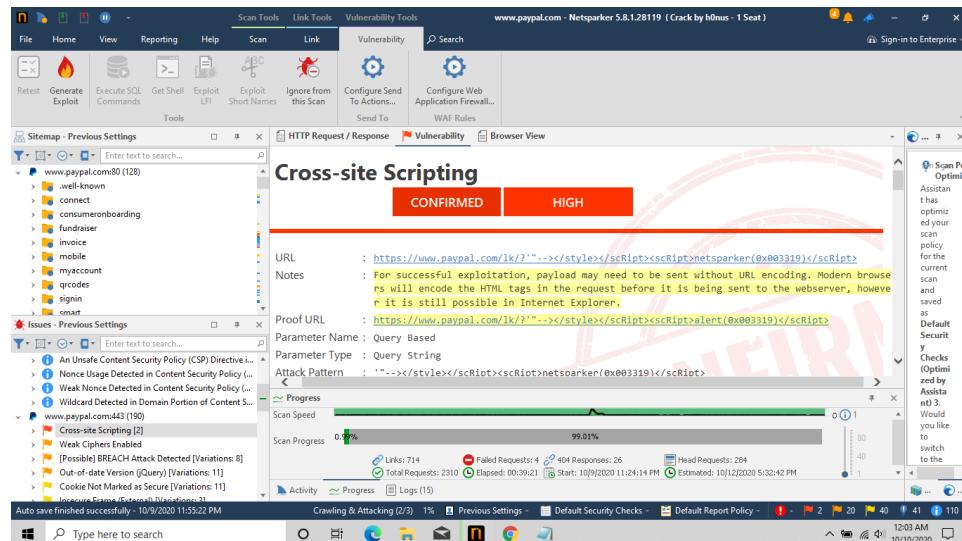
## Netsparker

Firstly, I used Netsparker to scan some of my sub domains. They are,

- paypal.com
- xoom.com
- braintreegateway.com
- paypal.me
- braintreepayments.com

Paypal.com:

- 7 high (same cross site scripting vulnerability has detected seven times)
- 23 mediums
- 77 low vulnerabilities.



CLASSIFICATION	
PCI DSS 3.2	<u>6.5.7</u>
OWASP 2013	A3
OWASP 2017	A7
CWE	79
CAPEC	19
WASC	8
HIPAA	<u>164.308(A)</u>
ISO27001	<u>A.14.2.5</u>

#### CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

---

#### CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/  
A:N

---

#### CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

---

#### CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/  
A:N

---

## Medium Vulnerabilities

**Weak Ciphers Enabled**

**CONFIRMED**    **MEDIUM**

URL : <https://www.paypal.com/>

List of Supported Weak Ciphers :

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)

Progress

Scan Speed: 0.92%    99.07%

Activity: Links: 722 Failed Requests: 4 404 Responses: 26 Head Requests: 316

Logs: Total Requests: 2493 Elapsed: 00:42:26 Start: 10/9/2020 11:24:14 PM Estimated: 10/13/2020 3:21:39 AM

Crawling & Attacking (2/3) 1% Previous Settings Default Security Checks Default Report Policy

Auto save finished successfully - 10/9/2020 11:55:22 PM

Type here to search

**[Possible] BREACH Attack Detected** MEDIUM

Certainty : [REDACTED]  
 URL : <https://www.paypal.com/us/home>  
 Reflected Parameter(s) : param1  
 Sensitive Keyword(s) : nonce

**Vulnerability Details**

CLASSIFICATION  
 OWASP 2013 A9  
 OWASP 2017 A9

Progress  
 Scan Speed  
 Scan Progress 95.70%  
 Links: 2508 Failed Requests: 21 404 Responses: 639 Head Requests: 2394 Total Requests: 32663

Activity Progress Logs (19)

Auto save finished successfully - 10/10/2020 1:46:57 PM Crawling & Attacking (2/3) 4% Previous Settings Default Security Checks Default Report Policy 1:49 PM 10/10/2020

Type here to search

**Out-of-date Version (jQuery)** MEDIUM

Certainty : [REDACTED]  
 URL : <https://www.paypal.com/lk/home>  
 Identified Version : 1.12.4  
 Latest Version : 1.12.4 (in this branch)  
 Branch Status : This branch has stopped receiving updates since 6/20/2016.  
 Vulnerability Database : Result is based on 04/27/2020 05:00:00 vulnerability database content.

**Vulnerability Details**

CLASSIFICATION  
 OWASP 2013 A9  
 OWASP 2017 A9

Progress  
 Scan Speed  
 Scan Progress 95.70%  
 Links: 2508 Failed Requests: 21 404 Responses: 639 Head Requests: 2394 Total Requests: 32669

Activity Progress Logs (19)

Auto save finished successfully - 10/10/2020 1:46:57 PM Crawling & Attacking (2/3) 4% Previous Settings Default Security Checks Default Report Policy 1:50 PM 10/10/2020

Type here to search

## Low Vulnerabilities

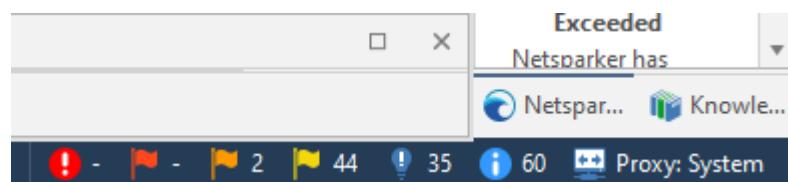
- Cookie not marked as secure
- Insecure frame (External)
- User controlled cookie
- [Possible] Cross-site request forgery
- [Possible] Internal IP address disclosure
- [Possible] Phishing by navigating browser tabs
- Cookie not marked as HTTPOnly
- Missing content-type header

paypal.com scan video:

[https://drive.google.com/file/d/1XmMaMcAGT0fHXYId6tHww\\_OjVii4A2MM/view?usp=sharing](https://drive.google.com/file/d/1XmMaMcAGT0fHXYId6tHww_OjVii4A2MM/view?usp=sharing)

xoom.com:

- 2 medium vulnerabilities
- 44 low vulnerabilities



## Medium Vulnerabilities

## CLASSIFICATION

PCI DSS 3.2	<u>6.5.4</u>
OWASP 2013	<u>A6</u>
OWASP 2017	<u>A3</u>
CWE	<u>327</u>
CAPEC	<u>217</u>
WASC	<u>4</u>
ISO27001	<u>A.14.1.3</u>

## CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

## CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/  
A:N

## CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

## CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/  
A:N

**HTTP Strict Transport Security (HSTS) Errors and Warnings**

MEDIUM

Certainty :

URL : <https://www.xoom.com/>

CLASSIFICATION	
OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
CWE	<a href="#">16</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.1.2</a>

Session loaded successfully. Scan status: finished.

## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
CWE	<a href="#">16</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.1.2</a>

## Low Vulnerabilities

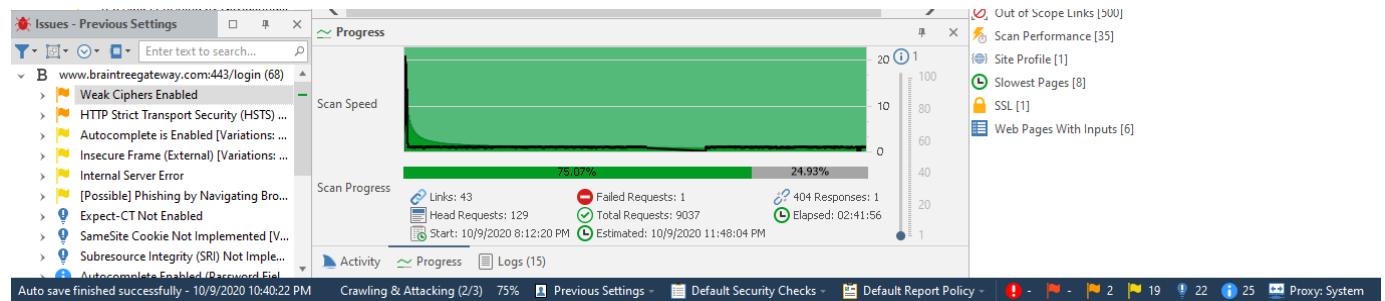
- Cookie Not Marked as HttpOnly
- Cookie Not Marked as Secure
- Insecure Frame (External)
- Internal Server Error
- [Possible] Cross-site Request Forgery
- Multiple Declarations in X-Frame-Options Header

xoom.com scan video:

<https://drive.google.com/file/d/1fE2sHzueBNVwBAq2t2LLjnwapqpiGpLN/view?usp=sharing>

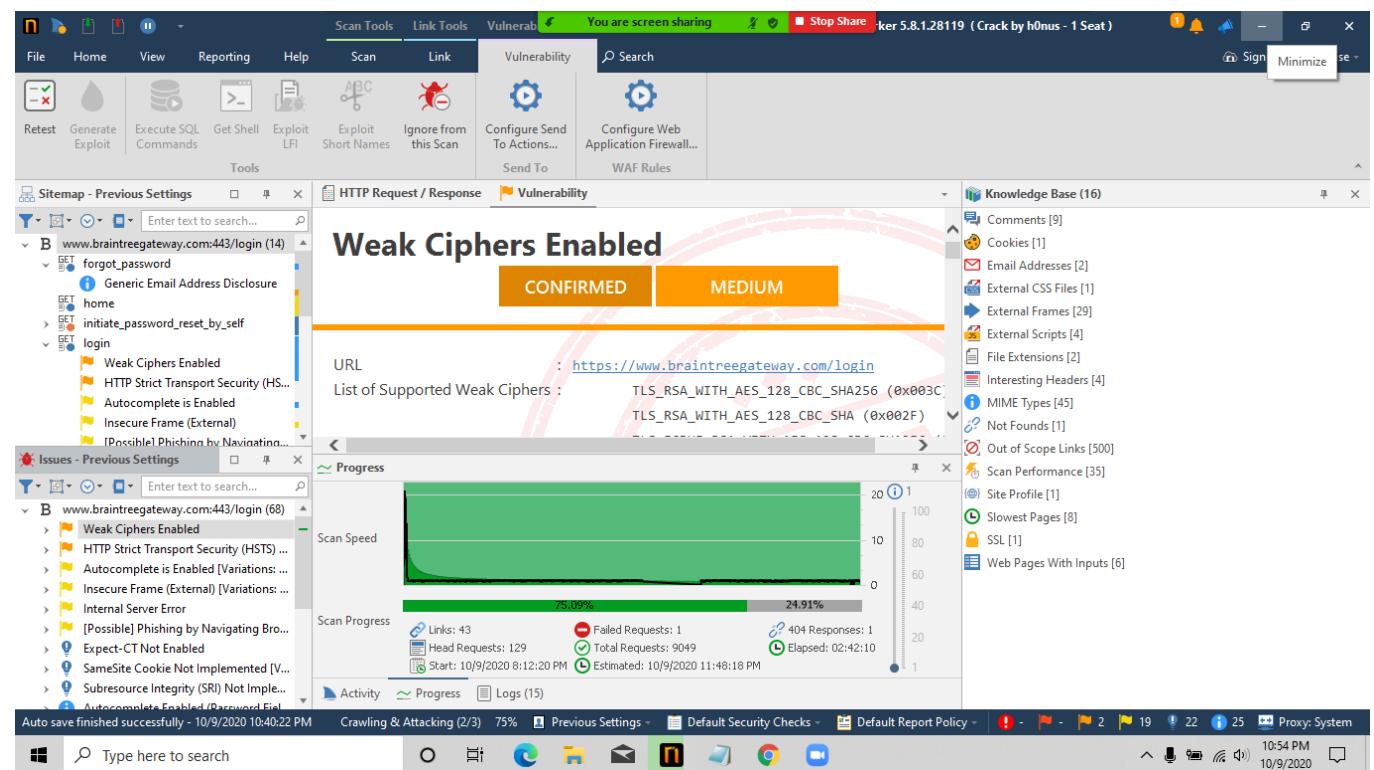
braintreegateway.com:

- 2 medium
- 19 low vulnerabilities.



## Medium Vulnerabilities

### 1. Weak Cipher Enabled



## CLASSIFICATION

PCI DSS 3.2	<u>6.5.4</u>
OWASP 2013	<u>A6</u>
OWASP 2017	<u>A3</u>
CWE	<u>327</u>
CAPEC	<u>217</u>
WASC	<u>4</u>
ISO27001	<u>A.14.1.3</u>

## CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

## 2. HTTP Strict Transport Security (HSTS) Errors and Warnings

The screenshot shows the ZAP interface with the following details:

- Scan Tools** tab is selected.
- HTTP Request / Response** tab is active.
- Vulnerability** tab is also visible.
- Issues - Previous Settings** panel on the left lists several HSTS-related issues:
  - B www.braintreegateway.com:443/login (14)
    - GET forgot\_password
    - GET home
    - GET initiate\_password\_reset\_by\_email
    - GET login
      - Weak Ciphers Enabled
      - HTTP Strict Transport Security (HSTS) ...
      - Autocomplete is Enabled [Variations: ...]
      - Insecure Frame (External)
      - [Possible] Phishing by Navigating Bro...
  - B www.braintreegateway.com:443/login (68)
    - Weak Ciphers Enabled
    - HTTP Strict Transport Security (HSTS) ...
    - Autocomplete is Enabled [Variations: ...]
    - Insecure Frame (External) [Variations: ...]
    - Internal Server Error
    - [Possible] Phishing by Navigating Bro...
    - Expect-CT Not Enabled
    - SameSite Cookie Not Implemented [V...
    - Subresource Integrity (SRI) Not Imple...
    - Autocomplete-Enabled (Resource File)
- HTTP Strict Transport Security (HSTS) Errors and Warnings** section in the center:
  - MEDIUM** risk level.
  - Certainty: [redacted]
  - URL: <https://www.braintreegateway.com/login>
- Classification** table on the right:
 

OWASP 2013	<u>A5</u>
OWASP 2017	<u>A6</u>
CWE	<u>16</u>
WASC	<u>15</u>
ISO27001	<u>A.14.1.2</u>
- Activity** and **Logs (15)** sections at the bottom.

## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
CWE	<a href="#">16</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.1.2</a>

### Low Vulnerabilities

#### Autocomplete is Enabled

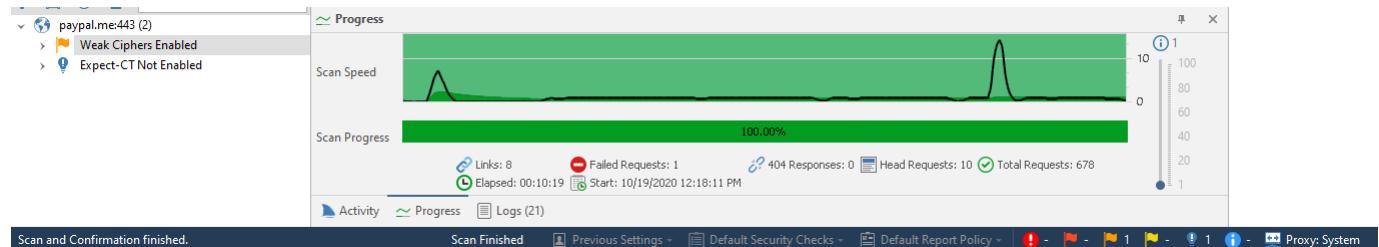
- Insecure Frame (External)
- Internal Server Error
- [Possible] Phishing by Navigating Browser Tabs

braintreegateway.com scan video:

<https://drive.google.com/file/d/1m6vcBxnjRVe-BxuJlqF4SNtYAxIndZLC/view?usp=sharing>

paypal.me:

only 1 medium vulnerability.



Screenshot of the Netsparker application interface showing a scan report for [paypal.me/](https://paypal.me/).

**Vulnerability Tools** tab is selected.

**Weak Ciphers Enabled** vulnerability is highlighted in the main pane.

**CONFIRMED** and **MEDIUM** severity levels are shown.

**URL**: <https://paypal.me/>

**List of Supported Weak Ciphers**:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003D)
- TLS\_PKA\_WITH\_AES\_128\_CBC\_SHA (0x002E)

**Scan Progress** chart shows Scan Speed and Scan Progress (100.00%).

Scan statistics:

- Links: 8
- Failed Requests: 1
- 404 Responses: 0
- Head Requests: 10
- Total Requests: 678

Scan started at 10/19/2020 12:18:11 PM and finished at 10/19/2020 12:31:19 PM.

Logs: 21

CLASSIFICATION	
PCI DSS 3.2	<a href="#">6.5.4</a>
OWASP 2013	<a href="#">A6</a>
OWASP 2017	<a href="#">A3</a>
CWE	<a href="#">327</a>
CAPEC	<a href="#">217</a>
WASC	<a href="#">4</a>
ISO27001	<a href="#">A.14.1.3</a>

### CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

### CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

## CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

## CVSS Vector String

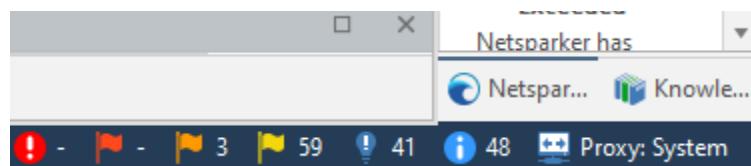
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

paypal.me scan video:

<https://drive.google.com/file/d/1-8tPYfdOVR18xNXAzWvVzYroOtTAHMJe/view?usp=sharing>

braintreepayments.com:

- 3 medium
- 59 low vulnerabilities



## Medium Vulnerabilities

### 1. Weak Ciphers Enabled

The screenshot shows a detailed report from Netsparker for the URL <https://www.braintreepayments.com/>. The main panel displays a list of 'Weak Ciphers Enabled' with two tabs: 'CONFIRMED' and 'MEDIUM'. Under 'CONFIRMED', it lists supported weak ciphers: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000A), TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035), TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F), TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C), TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013), TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014), TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027), and TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028). The 'CLASSIFICATION' section indicates the findings are 'CONFIRMED'. A sidebar on the right provides information about the current scan policy, mentioning an 'Assistant has optimized your scan policy for the current scan and saved as Default Security Check (Optimized by Assistant) 4. Would you like to switch to the optimized policy?'. It also notes a 'Warning: It is strongly advised to restart your scan to keep your scan coverage at its best after the scan policy is switched.' and a 'DOM Simulation Time Exceeded' message.

### 2. HTTP Strict Transport Security (HSTS) Errors and Warnings

The screenshot shows the Netsparker interface with the following details:

- Scan Tools** tab is selected.
- Link Tools** tab is visible.
- Vulnerability Tools** tab is visible.
- Scan** button is highlighted.
- Link** button is visible.
- Vulnerability** button is visible.
- Search** bar is present.
- www.braintreepayments.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)** is displayed in the title bar.
- HTTP Request / Response**, **Vulnerability**, and **Browser View** tabs are visible.
- HTTP Strict Transport Security (HSTS) Errors and Warnings** section is displayed.
- MEDIUM** severity level is indicated.
- Certainty**: [redacted]
- URL**: <https://www.braintreepayments.com/>
- CLASSIFICATION** section includes:
  - OWASP 2013: A5
  - OWASP 2017: A6
  - CWE: 16
  - WASC: 15
  - ISO27001: A.14.1.2
- Issues - Previous Settings** panel lists various findings, including "Weak Ciphers Enabled" and "HTTP Strict Transport Security (HSTS) Error...".
- Progress** panel shows activity, progress, and logs.
- Scan Paused** status is shown at the bottom.

### 3. Out-of-date Version (jQuery)

The screenshot shows the Netsparker interface with the following details:

- Scan Tools** tab is selected.
- Link Tools** tab is visible.
- Vulnerability Tools** tab is visible.
- Scan** button is highlighted.
- Link** button is visible.
- Vulnerability** button is visible.
- Search** bar is present.
- www.braintreepayments.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)** is displayed in the title bar.
- HTTP Request / Response**, **Vulnerability**, and **Browser View** tabs are visible.
- Out-of-date Version (jQuery)** section is displayed.
- MEDIUM** severity level is indicated.
- Certainty**: [redacted]
- URL**: <https://www.braintreepayments.com/cz/global-payments-report/partials/js>
- Identified Version**: 3.3.1
- Latest Version**: 3.4.1 (in this branch)
- Vulnerability Database**: Result is based on 04/27/2020 05:00:00 vulnerability database content.
- Vulnerability Details** section states: "Netsparker identified the target web site is using jQuery and detected that it is out of date."
- CLASSIFICATION** section includes:
  - PCI DSS 3.2: 6.2
  - OWASP 2013: A9
  - OWASP 2017: A9
  - CWE: 829
  - CAPEC: 310
- Issues - Previous Settings** panel lists various findings, including "Weak Ciphers Enabled" and "Out-of-date Version (jQuery)".
- Progress** panel shows activity, progress, and logs.
- Scan Paused** status is shown at the bottom.

## Low Vulnerabilities

- Cookie Not Marked as HttpOnly
- Cookie Not Marked as Secure
- Insecure Frame (External)
- Insecure Transportation Security Protocol Supported (TLS 1.0)
- [Possible] Cross-site Request Forgery
- [Possible] Phishing by Navigating Browser Tabs
- Missing X-Frame-Options Header

[braintreepayments.com](https://braintreepayments.com) scan video:

[https://drive.google.com/file/d/1eMnvm-y6UOhIKUXBUQwZX-upQP0rFzk /view?usp=sharing](https://drive.google.com/file/d/1eMnvm-y6UOhIKUXBUQwZX-upQP0rFzk/view?usp=sharing)

When I consider about overall scans which I did using NetSparker, I got only one HIGH vulnerability. It is Cross-site scripting.

### Cross-site scripting

It is a client-side code injection attack. In a victim's web browser, the attacker attempts to execute malicious scripts by inserting malicious code into a legitimate web page or web application. When the user enters the web page or web application that executes the malicious code, the actual attack takes place. Forums, message boards, and web pages allowing comments are widely used for cross-site scripting attacks. This occurs because the browser interprets the input entered by a user as HTML / JavaScript /VBScript.

There are three main types of XSS attacks. These are:

Reflected XSS, where the malicious script comes from the current HTTP request.

Stored XSS, where the malicious script comes from the website's database.

DOM-based XSS, where the vulnerability exists in client-side code rather than server-side code.

### Impact

By using cross-site scripting, there are several different attacks that can be leveraged, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

### Remedy

Output should be encoded according to the output position and meaning in order to prevent this. For example, if the output enters a JavaScript block within the HTML document, it is important to encode the output accordingly. Encoding can become very difficult, so using an encoding library like OWASP ESAPI and Microsoft Anti-cross-site scripting is highly recommended. Additionally, if an XSS vulnerability is accidentally implemented, you can enforce a strict Content security Policy (CSP) as a defense-in - depth measure. XSS vulnerabilities are still prevalent in web applications due to the difficulty of XSS prevention and the lack of stable standard actions in programming languages and frameworks.

And I got 4 common Medium vulnerabilities. They are:

## 1. Weak Ciphers Enabled

List of Supported Weak Ciphers:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

## Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
2. SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
3. Lighttpd:
4. ssl.honor-cipher-order = "enable"
5. ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
6. For Microsoft IIS, you should make some changes to the system registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.
  - a. Click Start, click Run, type regedt32 or type regedit, and then click OK.
  - b. In Registry Editor, locate the following registry key:  
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
  - c. Set "Enabled" DWORD to "0x0" for the following registry keys:
    7. SCHANNEL\Ciphers\DES 56/56
    - SCHANNEL\Ciphers\RC4 64/128
    - SCHANNEL\Ciphers\RC4 40/128
    - SCHANNEL\Ciphers\RC2 56/128
    - SCHANNEL\Ciphers\RC2 40/128
    - SCHANNEL\Ciphers\NULL
    - SCHANNEL\Hashes\MD5

## Remedy

Configure your web server to disallow using weak ciphers.

## External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

## 2. HTTP Strict Transport Security (HSTS) Errors and Warnings

### Error Resolution

preload directive not present Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

### Vulnerability Details

Netsparker detected errors during parsing of Strict-Transport-Security header.

### Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

### Remedy

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
- In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
  - The max-age must be at least 31536000 seconds (1 year)
  - The includeSubDomains directive must be specified
  - The preload directive must be specified
  - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

### External References

HTTP Strict Transport Security (HSTS) HTTP Header

Wikipedia - HTTP Strict Transport Security Implementation  
Check HSTS Preload status and eligibility

### **3. Out-of-date Version (jQuery)**

#### **Vulnerability Details**

Netsparker identified the target web site is using jQuery and detected that it is out of date.

#### **Impact**

Since this is an old version of the software, it may be vulnerable to attacks.

#### **Remedy**

Please upgrade your installation of jQuery to the latest stable version.

#### **Remedy References**

Downloading jQuery

Known Vulnerabilities in this Version

.medium{fill:#FF9900;} jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

#### **Affected Versions**

1.9.0 to 3.4.1

#### **External References**

CVE-2020-11023

.medium{fill:#FF9900;} jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

### **4. BREACH Attack Detected [Possible]**

#### **Vulnerability Details**

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

#### **Impact**

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic

and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic

### Remedy

Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies To mitigate the issue, we recommend the following solutions:
  1. If possible, disable HTTP level compression
  2. Separate sensitive information from user input
  3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
  4. Hide the length of the traffic by adding a random number of bytes to the responses.
  5. Add in a rate limit, so that the page maximum is reached five times per minute.

### External References

Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext  
Using the Same-Site Cookie Attribute to Prevent CSRF Attacks

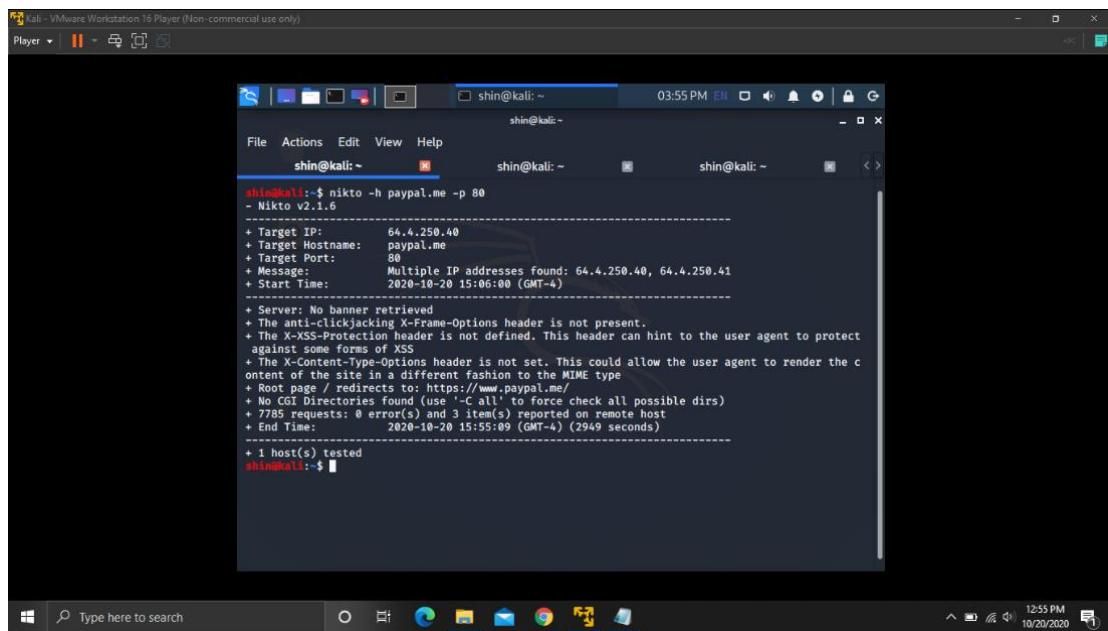
## **Nikto**

After scanning sub domains using Netsparker, I used Nikto to scan another sub domain set for port 80 and port 443.

They are,

- paypal.me
- paydiant.com
- paypalobjects.com
- prequal.swiftfinancial.com
- partner.swiftfinancial.com
- decision.swiftfinancial.com
- swiftcapital.com
- loanbuilder.com
- swiftfinancial.com
- api.swiftfinancial.com
- my.swiftfinancial.com
- api.loanbuilder.com
- my.loanbuilder.com

## paypal.me (port 80)



```

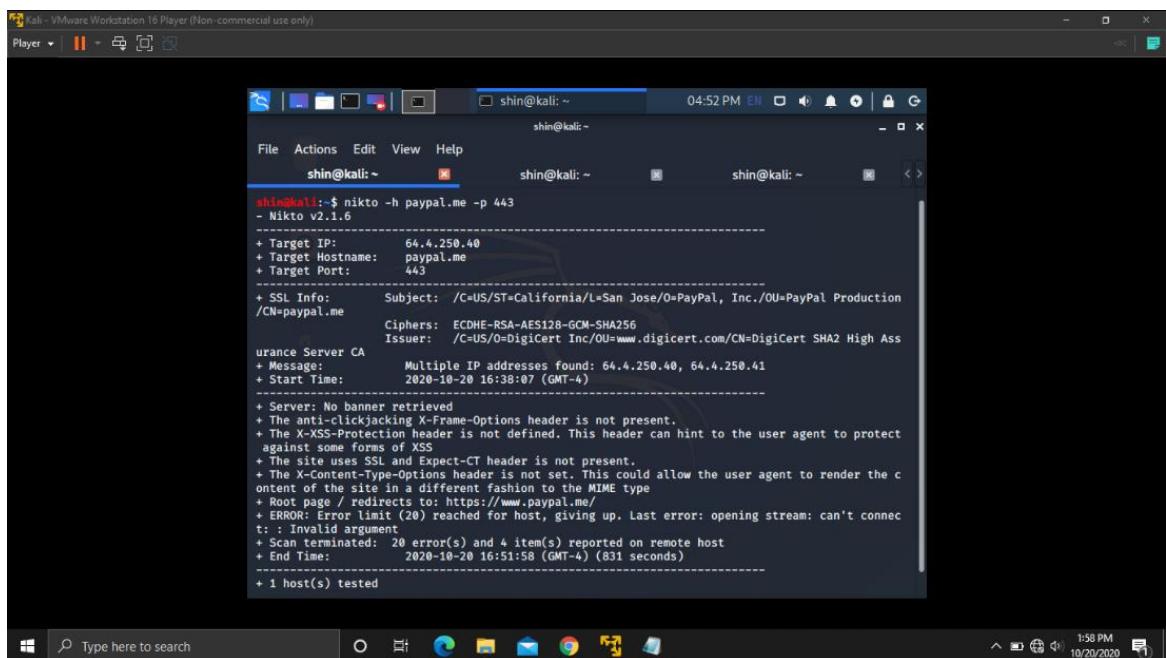
shin@kali:~$ nikto -h paypal.me -p 80
- Nikto v2.1.6
-----
+ Target IP:      64.4.250.40
+ Target Hostname: paypal.me
+ Target Port:    80
+ Message:        Multiple IP addresses found: 64.4.250.40, 64.4.250.41
+ Start Time:     2020-10-20 15:06:00 (GMT-4)
+ End Time:       2020-10-20 15:55:09 (GMT-4) (2949 seconds)

+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.paypal.me/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7785 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:       2020-10-20 15:55:09 (GMT-4) (2949 seconds)

+ 1 host(s) tested
shin@kali:~$ 

```

## paydiant.com (port 443)



```

shin@kali:~$ nikto -h paydiant.com -p 443
- Nikto v2.1.6
-----
+ Target IP:      64.4.250.40
+ Target Hostname: paydiant.com
+ Target Port:    443
+ SSL Info:       Subject: /C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PayPal Production
/CN=paypal.me
          Ciphers: ECDHE-RSA-AES128-GCM-SHA256
          Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Ass
urance Server CA
+ Message:        Multiple IP addresses found: 64.4.250.40, 64.4.250.41
+ Start Time:     2020-10-20 16:38:07 (GMT-4)
+ End Time:       2020-10-20 16:51:58 (GMT-4) (831 seconds)

+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.paydiant.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connec
t: : Invalid argument
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time:       2020-10-20 16:51:58 (GMT-4) (831 seconds)

+ 1 host(s) tested
shin@kali:~$ 

```

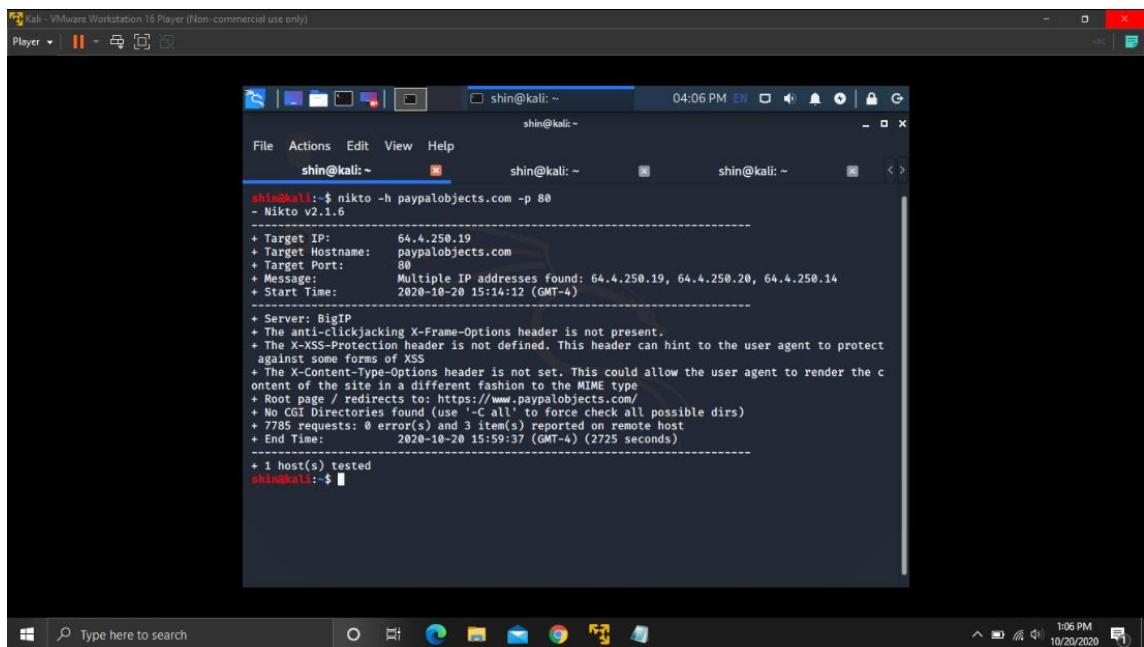
## paydiant.com (port 80)

```
shin@kali:~$ nikto -h paydiant.com -p 80
Nikto v2.1.6
=====
+ Target IP:      204.74.99.193
+ Target Hostname: paydiant.com
+ Target Port:    80
+ Start Time:    2020-10-20 15:13:18 (GMT-4)
+ Server:        UltraDNS Client Redirection Server
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: https://developer.paypal.com/docs/instore/paydiant/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7788 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:      2020-10-20 16:01:58 (GMT-4) (2920 seconds)
+ 1 host(s) tested
shin@kali:~$
```

## paydiant.com (port 443)

```
shin@kali:~$ nikto -h paydiant.com -p 443
Nikto v2.1.6
=====
+ No web server found on paydiant.com:443
+ 0 host(s) tested
shin@kali:~$
```

## paypalobjects.com (port 80)

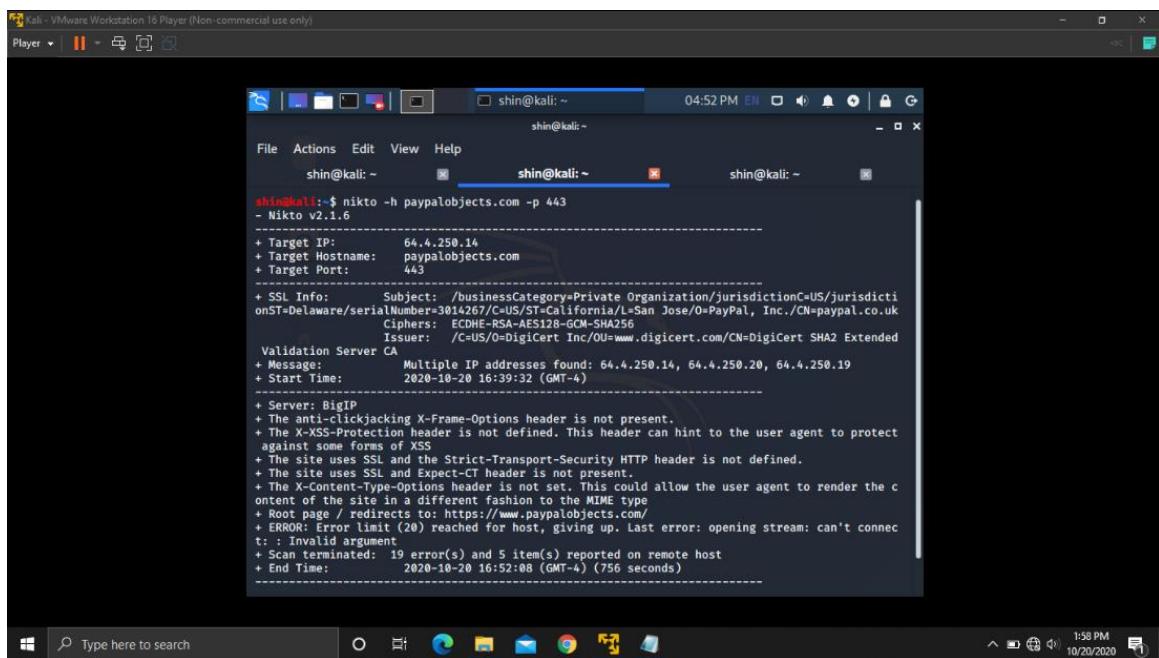


```

shin@kali:~$ nikto -h paypalobjects.com -p 80
- Nikto v2.1.6
-----
+ Target IP:      64.4.250.19
+ Target Hostname: paypalobjects.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 64.4.250.19, 64.4.250.20, 64.4.250.14
+ Start Time:    2020-10-20 15:14:12 (GMT-4)
-----
+ Server: BigIP
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.paypalobjects.com/
+ CGI Directories found (use -C all to force check all possible dirs)
+ 7785 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:      2020-10-20 15:19:37 (GMT-4) (2725 seconds)
-----
+ 1 host(s) tested
shin@kali:~$

```

## paypalobjects.com (port 443)

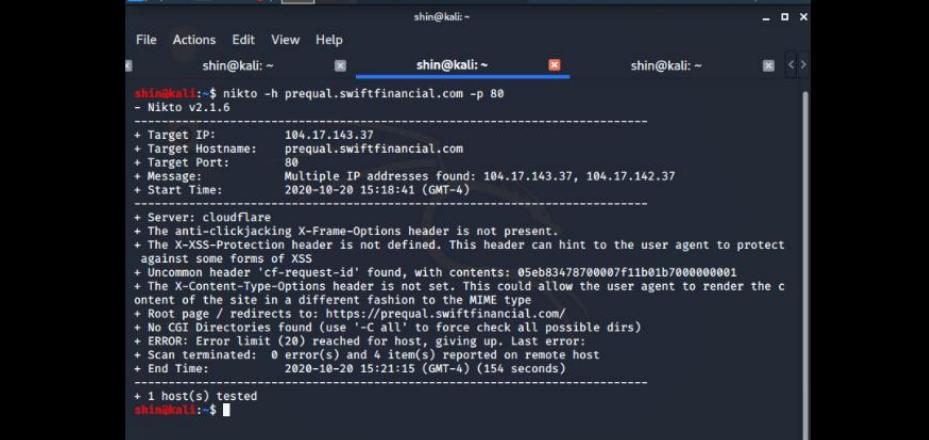


```

shin@kali:~$ nikto -h paypalobjects.com -p 443
- Nikto v2.1.6
-----
+ Target IP:      64.4.250.14
+ Target Hostname: paypalobjects.com
+ Target Port:    443
-----
+ SSL Info:       Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./CN=paypal.co.uk
                  Ciphers: ECDHE-RSA-AES128-GCM-SHA256
                  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA
+ Message:        Multiple IP addresses found: 64.4.250.14, 64.4.250.20, 64.4.250.19
+ Start Time:    2020-10-20 16:39:32 (GMT-4)
-----
+ Server: BigIP
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.paypalobjects.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connec
t: : Invalid argument
+ Scan terminated: 19 error(s) and 5 item(s) reported on remote host
+ End Time:      2020-10-20 16:52:08 (GMT-4) (756 seconds)

```

**prequal.swiftfinancial.com (port 80)**



Kali - VMware Workstation 16 Player (Non-commercial use only)

Player

shin@kali: ~

File Actions Edit View Help

shin@kali: ~ shin@kali: ~ shin@kali: ~

```
shin@kali:~$ nikto -h prequal.swiftfinancial.com -p 80
- Nikto v2.1.6
-----
+ Target IP:          104.17.143.37
+ Target Hostname:    prequal.swiftfinancial.com
+ Target Port:        80
+ Message:           Multiple IP addresses found: 104.17.143.37, 104.17.142.37
+ Start Time:         2020-10-20 15:18:41 (GMT-4)
-----
+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05eb83478700007f11b01b7000000001
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: https://prequal.swiftfinancial.com/
+ No CGI Directories Found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 errors) and 4 item(s) reported on remote host
+ End Time:           2020-10-20 15:21:15 (GMT-4) (154 seconds)
-----
+ 1 host(s) tested
shin@kali:~$
```

**prequal.swiftfinancial.com (port 443)**

## partner.swiftfinancial.com (port 80)

```

shin@kali:~$ nikto -h partner.swiftfinancial.com -p 80
- Nikto v2.1.6

+ Target IP:      104.17.143.37
+ Target Hostname:  partner.swiftfinancial.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 104.17.143.37, 104.17.142.37
+ Start Time:     2020-10-20 15:29:11 (GMT-4)

+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05eb8ce34000000f11bda7c000000001
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: https://partner.swiftfinancial.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 1 error(s) and 4 item(s) reported on remote host
+ End Time:       2020-10-20 15:32:31 (GMT-4) (208 seconds)

+ 1 host(s) tested
shin@kali:~$ 

```

## partner.swiftfinancial.com (port 443)

```

shin@kali:~$ nikto -h partner.swiftfinancial.com -p 443
- Nikto v2.1.6

+ Target IP:      104.17.142.37
+ Target Hostname:  partner.swiftfinancial.com
+ Target Port:    443
+ SSL Info:       Subject: /BusinessCategory=Private Organization/Jurisdiction=US/JurisdictionName=Delaware/SerialNumber=301e267/CN=ST=California/L=San Jose/O=PayPal, Inc./OU=PKI Product
on/CN=www.swiftfinancial.com
                  Ciphers: ECDHE-RSA-CHACHA20-POLY1305
                  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended
Validation Server: 2020-10-22 11:43:12 (GMT-4)
+ Message:        Multiple IP addresses found: 104.17.142.37, 104.17.143.37
+ Start Time:     2020-10-22 11:43:12 (GMT-4)

+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05fe929b6b0000f711a97b00000001
+ Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connec
tion will be dropped
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connec
t: SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake fa
ilure at /var/lib/nikto/plugins/LW2.pm line 5157.

+ Target IP:      104.17.142.37
+ Target Hostname:  partner.swiftfinancial.com
+ Target Port:    443
+ SSL Info:       Subject: /BusinessCategory=Private Organization/Jurisdiction=US/JurisdictionName=Delaware/SerialNumber=301e267/CN=ST=California/L=San Jose/O=PayPal, Inc./OU=PKI Product
on/CN=www.swiftfinancial.com
                  Ciphers: ECDHE-RSA-CHACHA20-POLY1305
                  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended
Validation Server: 2020-10-22 11:43:12 (GMT-4)
+ Message:        Multiple IP addresses found: 104.17.142.37, 104.17.143.37
+ Start Time:     2020-10-22 11:43:12 (GMT-4)

+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05fe929b6b0000f711a97b00000001
+ Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connec
tion will be dropped
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connec
t: SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake fa
ilure at /var/lib/nikto/plugins/LW2.pm line 5157.

+ 1 host(s) tested
shin@kali:~$ 

```

## decision.swiftfinancial.com (port 80)

```

shin@kali:~$ nikto -h decision.swiftfinancial.com -p 80
- Nikto v2.1.6
+ Target IP:      104.17.142.37
+ Target Hostname: decision.swiftfinancial.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 104.17.142.37, 104.17.143.37
+ Start Time:     2020-10-20 15:32:27 (GMT-4)
+ End Time:       2020-10-20 15:37:08 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05ebbf0d400007f1a0e0c0000000001
+ 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
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 3 item(s) reported on remote host
+ End Time:       2020-10-20 15:37:08 (GMT-4) (281 seconds)

+ 1 host(s) tested
shin@kali:~$ 

```

## decision.swiftfinancial.com (port 443)

```

shin@kali:~$ nikto -h decision.swiftfinancial.com -p 443
- Nikto v2.1.6
+ Target IP:      104.17.142.37
+ Target Hostname: decision.swiftfinancial.com
+ Target Port:    443
+ Message:        Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionState=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product
+ SSL Info:        Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionState=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product
+ Ciphers:        ECDSA-RSA-CHACHA20-POLY1305
+ Issuer:         /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA
+ Start Time:     2020-10-22 11:40:34 (GMT-4)
+ End Time:       2020-10-22 11:40:34 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05ef2305f00007f1a0e0c0000000001
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ Expect-Ct is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped.
+ 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
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect to SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure at /var/lib/nikto/plugins/LWZ.pm line 5157.
at /var/lib/nikto/plugins/LWZ.pm line 5157.

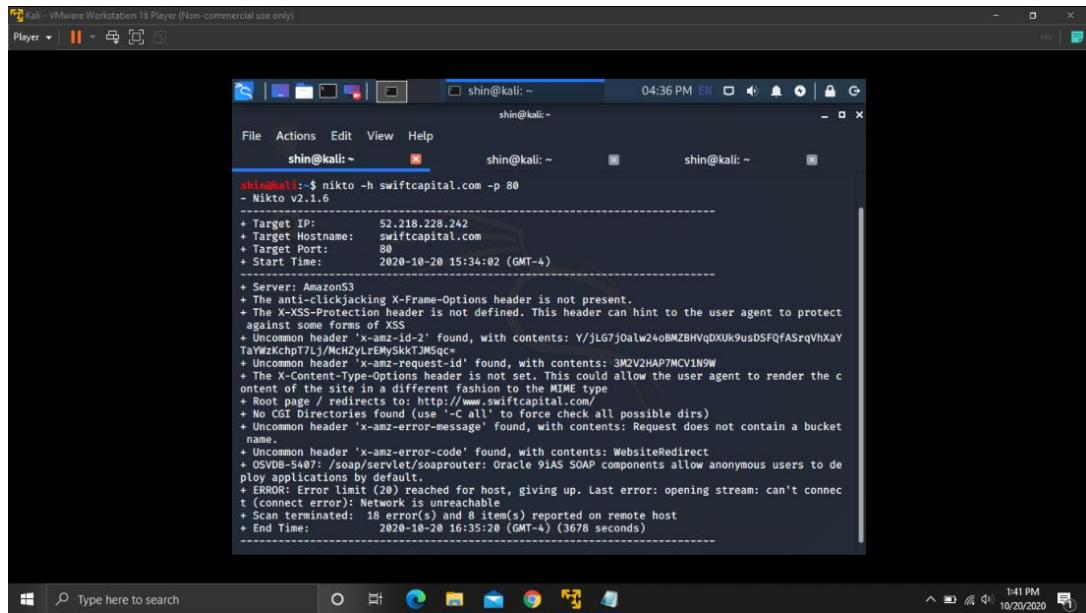
shin@kali:~$ nikto -h decision.swiftfinancial.com -p 443
- Nikto v2.1.6
+ Target IP:      104.17.142.37
+ Target Hostname: decision.swiftfinancial.com
+ Target Port:    443
+ Message:        Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionState=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product
+ SSL Info:        Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionState=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product
+ Ciphers:        ECDSA-RSA-CHACHA20-POLY1305
+ Issuer:         /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA
+ Start Time:     2020-10-22 11:40:34 (GMT-4)
+ End Time:       2020-10-22 11:40:34 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05ef2305f00007f1a0e0c0000000001
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ Expect-Ct is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped.
+ 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
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect to SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure at /var/lib/nikto/plugins/LWZ.pm line 5157.
at /var/lib/nikto/plugins/LWZ.pm line 5157.

shin@kali:~$ 

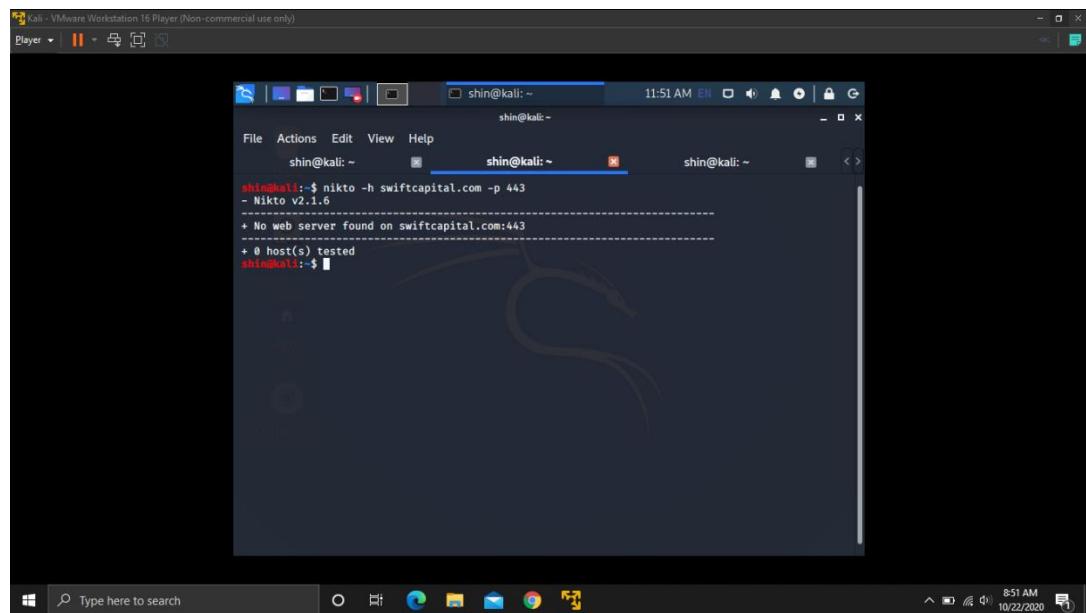
```

## swiftcapital.com (port 80)



```
shin@kali:~$ nikto -h swiftcapital.com -p 80
- Nikto v2.1.6
-----
+ Target IP:      52.218.228.242
+ Target Hostname: swiftcapital.com
+ Target Port:    80
+ Start Time:   2020-10-20 15:34:02 (GMT-4)
-----
+ Server: AmazonS3
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'x-amz-id-2' found, with contents: V/jLG7j0lw24oBMZBHqDXUk9usDSFQfASrqVhXAY
TaYmZxchpT7Lj/MChZyLrEMySkKTJMSc=
+ Uncommon header 'x-amz-request-id' found, with contents: 3M2V2HAP7MCV1N9W
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent type in a different fashion than the developer intended
+ Root page / redirects to: http://www.swiftcapital.com/
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Uncommon header 'x-amz-error-message' found, with contents: Request does not contain a bucket
name.
+ Uncommon header 'x-amz-error-code' found, with contents: WebsiteRedirect
+ OSVDB-5407: /soap/servlet/soaprouter: Oracle 9iAS SOAP components allow anonymous users to de
ploy applications by default.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connec
t (connect error): Network is unreachable
+ Scan terminated: 18 error(s) and 8 item(s) reported on remote host
+ End Time:   2020-10-20 16:35:20 (GMT-4) (3678 seconds)
```

## swiftcapital.com (port 443)



```
shin@kali:~$ nikto -h swiftcapital.com -p 443
- Nikto v2.1.6
-----
+ No web server found on swiftcapital.com:443
-----
+ 0 host(s) tested
shin@kali:~$
```

## loanbuilder.com (port 80)

```
shin@kali: ~ shin@kali: ~ shin@kali: ~
shin@kali: $ nikto -h loanbuilder.com -p 80
- Nikto v2.1.6
-----
+ Target IP:      52.218.249.59
+ Target Hostname: loanbuilder.com
+ Target Port:    80
+ Start Time:   2020-10-20 15:36:44 (GMT-4)
-----
+ Server: AmazonS3
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'x-amz-request-id' found, with contents: 01249E8DA2184434
+ Uncommon header 'x-amz-id-2' found, with contents: W08Dn@cz9n3zETzfQtRPV9QBWX1xpuqTfkreM8DRh
4IQJQDfAf37SsdhQj560LlhZE2zSqu/JE=
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: http://www.loanbuilder.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-amz-error-message' found, with contents: Request does not contain a bucket
name.
+ Uncommon header 'x-amz-error-code' found, with contents: WebsiteRedirect
+ OSVDB-5487: /soap/servlet/soaprouter: Oracle 9IAS SOAP components allow anonymous users to de
ploy applications by default
+ ERROR: Error limit (2) reached for host, giving up. Last error: opening stream: can't connec
t (errno=10060). Network is unreachable
+ Scan terminated: 19 error(s) and 8 item(s) reported on remote host
+ End Time:        2020-10-20 16:35:21 (GMT-4) (3517 seconds)
```

## loanbuilder.com (port 443)

```
shin@kali: ~ shin@kali: ~ shin@kali: ~
shin@kali: $ nikto -h loanbuilder.com -p 443
- Nikto v2.1.6
-----
+ No web server found on loanbuilder.com:443
-----
+ 0 host(s) tested
shin@kali: $
```

## swiftfinancial.com (port 80)

```

shin@kali:~$ nikto -h swiftfinancial.com -p 80
- Nikto v2.1.6
+ Target IP:      13.225.73.53
+ Target Hostname: swiftfinancial.com
+ Target Port:    80
+ Message:       Multiple IP addresses found: 13.225.73.53, 13.225.73.114, 13.225.73.75, 1
3.225.73.113
+ Start Time:    2020-10-20 15:38:02 (GMT-4)

+ Server: CloudFront
+ Retrieved via header: 1.1 Bz2e2811e641703aebf776da39317b9c.cloudfront.net (CloudFront)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'x-amz-cf-pop' found, with contents: FRA2-C2
+ Uncommon header 'x-amz-cf-id' found, with contents: M8C290LpsnFHG90iV8a0slAT7BFSBScingHk_A2x
BVTMj23e_g1Q0=
+ Uncommon header 'x-cache' found, with contents: Redirect from cloudfront
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: https://swiftfinancial.com/
+ CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connec
t (connect error): Network is unreachable
+ Scan terminated: 18 error(s) and 7 item(s) reported on remote host
+ End Time:      2020-10-20 16:35:20 (GMT-4) (3438 seconds)

+ 1 host(s) tested

```

## swiftfinancial.com (port 443)

```

shin@kali:~$ nikto -h swiftfinancial.com -p 443
- Nikto v2.1.6
+ Target IP:      54.192.86.45
+ Target Hostname: swiftfinancial.com
+ Target Port:    443
+ SSL Info:       Subject: /CN=*.swiftfinancial.com
                  Ciphers: TLS_AES_128_GCM_SHA256
                  Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message:        Multiple IP addresses found: 54.192.86.45, 54.192.86.73, 54.192.86.117, 5
4.192.86.128
+ Start Time:    2020-10-22 11:42:15 (GMT-4)

+ Server: AmazonS3
+ Retrieved via header: 1.1 ab1d15e856bdcedbea349504173a4eb.cloudfront.net (CloudFront)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: Miss from cloudfront
+ Uncommon header 'x-amz-cf-pop' found, with contents: AMS50-C1
+ Uncommon header 'x-amz-cf-id' found, with contents: b2d0JjR3Pv1MAa4c_hvnqF4juV2eAE9ahD66iVmqr
BorJLWignyH8Q=
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Root page / redirects to: http://www.swiftfinancial.com/index.html
+ No CGI Directories found (use '-C all' to force check all possible dirs)


```

```

shin@kali: ~          shin@kali: ~          shin@kali: ~
+ Start Time: 2020-10-22 11:42:15 (GMT-4)
-----
+ Server: AmazonS3
+ Retrieved via header: 1.1 ab1d15e056bdcedbea349504173a4ecb.cloudfront.net (CloudFront)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: Miss from cloudfront
+ Uncommon header 'x-amz-cf-pop' found, with contents: AMS50-C1
+ Uncommon header 'x-amz-cf-id' found, with contents: b2d0Jr3Pv1MAa4c_hvnqF4juV2eAE9ahD66ivMqRBorJLWtgnvH8o=-
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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 MIM type
+ Root page / redirects to: http://www.swiftfinancial.com/index.html
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'AmazonS3' to 'CloudFront' which may suggest a WAF, load balancer or proxy is in place
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect to SSL negotiation failed: error:1408F10B:SSL routines:ssl3_get_record:wrong version number at /var/lib/nikto/plugins/LW2.pm line 5157.
at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 9 item(s) reported on remote host
+ End Time: 2020-10-22 11:53:40 (GMT-4) (685 seconds)

+ 1 host(s) tested
shin@kali: ~

```

**api.swiftfinancial.com (port 80)**

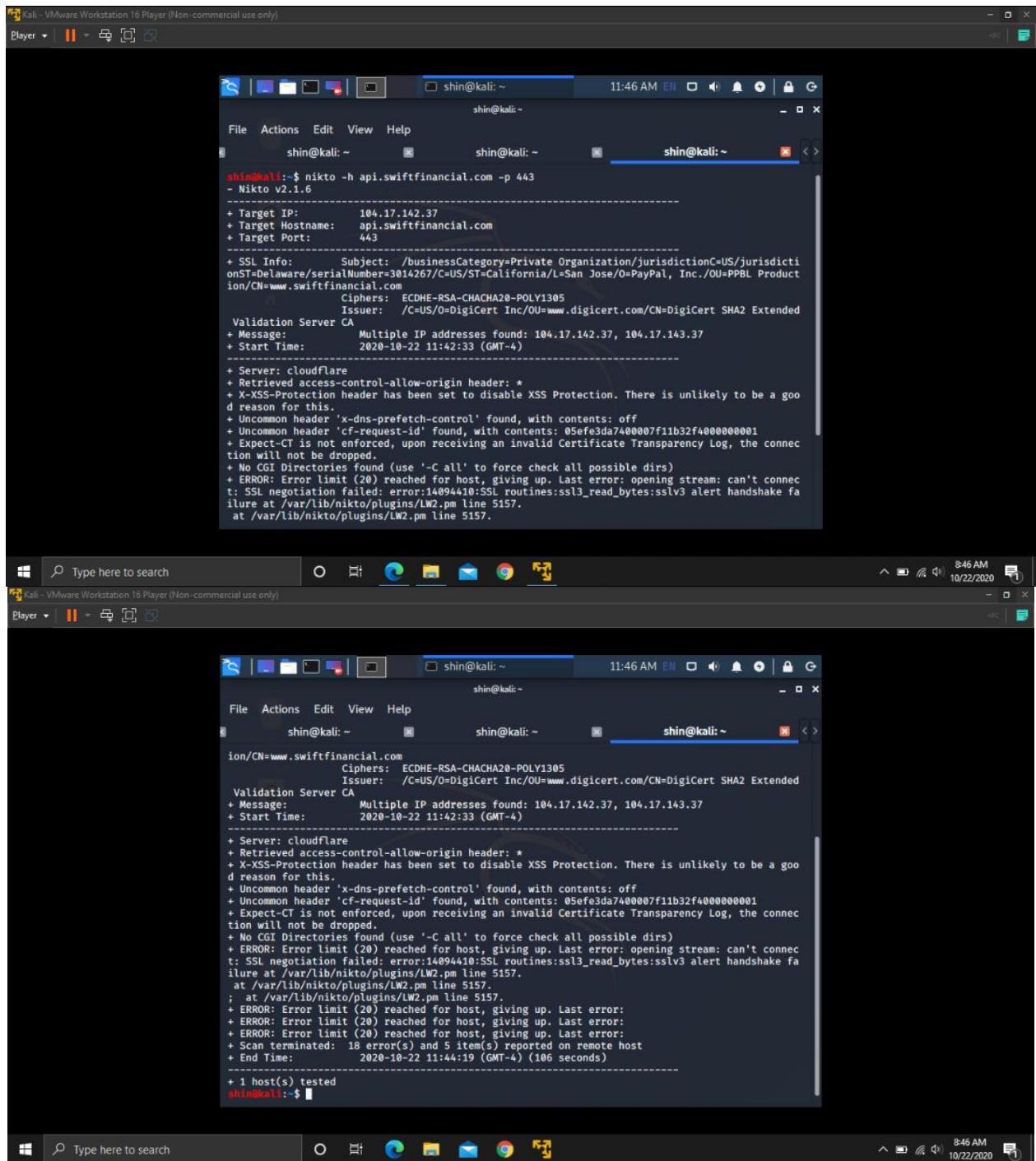
```

shin@kali: ~          shin@kali: ~          shin@kali: ~
shin@kali: ~$ nikto -h api.swiftfinancial.com -p 80
- Nikto v2.1.6
-----
+ Target IP: 104.17.142.37
+ Target Hostname: api.swiftfinancial.com
+ Target Port: 80
+ Message: Multiple IP addresses found: 104.17.142.37, 104.17.143.37
+ Start Time: 2020-10-20 15:39:07 (GMT-4)
-----
+ Server: cloudFlare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-f-request-id' found, with contents: a5eb05fa5200007f23189df0000000001
+ 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 MIM type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2020-10-20 15:41:59 (GMT-4) (172 seconds)

+ 1 host(s) tested
shin@kali: ~

```

## api.swiftfinancial.com (port 443)



```

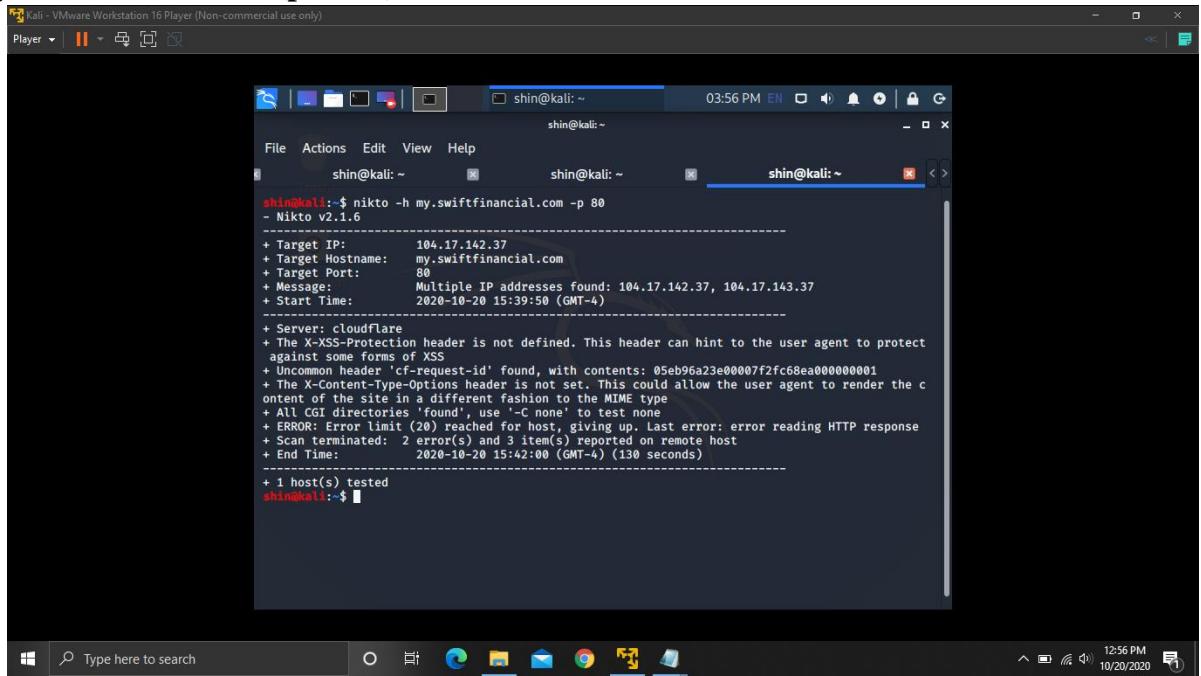
shin@kali:~$ nikto -h api.swiftfinancial.com -p 443
- Nikto v2.1.6

+ Target IP:      104.17.142.37
+ Target Hostname: api.swiftfinancial.com
+ Target Port:    443
-----
+ SSL Info:       Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product
+ Ciphers:        ECDHE-RSA-CHACHA20-POLY1305
+ Issuer:         /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended
Validation Server CA
+ Message:        Multiple IP addresses found: 104.17.142.37, 104.17.143.37
+ Start Time:     2020-10-22 11:42:33 (GMT-4)
-----
+ Server:         cloudflare
+ Retrieved access-control-allow-origin header: *
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'x-dns-prefetch-control' found, with contents: off
+ Uncommon header 'cf-request-id' found, with contents: 05fe3da7400007f11b32f40000000001
+ Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect to SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
at /var/lib/nikto/plugins/LW2.pm line 5157.

shin@kali:~$ 

```

## my.swiftfinancial.com (port 80)

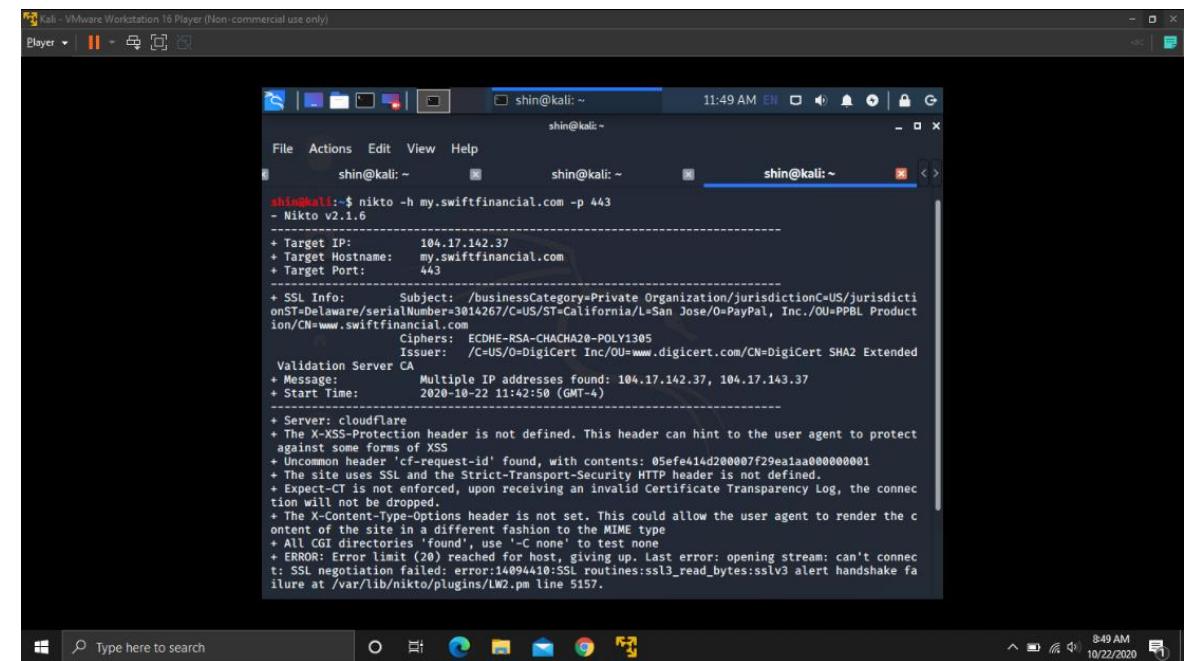


```

shin@kali:~$ nikto -h my.swiftfinancial.com -p 80
- Nikto v2.1.6
-----
+ Target IP:      104.17.142.37
+ Target Hostname: my.swiftfinancial.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 104.17.142.37, 104.17.143.37
+ Start Time:    2020-10-20 15:39:50 (GMT-4)
-----
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05eb96a23e00007f2fc68ea0000000001
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 2 error(s) and 3 item(s) reported on remote host
+ End Time:      2020-10-20 15:42:00 (GMT-4) (130 seconds)
-----
+ 1 host(s) tested
shin@kali:~$ 

```

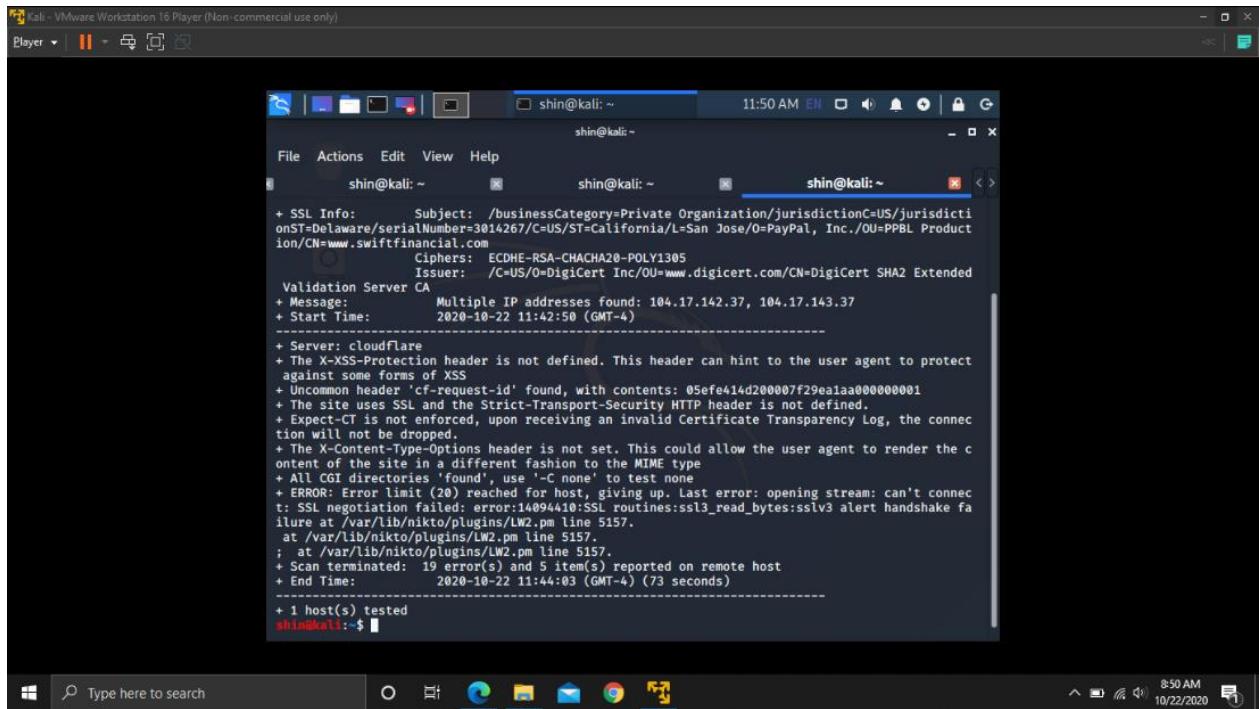
## my.swiftfinancial.com (port 443)



```

shin@kali:~$ nikto -h my.swiftfinancial.com -p 443
- Nikto v2.1.6
-----
+ Target IP:      104.17.142.37
+ Target Hostname: my.swiftfinancial.com
+ Target Port:    443
-----
+ SSL Info:       Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdicti
onST=Delaware/serialNumber=3014267/...=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product
ion/CN=www.swiftfinancial.com
          Ciphers:  ECDHE-RSA-CHACHA20-POLY1305
          Issuer:   /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended
          Validation Server CA
+ Message:        Multiple IP addresses found: 104.17.142.37, 104.17.143.37
+ Start Time:    2020-10-22 11:42:50 (GMT-4)
-----
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05efc414d200007f29eaa0000000001
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connec
tion will not be dropped
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connec
t: SSL negotiation failed: error:14094420:SSL routines:ssl3_read_bytes:sslv3 alert handshake fa
ilure at /var/lib/nikto/plugins/LM2.pm line 5157.

```



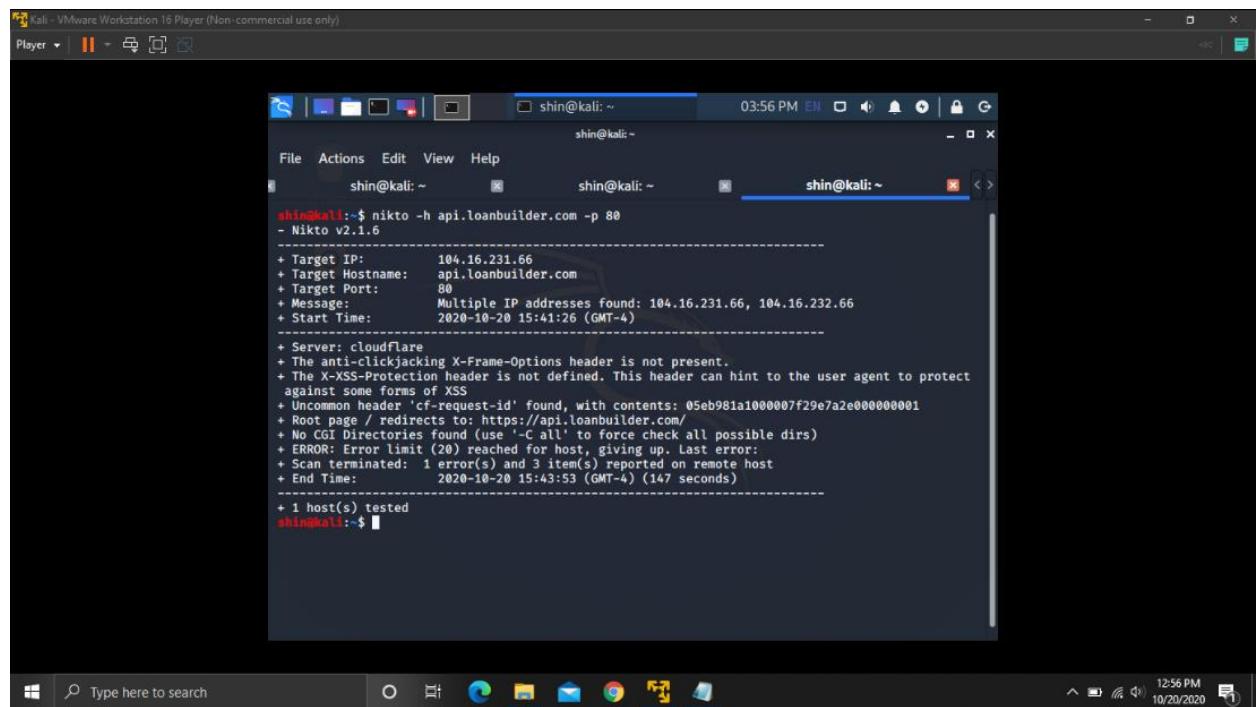
```

shin@kali:~$ nikto -h www.swiftfinancial.com
[+] SSL Info: Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product/CN=www.swiftfinancial.com
[+] Ciphers: ECDHE-RSA-CHACHA20-POLY1305
[+] Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA
[+] Message: Multiple IP addresses found: 104.17.142.37, 104.17.143.37
[+] Start Time: 2020-10-22 11:42:50 (GMT-4)
[+] Server: cloudflare
[+] The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
[+] Uncommon header 'cf-request-id' found, with contents: 05e6e41d20000f29ea1aa000000001
[+] The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
[+] Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped.
[+] 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
[+] All CGI directories 'found', use '-C none' to test none
[+] ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect to SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
[+] Scan terminated: 19 error(s) and 5 item(s) reported on remote host
[+] End Time: 2020-10-22 11:44:03 (GMT-4) (73 seconds)

+ 1 host(s) tested
shin@kali:~$ 

```

## api.loanbuilder.com (port 80)



```

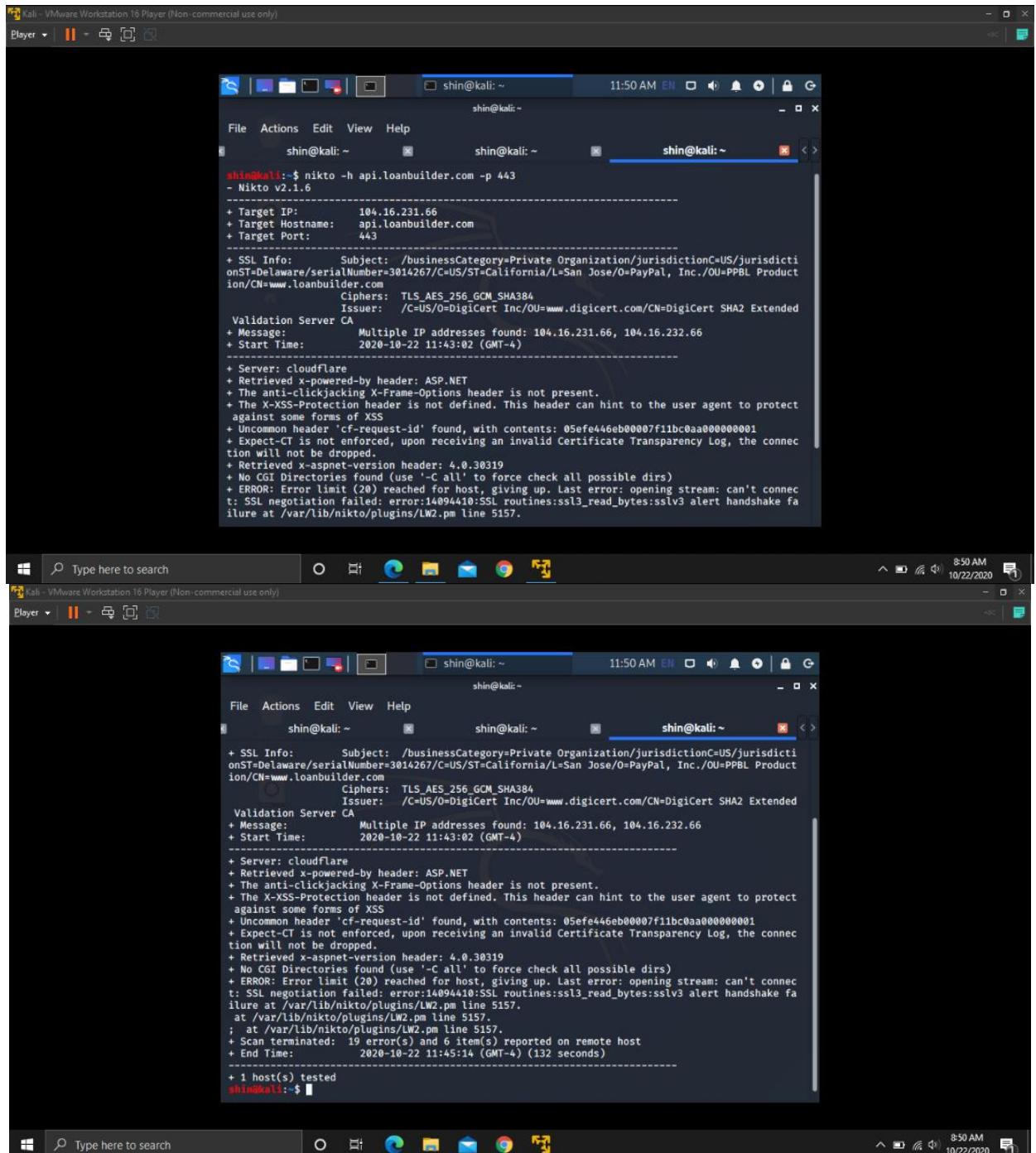
shin@kali:~$ nikto -h api.loanbuilder.com -p 80
[+] Nikto v2.1.6
[+] Target IP: 104.16.231.66
[+] Target Hostname: api.loanbuilder.com
[+] Target Port: 80
[+] Message: Multiple IP addresses found: 104.16.231.66, 104.16.232.66
[+] Start Time: 2020-10-20 15:41:26 (GMT-4)

[+] Server: cloudflare
[+] The anti-clickjacking X-Frame-Options header is not present.
[+] The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
[+] Uncommon header 'cf-request-id' found, with contents: 05eb981a100000f29e7a2e000000001
[+] Root page / redirects to: https://api.loanbuilder.com/
[+] No CGI Directories found (use '-C all' to force check all possible dirs)
[+] ERROR: Error limit (20) reached for host, giving up. Last error:
[+] Scan terminated: 1 error(s) and 3 item(s) reported on remote host
[+] End Time: 2020-10-20 15:43:53 (GMT-4) (147 seconds)

+ 1 host(s) tested
shin@kali:~$ 

```

## api.loanbuilder.com (port 443)



```

shin@kali:~$ nikto -h api.loanbuilder.com -p 443
- Nikto v2.1.6
-----
+ Target IP:      104.16.231.66
+ Target Hostname: api.loanbuilder.com
+ Target Port:    443
+ SSL Info:       Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product/CN=www.loanbuilder.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA
+ Message:        Multiple IP addresses found: 104.16.231.66, 104.16.232.66
+ Start Time:     2020-10-22 11:43:02 (GMT-4)
-----
+ Server: cloudflare
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05efe446eb00007f11bc0aa0000000001
+ Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped.
+ Retrieved x-aspart-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
-----
+ Server: cloudflare
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05efe446eb00007f11bc0aa0000000001
+ Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped.
+ Retrieved x-aspart-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 19 error(s) and 6 item(s) reported on remote host
+ End Time:       2020-10-22 11:45:14 (GMT-4) (132 seconds)
-----
+ 1 host(s) tested
shin@kali:~$ 

```

## my.loanbuilder.com (port 80)

```

shin@kali:~$ nikto -h my.loanbuilder.com -p 80
- Nikto v2.1.6
-----
+ Target IP:      104.16.231.66
+ Target Hostname: my.loanbuilder.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 104.16.231.66, 104.16.232.66
+ Start Time:     2020-10-20 15:41:58 (GMT-4)
-----
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05eb98973c00007f35372b40000000001
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 2 item(s) reported on remote host
+ End Time:       2020-10-20 15:45:36 (GMT-4) (218 seconds)

+ 1 host(s) tested
shin@kali:~$ 

```

## my.loanbuilder.com (port 443)

```

shin@kali:~$ nikto -h my.loanbuilder.com -p 443
- Nikto v2.1.6
-----
+ Target IP:      104.16.231.66
+ Target Hostname: my.loanbuilder.com
+ Target Port:    443
-----
+ SSL Info:       Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PPBL Product
ion/CN=www.loanbuilder.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended
Validation Server CA
+ Message:        Multiple IP addresses found: 104.16.231.66, 104.16.232.66
+ Start Time:     2020-10-22 11:43:14 (GMT-4)
-----
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05efe4713c00007f35412d9000000001
+ Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connec
tion will not be dropped.
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connec
t: SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake fa
ilure at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host

```

```

shin@kali: ~ shin@kali: ~ shin@kali: ~
+ Target Hostname: my.loanbuilder.com
+ Target Port: 443
-----
+ SSL Info: Subject: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=Delaware/serialNumber=3014267/C=US/ST=California/L=San Jose/O=PayPal, Inc./OU=PBL Product/CN=www.loanbuilder.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA
+ Message: Multiple IP addresses found: 104.16.231.66, 104.16.232.66
+ Start Time: 2020-10-22 11:43:14 (GMT-4)
-----
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05efe4713c0000f35412d90000000001
+ Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped.
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect to SSL negotiation failed: error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2020-10-22 11:44:24 (GMT-4) (70 seconds)
-----
+ 1 host(s) tested
shin@kali: ~

```

#### **1. The anti-clickjacking X-Frame-Options header is not present:**

Clickjacking, also known as a “UI redress attack”, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is “hijacking” clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both

Severity: Low  
CWE-693

#### **2. The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS:**

It means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Severity: Low

CWE: 693

#### **3. 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:**

This means that this website could be at risk of a MIME-sniffing attacks

Severity: Low

CWE-16

#### **4. Missing 'Expect-CT' Header:**

Severity: Low

CWE: 693

**5. Missing 'X-XSS-Protection' Header:**

Severity: Low

CWE: 693

## References:

- Tenable®. 2020. *Tenable® - The Cyber Exposure Company*. [online] Available at: <<https://www.tenable.com/>> [Accessed 23 October 2020].
- Owasp.org. 2020. *OWASP Foundation / Open Source Foundation For Application Security*. [online] Available at: <<https://owasp.org/>> [Accessed 23 October 2020].
- Netsparker.com. 2020. *Web Vulnerability & Security Checks / Netsparker*. [online] Available at: <<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/>> [Accessed 23 October 2020].
- Academy, W. and scripting, C., 2020. *What Is Cross-Site Scripting (XSS) And How To Prevent It? / Web Security Academy*. [online] Portswigger.net. Available at: <<https://portswigger.net/web-security/cross-site-scripting>> [Accessed 23 October 2020].
2020. [online] Available at: <<https://www.acunetix.com/websitetecurity/cross-site-scripting/>> [Accessed 23 October 2020].
- Netsparker.com. 2020. *Missing X-Frame-Options Header / Netsparker*. [online] Available at: <<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-x-frame-options-header/>> [Accessed 23 October 2020].

### **Final Video Link:**

<https://drive.google.com/file/d/1L3KT7PY8zWwJ8KkrWQy4h1ZjuiR1ty1J/view?usp=sharing>