BSc (Hons) in Information Technology Specializing in Cyber Security
2nd Year, 2nd Semester.

Web Security - IE2062
2023/FEB
Individual Assignment

Web Security BB Assignment Description

https://www.amexglobalbusinesstravel.com

Student Registration Number	Student Name
IT21195402	Gunathilaka D.J.V.

Table of Contents

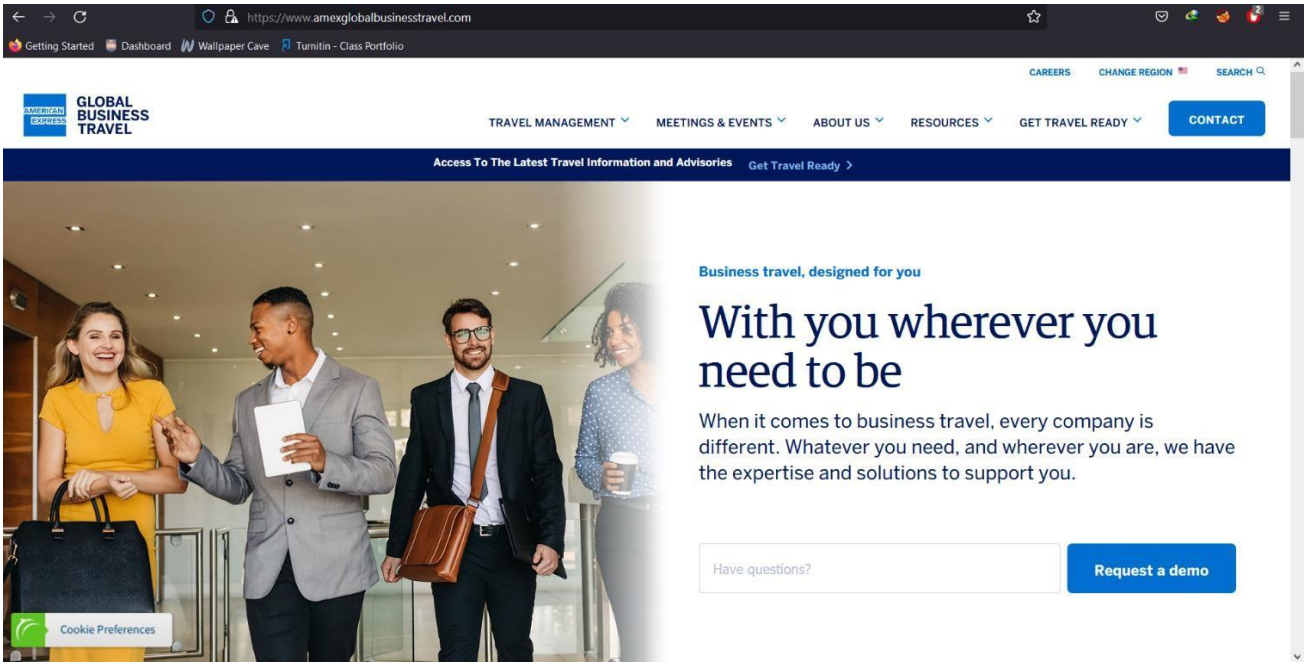
ACKNOWLEDGMENT

In Web Security module we learnt many theories. Using this assignment, I am trying to apply the theories what I learnt in the module as much as I can into practice.

I am especially grateful to Dr. Lakmal Rupasinghe and Ms. Chethana Liyanapathirana and assistant lecturers who did utmost to give us best.

OBJECTIVE

My objective is to do a vulnerability assessment on https://bugcrowd.com/amexgbt-vdp in Bugcrowed bug bounty platform to use my theoretical knowledge in a practical way. The main purpose of this project is to find bugs as much as I can, withing the given scope of https://bugcrowd.com/amexgbt-vdp



OWASP Top 10

What is OWASP and OWASP top 10?

Open Web Application Security Project (OWASP) is an organization which helps security researchers and developers to improve the security of websites without a profit.

OWASP top 10 is a document that we can find on OWASP website, and it gives the details of the most common and critical web security risks timely. OWASP update the OWASP top 10 time to time since 2003 according to the changes happen. [1] [2] As in the https://owasp.org/www-project-top-ten/ Top 10 in 2021 are,

1. Broken Access Control.
2. Cryptographic Failures.
3. Injection.
4. Insecure Design.
5. Security Misconfiguration.
6. Vulnerable and Outdated Components.
7. Identification and Authentication Failures.
8. Software and Data Integrity Failures.
9. Security Logging and Monitoring Failures.
10. Server-Side Request Forgery.

01) Broken Access Control

User authentication systems are verifying the identities of users. Therefore, in web application security user authentications doing very special task. If an unauthorized party detect a vulnerability in such authentication system, that gives the ability to the attacker to imitate the real user. Some of the common attacks to such authentication systems are, [3]

- Use weak credentials.
- Brute force attack to the user credentials.

- Weak session cookies.

02) Cryptographic Failure

Previously cryptographic failure known as Sensitive Data Exposure, and it took third place in the list. In 2021 updated top 10, Cryptographic Failure reached to second place. In cryptographic failure, both sensitive and unsensitive data of user can be visible to an unauthorized party. In such situation attackers able to update, delete or steal user data according to their preferences. [4]

03) Injection

According to 2021 updated top 10, injection reached down from place one to place two in the list. Nearly 94% of web applications are testing for different injection forms. When user input data are not validating or filter by the web application, that is a vulnerability. Some most common types of injection are, OS command, SQL, NoSQL, Expression Language, Object Relational Mapping, Object Graph Navigation Library injection. [5]

04) Insecure Design

Insecure Design is newly added category to the OWASP Top 10 which mainly focus on the risks towards architectural and design flaw. Insecure implementation and insecure design are not the same. The difference is root causes of those two and remediation are non-identical to each other. Secure design may consist of implementational defects which leads to exploitable vulnerabilities. [6]

05) Secure Misconfiguration

In previous OWASP Top 10 list, Secure Misconfiguration took sixth position. However, in 2021 latest OWASP Top 10 list Secure Misconfiguration reached to fifth position. XML External Entity category which was there in the previous OWASP Top 10 list, at present part of the Secure Misconfiguration category. Approximately 90% of web applications tested for different kind of misconfigurations and marked 4% rate of average incidents. Secure Misconfiguring occur when,

- Default accounts which do not change the passwords and username.
- Install or enable needless features (useless services, ports, accounts etc.).
- Vulnerable or outdated software.
- Unconfigured secure features in updated systems.
- Servers which have not properly implemented headers, directives, or their values.

Applications with repeatable security features always carry a higher risk. [7]

06) Vulnerable and Outdated Components

Vulnerable and Outdated Components category previously took ninth position among OWASP Top 10 list and now reached to sixth position in the list. When building of an application, if the using components are outdated and they are vulnerable (it can be Operating System, libraries, applications etc.), then there is a high possibility of finding exploitable vulnerabilities in the application which impact on both the users and the creator. At the same time security should be maintain in the components and regular scan to detect vulnerabilities of the components which use to build the application should done to avoid vulnerabilities. [8] [9]

07) Identification and Authentication

Identification and Authentication previously known as Broken Authentication, and it reached down to seventh position of the list from the second position. Attacks related to authentication should be mitigate as much as possible to keep users' privacy. Verifying the user identity is done under authentication, session management are implementing to mitigate such risks to the identification and authentication. If the web application grants the ability to brute forcing or related other automated attacks that is a weakness in the authentication. Some of the other weaknesses are [10],

- Session identifier shown in URL.
- Use common passwords and guessable passwords.
- Use unencrypted, plain text or weak hash passwords.
- Futile multi-factor authentication.
- Use session identifier recursively.

08) Software and Data Integrity Failures

Software and Data Integrity Failures is a new category in 2021 OWASP Top 10. Infrastructure and code which does not secure in case of integrity violation related to data integrity failures and software. As for an example application depend on libraries, repositories, plugins etc. can be given. Moreover, now most of the applications give the auto update facility to the application without a proper integrity verification and apply the changes into the original application. Thus, attackers able to insert their codes into those updates and can have the control over the application. [11]

09) Secure Logging and Monitoring Failures

Reached nineth place from the tenth place in previous list. Failures in here directly affect to incident alerting, forensics, and visibility. Secure Logging and Monitoring Failure helps to detect and respond to escalate and active breaches respectively. Detecting breaches cannot be done without monitoring and login. Insufficient monitoring, active responses, detection, and logging can be occurred in any time. Visible of alerting events and the logging to the user is vulnerable and leads to information leakage. [12]

10) Server-Side Request Forgery

When comparing to the other categories Server-Side Request Forgery carry low incident rates averagely. Without validating a URL supply by the user when requesting remote resources Server-side request forgeries are occurring. Although use of VPN, firewall or ACL, attacker will be able to force the web application to send a request to unforeseen destination. Since latest web applications supply convenient features to the end-users, URL fetching became a common scenario. Due to architectural complexity and the cloud services, the ferocity of SSRF becomes outrageous. [13]

RISK SEVERITY RATINGS

To decide what vulnerabilities to solve first, risk score will give to the vulnerability. Mainly there are four levels of vulnerability levels and two extras. Main four levels are [14],

- Critical.
- High.
- Medium.
- Low

Additional vulnerability levels are,

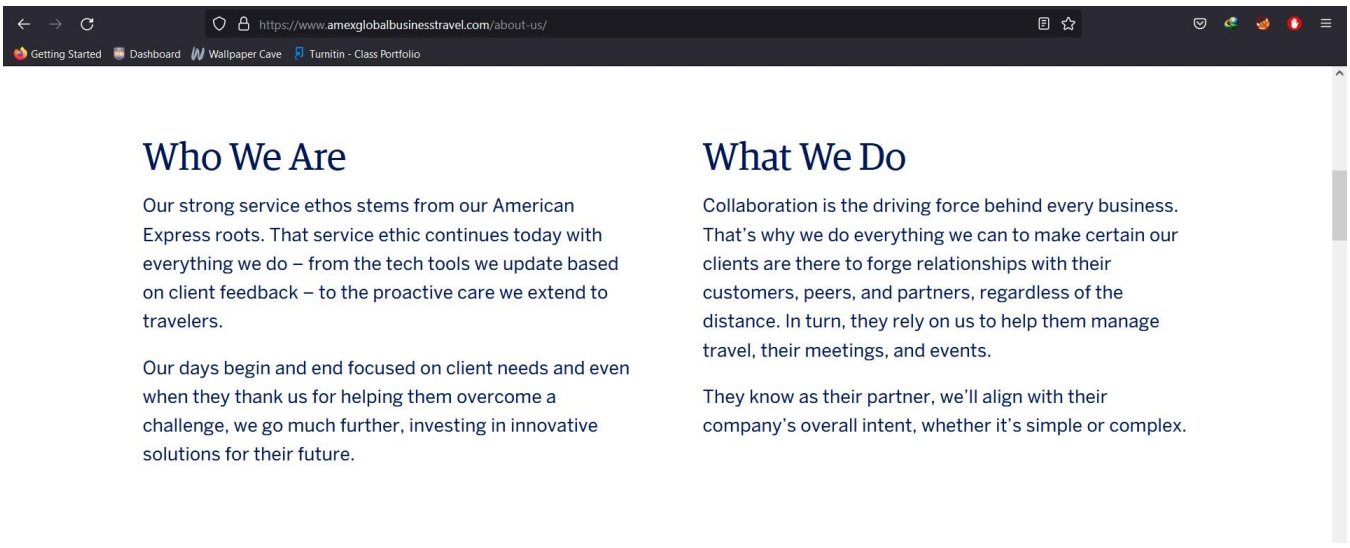
- Best Practice.
- Information Alerts.

Critical	Critical Severity let attackers to run codes on the server, web application or access important sensitive data. As for an example, SQL Injection, Command Injection and Remote Code Execution. Here attackers can deploy various kinds of attacks which affect to application's Confidentiality, Integrity and Availability at risk. In short, Critical Severity risk means, the website or the application can be hacked anytime.
High	High Severity let attackers to access data and resources of the web application. Attackers able to steal sensitive data and session information from the server or the application. The difference in high severity here is, attackers are not able to run command or a code on the server or web application.
Medium	Medium Severity emerge due to deficiencies and errors of the application configuration. Attackers can access to the sensitive information by exploiting. Issues at this risk level does not have a direct impact on the system or application, however the issues should be fixed.

Low	Low Severity comprise of information leakage, lack of security measures and error configuration. Low Severity sometimes consist of higher severity level issues.

ABOUT THE TARGET

American Express Global Business Travel (AMEX – GBT) is a leading multinational company and a business partner to manage travel (https://www.amexglobalbusinesstravel.com). They help companies and employees by assuring travelers present whenever the clients want. AMEX GBT provides their service over 140 countries. Most of the companies around the world depend on AMEX GBT when it comes to organizing events and meetings, travel management, and business travel consulting. Although the name is AMEX GBT, it is not fully owned by American Express Company. AMEX word and the AMEX logo is using under bounded license. Since the popularity and the usability of the AMEX GBT has increased, they initiate a bug bounty program using Bugcrowed platform (https://bugcrowd.com/amexgbt-vdp) to find more vulnerabilities to find solutions for them.



ASSESSMENT SCOPE

According to Bugcrowed platform they have clearly mention the In Scope targets and Out of Scopes as follows.

In Scope targets

- *.amexglobalbusinesstravel.com
- *.amexgbt.com
- *.banks-sadler.com
- www.bienquiries.co.uk
- https://www.ebrdevents.co.uk/
- *.gbtad.com
- *.gbtexternal.com
- *GBTNTA.com
- *.gbtspain.com
- *.hrgnorthamerica.com
- *.hrgworldwide.com
- *.meetingsexpreess.com
- *.meetingsexpress.com
- *.meetingssource.com
- www.mytravelsolution.com
- *.mykds.com
- https://pat.itq.in/
- *.uathrg-isuite.com
- *.uathrgisuite.com
- www.winnerscircleregistration.com
- 203.125.28.128/28

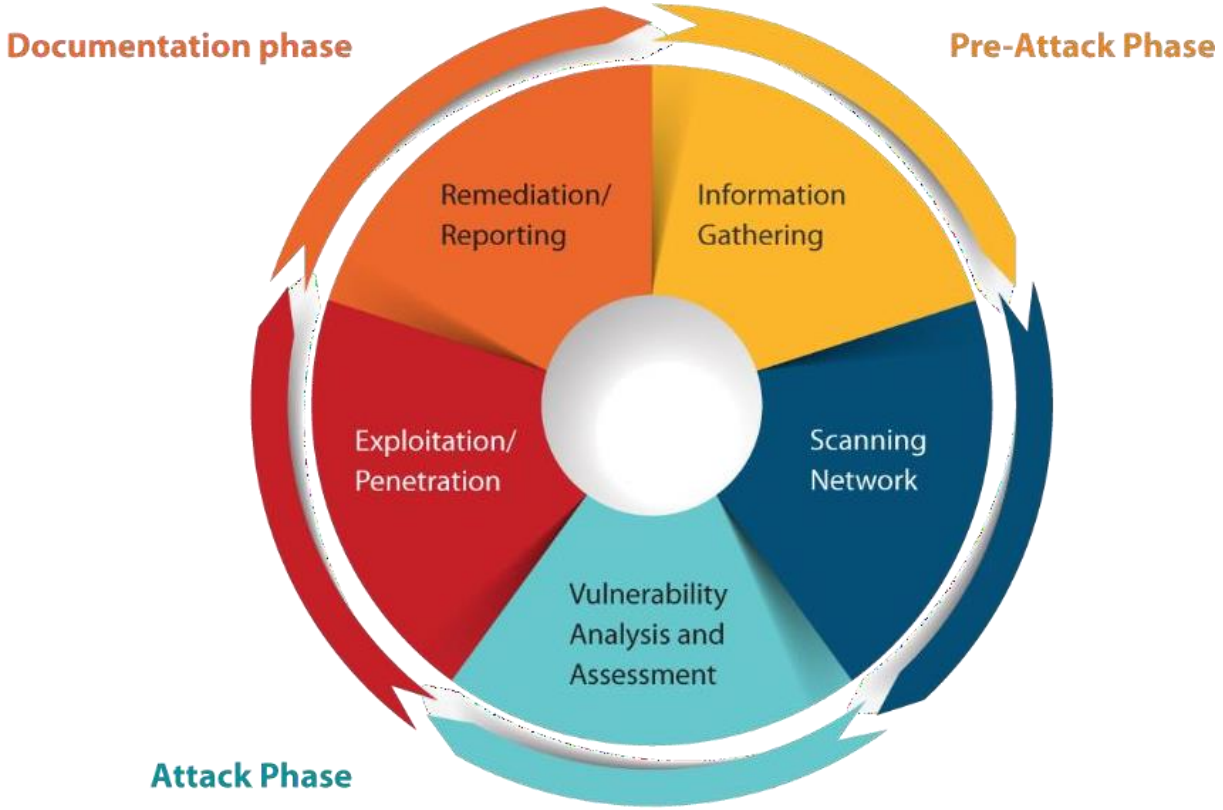
- *.kds.com
- *.ovationtravel.com
- *.lawyerstravel.com
- *.miclientool.com/
- *.supplierstool.com
- *.mieventool.com
- *.miwebtool.com
- *.sourcingcenteramexgbt.com
- gbt-invoicing.com

Out of Scope Targets

- https://register.banks-sadler.com
- DDoS is out of scope.

Vulnerability Assessment Methodology

When conducting a proper vulnerability assessment, it has a set of stages to follow. By following those steps accordingly into the proper order, will give the maximum output at the end of a vulnerability assessment. This vulnerability assessment follows the proper steps of Vulnerability Assessment and Penetration Testing which consist of five phases. Since this is a vulnerability assessment, exploitation/penetration testing phase will not be conduct.



First, we should select a legal target to do the vulnerability assessment. Bugcrowd, HackerOne, Cobalt, and Synack are some bounty platforms that offer pen testers and other related people legal targets to do vulnerability assessments and penetration testing. Since I have already selected a legal target (https://bugcrowd.com/amexgbt-vdp) from Bugcrowed platform, from this moment onwards I am proceeding to Information Gathering phase.

INFORMATION GATHERING

In short, in Information Gathering phase we collect as much as relevant details about our targeted system, or the application. This is the beginning or the starting phase of the vulnerability assessment or the penetration testing, and this phase carries massive weight since information gathering is very important to have a proper idea about how the application or the system works. Without having a right comprehension about the target, possibility of accomplishing the aim become less. If the tester has more details about the target, success rate is high. That is the common theory for all pen testers and hackers. Various tools, websites, techniques, and public sources are there to gather information. Mainly there are three significant categories in Information Gathering [15],

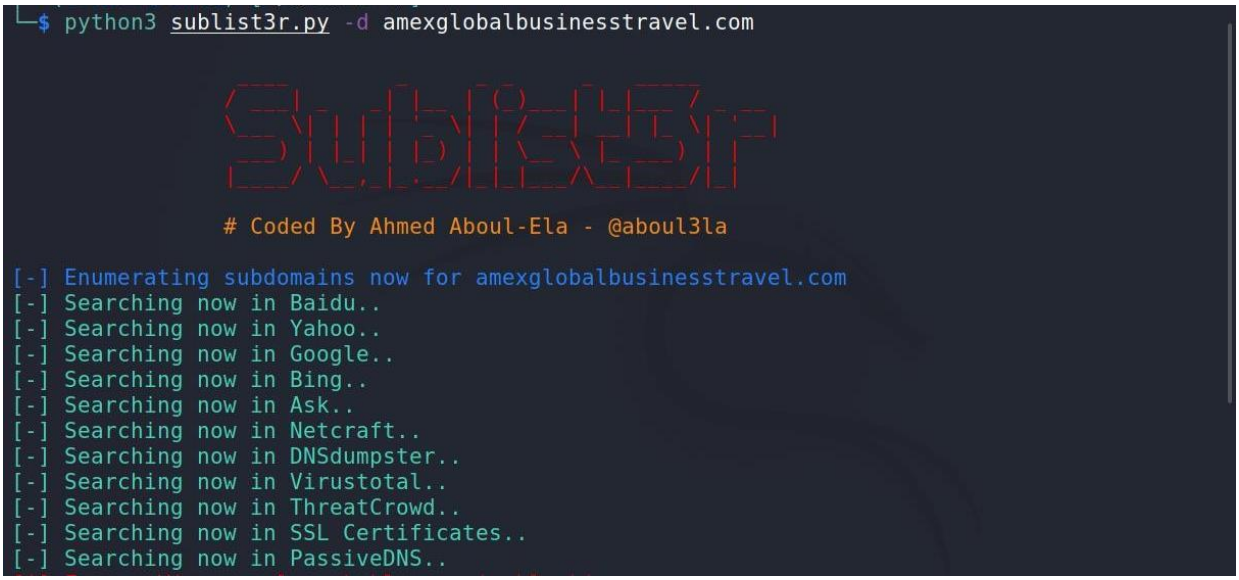
1. Foot printing	Is a way to collect information as much as possible regarding the target. It can be active or passive.
2. Scanning	A technique which uses to detect ports, hosts, and different services inside the network of the target. Hackers, pen testers and other related
3. Enumeration	Active connection creates to the application or the system and execute directed queries to obtain information over the target [16].

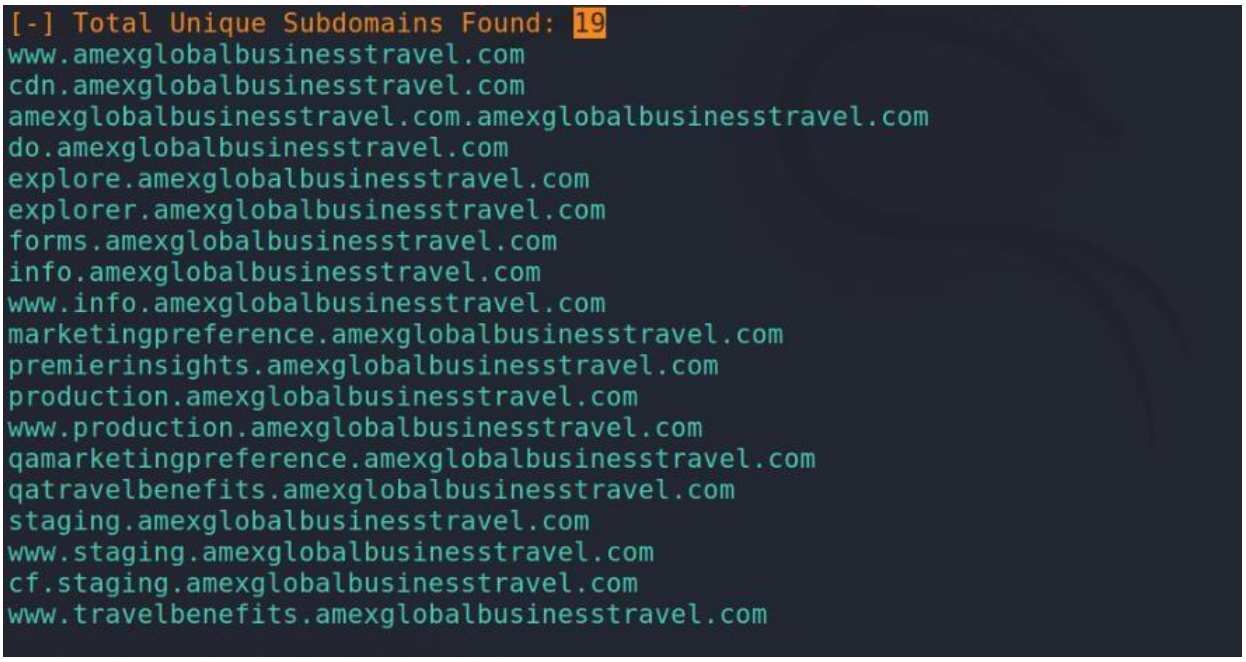
Subdomain Hunting

Subdomains are sub parts under the key domain. Content of subdomains can be both independent and dependent on key domain. Subdomains are possible to have vulnerabilities. Therefor, hunting subdomain is a beneficial in testers perspective. Since discovering subdomains under key domain has a major impact, there are many subdomains hunting tools. Sublist3r, crt.ch, Google Fu and many more.

Sublist3r to Hunt Subdomains

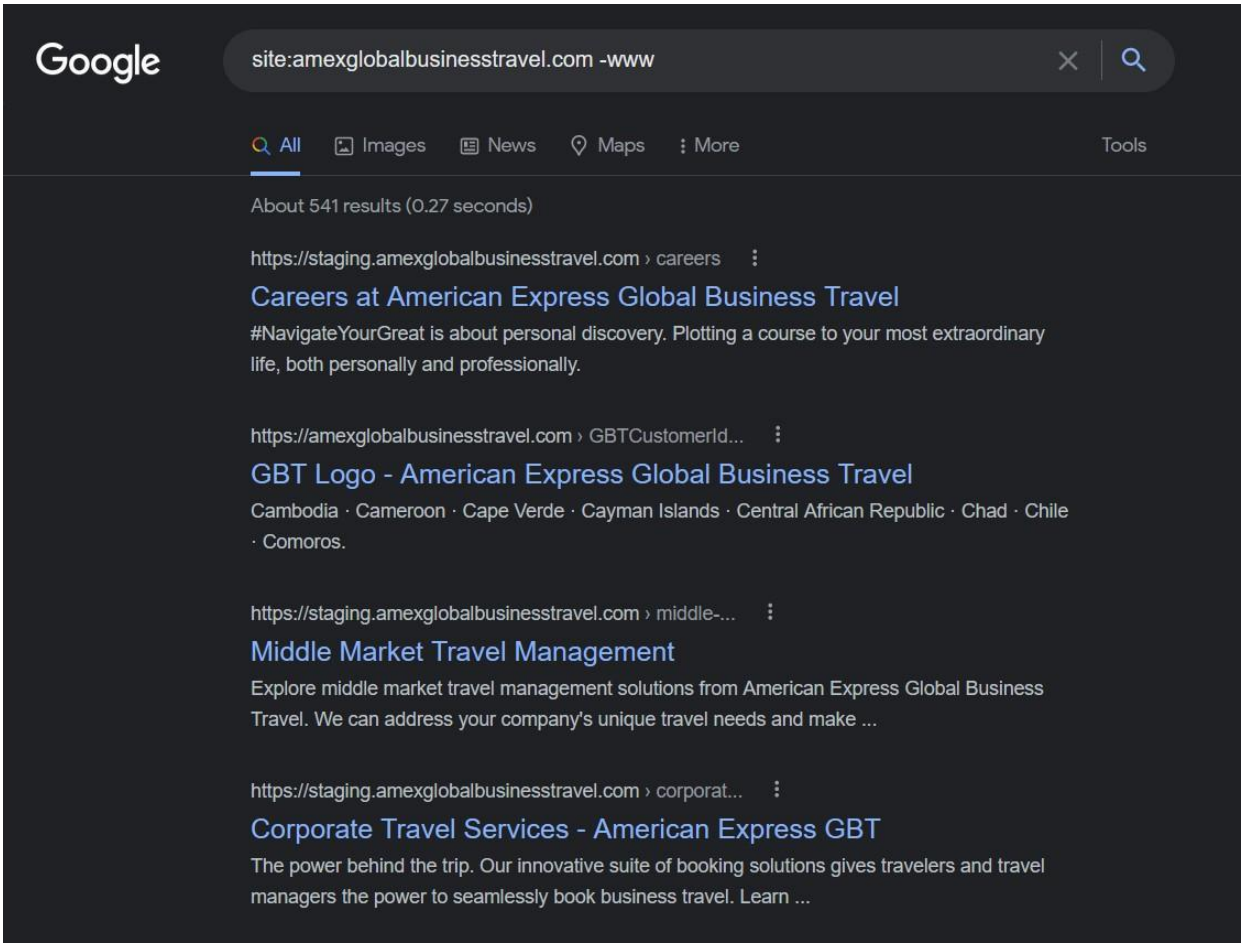
Sublist3r is a tool which can be used to hunt subdomains. This tool is not a pre-installed one. Therefore, we have to get the git clone as a begin. Then after downloading and installing it we can type the command “python3 subist3r.py -d (whatever the link of your target)”. In my case, “python3 sublist3r.py -d amexglobalbusinesstravel.com”.




[-] Total Unique Subdomains Found: 19
www.amexglobalbusinesstravel.com
cdn.amexglobalbusinesstravel.com
amexglobalbusinesstravel.com.amexglobalbusinesstravel.com
do.amexglobalbusinesstravel.com
explore.amexglobalbusinesstravel.com
explorer.amexglobalbusinesstravel.com
forms.amexglobalbusinesstravel.com
info.amexglobalbusinesstravel.com
www.info.amexglobalbusinesstravel.com
marketingpreference.amexglobalbusinesstravel.com
premierinsights.amexglobalbusinesstravel.com
production.amexglobalbusinesstravel.com
www.production.amexglobalbusinesstravel.com
qamarketingpreference.amexglobalbusinesstravel.com
qatravelbenefits.amexglobalbusinesstravel.com
staging.amexglobalbusinesstravel.com
www.staging.amexglobalbusinesstravel.com
cf.staging.amexglobalbusinesstravel.com
www.travelbenefits.amexglobalbusinesstravel.com

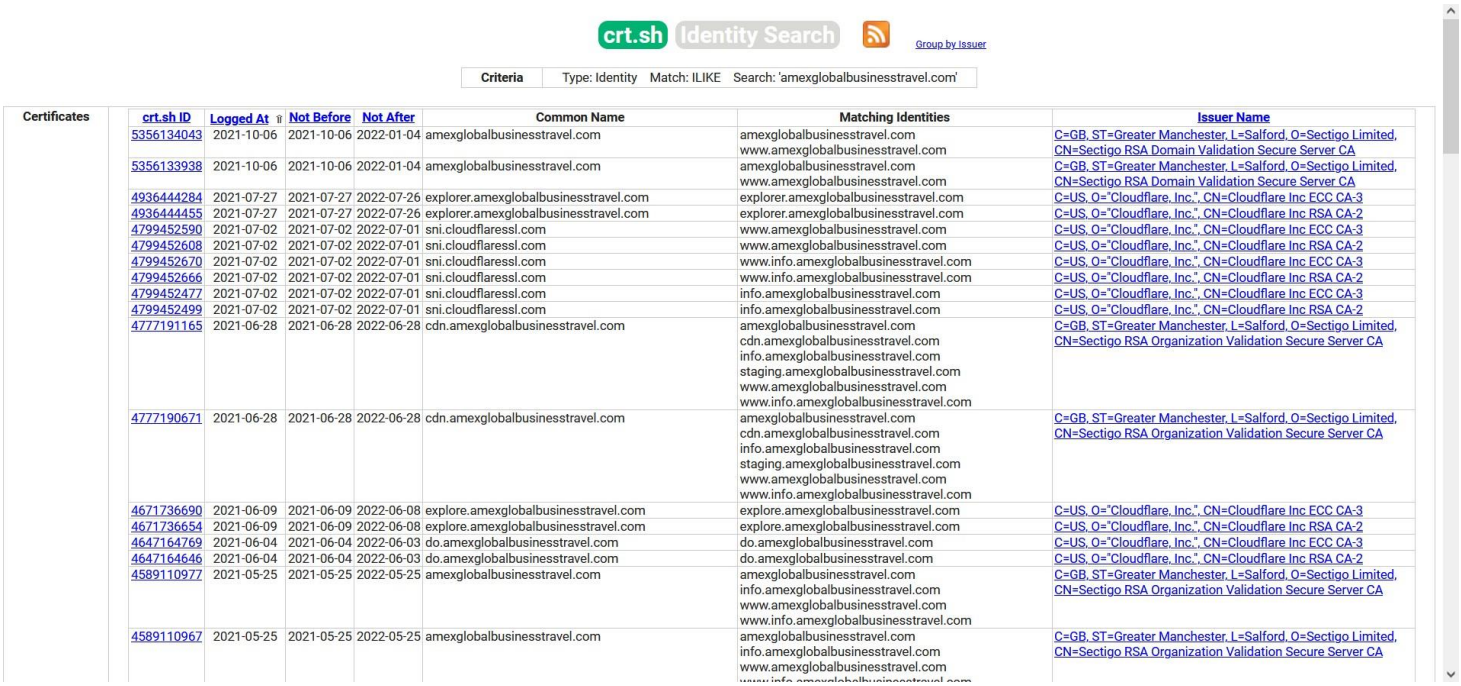
Google-Fu to hunt subdomains.

If we properly use Google-Fu we will be able to find everything regarding to domain, we give. As for an example, I want to find the websites which belongs to amexglobalbusinesstravel.com. In that case we have to type in google search box “site:amexglobalbusinesstravel.com -www”.



crt.sh to hunt subdomains.

crt.sh is another free online tool which we can use to find subdomains belong to key domain. When using the crt.sh, we can find more subdomains, even fourth level ones using wildcards. We only need to give the wildcard and the domain name to the search box like "%.amexglobalbusinesstravel.com".



crt.sh Identity Search Group by Issuer

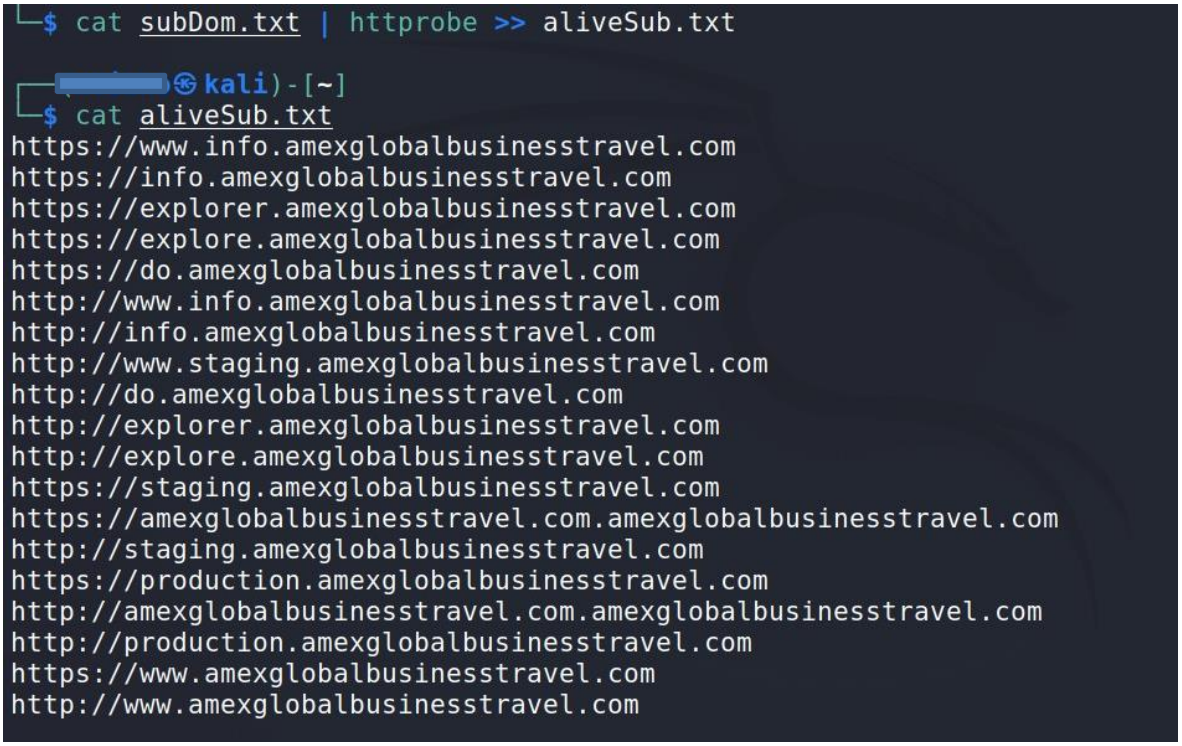
Criteria | Type: Identity | Match: ILIKE | Search: 'amexglobalbusinesstravel.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
5356134043	2021-10-06	2021-10-06	2022-01-04	amexglobalbusinesstravel.com	amexglobalbusinesstravel.com www.amexglobalbusinesstravel.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
5356133938	2021-10-06	2021-10-06	2022-01-04	amexglobalbusinesstravel.com	amexglobalbusinesstravel.com www.amexglobalbusinesstravel.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
4936444284	2021-07-27	2021-07-27	2022-07-26	explorer.amexglobalbusinesstravel.com	explorer.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
4936444455	2021-07-27	2021-07-27	2022-07-26	explorer.amexglobalbusinesstravel.com	explorer.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
4799452590	2021-07-02	2021-07-02	2022-07-01	sni.cloudflaressl.com	www.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
4799452608	2021-07-02	2021-07-02	2022-07-01	sni.cloudflaressl.com	www.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
4799452670	2021-07-02	2021-07-02	2022-07-01	sni.cloudflaressl.com	www.info.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
4799452666	2021-07-02	2021-07-02	2022-07-01	sni.cloudflaressl.com	www.info.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
4799452477	2021-07-02	2021-07-02	2022-07-01	sni.cloudflaressl.com	info.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
4799452499	2021-07-02	2021-07-02	2022-07-01	sni.cloudflaressl.com	info.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
4777191165	2021-06-28	2021-06-28	2022-06-28	cdn.amexglobalbusinesstravel.com	amexglobalbusinesstravel.com cdn.amexglobalbusinesstravel.com info.amexglobalbusinesstravel.com staging.amexglobalbusinesstravel.com www.amexglobalbusinesstravel.com www.info.amexglobalbusinesstravel.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
4777190671	2021-06-28	2021-06-28	2022-06-28	cdn.amexglobalbusinesstravel.com	amexglobalbusinesstravel.com cdn.amexglobalbusinesstravel.com info.amexglobalbusinesstravel.com staging.amexglobalbusinesstravel.com www.amexglobalbusinesstravel.com www.info.amexglobalbusinesstravel.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
4671736690	2021-06-09	2021-06-09	2022-06-08	explore.amexglobalbusinesstravel.com	explore.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
4671736654	2021-06-09	2021-06-09	2022-06-08	explore.amexglobalbusinesstravel.com	explore.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
4647164769	2021-06-04	2021-06-04	2022-06-03	do.amexglobalbusinesstravel.com	do.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
4647164646	2021-06-04	2021-06-04	2022-06-03	do.amexglobalbusinesstravel.com	do.amexglobalbusinesstravel.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
4589110977	2021-05-25	2021-05-25	2022-05-25	amexglobalbusinesstravel.com	amexglobalbusinesstravel.com info.amexglobalbusinesstravel.com www.amexglobalbusinesstravel.com www.info.amexglobalbusinesstravel.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
4589110967	2021-05-25	2021-05-25	2022-05-25	amexglobalbusinesstravel.com	amexglobalbusinesstravel.com info.amexglobalbusinesstravel.com www.amexglobalbusinesstravel.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA

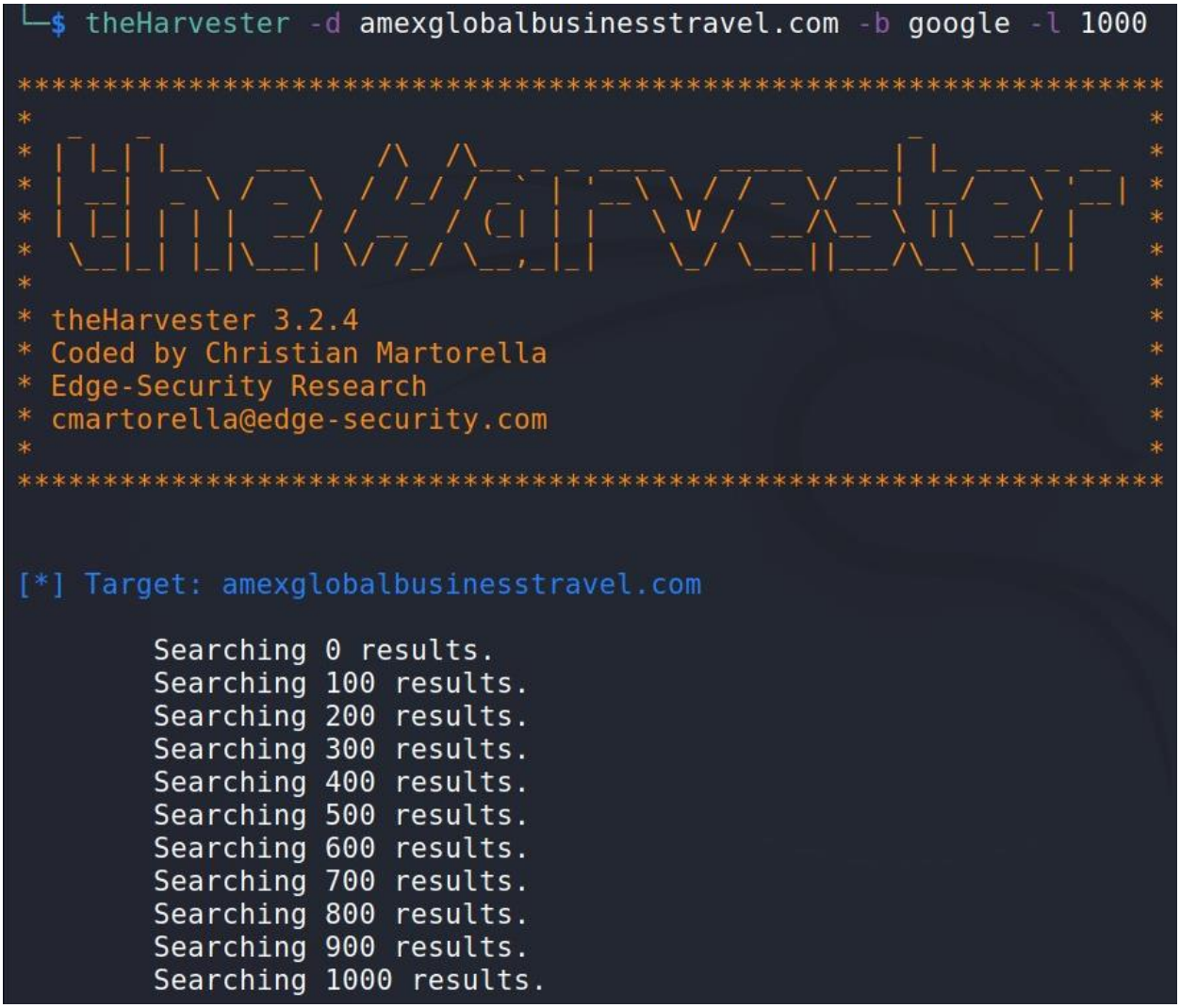
Finding Alive Subdomains

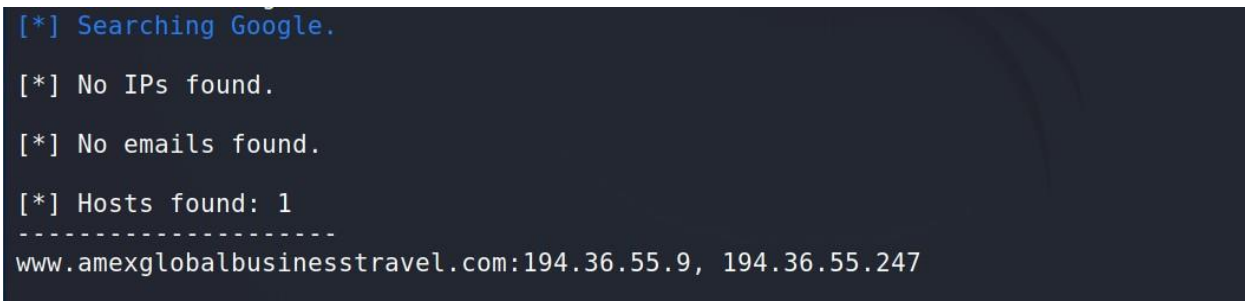
Although we found subdomains, all of them may not working. Therefore, we have to find alive subdomains. To do that I have copied the subdomains which I found previously and insert them to a text file. Then using httprobe tool we can find the alive subdomains among all subdomains we captured. First, we have to download and install the httprobe tool to use it.



E-mail harvest using theHarvester tool.

I used theHarvester tool which is already available in Kali as a pre-installed tool to search for emails and user credentials. But I was not able to find any leaked email address.



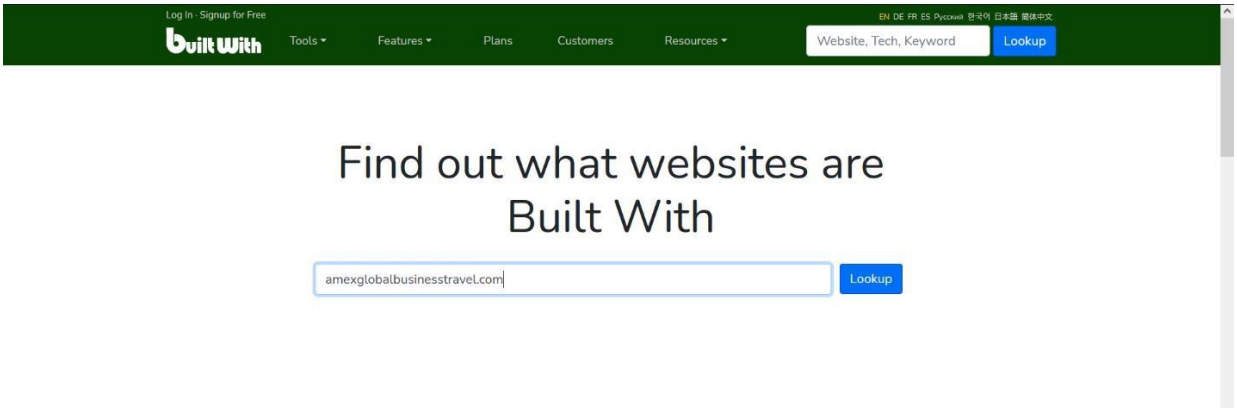


Spot Web Technologies

Underlying technologies like frameworks and content management system may contain vulnerabilities withing the used technologies. Therefore, finding underlying technologies are beneficial.

Use builtwith.com to spot website technologies.

Builtwith is a useful website which we can use to collect information regarding technologies that are used by the target. Use of builtwith is very straightforward, we want to give the target name as shown below.



Search Results of builtwith.com

Frameworks View Global Trends

Bug Bounty

Bug Bounty Usage Statistics · Download List of All Websites using Bug Bounty
The website has some form of responsible disclosure mechanism for the reporting of security vulnerabilities.

PHP

PHP Usage Statistics · Download List of All Websites using PHP
PHP is a widely used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

PHP 7

PHP 7 Usage Statistics · Download List of All Websites using PHP 7
Version 7 of the PHP framework.

JavaScript Libraries and Functions View Global Trends

RequireJS

RequireJS Usage Statistics · Download List of All Websites using RequireJS
RequireJS is a JavaScript file and module loader.

Popper.js

Popper.js Usage Statistics · Download List of All Websites using Popper.js
A library to manage your pop ups.

Flickity

Flickity Usage Statistics · Download List of All Websites using Flickity
Touch responsive flickable carousels.

Slick

Slick Usage Statistics · Download List of All Websites using Slick
Standalone CSS Selector Parser and Engine from MooTools.

Modernizr

Modernizr Usage Statistics · Download List of All Websites using Modernizr

Modernizr allows you to target specific browser functionality in your stylesheet.

Compatibility

Fancybox

Fancybox Usage Statistics · Download List of All Websites using Fancybox

FancyBox is a tool for displaying images, html content and multi-media in a Mac-style "lightbox" that floats overtop of web page.

Polyfill IO

Polyfill IO Usage Statistics · Download List of All Websites using Polyfill IO

Hosted polyfill script.

JavaScript Library

GSAP

GSAP Usage Statistics · Download List of All Websites using GSAP

GSAP is a suite of tools for scripted, high-performance HTML5 animations that work in all major browsers from GreenSock.

Animation

Content Management System

View Global Trends

WordPress

WordPress Usage Statistics · Download List of All Websites using WordPress

WordPress is a state-of-the-art semantic personal publishing platform with a focus on aesthetics, web standards, and usability.

Open Source · Blog

WordPress 5.5

WordPress 5.5 Usage Statistics · Download List of All Websites using WordPress 5.5

WordPress version 5.5.*

Network discovery using Nmap tool.

Network Mapper or the Nmap is an open-source utility which can be used to security auditing and network discovery. Raw IP packets are used by Nmap to discover the available hosts in a network, what versions and applications those hosts provide, and types of operating systems they run, and the types of firewalls and filters use and many more. Both large networks and single hosts can scan rapidly using Nmap.

```
└─$ sudo nmap -sS amexglobalbusinesstravel.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-12 10:19 EDT
Nmap scan report for amexglobalbusinesstravel.com (148.9.212.123)
Host is up (0.35s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
25/tcp   open   smtp
80/tcp   open   http
443/tcp  open   https
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 32.51 seconds
```

Vulnerability Assessment

This is the stage where we scan the target to identify vulnerabilities and prioritize them according to the risk level of the targeted websites. Vulnerability assessments are beneficial in every aspect since it gives the needful information regarding to the selected websites. There are two types of vulnerability scans,

1. Automated Scan.
2. Manual Scan.

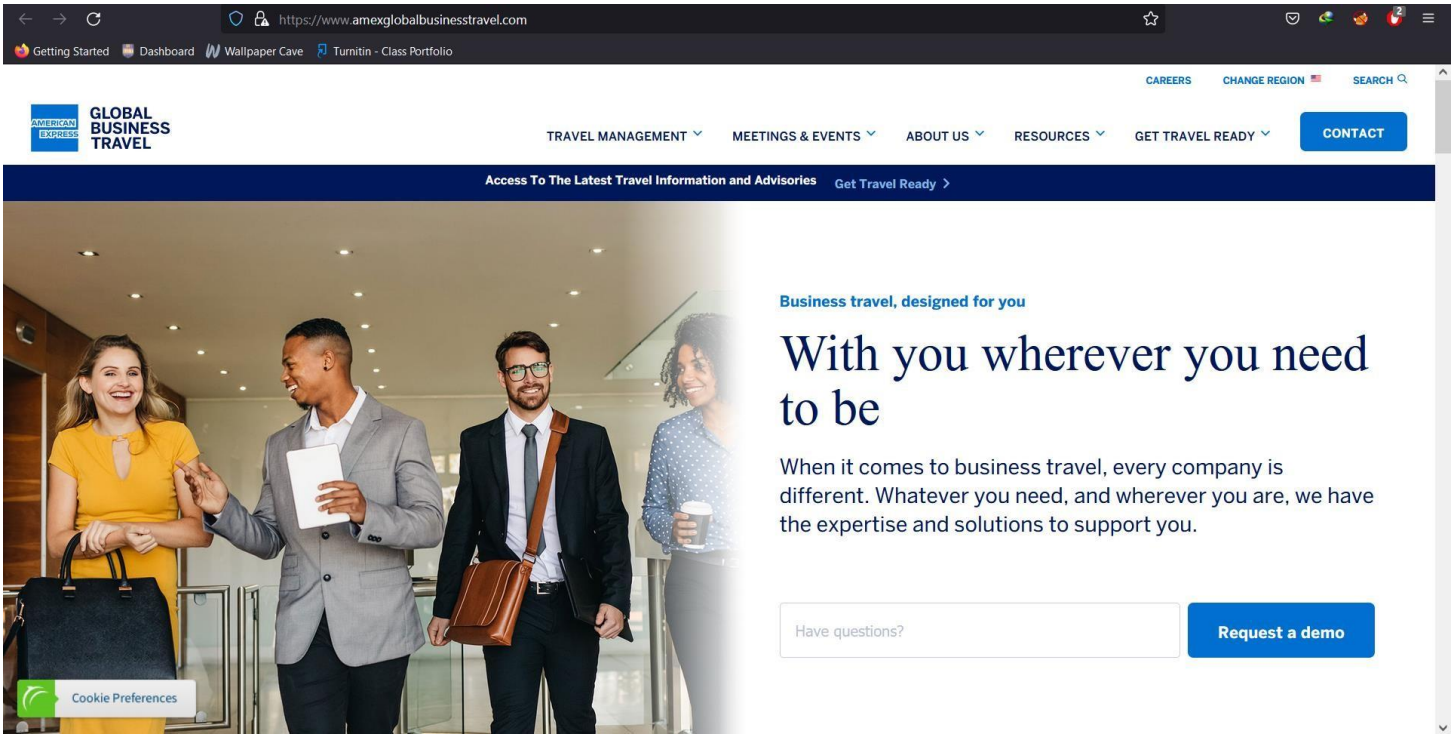
For this vulnerability assessment, I am planning to use both automated and manual scanning to find vulnerabilities of the subdomains I choose. Tools which I hope to use for the automated scanning are OWASP ZAP, Nmap, Sublist3r, Netsparker. And for the manual scan I choose few vulnerabilities of OWASP Top 10.

Target Subdomains

1. https://www.amexglobalbusinesstravel.com/
2. https://www.banks-sadler.com/
3. https://www.ovationtravel.com/home
4. https://www.lawyerstravel.com/
5. https://www.mytravelsolution.com/

Domain 1

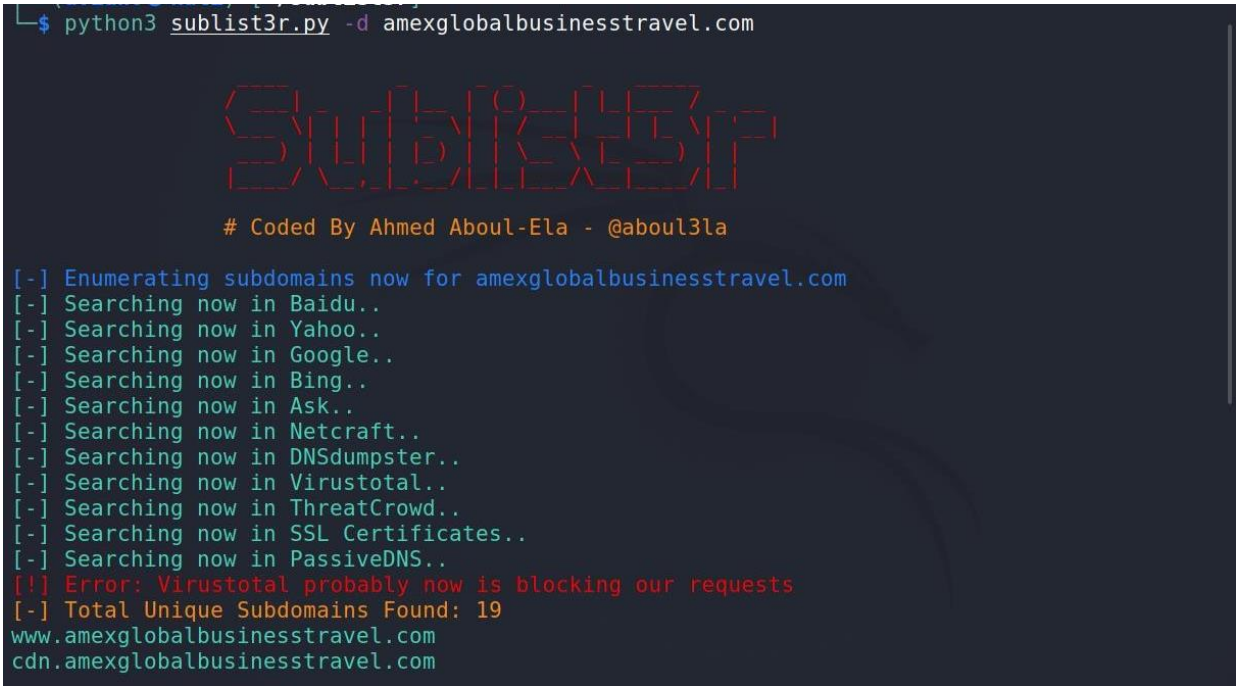
https://www.amexglobalbusinesstravel.com/

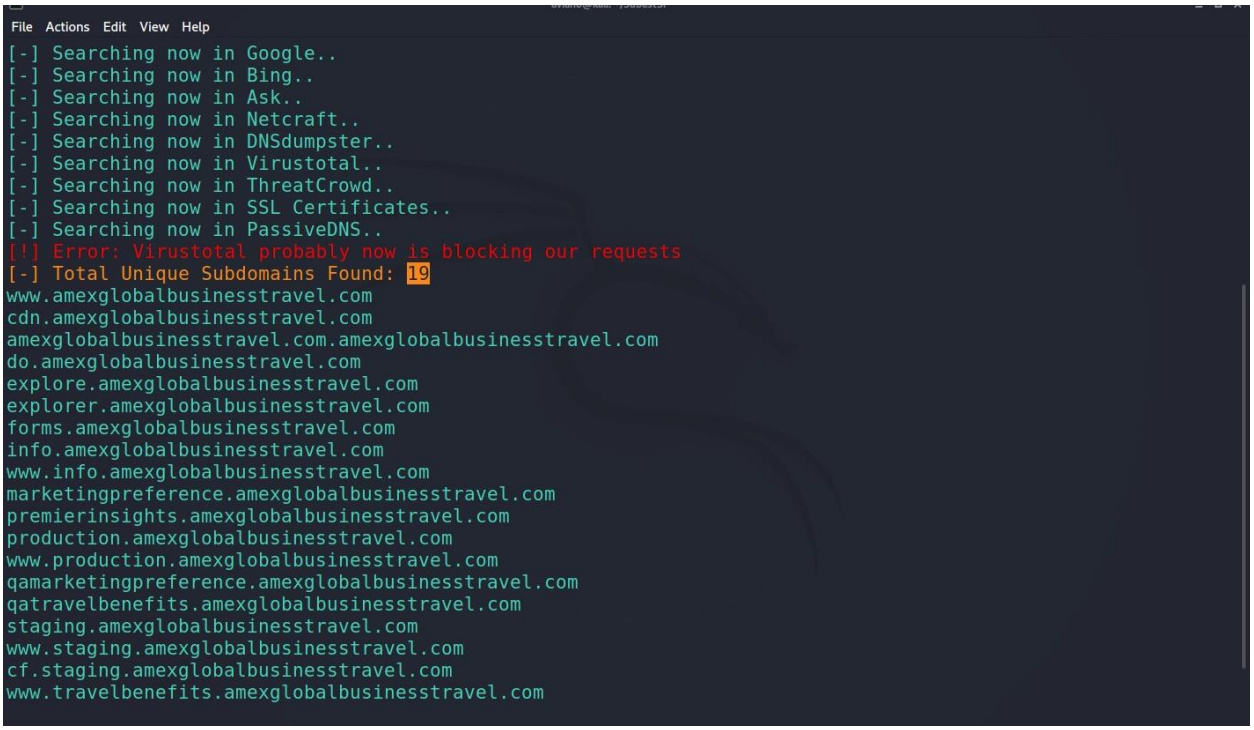


Automated Scans

Sublist3r Scan

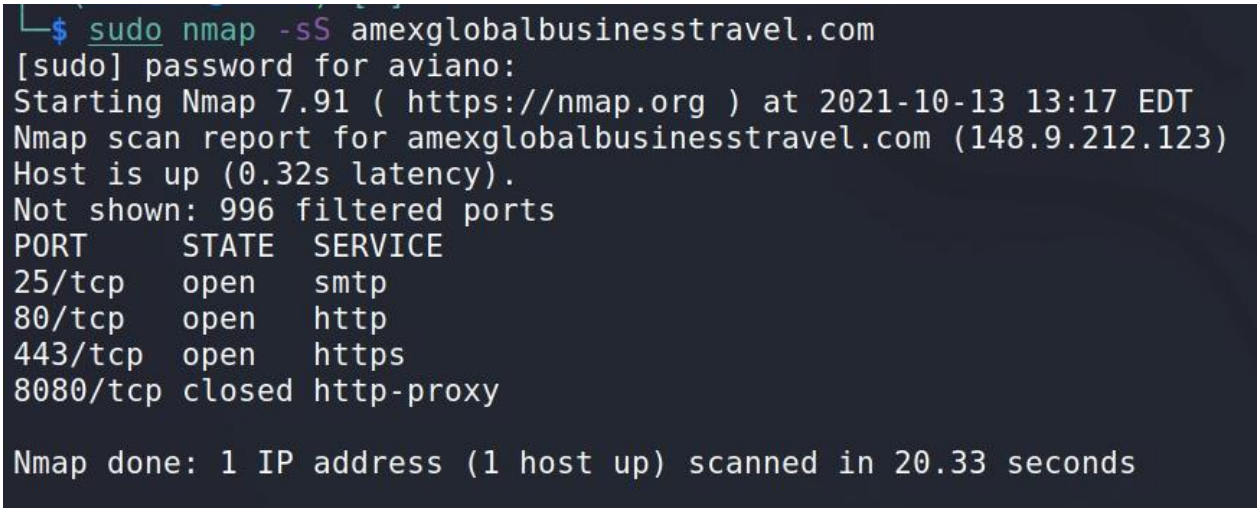
A Python programme called Sublist3r is intended to use OSINT to list the subdomains of websites. It facilitates the collection and gathering of subdomains for the target domain by penetration testers and bug hunters. Several search engines, including Google, Yahoo, Bing, Baidu, and Ask are used by Sublist3r to count subdomains.





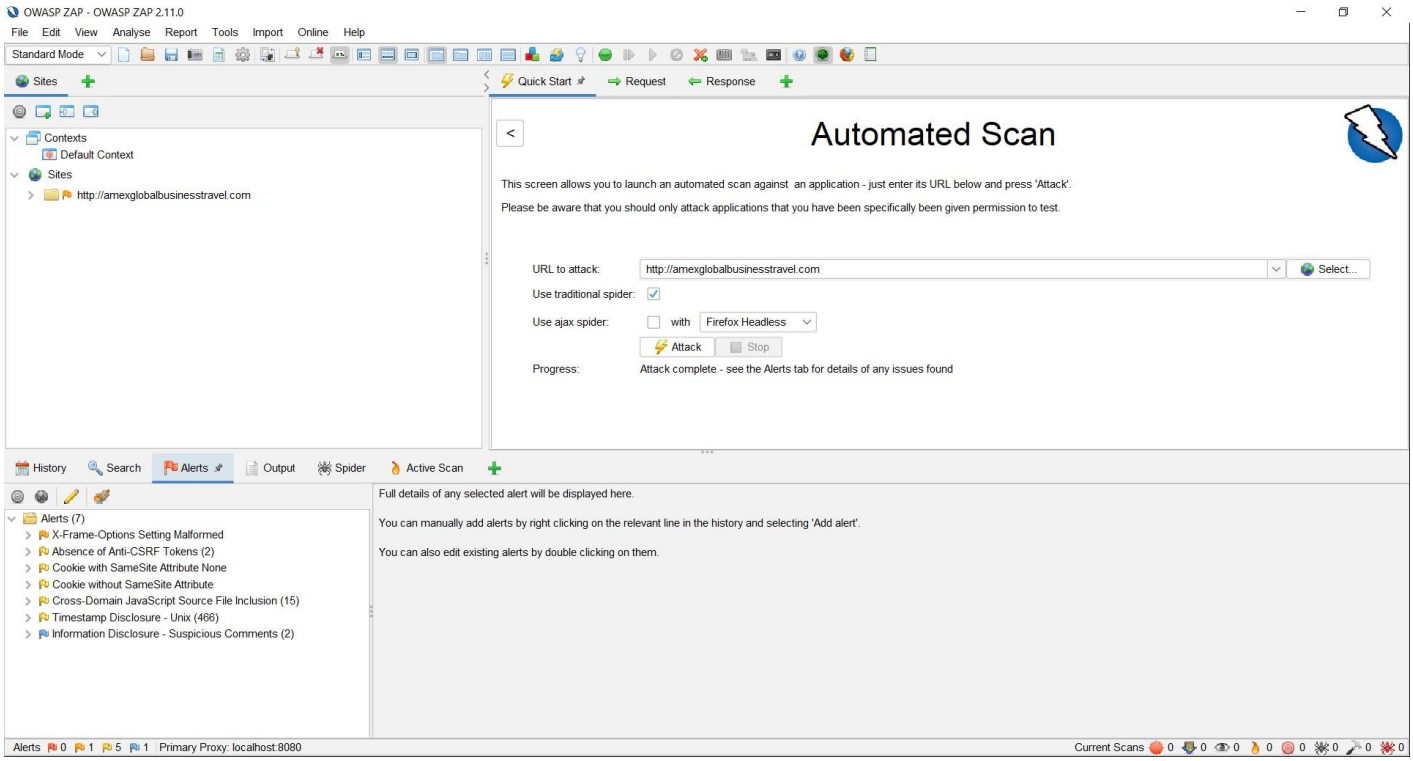
After finishing the Sublist3r scan, I found 19 subdomains under the main domain.

Nmap scan



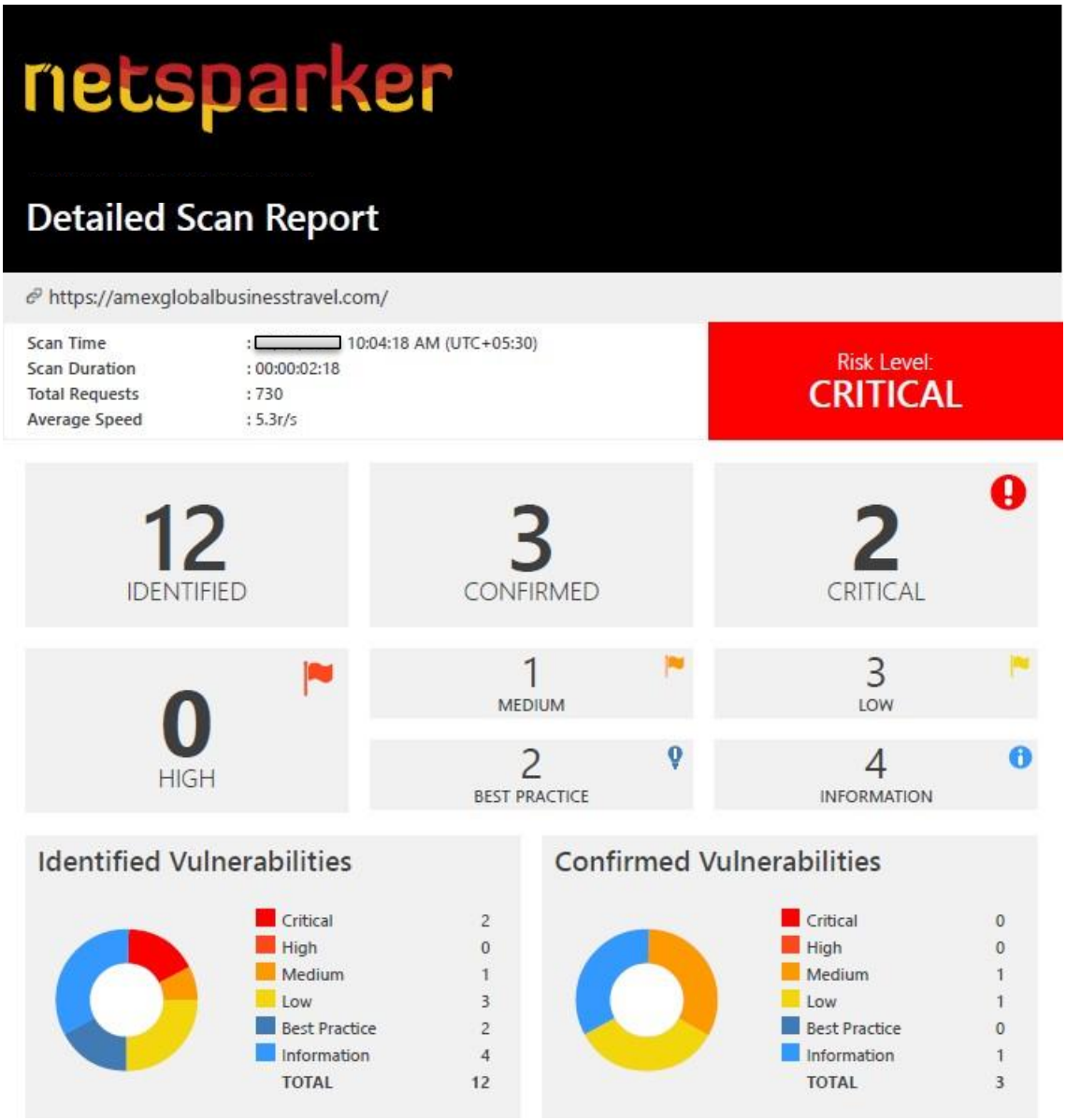
I found three open ports (smtp, http, https) and one closed port (http-proxy).

OWASP ZAP



I did an automated scan using OWASP ZAP. According to that report I found 7 types of flows on the https://www.amexglobalbusinesstravel.com/ website. However, I rescan the domain using Netsparker tool, and I received well detailed report as shown below.

Netsparker



By scanning the https://www.amexglobalbusinesstravel.com/ website, I found total of twelve (12) vulnerabilities. Three of them were confirmed vulnerabilities and the risk levels are medium, low. Overall risk level of the website is Critical, which means the website need to take actions as soon as possible. Or else attackers are possible to use above vulnerabilities to exploit them.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Apache)	GET	https://amexglobalbusinesstravel.com/	
	Out-of-date Version (WordPress)	GET	https://amexglobalbusinesstravel.com/wp-includes/images/arrow-pointer-blue.png	
	Weak Ciphers Enabled	GET	https://amexglobalbusinesstravel.com/	
	Version Disclosure (Apache)	GET	https://amexglobalbusinesstravel.com/	
	Version Disclosure (PHP)	GET	https://amexglobalbusinesstravel.com/	
	Internal Server Error	GET	https://amexglobalbusinesstravel.com/.well-known/phpinfo.php	URI-BASED
	Expect-CT Not Enabled	GET	https://amexglobalbusinesstravel.com/	
	SameSite Cookie Not Implemented	GET	https://amexglobalbusinesstravel.com/	
	Apache Web Server Identified	GET	https://amexglobalbusinesstravel.com/	
	Out-of-date Version (PHP)	GET	https://amexglobalbusinesstravel.com/	
	WordPress Detected	GET	https://amexglobalbusinesstravel.com/wp-includes/images/arrow-pointer-blue.png	
	Forbidden Resource	GET	https://amexglobalbusinesstravel.com/.htaccess	URI-BASED

According to the report generated by Netsparker, the confirmed vulnerabilities are Weak Ciphers Enabled, Internal Server Error, and Forbidden Resource. Although no confirmation yet, Out-of-date Version (Apache), and Out-of-date Version (WordPress) can be seen as critical vulnerabilities of the website.

Confirmed Vulnerabilities in details.

3. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

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.

Vulnerabilities

3.1. https://amexglobalbusinesstravel.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

- **Action to take.**

1. The SSLCipherSuit directive in httpd.conf should modify for Apache.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. Change some parts of system registry for Microsoft IIS. Inaccurate editing of registry able to damage the system severely. However, before starting the process of changing the parts of system registry we should backup important data on the 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:

```
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 the web server to disallow use of weak cipher.

4. Internal Server Error

LOW 1 CONFIRMED 1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Vulnerabilities

4.1. https://amexglobalbusinesstravel.com/.well-known/phpinfo.php

CONFIRMED

Method	Parameter	Value
GET	URI-BASED	phpinfo.php

Request

```
GET /.well-known/phpinfo.php HTTP/1.1
Host: amexglobalbusinesstravel.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 5a8f83462e58deac4b837c6a524e4ad0=89d4201900c314df2ecf7c0a79d64513
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 595.2274 Total Bytes Received : 889 Body Length : 532 Is Compressed : No

```
HTTP/1.1 500 Internal Server Error

Server: Apache/2.4.46 (Debian)
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 532
X-Frame-Options: ALLOW-FROM https://gbt.seismic.com/
Strict-Transport-Security: max-age=16070400; includeSubDomains
Content-Type: text/html; charset=iso-8859-1
Date: Wed, 13 Oct 2021 04:35:14 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator at
webmaster@localhost to inform them of the time this error occurred,
and the actions you performed just before this error.</p>
<p>More information about this error may be available
in the server error log.</p>
</body></html>
```

Remedy

To handle the unpredicted errors, inspect the issue and evaluate the application code; this should be a common practice that does not reveal more information about an error. All errors should handle only in server-side.

10. Forbidden Resource

INFORMATION 1 | CONFIRMED 1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

10.1. https://amexglobalbusinesstravel.com/.htaccess

CONFIRMED

Method	Parameter	Value
GET	URI-BASED	.htaccess

Request

```
GET /.htaccess HTTP/1.1
Host: amexglobalbusinesstravel.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 5a8f83462e58deac4b837c6a524e4ad0=89d4201900c314df2ecf7c0a79d64513
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 305.8952 Total Bytes Received : 544 Body Length : 199 Is Compressed : No

```
HTTP/1.1 403 Forbidden

Server: Apache/2.4.46 (Debian)
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 199
X-Frame-Options: ALLOW-FROM https://gbt.seismic.com/
Strict-Transport-Security: max-age=16070400; includeSubDomains
Content-Type: text/html; charset=iso-8859-1
Date: Wed, 13 Oct 2021 04:35:18 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
</body></html>
```

Unconfirmed Critical Vulnerabilities

1. Out-of-date Version (Apache)

CRITICAL 1

Netsparker identified you are using an out-of-date version of Apache.

Impact

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

Apache HTTP Server Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Vulnerability

ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

Affected Versions

2.2.31 to 2.4.48

External References

- CVE-2021-39275

Apache HTTP Server Server-Side Request Forgery (SSRF) Vulnerability

A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

Affected Versions

2.4.30 to 2.4.48

External References

- CVE-2021-40438

Apache HTTP Server Out-of-bounds Read Vulnerability

A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

Affected Versions

2.4.30 to 2.4.48

External References

- CVE-2021-36160

Apache HTTP Server NULL Pointer Dereference Vulnerability

Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

Affected Versions

0.8.11 to 2.4.48

Vulnerabilities

1.1. https://amexglobalbusinesstravel.com/

Identified Version

- 2.4.46

Latest Version

- 2.4.50 (in this branch)

Vulnerability Database

- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: amexglobalbusinesstravel.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 979.5892 Total Bytes Received : 517 Body Length : 0 Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: 5a8f83462e58deac4b837c6a524e4ad0=89d4201900c314df2ecf7c0a79d64513; path=/; HttpOnly; Secure
Server: Apache/2.4.46 (Debian)

X-Content-Type-Options: nosniff
X-Powered-By: PHP/8.0.7
X-XSS-Protection: 1; mode=block
Content-Length: 0
X-Frame-Options: ALLOW-FROM https://gbt.seismic.com/
Strict-Transport-Security: max-age=16070400; includeSubDomains
Content-Type: text/html; charset=UTF-8
Location: https://www.amexglobalbusinesstravel.com/
Date: Wed, 13 Oct 2021 04:34:19 GMT
```

Remedy

Update the Apache installation to the latest firm version.

2. Out-of-date Version (WordPress)

CRITICAL | 1

Netsparker identified the target web site is using WordPress and detected that it is out of date. WordPress is a free and open-source content management system (CMS) based on PHP and MySQL.

Impact

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

WordPress Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. ### Impact The issue allows an authenticated but low-privileged user (like contributor/author) to execute XSS in the editor. This bypasses the restrictions imposed on users who do not have the permission to post `unfiltered_html`. ### Patches This has been patched in WordPress 5.8, and will be pushed to older versions via minor releases (automatic updates). It's strongly recommended that you keep auto-updates enabled to receive the fix. ### References https://wordpress.org/news/category/releases/ https://hackerone.com/reports/1142140 ### For more information If you have any questions or comments about this advisory: * Open an issue in [HackerOne](https://hackerone.com/wordpress)

Affected Versions

5.7.1 to 5.7.3

External References

- CVE-2021-39201

WordPress Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. In affected versions output data of the function wp_die() can be leaked under certain conditions, which can include data like nonces. It can then be used to perform actions on your behalf. This has been patched in WordPress 5.8.1, along with any older affected versions via minor releases. It's strongly recommended that you keep auto-updates enabled to receive the fix.

Affected Versions

5.7.1 to 5.8

External References

- CVE-2021-39200

WordPress Improperly Controlled Modification of Dynamically-Determined Object Attributes Vulnerability

PHPMailer before 5.2.27 and 6.x before 6.0.6 is vulnerable to an object injection attack. WordPress Source: https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/

Affected Versions

5.7 to 5.7.1

External References

- CVE-2018-19296

WordPress Deserialization of Untrusted Data Vulnerability

PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname. NOTE: this is similar to CVE-2018-19296, but arose because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. As an unintended side effect, this fix eliminated the code that blocked addAttachment exploitation. WordPress Source: https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/

Affected Versions
5.7 to 5.7.1

External References
- CVE-2020-36326

Vulnerabilities

2.1. https://amexglobalbusinesstravel.com/wp-includes/images/arrow-pointer-blue.png

Identified Versions
- 5.7.2, 5.7.1

Latest Version
- 5.7.3 (in this branch)

Vulnerability Database
- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Request

```
GET /wp-includes/images/arrow-pointer-blue.png HTTP/1.1
Host: amexglobalbusinesstravel.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 5a8f83462e58deac4b837c6a524e4ad0=89d4201900c314df2ecf7c0a79d64513
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3043.0885 Total Bytes Received : 1982 Body Length : 1569 Is Compressed : No

```
Binary response detected, response has not saved.
```

Remedy

Upgrade the WordPress installation to the latest firm version.

Manual Scans

SSLyze Scan to inspect cipher strength

SSLyze is a Python tool which can inspect SSL configuration by connecting to a server. This tool is broad and fast when identifying misconfigurations that affects to SSL server.

```
 * Certificates Information:
       Hostname sent for SNI:             amexglobalbusinesstravel.com
       Number of certificates detected:   1


     Certificate #0 ( _RSAPublicKey )
       SHA1 Fingerprint:                  ef80273ab7c6cfa0e9ae314428f4b1b964d2d65a
       Common Name:                       amexglobalbusinesstravel.com
       Issuer:                            Sectigo RSA Organization Validation Secure Server CA
       Serial Number:                     286856906833765378133939490483103089758
       Not Before:                        2021-05-25
       Not After:                         2022-05-25
       Public Key Algorithm:              _RSAPublicKey
       Signature Algorithm:               sha256
       Key Size:                          2048
       Exponent:                          65537
       DNS Subject Alternative Names:     ['amexglobalbusinesstravel.com', 'gettravelready.amexgbt.com', 'i
nfo.amexglobalbusinesstravel.com', 'meetingsexpert.com', 'privacy.amexgbt.com', 'www.amexglobalbusinesstrav
el.com', 'www.gettravelready.amexgbt.com', 'www.info.amexglobalbusinesstravel.com', 'www.meetingsexpert.com
', 'www.privacy.amexgbt.com']

     Certificate #0 - Trust
       Hostname Validation:               OK - Certificate matches server hostname
       Android CA Store (9.0.0_r9):       OK - Certificate is trusted
       Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is trusted
       Java CA Store (jdk-13.0.2):        OK - Certificate is trusted
       Mozilla CA Store (2021-01-24):     OK - Certificate is trusted
       Windows CA Store (2021-02-08):     OK - Certificate is trusted
       Symantec 2018 Deprecation:         OK - Not a Symantec-issued certificate
       Received Chain:                    amexglobalbusinesstravel.com --> Sectigo RSA Organization Validat
```

```
       Received Chain:                    amexglobalbusinesstravel.com --> Sectigo RSA Organization Validat
ion Secure Server CA --> USERTrust RSA Certification Authority --> AAA Certificate Services
       Verified Chain:                    amexglobalbusinesstravel.com --> Sectigo RSA Organization Validat
ion Secure Server CA --> USERTrust RSA Certification Authority
       Received Chain Contains Anchor:    OK - Anchor certificate not sent
       Received Chain Order:              OK - Order is valid
       Verified Chain contains SHA1:      OK - No SHA1-signed certificate in the verified certificate chain

     Certificate #0 - Extensions
       OCSP Must-Staple:                  NOT SUPPORTED - Extension not found
       Certificate Transparency:          OK - 3 SCTs included

     Certificate #0 - OCSP Stapling
                                          NOT SUPPORTED - Server did not send back an OCSP response

 * Downgrade Attacks:
       TLS_FALLBACK_SCSV:                 OK - Supported

 * TLS 1.2 Session Resumption Support:
      With Session IDs: OK - Supported (5 successful resumptions out of 5 attempts).
      With TLS Tickets: NOT SUPPORTED - Server did not return a TLS ticket.

 * TLS 1.3 Cipher Suites:
     Attempted to connect using 5 cipher suites; the server rejected all cipher suites.

 * Elliptic Curve Key Exchange:
       Supported curves:                  X25519, prime256v1, secp384r1
       Rejected curves:                   X448, prime192v1, secp160k1, secp160r1, secp160r2, secp192k1, sec
p224k1, secp224r1, secp256k1, secp521r1, sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1,
sect233r1, sect239k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1
```

```
* ROBOT Attack:
                                     OK - Not vulnerable, RSA cipher suites not supported.

* Session Renegotiation:
      Client Renegotiation DoS Attack:   OK - Not vulnerable
      Secure Renegotiation:              OK - Supported

* TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites.

    The server accepted the following 13 cipher suites:
       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256       256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384             256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384             256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256             128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256             128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1 (256 bits)
       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384               256       DH (1024 bits)
       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256               256       DH (1024 bits)
       TLS_DHE_RSA_WITH_AES_256_CBC_SHA                  256       DH (1024 bits)
       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256               128       DH (1024 bits)
       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256               128       DH (1024 bits)
       TLS_DHE_RSA_WITH_AES_128_CBC_SHA                  128       DH (1024 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                   OK - Supported
      Legacy RC4 Algorithm              OK - Not Supported


* TLS 1.1 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.


SCAN COMPLETED IN 72.84 S
```

We can see this site is not vulnerable to Client Renegotiation DoS Attacks, Robot Attacks, Downgrade attacks, OpenSSL CCS Injection attacks, and OpenSSL heartbeat. By analyzing the whole report, we can conclude that no cipher issues in this website.

CORS Misconfiguration test

CORS protocol allows trusted subdomains and third-party applications to access to the resources on trusted origins and other properties. If this protocol has configured incorrectly, it gives an attacker a chance to access to the valuable or the sensitive resources by exploiting the vulnerabilities.

We use Corsy python tool to identify CORS misconfiguration.

- No misconfigurations in here.

Open Redirection Vulnerability testing.

Open redirection vulnerability is an attacker can control the targeted website to redirect it to a malicious website. Oralyzer is a tool which van be used to test against Open Redirection Vulnerability.

```
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/x00http://google.com ➤ https://www.amexglobalbusinesstravel.com/x00http:/google.com
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/%5Cx20http://google.com ➤ https://www.amexglobalbusinesstravel.com/%5Cx20http:/google.com
[•] https://www.amexglobalbusinesstravel.com/216.58.214.206 [404]
[•] https://www.amexglobalbusinesstravel.com/172.217.167.46 [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com//216.58.214.206 ➤ https://www.amexglobalbusinesstravel.com/216.58.214.206
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com////216.58.214.206 ➤ https://www.amexglobalbusinesstravel.com/216.58.214.206
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com//%5C216.58.214.206 ➤ https://www.amexglobalbusinesstravel.com/%5C216.58.214.206
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com///216.58.214.206 ➤ https://www.amexglobalbusinesstravel.com/216.58.214.206
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com////216.58.214.206 ➤ https://www.amexglobalbusinesstravel.com/216.58.214.206
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com///google%E3%80%82com ➤ https://www.amexglobalbusinesstravel.com/google%E3%80%82com
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com///google%E3%80%82com ➤ https://www.amexglobalbusinesstravel.com/google%E3%80%82com
[•] https://www.amexglobalbusinesstravel.com/http%5Cx3A%5Cx2F%5Cx2Fgoogle.com [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com////google.com/.. ➤ https://www.amexglobalbusinesstravel.com/google.com/
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com////google.com/.. ➤ https://www.amexglobalbusinesstravel.com/google.com/
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com///google.com/.. ➤ https://www.amexglobalbusinesstravel.com/google.com/
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com//google.com/.. ➤ https://www.amexglobalbusinesstravel.com/google.com/
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com///google.com/.. ➤ https://www.amexglobalbusinesstravel.com/google.com/
[•] https://www.amexglobalbusinesstravel.com////google.com/..%2F [404]
[•] https://www.amexglobalbusinesstravel.com////google.com/..%2F [404]
[•] https://www.amexglobalbusinesstravel.com////google.com/..%2F [404]
[•] https://www.amexglobalbusinesstravel.com////google.com/%2F.. [404]
```

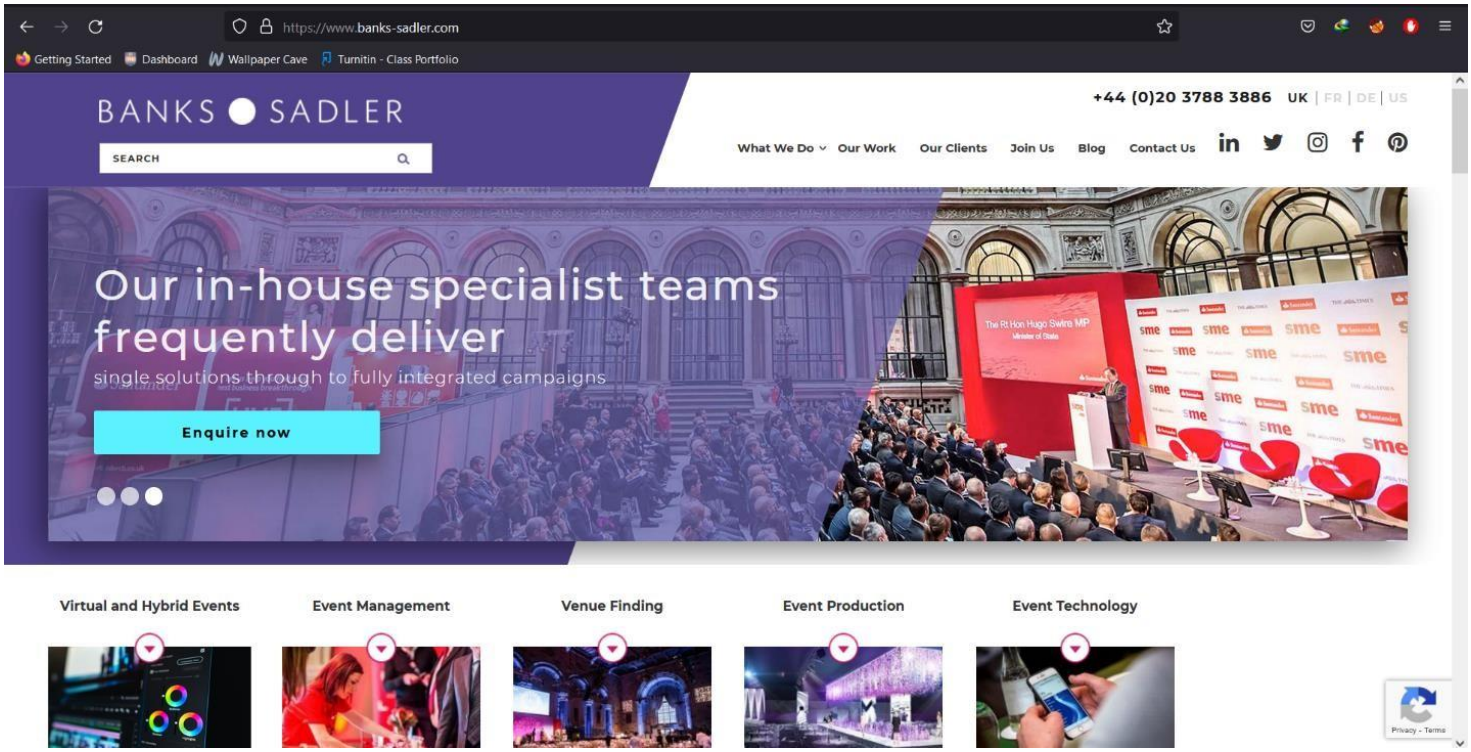
```
[•] https://www.amexglobalbusinesstravel.com///google.com/..%2F [404]
[•] https://www.amexglobalbusinesstravel.com////google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com////google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com///google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com///google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com//google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com////google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com////google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com///google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com//google.com/%2F.. [404]
[•] https://www.amexglobalbusinesstravel.com///google.com//%2F.. [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/http://%5B::ffff:216.58.214.206%5D ➤ https://www.amexglobalbusinesstravel.com/http:/%5B::ffff:216.58.214.206%5D
[•] https://www.amexglobalbusinesstravel.com/http:%5B::ffff:216.58.214.206%5D [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/http://00330.00072.0000326.00000316 ➤ https://www.amexglobalbusinesstravel.com/http:/00330.00072.0000326.00000316
[•] https://www.amexglobalbusinesstravel.com/http:00330.00072.0000326.00000316 [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/http://00330.0x3a.54990 ➤ https://www.amexglobalbusinesstravel.com/http:/00330.0x3a.54990
[•] https://www.amexglobalbusinesstravel.com/http:00330.0x3a.54990 [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/http://00330.3856078 ➤ https://www.amexglobalbusinesstravel.com/http:/00330.3856078
[•] https://www.amexglobalbusinesstravel.com/http:00330.3856078 [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/http://0330.072.0326.0316 ➤ https://www.amexglobalbusinesstravel.com/http:/0330.072.0326.0316
[•] https://www.amexglobalbusinesstravel.com/http:0330.072.0326.0316 [404]
[•] https://www.amexglobalbusinesstravel.com/http:%0A%0D%E2%93%81%F0%9D%90%A8%F0%9D%97%B0%EF%BF%BD%F0%9D%95%9D%E2%85%86%F0%9D%93%B8%E2%93%9C%E2%82%90%E2%84%B9%E2%93%83%EF%BD%A1%EF%BC%B0%E2%93%A6 [404]
[•] https://www.amexglobalbusinesstravel.com/http:%0A%0Dgoogle.com [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/http://0xd8.072.54990 ➤ https://www.amexglobalbusinesstravel.com/http:/0xd8.072.54990
[•] https://www.amexglobalbusinesstravel.com/http:0xd8.072.54990 [404]
[•] Header Based Redirection : https://www.amexglobalbusinesstravel.com/http://0xd8.0x3a.0xd6.0xce ➤ https://www.amexglobalbusinesstravel.com/http:/0xd8.0x3a.0xd6.0xce
[•] https://www.amexglobalbusinesstravel.com/http:0xd8.0x3a.0xd6.0xce [404]
```

Not Vulnerable to Open Redirection vulnerability since the requests get 404 error code to requests.

Subdomain 2

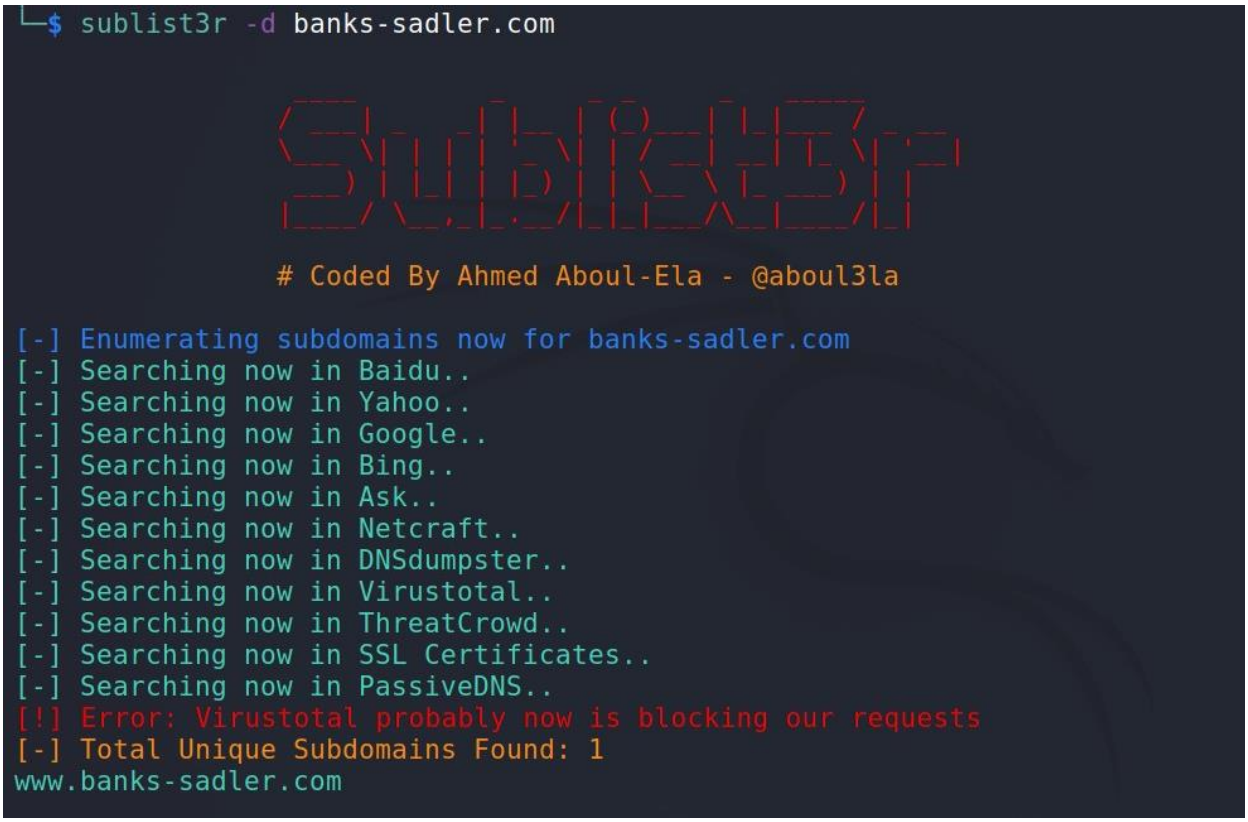
BANKS.SADLER

https://www.banks-sadler.com/



Automated Scans

Sublist3r Scan

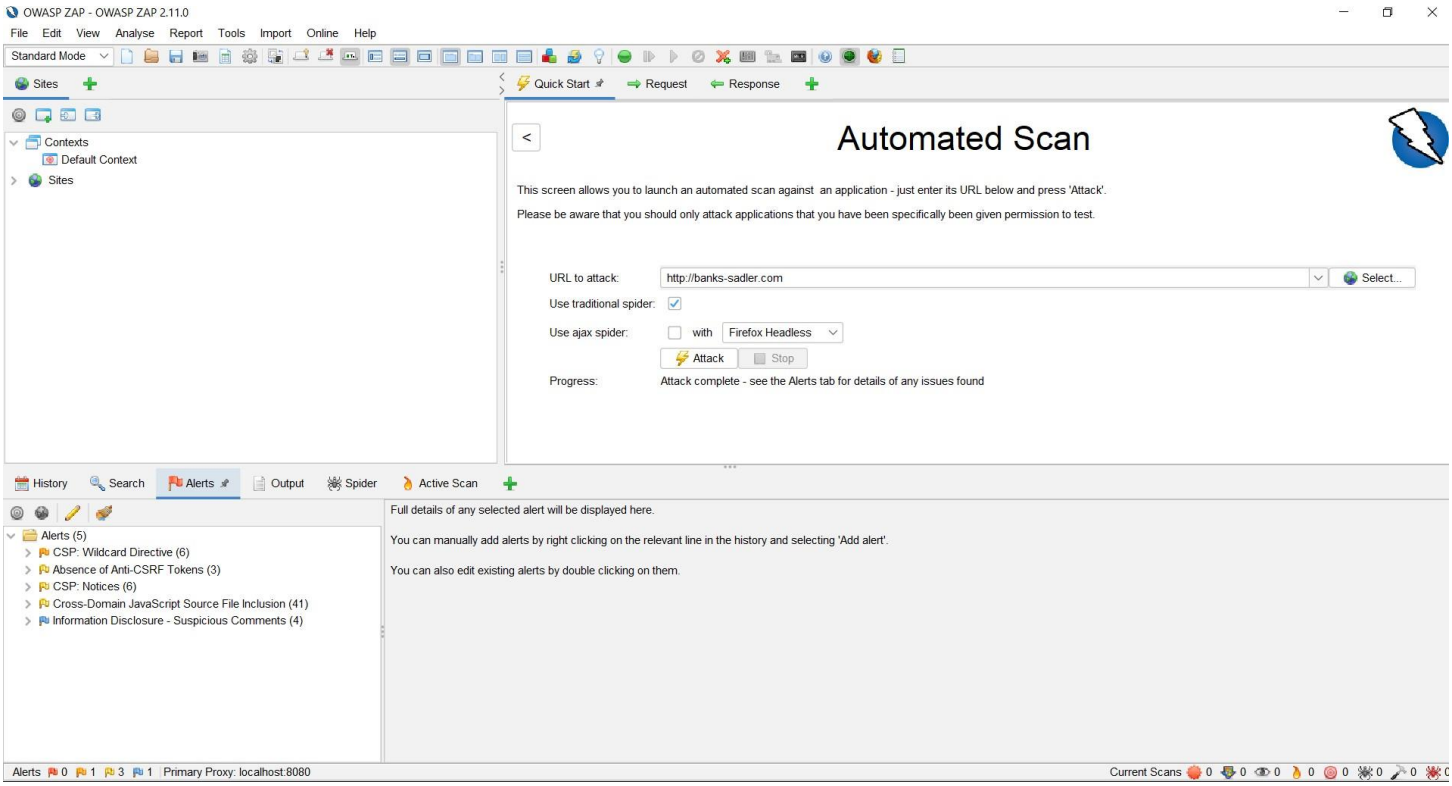


Nmap scan

```
└─$ sudo nmap -sS banks-sadler.com
[sudo] password for aviano:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-13 23:20 EDT
Nmap scan report for banks-sadler.com (185.151.30.167)
Host is up (0.20s latency).
rDNS record for 185.151.30.167: 185-151-30-167.ptr4.stackcp.net
Not shown: 997 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

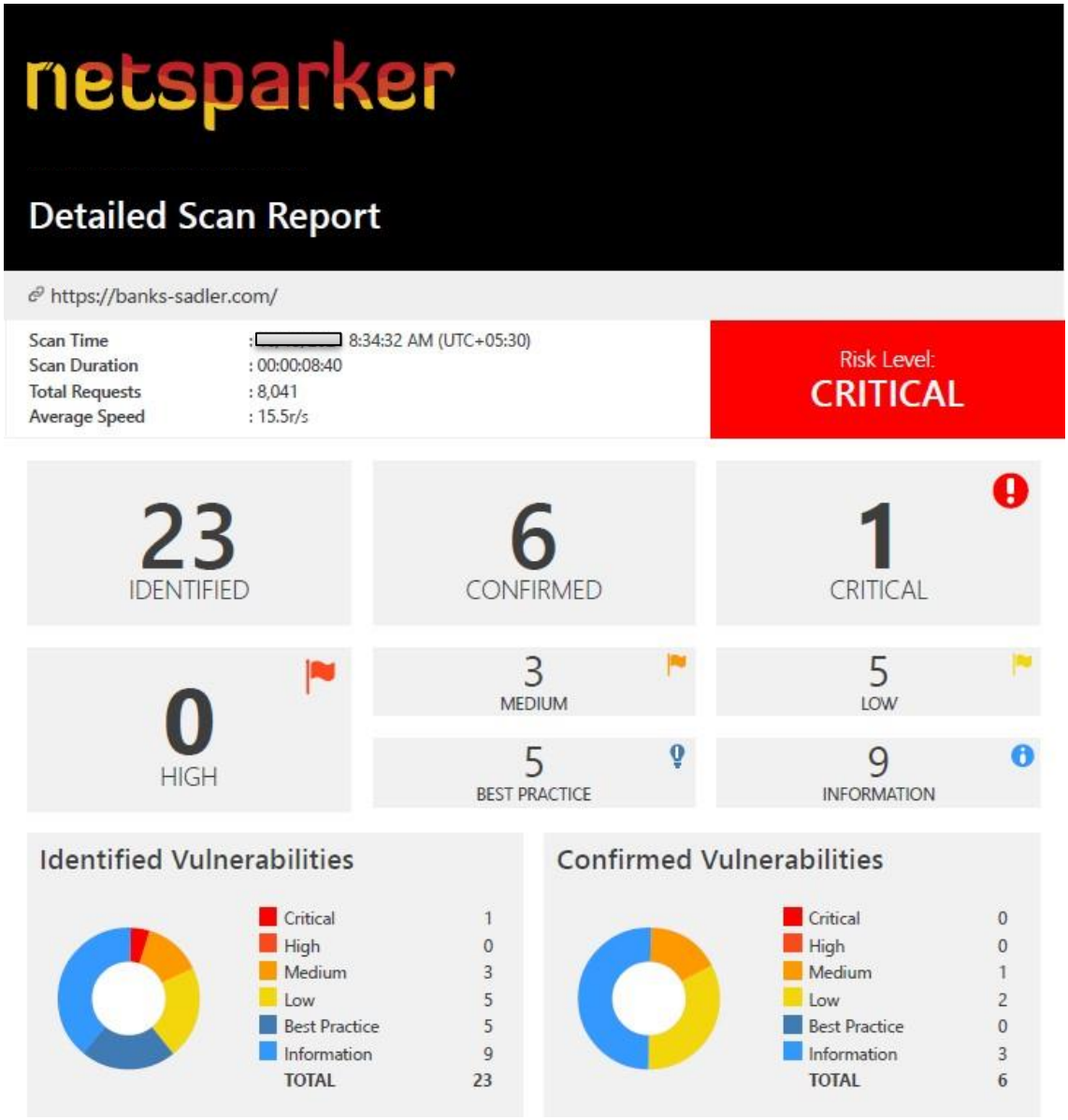
- Found three open ports; smtp, http, and https.

OWASP ZAP Scan



According to the report regenerated for the http://www.banks-sadler.com/ website by OWASP ZAP, there are 5 types of flows can be found. However, I did the same scan using Netsparker tool and it gave me very comprehensive detailed report on the vulnerabilities that can find in this subdomain.

Netsparker Scan



According to the report generated by Netsparker regarding to https://www.banks-sadler.com/ website, total of 23 vulnerabilities have identified. Six (06) of them are confirmed vulnerabilities. Furthermore, one (01) critical level vulnerability found among 23 vulnerabilities. Overall risk level of the website is in Critical, which means it need to take actions as soon as possible.

Vulnerability Summery

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Nginx)	GET	https://banks-sadler.com/wp-login.php	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://banks-sadler.com/	
	Out-of-date Version (jQuery)	GET	https://banks-sadler.com/wp-content/plugins/enable-jquery-migrate-helper/js/jquery/jquery-1.12.4-wp.js?ver=1.12.4-wp	
	Weak Ciphers Enabled	GET	https://banks-sadler.com/	
	[Possible] Cross-site Request Forgery	GET	https://banks-sadler.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbanks-sadler.com%2Fwp-admin%2F	
	Missing X-Frame-Options Header	GET	https://banks-sadler.com/.well-known/apple-app-site-association	
	Version Disclosure (Nginx)	GET	https://banks-sadler.com/wp-login.php	
	Insecure Frame (External)	GET	https://banks-sadler.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbanks-sadler.com%2Fwp-admin%2F	
	Internal Server Error	GET	https://banks-sadler.com/wp-content/themes/genesis/	
	Content Security Policy (CSP) Not Implemented	GET	https://banks-sadler.com/.well-known/apple-app-site-association	
	Expect-CT Not Enabled	GET	https://banks-sadler.com/.well-known/apple-app-site-association	
	Missing X-XSS-Protection Header	GET	https://banks-sadler.com/.well-known/apple-app-site-association	
	Referrer-Policy Not Implemented	GET	https://banks-sadler.com/.well-known/apple-app-site-association	
	Subresource Integrity (SRI) Not Implemented	GET	https://banks-sadler.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbanks-sadler.com%2Fwp-admin%2F	
	Apache Web Server Identified	GET	https://banks-sadler.com/	
	Email Address Disclosure	POST	https://banks-sadler.com/	
	Expect-CT in Report Only Mode	GET	https://banks-sadler.com/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Missing object-src in CSP Declaration	GET	https://banks-sadler.com/wp-admin/admin-ajax.php	
	Nginx Web Server Identified	POST	https://banks-sadler.com/wp-login.php	
	WordPress Detected	GET	https://banks-sadler.com/wp-includes/images/arrow-pointer-blue.png	
	Autocomplete Enabled (Password Field)	GET	https://banks-sadler.com/wp-login.php/etc/passwd	URI-BASED
	Forbidden Resource	GET	https://banks-sadler.com/.well-known/apple-app-site-association	
	Robots.txt Detected	GET	https://banks-sadler.com/robots.txt	

According to the report generated by Netsparker, the confirmed vulnerabilities are, Weak Cipher Enabled, Insecure Frame (External), Internal Server Error, Autocomplete Enabled (Password Field), Forbidden Resources, Robots.txt Detected. Since the last three of them are informational, they are no risky issues with them. Other than that, as a critical vulnerability, Out-of-date Version (Nginx) was found.

Confirmed Vulnerabilities in details.

4. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

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.

Vulnerabilities

4.1. https://banks-sadler.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

- **Action to take.**

  Same actions should perform as mentioned in the previously scanned domain (https://www.amexglobalbusinesstravel.com/). For the easy access I have add the same thing here as well.

  1. The SSLCipherSuit directive in httpd.conf should modify for Apache.

     ```
     SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
     ```

  2. Lighttpd

     ```
     ssl.honor-cipher-order = "enable"
     ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
     ```

  3. Change some parts of system registry for Microsoft IIS. Inaccurate editing of registry able to damage the system severely. However, before starting the process of changing the parts of system registry we should backup important data on the 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:

     ```
     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 the web server to disallow use of weak cipher (mentioned previously in the scan of main domain as well).

6. Insecure Frame (External)

LOW 1 CONFIRMED 1

Netsparker identified an external insecure or misconfigured iframe.

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as *http://site.com*:

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as *http://site.com*:

http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

When the sandboxattribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the sandboxattribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandboxcontaining a value of :

- `allow-same-origin`will not treat it as a unique origin.
- `allow-top-navigation`will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- `allow-forms`will allow form submissions from inside the iframe.
- `allow-popups`will allow popups.
- `allow-scripts`will allow malicious script execution however it won't allow to create popups.

Vulnerabilities

6.1. https://banks-sadler.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbanks-sadler.com%2Fwp-admin%2F

CONFIRMED

Method	Parameter	Value
GET	redirect_to	https%3A%2F%2Fbanks-sadler.com%2Fwp-admin%2F
GET	reauth	1

Frame Name(s)

- a-2i45ft4l3nk6

Sandbox Value(s)

- allow-forms allow-popups allow-same-origin allow-scripts allow-top-navigation allow-modals allow-popups-to-escape-sandbox

Parsing Source

- DOM Parser

Request

```
GET /wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fbanks-sadler.com%2Fwp-admin%2F HTTP/1.1
Host: banks-sadler.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://banks-sadler.com/wp-admin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 345.7094 Total Bytes Received : 1663 Body Length : 1383 Is Compressed : No

```
HTTP/1.1 401 Unauthorized
server: nginx/1.16.1
x-service-level: wordpress
x-cdn-cache-status: MISS
x-via: MAD1
content-type: text/html; charset=UTF-8
transfer-encoding: chunked
x-backend-server: stackprotect2
date: Wed, 13 Oct 2021 03:04:51 GMT
cache-control: Private

<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
 integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anony
mous">
<script src="https://www.google.com/recaptcha/api.js?render=6LdZXJwUAAAAAE1ERIs8cDyw2wNhHNuMxBJWG0Aa">
</script>
<title>Bot Verification</title>
<script>
function stackProtect() {
grecaptcha.ready(function() {
grecaptcha.execute('6LdZXJwUAAAAAE1ERIs8cDyw2wNhHNuMxBJWG0Aa', {}).then(function(token) {
document.getElementById('token').value = token
document.getElementById('stackprotectform').submit()
});
});
}
setInterval(stackProtect, 5000);
</script>
</head>
<body>
<div class="text-center">
<br><br>
<p>To help us keep this website secure, please wait while we verify you're not a robot! It will only ta
ke a few seconds...</p>
<div class="spinner-border m-5" role="status">
<span class="sr-only">Loading...</span>
</div>
<form action="" method="post" id="stackprotectform">
<input type="hidden" id="token" name="g-recaptcha-response" value="">
</form>

</div>
</body>
</html>
```

Remedy

- Inside inline frame, apply sandboxing.

```
<iframe sandbox src="framed-page-url"></iframe>
```

- Avoid the utilize of allow-top-navigation, seamless attribute, and allow-popupsand allow-scriptsin sandbox attribute for untrusted content.

7. Internal Server Error

LOW 1 CONFIRMED 1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Vulnerabilities

7.1. https://banks-sadler.com/wp-content/themes/genesis/

CONFIRMED

Request

```
GET /wp-content/themes/genesis/ HTTP/1.1
Host: banks-sadler.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: wordpress_test_cookie=WP%20Cookie%20check
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1070.0616 Total Bytes Received : 848 Body Length : 0 Is Compressed : No

```
HTTP/1.1 500 Internal Server Error

feature-policy: geolocation 'self'; vibrate 'none'
expect-ct: max-age=60, report-uri="https://reportmydomain.com/report"
x-permitted-cross-domain-policies: master-only;
x-service-level: wordpress
strict-transport-security: max-age=63072000; includeSubDomains
strict-transport-security: max-age=5184000; includeSubDomains; preload
x-provided-by: StackCDN
x-provided-by: StackCDN
server: Apache
x-content-type-options: nosniff
x-origin-cache-status: MISS
x-xss-protection: 1; mode=block
x-cdn-cache-status: MISS
referrer-policy: same-origin
x-frame-options: SAMEORIGIN
x-via: MAD1
content-length: 0
content-type: text/html; charset=UTF-8
x-backend-server: web83.hosting.stackcp.net
content-security-policy: https://www.banks-sadler.com/contact-us 'self';
date: Wed, 13 Oct 2021 03:12:41 GMT
```

Remedy

Examine the issue and evaluate the application code to handle unpredicted errors. All errors must be handled in server-side only.

16. Autocomplete Enabled (Password Field)

INFORMATION 1 | CONFIRMED 1

Netsparker detected that autocomplete is enabled in one or more of the password fields.

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Vulnerabilities

16.1. https://banks-sadler.com/wp-login.php/etc/passwd

CONFIRMED

Method	Parameter	Value
GET	URI-BASED	/etc/passwd

Identified Field Name

- pwd

Request

```
GET /wp-login.php/etc/passwd HTTP/1.1
Host: banks-sadler.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: wordpress_test_cookie=WP%20Cookie%20check
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3273.3541 Total Bytes Received : 8999 Body Length : 7927 Is Compressed : No

```
HTTP/1.1 200 OK
feature-policy: geolocation 'self'; vibrate 'none'
expect-ct: max-age=60, report-uri="https://reportmydomain.com/report"
cache-control: no-cache, must-revalidate, max-age=0
set-cookie: wordpress_test_cookie=WP%20Cookie%20check; path=/; secure
strict-transport-security: max-age=63072000; includeSubDomains
strict-transport-security: max-age=5184000; includeSubDomains; preload
transfer-encoding: chunked
x-provided-by: StackCDN
server: Apache
x-backend-server: web83.hosting.stackcp.net
x-content-type-options: nosniff
x-origin-cache-status: MISS
x-xss-protection: 1; mode=block
x-service-level: wordpress
x-cdn-cache-status: MISS
referrer-policy: same-origin
expires: Wed, 11 Jan 1984 05:00:00 GMT
x-frame-options: SAMEORIGIN
x-frame-options: SAMEORIGIN
vary: Accept-Encoding
vary: Accept-Encoding
x-via: MAD1
content-type: text/html; charset=UTF-8
x-permitted-cross-domain-policies: master-only;
content-security-policy: https://www.banks-sadler.com/contact
…
name="log" id="user_login" class="input" value="" size="20" autocapitalize="off" />
</p>

<div class="user-pass-wrap">
<label for="user_pass">Password</label>
<div class="wp-pwd">
<input type="password" name="pwd" id="user_pass" class="input password-input" value="" size="20" />
<button type="button" class="button button-secondary wp-hide-pw hide-if-no-js" data-toggle="0" aria-lab
el="Show password">
<span class="dashicons dashicons-visibility" aria-hidden="true"><
…
```

Remedy

- Set the attribute “autocomplete = off” to the individual “input” fields or to the form tag. Anyhow, browsers do not respect this directive and offer users to stock their passwords internally since early 2014.
- After solving the issues identified, re-scan the application to check the security again.

19. Forbidden Resource

INFORMATION 1 | CONFIRMED 1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

19.1. https://banks-sadler.com/.well-known/apple-app-site-association

CONFIRMED

Request

```
GET /.well-known/apple-app-site-association HTTP/1.1
Host: banks-sadler.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://banks-sadler.com/.well-known/apple-app-site-association
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 788.4099 Total Bytes Received : 596 Body Length : 261 Is Compressed : No

```
HTTP/1.1 403 Forbidden

server: Apache
x-origin-cache-status: MISS
x-cdn-cache-status: HIT
content-encoding:
x-via: MAD1
x-service-level: wordpress
content-type: text/html; charset=iso-8859-1
transfer-encoding: chunked
x-backend-server: web83.hosting.stackcp.net
date: Wed, 13 Oct 2021 03:04:41 GMT
vary: Accept-Encoding

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.Server unable to read htaccess file, denying acces
s to be safe</p>
</body></html>
```

22. Robots.txt Detected

INFORMATION 1 CONFIRMED 1

Netsparker detected a Robots.txtfile with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Vulnerabilities

22.1. https://banks-sadler.com/robots.txt

CONFIRMED

Interesting Robots.txt Entries

- Disallow: /wp-admin/
- Sitemap: https://www.banks-sadler.com/sitemap_index.xml

Request

```
GET /robots.txt HTTP/1.1
Host: banks-sadler.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 208.9153 Total Bytes Received : 1042 Body Length : 127 Is Compressed : No

```
HTTP/1.1 200 OK
feature-policy: geolocation 'self'; vibrate 'none'
expect-ct: max-age=60, report-uri="https://reportmydomain.com/report"
x-permitted-cross-domain-policies: master-only;
etag: W/"7f-5a074cd072000"
x-service-level: wordpress
strict-transport-security: max-age=63072000; includeSubDomains
strict-transport-security: max-age=5184000; includeSubDomains; preload
transfer-encoding: chunked
x-provided-by: StackCDN
server: Apache
x-content-type-options: nosniff
x-origin-cache-status: MISS
x-xss-protection: 1; mode=block
x-cdn-cache-status: HIT
referrer-policy: same-origin
x-frame-options: SAMEORIGIN
vary: Accept-Encoding
x-via: MAD1
last-modified: Tue, 10 Mar 2020 00:00:00 GMT
content-type: text/plain
x-backend-server: web83.hosting.stackcp.net
content-security-policy: https://www.banks-sadler.com/contact-us 'self';
date: Wed, 13 Oct 2021 03:04:51 GMT
content-encoding:

User-agent:*
Disallow:/wp-admin/
Allow:/wp-admin/admin-ajax.php

Sitemap: https://www.banks-sadler.com/sitemap_index.xml
```

Remedy

Ensure not to exposed sensitive data withing the file, like path of an administration panel. By means of authentication, if forbidden paths should keep away from unauthorized access and they are highly sensitive, then make sure not to write those in the Robots.txt and ensure their security.

Using bellow block, it can notify the crawler to index files under/web/and ignore the rest unless for specified directories. That way search engines will not index the website.

```
User-Agent: *
Allow: /web/
Disallow: /
```

In the response header, X-Robots-Tag can be set to tell crawlers whether the file should be indexed or not. That helps to hide specific parts of the website from the search engines if any case of need.

Index files generally indexing, and it cannot be prevent using Robots meta tags. That problem also can be solved using X-Robots-Tag.

For Apache server, bellow instructions can be used to restrict crawlers to index multimedia files without revealing them in Robots.txt.

```
<Files ~ "\.pdf$">
# Don't index PDF files.
Header set X-Robots-Tag "noindex, nofollow"
</Files>
```

```
<Files ~ "\.(png|jpe?g|gif)$">
#Don't index image files.
Header set X-Robots-Tag "noindex"
</Files>
```

Unconfirmed Critical Vulnerabilities

1. Out-of-date Version (Nginx)

CRITICAL 1

Netsparker identified you are using an out-of-date version of Nginx.

Impact

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

Nginx Off-by-one Error Vulnerability

A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

Affected Versions

1.7.4 to 1.20.0

External References

- CVE-2021-23017

Vulnerabilities

1.1. https://banks-sadler.com/wp-login.php

Identified Version

- 1.16.1

Latest Version

- 1.21.3 (in this branch)

Vulnerability Database

- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Request

```
GET /wp-login.php HTTP/1.1
Host: banks-sadler.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 305.6733 Total Bytes Received : 1663 Body Length : 1383 Is Compressed : No

```
HTTP/1.1 401 Unauthorized
server: nginx/1.16.1
x-service-level: wordpress
x-cdn-cache-status: MISS
x-via: MAD1
content-type: text/html; charset=UTF-8
transfer-encoding: chunked
x-backend-server: stackprotect2
date: Wed, 13 Oct 2021 03:04:51 GMT
cache-control: Private

<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
 integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anony
mous">
<script src="https://www.google.com/recaptcha/api.js?render=6LdZXJwUAAAAAE1ERIs8cDyw2wNhHNuMxBJWG0Aa">
</script>
<title>Bot Verification</title>
<script>
function stackProtect() {
grecaptcha.ready(function() {
grecaptcha.execute('6LdZXJwUAAAAAE1ERIs8cDyw2wNhHNuMxBJWG0Aa', {}).then(function(token) {
document.getElementById('token').value = token
document.getElementById('stackprotectform').submit()
});
});
}
setInterval(stackProtect, 5000);
</script>
</head>
<body>
<div class="text-center">
<br><br>
<p>To help us keep this website secure, please wait while we verify you're not a robot! It will only ta
ke a few seconds...</p>
<div class="spinner-border m-5" role="status">
<span class="sr-only">Loading...</span>
</div>
<form action="" method="post" id="stackprotectform">
<input type="hidden" id="token" name="g-recaptcha-response" value="">
</form>

</div>
</body>
</html>
```

Remedy

Nginx installation should be upgraded to the latest secure version.

Manual Scans

SSLyze Scan to inspect cipher strength

```
└─$ sslyze --regular banks-sadler.com

CHECKING HOST(S) AVAILABILITY
-----------------------------

  banks-sadler.com:443                      => 185.151.30.167



SCAN RESULTS FOR BANKS-SADLER.COM:443 - 185.151.30.167
------------------------------------------------------

* TLS 1.1 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* Downgrade Attacks:
      TLS_FALLBACK_SCSV:                OK - Supported

* TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites.

    The server accepted the following 22 cipher suites:
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 256
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 128
       TLS_RSA_WITH_AES_256_GCM_SHA384                   256
       TLS_RSA_WITH_AES_256_CBC_SHA256                   256
       TLS_RSA_WITH_AES_256_CBC_SHA                      256
       TLS_RSA_WITH_AES_128_GCM_SHA256                   128
       TLS_RSA_WITH_AES_128_CBC_SHA256                   128
```

```
      TLS_RSA_WITH_AES_128_CBC_SHA                      128
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384             256       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384             256       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256             128       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256             128       ECDH: prime256v1 (256 bits)
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1 (256 bits)
      TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA             256       DH (2048 bits)
      TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA             128       DH (2048 bits)
      TLS_DHE_RSA_WITH_AES_256_GCM_SHA384               256       DH (2048 bits)
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA256               256       DH (2048 bits)
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA                  256       DH (2048 bits)
      TLS_DHE_RSA_WITH_AES_128_GCM_SHA256               128       DH (2048 bits)
      TLS_DHE_RSA_WITH_AES_128_CBC_SHA256               128       DH (2048 bits)
      TLS_DHE_RSA_WITH_AES_128_CBC_SHA                  128       DH (2048 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                   OK - Supported
      Legacy RC4 Algorithm              OK - Not Supported


 * Elliptic Curve Key Exchange:
      Supported curves:                 prime256v1
      Rejected curves:                  X25519, X448, prime192v1, secp160k1, secp160r1, secp160r2, secp19
2k1, secp224k1, secp224r1, secp256k1, secp384r1, secp521r1, sect163k1, sect163r1, sect163r2, sect193r1, sec
t193r2, sect233k1, sect233r1, sect239k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1

 * SSL 2.0 Cipher Suites:
    Attempted to connect using 7 cipher suites; the server rejected all cipher suites.
```

```
 * Session Renegotiation:
      Client Renegotiation DoS Attack:   OK - Not vulnerable
      Secure Renegotiation:              OK - Supported

 * TLS 1.3 Cipher Suites:
    Attempted to connect using 5 cipher suites; the server rejected all cipher suites.

 * OpenSSL CCS Injection:
                                         OK - Not vulnerable to OpenSSL CCS injection

 * TLS 1.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 * TLS 1.2 Session Resumption Support:
     With Session IDs: OK - Supported (5 successful resumptions out of 5 attempts).
     With TLS Tickets: OK - Supported.

 * Certificates Information:
      Hostname sent for SNI:             banks-sadler.com
      Number of certificates detected:   1


    Certificate #0 ( _RSAPublicKey )
      SHA1 Fingerprint:                  6dca04a7b144deb616e290b625de975f8cdf7598
      Common Name:                       banks-sadler.com
      Issuer:                            Sectigo RSA Domain Validation Secure Server CA
      Serial Number:                     721751687810033135453193857631581064l9
      Not Before:                        2021-06-03
      Not After:                         2022-06-03
      Public Key Algorithm:              _RSAPublicKey
      Signature Algorithm:               sha256
```

```
      Key Size:                          2048
      Exponent:                          65537
      DNS Subject Alternative Names:     ['banks-sadler.com', 'www.banks-sadler.com']

    Certificate #0 - Trust
      Hostname Validation:               OK - Certificate matches server hostname
      Android CA Store (9.0.0_r9):       OK - Certificate is trusted
      Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is trusted
      Java CA Store (jdk-13.0.2):        OK - Certificate is trusted
      Mozilla CA Store (2021-01-24):     OK - Certificate is trusted
      Windows CA Store (2021-02-08):     OK - Certificate is trusted
      Symantec 2018 Deprecation:         OK - Not a Symantec-issued certificate
      Received Chain:                    banks-sadler.com --> Sectigo RSA Domain Validation Secure Server
CA --> USERTrust RSA Certification Authority
      Verified Chain:                    banks-sadler.com --> Sectigo RSA Domain Validation Secure Server
CA --> USERTrust RSA Certification Authority
      Received Chain Contains Anchor:    OK - Anchor certificate not sent
      Received Chain Order:              OK - Order is valid
      Verified Chain contains SHA1:      OK - No SHA1-signed certificate in the verified certificate chain

    Certificate #0 - Extensions
      OCSP Must-Staple:                  NOT SUPPORTED - Extension not found
      Certificate Transparency:          OK - 3 SCTs included

    Certificate #0 - OCSP Stapling
                                         NOT SUPPORTED - Server did not send back an OCSP response

 * Deflate Compression:
                                         OK - Compression disabled
```

```
 * OpenSSL Heartbleed:
                                        OK - Not vulnerable to Heartbleed

 * SSL 3.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 * ROBOT Attack:
                                        OK - Not vulnerable.


 SCAN COMPLETED IN 51.88 S
 -------------------------
```

We can see Robot Attack, OpenSSL Heartbleed, OpenSSL CCS Injection, Downgrade attacks can not execute against to the website. That means to those attacks, the site is not vulnerable. That means the site is free from cipher issues.

CORS Misconfiguration test

```
└─$ python3 corsy.py -u https://www.banks-sadler.com/

    C O R S Y   {v1.0-beta}

 - No misconfigurations found.
```

No CORS misconfiguration on the website.

Open Redirection Vulnerability testing.

```
└─$
python3 oralyzer.py -u https://www.banks-sadler.com
   ____                  __
  / __ \_____  ____ _   / /_  ____ ___  ____
 / / / / ___/ / __ `/  / / / / / __ `__ \/ __ \
/ /_/ / /  _ / /_/ /  / / /_/ / / / / / / /_/ /
\____/_/  (_)\__,_/  /_/\__, /_/ /_/ /_/ .___/
                       /____/          /_/

[•] Appending payloads just after the URL
[•] Infusing payloads
[•] Header Based Redirection : https://www.banks-sadler.com/http://www.google.com ➤  https://www.banks-sadler.com/http:/www.google.com
[•] Header Based Redirection : https://www.banks-sadler.com/http%3A%2F%2Fwww.google.com ➤  https://www.banks-sadler.com/http:/www.google.com
[•] https://www.banks-sadler.com/https%3A%2F%2Fwww.google.com [404]
[•] Header Based Redirection : https://www.banks-sadler.com///www.google.com ➤  https://www.banks-sadler.com/www.google.com
[•] https://www.banks-sadler.com/https:www.google.com [404]
[•] https://www.banks-sadler.com/google.com [404]
[•] Header Based Redirection : https://www.banks-sadler.com//%5C/%5Cgoogle.com ➤  https://www.banks-sadler.com/%5C/%5Cgoogle.com
[•] Header Based Redirection : https://www.banks-sadler.com//%5C/google.com ➤  https://www.banks-sadler.com/%5C/google.com
[•] Header Based Redirection : https://www.banks-sadler.com/////google.com ➤  https://www.banks-sadler.com/google.com
[•] Header Based Redirection : https://www.banks-sadler.com/HtTP://google.com ➤  https://www.banks-sadler.com/HtTP:/google.com
[•] Header Based Redirection : https://www.banks-sadler.com/HTTP://google.com ➤  https://www.banks-sadler.com/HTTP:/google.com
[•] Header Based Redirection : https://www.banks-sadler.com/hTTp://google.com ➤  https://www.banks-sadler.com/hTTp:/google.com
```

```
[•] Header Based Redirection : https://www.banks-sadler.com/HtTPs://google.com ➤  https://www.banks-sadler.com/HtTPs:/google.com
[•] Header Based Redirection : https://www.banks-sadler.com/hthttp://tp://google.com ➤  https://www.banks-sadler.com/hthttp:/tp:/google.com
[•] Header Based Redirection : https://www.banks-sadler.com/x00http://google.com ➤  https://www.banks-sadler.com/x00http:/google.com
[•] Header Based Redirection : https://www.banks-sadler.com/%5Cx20http://google.com ➤  https://www.banks-sadler.com/%5Cx20http:/google.com
[•] https://www.banks-sadler.com/216.58.214.206 [404]
[•] https://www.banks-sadler.com/172.217.167.46 [404]
[•] Header Based Redirection : https://www.banks-sadler.com//216.58.214.206 ➤  https://www.banks-sadler.com/216.58.214.206
[•] Header Based Redirection : https://www.banks-sadler.com/////216.58.214.206 ➤  https://www.banks-sadler.com/216.58.214.206
[•] Header Based Redirection : https://www.banks-sadler.com//%5C216.58.214.206 ➤  https://www.banks-sadler.com/%5C216.58.214.206
[•] Header Based Redirection : https://www.banks-sadler.com///216.58.214.206 ➤  https://www.banks-sadler.com/216.58.214.206
[•] Header Based Redirection : https://www.banks-sadler.com////216.58.214.206 ➤  https://www.banks-sadler.com/216.58.214.206
[•] Header Based Redirection : https://www.banks-sadler.com///google%E3%80%82com ➤  https://www.banks-sadler.com/google%E3%80%82com
[•] Header Based Redirection : https://www.banks-sadler.com///google%E3%80%82com ➤  https://www.banks-sadler.com/google%E3%80%82com
[•] https://www.banks-sadler.com/http%5Cx3A%5Cx2F%5Cx2Fgoogle.com [404]
[•] Header Based Redirection : https://www.banks-sadler.com/////google.com/.. ➤  https://www.banks-sadler.com/google.com/
[•] Header Based Redirection : https://www.banks-sadler.com////google.com/.. ➤  https://www.banks-sadler.com/google.com/
[•] Header Based Redirection : https://www.banks-sadler.com///google.com/.. ➤  https://www.banks-sadler.com
```

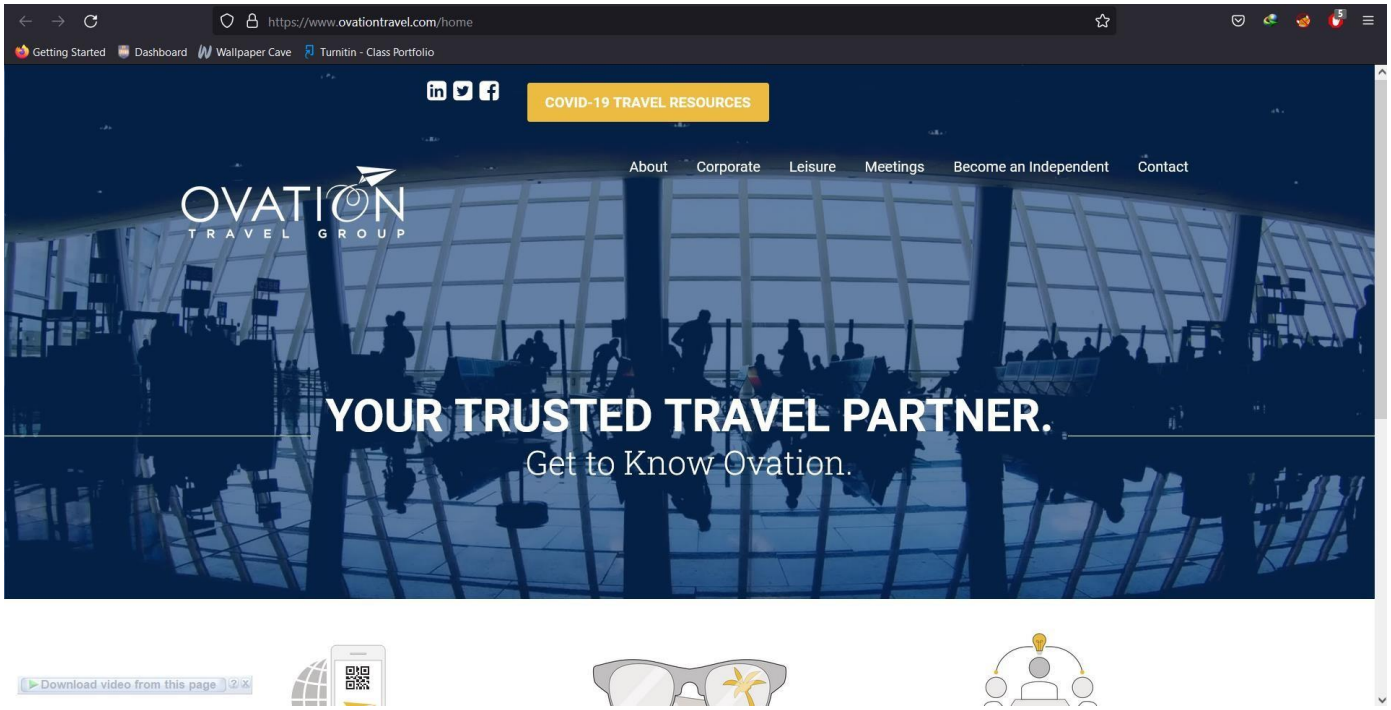
```
[•] Header Based Redirection : https://www.banks-sadler.com//google.com/.. ➤  https://www.banks-sadler.com/google.com/
[•] Header Based Redirection : https://www.banks-sadler.com///google.com/.. ➤  https://www.banks-sadler.com/google.com/
[•] Header Based Redirection : https://www.banks-sadler.com/////google.com/..%2F ➤  https://www.banks-sadler.com/google.com/
[•] Header Based Redirection : https://www.banks-sadler.com////google.com/..%2F ➤  https://www.banks-sadler.com/google.com/
[•] Header Based Redirection : https://www.banks-sadler.com///google.com/..%2F ➤  https://www.banks-sadler.com/google.com/
[•] https://www.banks-sadler.com/////google.com/%2F.. [404]
[•] https://www.banks-sadler.com////google.com/%2F.. [404]
[•] https://www.banks-sadler.com///google.com/%2F.. [404]
[•] https://www.banks-sadler.com///google.com/%2F.. [404]
[•] https://www.banks-sadler.com//google.com/%2F.. [404]
[•] https://www.banks-sadler.com/////google.com/%2F.. [404]
[•] https://www.banks-sadler.com////google.com/%2F.. [404]
[•] https://www.banks-sadler.com///google.com/%2F.. [404]
[•] https://www.banks-sadler.com//google.com/%2F.. [404]
[•] https://www.banks-sadler.com///google.com//%2F.. [404]
[•] Header Based Redirection : https://www.banks-sadler.com/http://%5B::ffff:216.58.214.206%5D ➤  https://www.banks-sadler.com/http:/%5B::ffff:216.58.214.206%5D
[•] https://www.banks-sadler.com/http:%5B::ffff:216.58.214.206%5D [404]
[•] Header Based Redirection : https://www.banks-sadler.com/http://00330.00072.0000326.00000316 ➤  https://www.banks-sadler.com/http:/00330.00072.0000326.00000316
[•] https://www.banks-sadler.com/http:00330.00072.0000326.00000316 [404]
[•] Header Based Redirection : https://www.banks-sadler.com/http://00330.0x3a.54990 ➤  https://www.banks-sadler.com/http:/00330.0x3a.54990
[•] https://www.banks-sadler.com/http:00330.0x3a.54990 [404]
[•] Header Based Redirection : https://www.banks-sadler.com/http://00330.3856078 ➤  https://www.banks-sadler.com/http:/00330.3856078
[•] https://www.banks-sadler.com/http:00330.3856078 [404]
```

```
[•] Header Based Redirection : https://www.banks-sadler.com/http://0330.072.0326.0316 ➤  https://www.banks-
sadler.com/http:/0330.072.0326.0316
[•] https://www.banks-sadler.com/http:0330.072.0326.0316 [404]
[•] https://www.banks-sadler.com/http:%0A%0D%E2%93%81%F0%9D%90%A8%F0%9D%97%B0%EF%BF%BD%F0%9D%95%9D%E2%85%86
%F0%9D%93%B8%E2%93%9C%E2%82%90%E2%84%B9%E2%93%83%EF%BD%A1%EF%BC%B0%E2%93%A6 [403]
[•] https://www.banks-sadler.com/http:%0A%0Dgoogle.com [403]
[•] Header Based Redirection : https://www.banks-sadler.com/http://0xd8.072.54990 ➤  https://www.banks-sadl
er.com/http:/0xd8.072.54990
[•] https://www.banks-sadler.com/http:0xd8.072.54990 [404]
[•] Header Based Redirection : https://www.banks-sadler.com/http://0xd8.0x3a.0xd6.0xce ➤  https://www.banks
-sadler.com/http:/0xd8.0x3a.0xd6.0xce
[•] https://www.banks-sadler.com/http:0xd8.0x3a.0xd6.0xce [404]
[•] Header Based Redirection : https://www.banks-sadler.com/http://0xd8.3856078 ➤  https://www.banks-sadler
.com/http:/0xd8.3856078
[•] https://www.banks-sadler.com/http:0xd8.3856078 [404]
[•] Header Based Redirection : https://www.banks-sadler.com/http://0xd83ad6ce ➤  https://www.banks-sadler.c
om/http:/0xd83ad6ce
[•] https://www.banks-sadler.com/http:0xd83ad6ce [404]
[•] Header Based Redirection : https://www.banks-sadler.com/http://%5B::216.58.214.206%5D ➤  https://www.ba
nks-sadler.com/http:/%5B::216.58.214.206%5D
[•] https://www.banks-sadler.com/http:%5B::216.58.214.206%5D [404]
```

By analyzing the report, we can see that the website is not vulnerable to Open Redirection Vulnerability since it gave the 404 error codes to the requests.

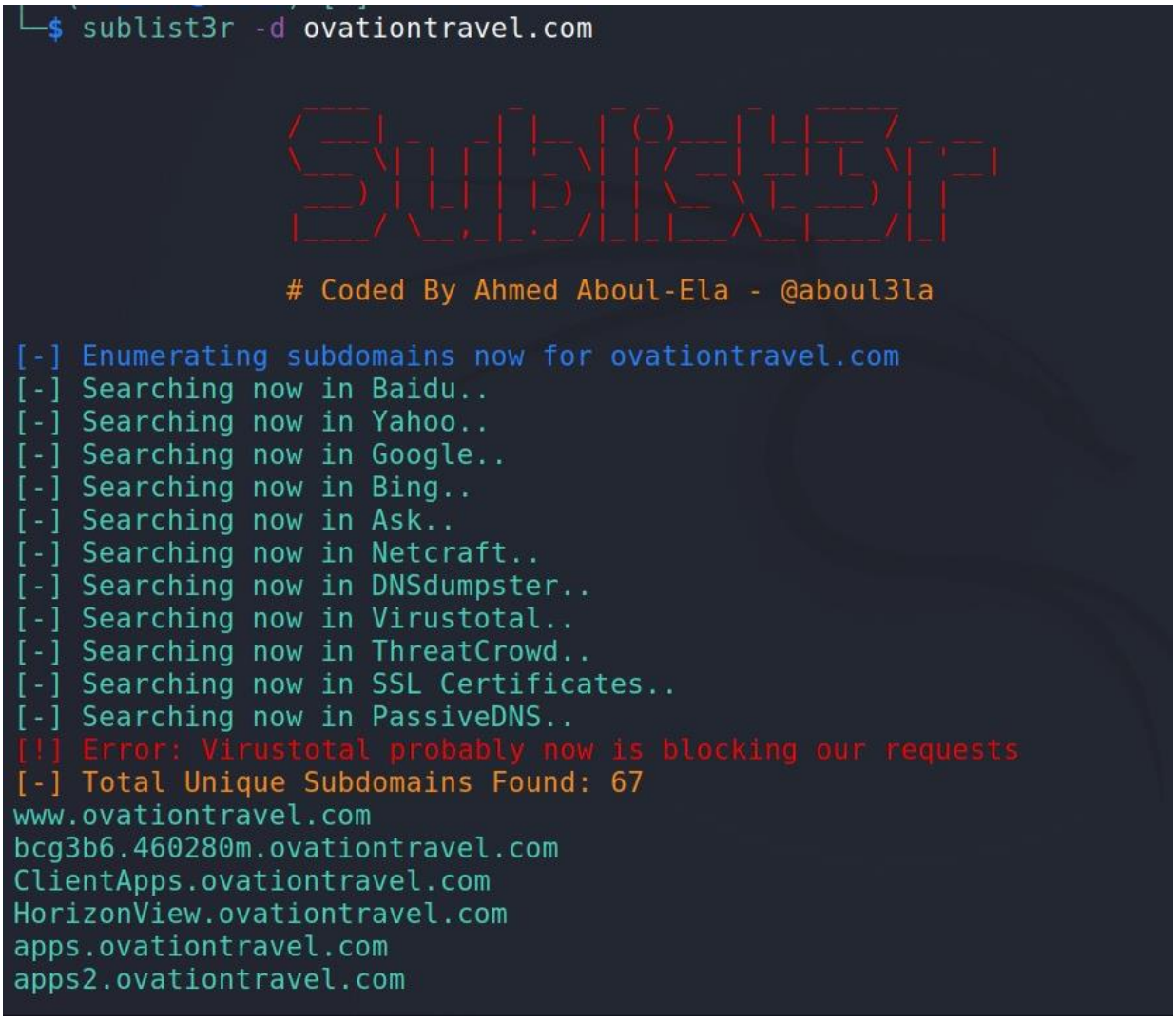
Subdomain 3

https://www.ovationtravel.com/home



Automated Scans

Sublist3r Scan

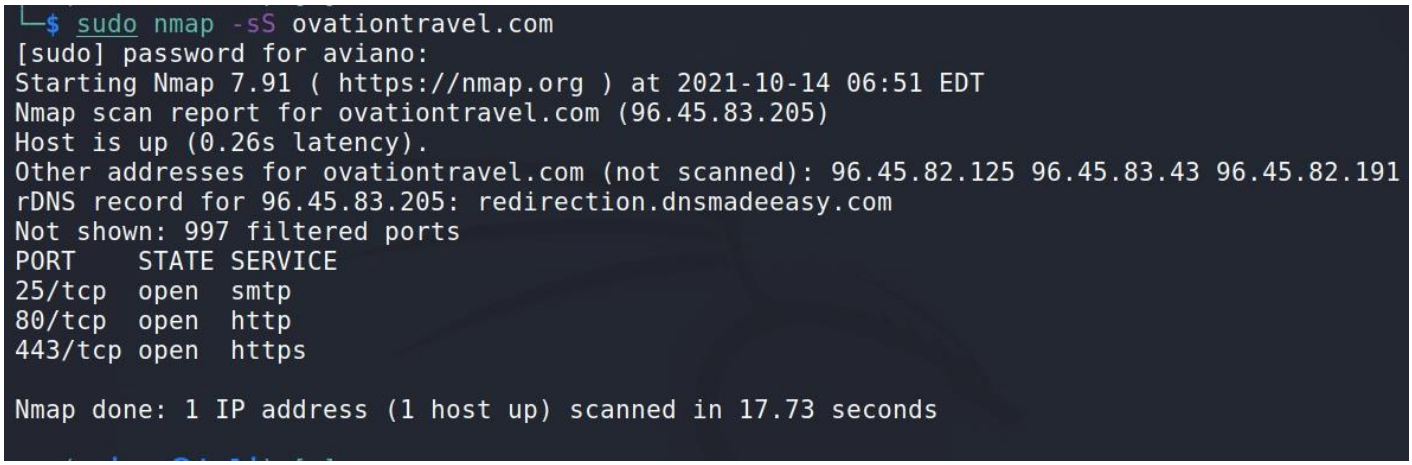


```
www.uat.atc.ovationtravel.com
autodiscover.ovationtravel.com
cdn.ovationtravel.com
commissions.ovationtravel.com
conman.ovationtravel.com
cpmconfig.ovationtravel.com
crm.ovationtravel.com
devportal.ovationtravel.com
enterpriseregistration.ovationtravel.com
forms.ovationtravel.com
ftp.ovationtravel.com
ftp99.ovationtravel.com
grouptravel.ovationtravel.com
in.ovationtravel.com
o1.info.ovationtravel.com
legacy.ovationtravel.com
login.ovationtravel.com
mail.ovationtravel.com
mail2.ovationtravel.com
mca.ovationtravel.com
media.ovationtravel.com
mydesktop.ovationtravel.com
nycmas1.ovationtravel.com
ols.ovationtravel.com
ovationapps.ovationtravel.com
ovationsurvey.ovationtravel.com
portal.ovationtravel.com
preferredhotels.ovationtravel.com
profiles.ovationtravel.com
pubapi.ovationtravel.com
rfp.ovationtravel.com
saks.ovationtravel.com
```

```
sccm.ovationtravel.com
secure.ovationtravel.com
secureflight.ovationtravel.com
seg.ovationtravel.com
sftp.ovationtravel.com
ssldfw.ovationtravel.com
sslvpn.ovationtravel.com
support.ovationtravel.com
svr-vdiconn-01.ovationtravel.com
svr-vdiconn-02.ovationtravel.com
tableau.ovationtravel.com
test.ovationtravel.com
travelportal.ovationtravel.com
travelportrcs.ovationtravel.com
traveltrax.ovationtravel.com
uca.ovationtravel.com
utt.ovationtravel.com
vdi.ovationtravel.com
vdiconn-01.ovationtravel.com
vdiconn-02.ovationtravel.com
vpn.ovationtravel.com
vpn2.ovationtravel.com
vpnch.ovationtravel.com
vpndfw.ovationtravel.com
vpnnyc.ovationtravel.com
webmail.ovationtravel.com
webmail2.ovationtravel.com
webman.ovationtravel.com
```

By scanning the subdomain using Sublist3r, I found total of 67 subdomains under ovationtravel.com.

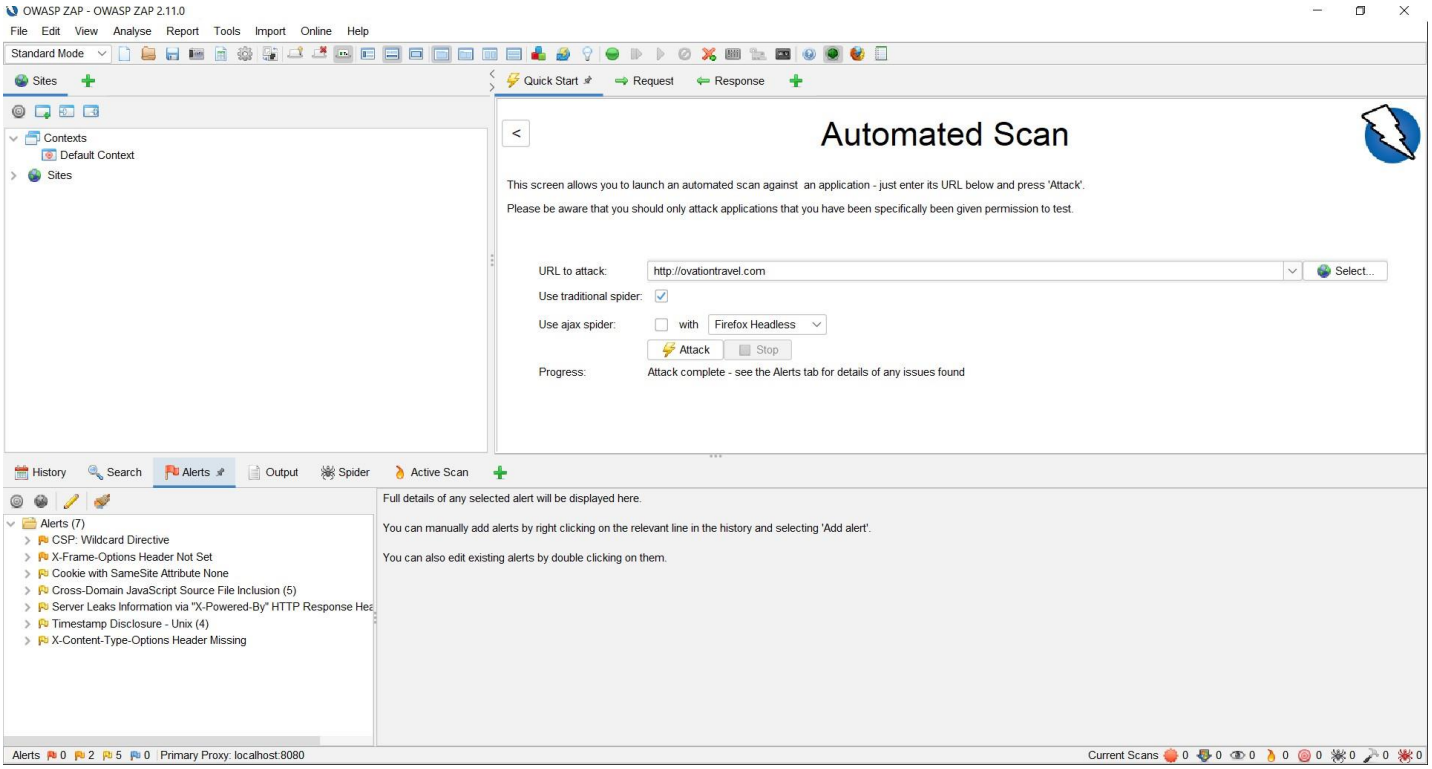
Nmap Scan



Found three open ports of ovationtravel.com,

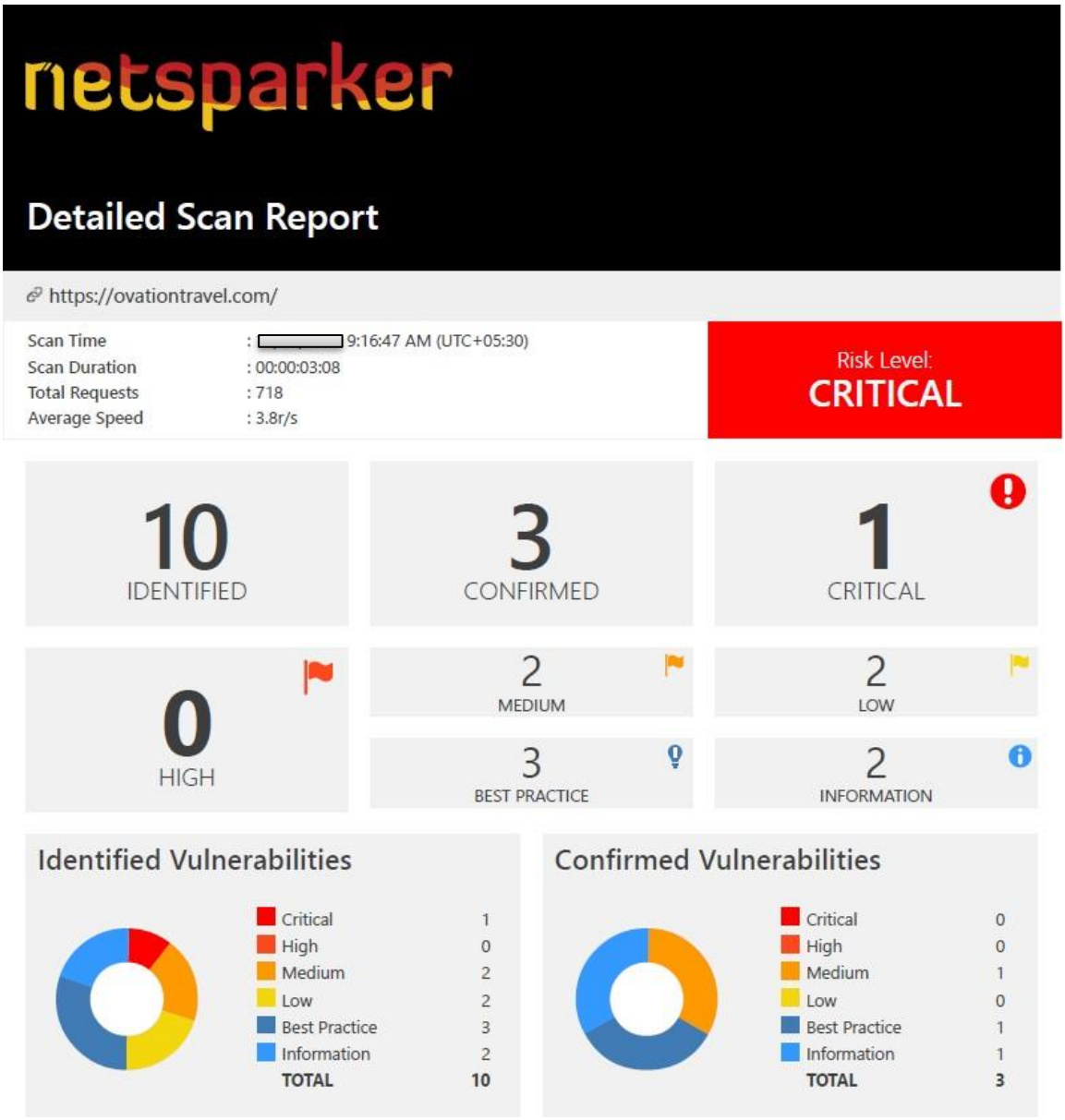
- Simple Mail Transport protocol (smtp)
- HTTP
- HTTPS

OWASP ZAP Scan



By doing an automated scan using OWASP ZAP I found seven (07) types of security flows/ vulnerabilities on the subdomain (http://www.ovationtravel.com). However, I did another scan using Netsparker for this subdomain and it gave me a well-defined report on vulnerabilities as shown below.

Netsparker Scan



Netsparker identified 10 total vulnerabilities of the website https://www.ovationtravel.com/home. Three vulnerabilities withing them are confirmed, and one critical vulnerability which still not confirmed was also detected by the scan. Overall risk severity level is in critical, which means the subdomain needs to fix vulnerabilities without consuming more time.

Vulnerability Summery

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Nginx)	HEAD	https://ovationtravel.com/opensearch	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://ovationtravel.com/	
	Weak Ciphers Enabled	GET	https://ovationtravel.com/	
	Missing X-Frame-Options Header	HEAD	https://ovationtravel.com/opensearch	
	Version Disclosure (Nginx)	HEAD	https://ovationtravel.com/opensearch	
	Expect-CT Not Enabled	GET	https://ovationtravel.com/	
	Missing X-XSS-Protection Header	HEAD	https://ovationtravel.com/opensearch	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://ovationtravel.com/	
	Nginx Web Server Identified	HEAD	https://ovationtravel.com/opensearch	
	Forbidden Resource	POST	https://ovationtravel.com/	

Confirmed Vulnerabilities in details

3. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

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.

Vulnerabilities

3.1. https://ovationtravel.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xC077)
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xC076)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00C0)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00BA)

Request

```
[NETSPARKER] SSL Connection
```

Response

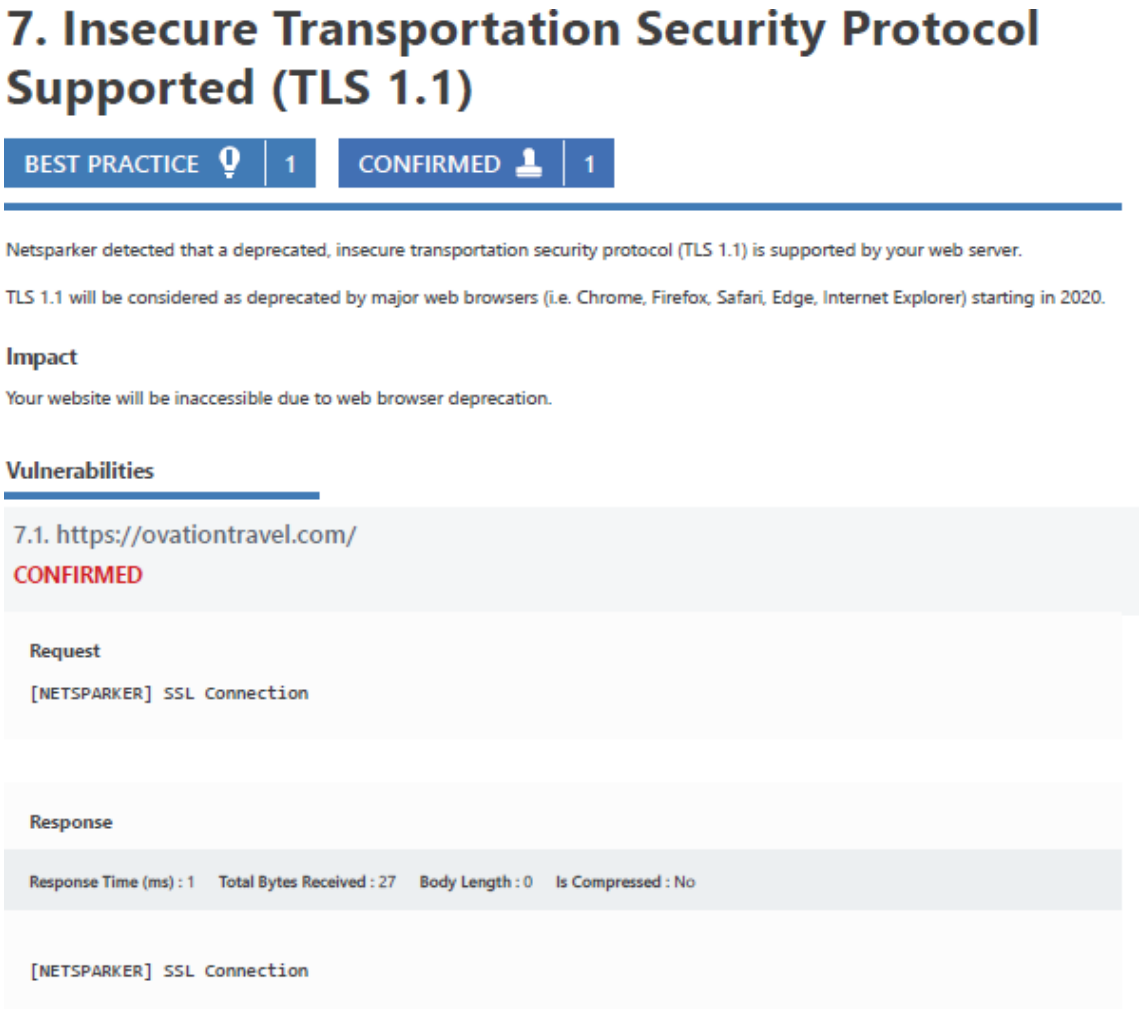
Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Same actions should take for this exact same vulnerability as I mentioned in the previous sub domain.

Remedy

The web server should configure to forbid use of weak ciphers.



7. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE 1 CONFIRMED 1

Netsparker detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge, Internet Explorer) starting in 2020.

Impact

Your website will be inaccessible due to web browser deprecation.

Vulnerabilities

7.1. https://ovationtravel.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Actions to take

Replace TLS 1.1 with TLS 1.2 or higher.

Remedy

Disallow to use weak ciphers by configuring the web server. To enable the changes that are applied, need to restart the web server.

- The SSLProtocol directive which provide by mod_ssl module for the Apache server should be adjust. SSLProtocal directive can be configure in virtual host or at server level.

```
SSLProtocol +TLSv1.2
```

- Detect any operate of directive ssl_protocols in nginx.conf file and disconnect TLSv1.1 for Nginx.

```
ssl_protocols TLSv1.2;
```

- Do few changes in system registry for Microsoft IIS. Configuring system registry in a wrong way is harmful to the system. Anyway prior to making changes, backing up of important data on the computer is important.

1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

3. Locate a key named `Server` or create if it doesn't exist.
4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".

- Put the below lines in to the configuration file for lighttpd.

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

9. Forbidden Resource

INFORMATION 1 | CONFIRMED 1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

9.1. https://ovationtravel.com/

CONFIRMED

Request

```
POST / HTTP/1.1
Host: ovationtravel.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 807.1782 Total Bytes Received : 705 Body Length : 555 Is Compressed : No

```
HTTP/1.1 403 Forbidden

Server: nginx/1.18.0
Connection: close
Content-Length: 555
Content-Type: text/html
Date: Wed, 13 Oct 2021 03:47:50 GMT

<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Unconfirmed Critical Vulnerabilities

1. Out-of-date Version (Nginx)

CRITICAL 1

Netsparker identified you are using an out-of-date version of Nginx.

Impact

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

Nginx Off-by-one Error Vulnerability

A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

Affected Versions

1.7.4 to 1.20.0

External References

- CVE-2021-23017

Vulnerabilities

1.1. https://ovationtravel.com/opensearch

Identified Version

- 1.18.0

Latest Version

- 1.21.3 (in this branch)

Vulnerability Database

- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Request

```
HEAD /opensearch HTTP/1.1
Host: ovationtravel.com
Accept: netsparker/check
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 845.591 Total Bytes Received : 172 Body Length : 0 Is Compressed : No

```
HTTP/1.1 503 Service Temporarily Unavailable
Server: nginx/1.18.0
Connection: close
Content-Length: 599
Content-Type: text/html
Date: Wed, 13 Oct 2021 03:46:56 GMT
```

Remedy

Nginx installation should be upgraded to the latest secure version.

Manual Scans

SSLyze Scan to inspect cipher strength

```
└─$
sslyze --regular ovationtravel.com

 CHECKING HOST(S) AVAILABILITY
 -----------------------------

   ovationtravel.com:443                       => 96.45.82.125



 SCAN RESULTS FOR OVATIONTRAVEL.COM:443 - 96.45.82.125
 -----------------------------------------------------

 * Certificates Information:
       Hostname sent for SNI:             ovationtravel.com
       Number of certificates detected:   1


     Certificate #0 ( _RSAPublicKey )
       SHA1 Fingerprint:                  50a9a2fbe8644882c612b8dadc8ded67e3feecd8
       Common Name:                       *.dnsmadeeasy.com
       Issuer:                            Sectigo RSA Domain Validation Secure Server CA
       Serial Number:                     128674998968921170630697350153431975050
       Not Before:                        2020-03-23
       Not After:                         2022-06-25
       Public Key Algorithm:              _RSAPublicKey
       Signature Algorithm:               sha256
       Key Size:                          2048
       Exponent:                          65537
```

```
      Key Size:                          2048
      Exponent:                          65537
      DNS Subject Alternative Names:     ['*.dnsmadeeasy.com', 'dnsmadeeasy.com']

    Certificate #0 - Trust
      Hostname Validation:               FAILED - Certificate does NOT match server hostname
      Android CA Store (9.0.0_r9):       OK - Certificate is trusted
      Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is trusted
      Java CA Store (jdk-13.0.2):        OK - Certificate is trusted
      Mozilla CA Store (2021-01-24):     OK - Certificate is trusted
      Windows CA Store (2021-02-08):     OK - Certificate is trusted
      Symantec 2018 Deprecation:         OK - Not a Symantec-issued certificate
      Received Chain:                    *.dnsmadeeasy.com --> USERTrust RSA Certification Authority --> S
ectigo RSA Domain Validation Secure Server CA --> AddTrust External CA Root
      Verified Chain:                    *.dnsmadeeasy.com --> Sectigo RSA Domain Validation Secure Server
 CA --> USERTrust RSA Certification Authority
      Received Chain Contains Anchor:    OK - Anchor certificate not sent
      Received Chain Order:              FAILED - Certificate chain out of order!
      Verified Chain contains SHA1:      OK - No SHA1-signed certificate in the verified certificate chain

    Certificate #0 - Extensions
      OCSP Must-Staple:                  NOT SUPPORTED - Extension not found
      Certificate Transparency:          OK - 4 SCTs included

    Certificate #0 - OCSP Stapling
                                         NOT SUPPORTED - Server did not send back an OCSP response

 * OpenSSL CCS Injection:
                                         OK - Not vulnerable to OpenSSL CCS injection

 * SSL 2.0 Cipher Suites:
    Attempted to connect using 7 cipher suites; the server rejected all cipher suites.
```

```
 * TLS 1.2 Session Resumption Support:
     With Session IDs: OK - Supported (5 successful resumptions out of 5 attempts).
     With TLS Tickets: OK - Supported.

 * ROBOT Attack:
                                         OK - Not vulnerable.

 * Elliptic Curve Key Exchange:
      Supported curves:                  X25519, X448, prime256v1, secp384r1, secp521r1
      Rejected curves:                   prime192v1, secp160k1, secp160r1, secp160r2, secp192k1, secp224k1
, secp224r1, secp256k1, sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1, sect233r1, sect23
9k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1

 * SSL 3.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 * TLS 1.1 Cipher Suites:
    Attempted to connect using 80 cipher suites.

    The server accepted the following 6 cipher suites:
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                256
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                128
       TLS_RSA_WITH_AES_256_CBC_SHA                     256
       TLS_RSA_WITH_AES_128_CBC_SHA                     128
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA               256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA               128       ECDH: prime256v1 (256 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                  OK - Supported
      Legacy RC4 Algorithm             OK - Not Supported
```

```
* Downgrade Attacks:
      TLS_FALLBACK_SCSV:                OK - Supported

* TLS 1.3 Cipher Suites:
    Attempted to connect using 5 cipher suites; the server rejected all cipher suites.

* OpenSSL Heartbleed:
                                        OK - Not vulnerable to Heartbleed

* TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites.

    The server accepted the following 27 cipher suites:
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256              256
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 256
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256              128
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 128
       TLS_RSA_WITH_ARIA_256_GCM_SHA384                  256
       TLS_RSA_WITH_ARIA_128_GCM_SHA256                  128
       TLS_RSA_WITH_AES_256_GCM_SHA384                   256
       TLS_RSA_WITH_AES_256_CCM_8                        128
       TLS_RSA_WITH_AES_256_CCM                          256
       TLS_RSA_WITH_AES_256_CBC_SHA256                   256
       TLS_RSA_WITH_AES_256_CBC_SHA                      256
       TLS_RSA_WITH_AES_128_GCM_SHA256                   128
       TLS_RSA_WITH_AES_128_CCM_8                        128
       TLS_RSA_WITH_AES_128_CCM                          128
       TLS_RSA_WITH_AES_128_CBC_SHA256                   128
       TLS_RSA_WITH_AES_128_CBC_SHA                      128
       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256       256       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384        256       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256        128       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384            256       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256            128       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384             256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384             256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256             128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256             128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1 (256 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                   OK - Supported
      Legacy RC4 Algorithm              OK - Not Supported


* Session Renegotiation:
      Client Renegotiation DoS Attack:  OK - Not vulnerable
      Secure Renegotiation:             OK - Supported

* TLS 1.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* Deflate Compression:
                                        OK - Compression disabled


SCAN COMPLETED IN 68.80 S
-------------------------
```

According to the report it has identified the website is not vulnerable to ROBOT Attack, OpenSSL Heartbleed, OpenSSL CCS Injection, Client Renegotiation DoS attack, an Downgrade attacks.

CORS Misconfiguration test

No CORS misconfiguration detected.

Open Redirection Vulnerability testing.

```
└─$ python3 corsy.py -u https://www.ovationtravel.com/home

    C O R S Y   {v1.0-beta}

 - No misconfigurations found.
```

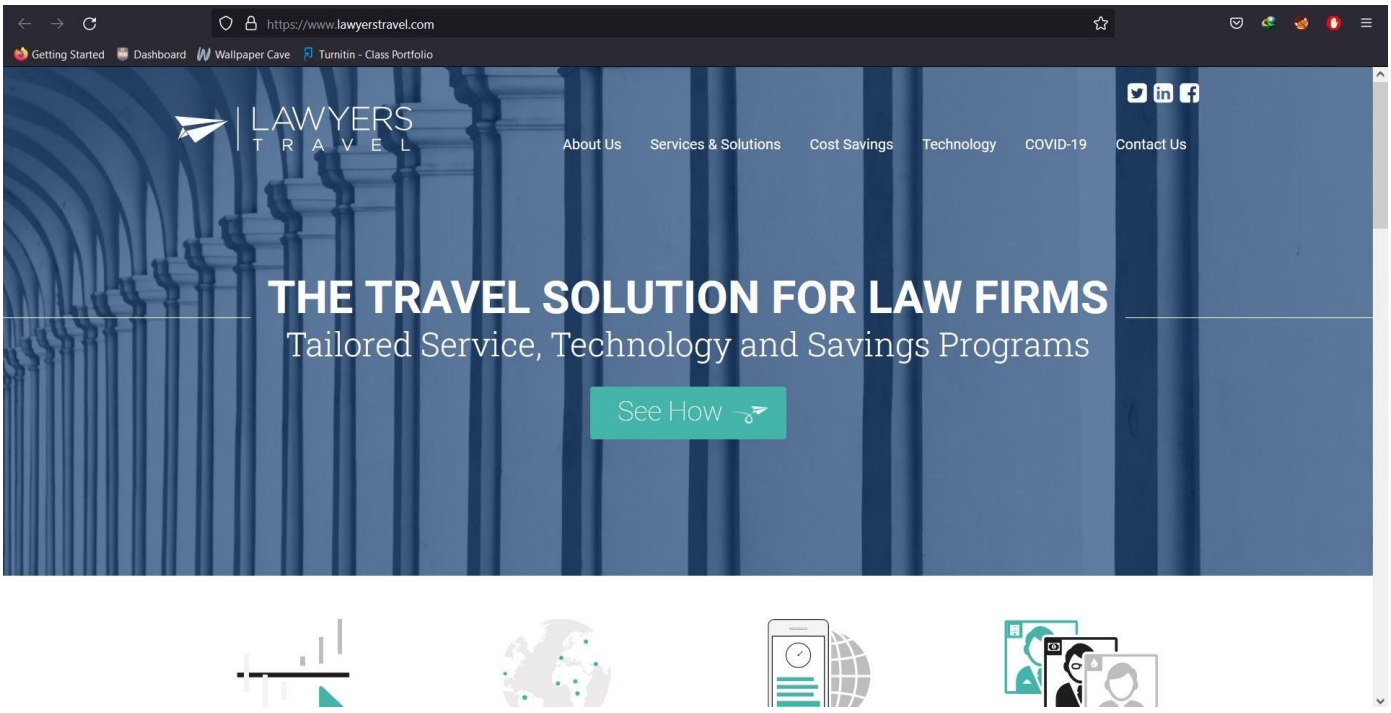
```
└─$ python3 oralyzer.py -u https://www.ovationtravel.com/home
   _____                  __
  / ___ \_______ _/ /_ _____ ___ ____
 / /_/ / __/ _ `/ / // / _ // -_) __/
 \____/_/  \_,_/_/\_, //__/\__/_/
                 /___/

[•] Appending payloads just after the URL
[•] Infusing payloads
[•] https://www.ovationtravel.com/home/http://www.google.com [404]
[•] https://www.ovationtravel.com/home/http%3A%2F%2Fwww.google.com [404]
[•] https://www.ovationtravel.com/home/https%3A%2F%2Fwww.google.com [404]
[•] https://www.ovationtravel.com/home///www.google.com [404]
[•] https://www.ovationtravel.com/home/https:www.google.com [404]
[•] https://www.ovationtravel.com/home/google.com [404]
[•] https://www.ovationtravel.com/home//%5C/%5Cgoogle.com [404]
[•] https://www.ovationtravel.com/home//%5C/google.com [404]
[•] https://www.ovationtravel.com/home/////google.com [404]
[•] https://www.ovationtravel.com/home/HtTP://google.com [404]
[•] https://www.ovationtravel.com/home/HTTP://google.com [404]
[•] https://www.ovationtravel.com/home/hTTp://google.com [404]
[•] https://www.ovationtravel.com/home/HtTPs://google.com [404]
[•] https://www.ovationtravel.com/home/hthttp://tp://google.com [404]
[•] https://www.ovationtravel.com/home/x00http://google.com [404]
[•] https://www.ovationtravel.com/home/%5Cx20http://google.com [404]
[•] https://www.ovationtravel.com/home/216.58.214.206 [404]
[•] https://www.ovationtravel.com/home/172.217.167.46 [404]
[•] https://www.ovationtravel.com/home//216.58.214.206 [404]
[•] https://www.ovationtravel.com/home/////216.58.214.206 [404]
[•] https://www.ovationtravel.com/home//%5C216.58.214.206 [404]
```

```
[•] https://www.ovationtravel.com/home///216.58.214.206 [404]
[•] https://www.ovationtravel.com/home////216.58.214.206 [404]
[•] https://www.ovationtravel.com/home///google%E3%80%82com [404]
[•] https://www.ovationtravel.com/home///google%E3%80%82com [404]
[•] https://www.ovationtravel.com/home/http%5Cx3A%5Cx2F%5Cx2Fgoogle.com [404]
[•] Header Based Redirection : https://www.ovationtravel.com/home/////google.com/.. ➤  https://www.ovationt
ravel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home////google.com/.. ➤  https://www.ovationtr
avel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home///google.com/.. ➤  https://www.ovationtra
vel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home//google.com/.. ➤  https://www.ovationtrav
el.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home///google.com/.. ➤  https://www.ovationtra
vel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home/////google.com/..%2F ➤  https://www.ovati
ontravel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home////google.com/..%2F ➤  https://www.ovatio
ntravel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home///google.com/..%2F ➤  https://www.ovation
travel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home/////google.com/%2F.. ➤  https://www.ovati
ontravel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home////google.com/%2F.. ➤  https://www.ovatio
ntravel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home///google.com/%2F.. ➤  https://www.ovation
travel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home///google.com/%2F.. ➤  https://www.ovation
travel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home//google.com/%2F.. ➤  https://www.ovationt
ravel.com/home
ontravel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home////google.com/%2F.. ➤  https://www.ovatio
ntravel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home///google.com/%2F.. ➤  https://www.ovation
travel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home//google.com/%2F.. ➤  https://www.ovationt
ravel.com/home
[•] Header Based Redirection : https://www.ovationtravel.com/home///google.com//%2F.. ➤  https://www.ovatio
ntravel.com/home
[•] https://www.ovationtravel.com/home/http://%5B::ffff:216.58.214.206%5D [404]
[•] https://www.ovationtravel.com/home/http:%5B::ffff:216.58.214.206%5D [404]
[•] https://www.ovationtravel.com/home/http://00330.00072.0000326.00000316 [404]
[•] https://www.ovationtravel.com/home/http:00330.00072.0000326.00000316 [404]
[•] https://www.ovationtravel.com/home/http://00330.0x3a.54990 [404]
[•] https://www.ovationtravel.com/home/http:00330.0x3a.54990 [404]
[•] https://www.ovationtravel.com/home/http://00330.3856078 [404]
[•] https://www.ovationtravel.com/home/http:00330.3856078 [404]
[•] https://www.ovationtravel.com/home/http://0330.072.0326.0316 [404]
[•] https://www.ovationtravel.com/home/http:0330.072.0326.0316 [404]
[•] https://www.ovationtravel.com/home/http:%0A%0D%E2%93%81%F0%9D%90%A8%F0%9D%97%B0%EF%BF%BD%F0%9D%95%9D%E2
%85%86%F0%9D%93%B8%E2%93%9C%E2%82%90%E2%84%B9%E2%93%83%EF%BD%A1%EF%BC%B0%E2%93%A6 [404]
[•] https://www.ovationtravel.com/home/http:%0A%0Dgoogle.com [404]
[•] https://www.ovationtravel.com/home/http://0xd8.072.54990 [404]
[•] https://www.ovationtravel.com/home/http:0xd8.072.54990 [404]
[•] https://www.ovationtravel.com/home/http://0xd8.0x3a.0xd6.0xce [404]
[•] https://www.ovationtravel.com/home/http:0xd8.0x3a.0xd6.0xce [404]
[•] https://www.ovationtravel.com/home/http://0xd8.3856078 [404]
[•] https://www.ovationtravel.com/home/http:0xd8.3856078 [404]
[•] https://www.ovationtravel.com/home/http://0xd83ad6ce [404]
[•] https://www.ovationtravel.com/home/http:0xd83ad6ce [404]
[•] https://www.ovationtravel.com/home/http://%5B::216.58.214.206%5D [404]
[•] https://www.ovationtravel.com/home/http:%5B::216.58.214.206%5D [404]
```

The site is not vulnerable to Open Redirection.

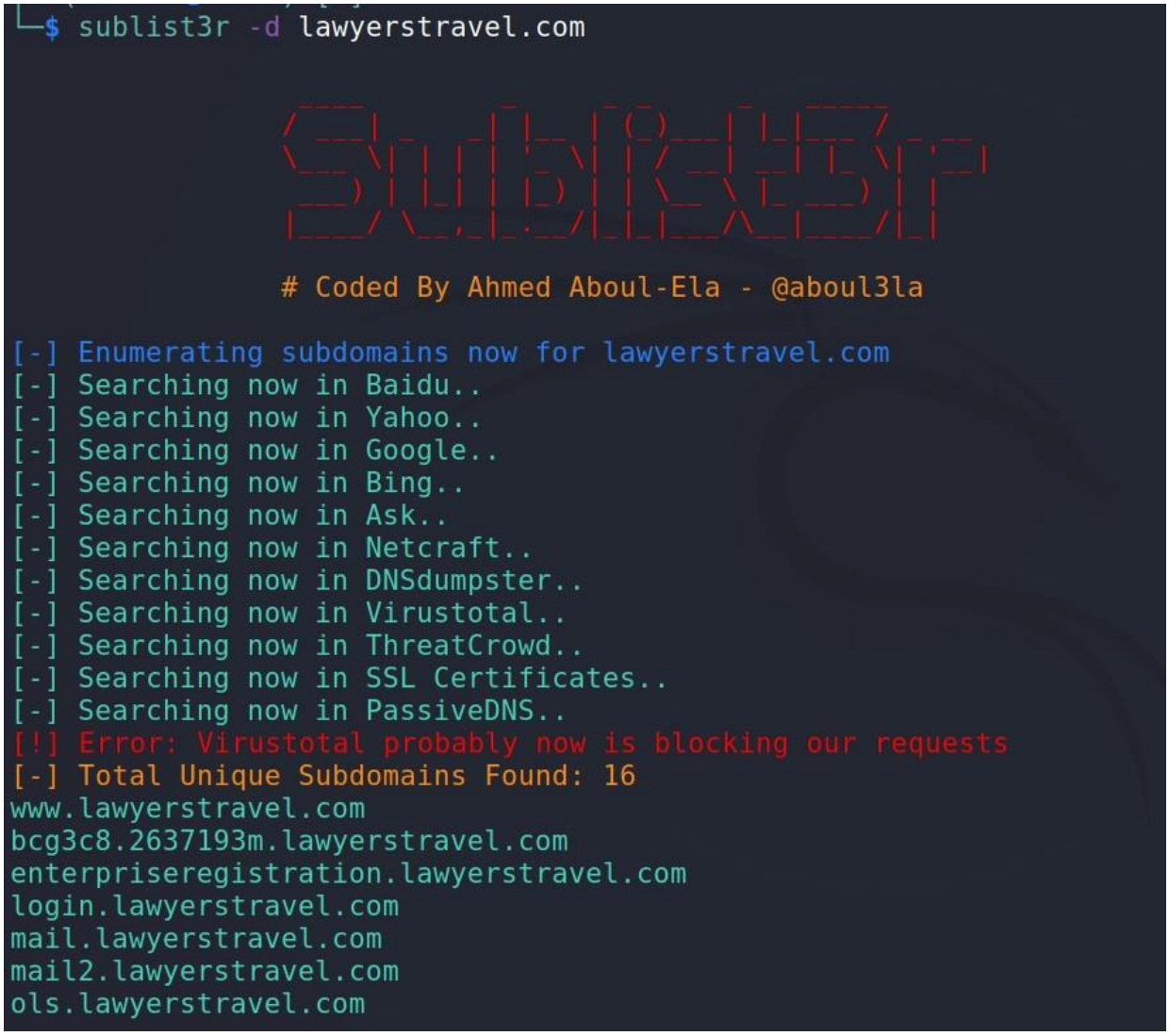
Subdomain 4

https://www.lawyerstravel.com/



Automated Scans

Sublist3r Scan



```
portal.lawyerstravel.com
preferredhotels.lawyerstravel.com
profiles.lawyerstravel.com
secureflight.lawyerstravel.com
smtp.lawyerstravel.com
tableau.lawyerstravel.com
travelportal.lawyerstravel.com
travelportrcs.lawyerstravel.com
traveltrax.lawyerstravel.com
```

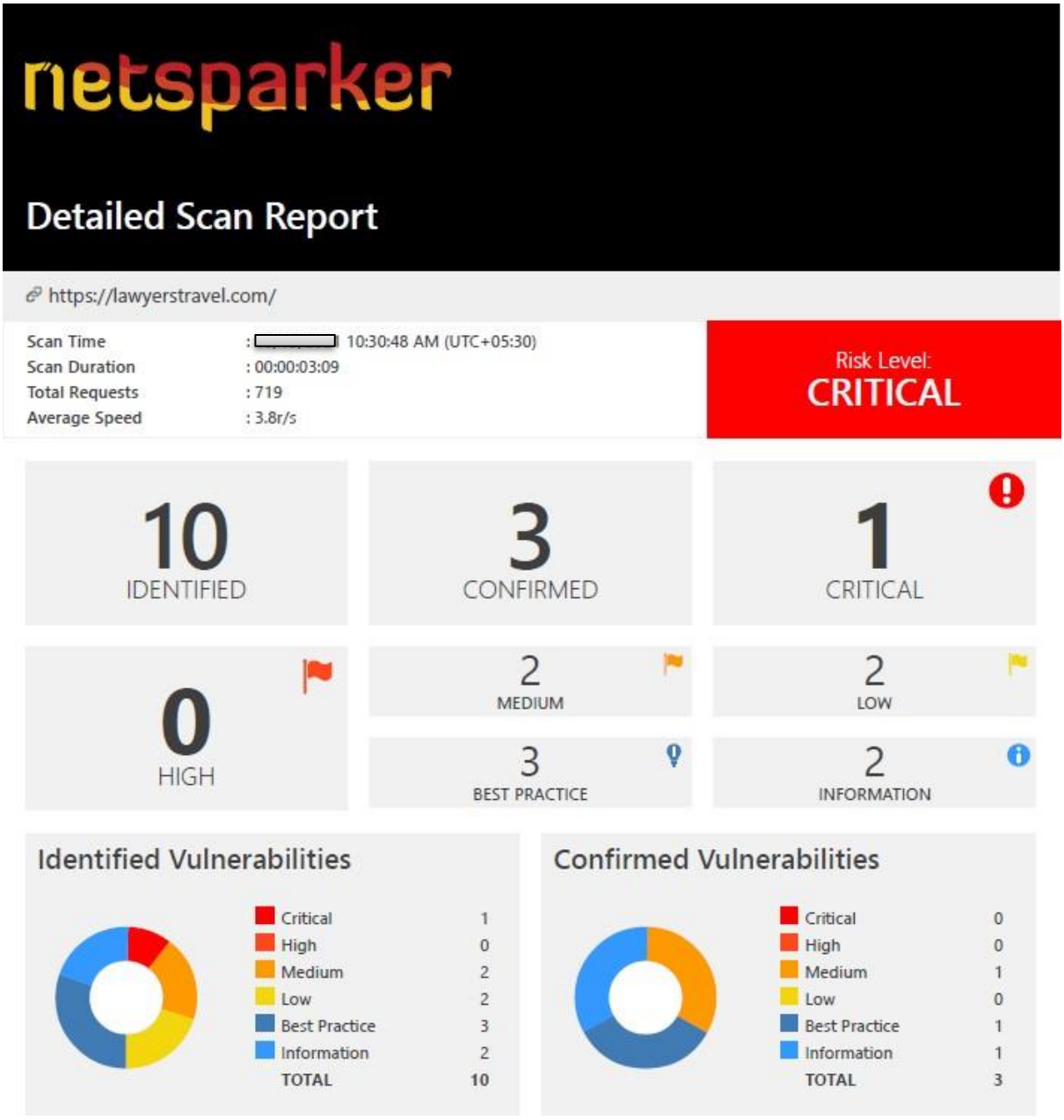
From this scan, I found sixteen subdomains under the lawyerstravel.com

Nmap Scan

```
└─$ sudo nmap -sS lawyerstravel.com
[sudo] password for aviano:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-14 09:31 EDT
Nmap scan report for lawyerstravel.com (96.45.83.205)
Host is up (0.27s latency).
Other addresses for lawyerstravel.com (not scanned): 96.45.83.43 96.45.82.125 96.45.82.191
rDNS record for 96.45.83.205: redirection.dnsmadeeasy.com
Not shown: 997 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 18.34 seconds
```

There are three open ports (smtp, http, https) have been identified using Nmap scan.

Netsparker Scan



According to the record generated for the automated scan for https://www.lawyerstravel.com/ website by Netsparker, there are total of 10 vulnerabilities have identified. Three of them are confirmed while one unconfirmed vulnerability detected as critical. The overall risk severity level is critical.

Vulnerability Summery

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Nginx)	HEAD	https://lawyerstravel.com/opensearch	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://lawyerstravel.com/	
	Weak Ciphers Enabled	GET	https://lawyerstravel.com/	
	Missing X-Frame-Options Header	HEAD	https://lawyerstravel.com/opensearch	
	Version Disclosure (Nginx)	HEAD	https://lawyerstravel.com/opensearch	
	Expect-CT Not Enabled	GET	https://lawyerstravel.com/	
	Missing X-XSS-Protection Header	HEAD	https://lawyerstravel.com/opensearch	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://lawyerstravel.com/	
	Nginx Web Server Identified	HEAD	https://lawyerstravel.com/opensearch	
	Forbidden Resource	POST	https://lawyerstravel.com/	

Confirmed Vulnerabilities in details.

3. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

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.

Vulnerabilities

3.1. https://lawyerstravel.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xC077)
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xC076)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00C0)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00BA)

Request

```
[NETSPARKER] SSL Connection
```

Response

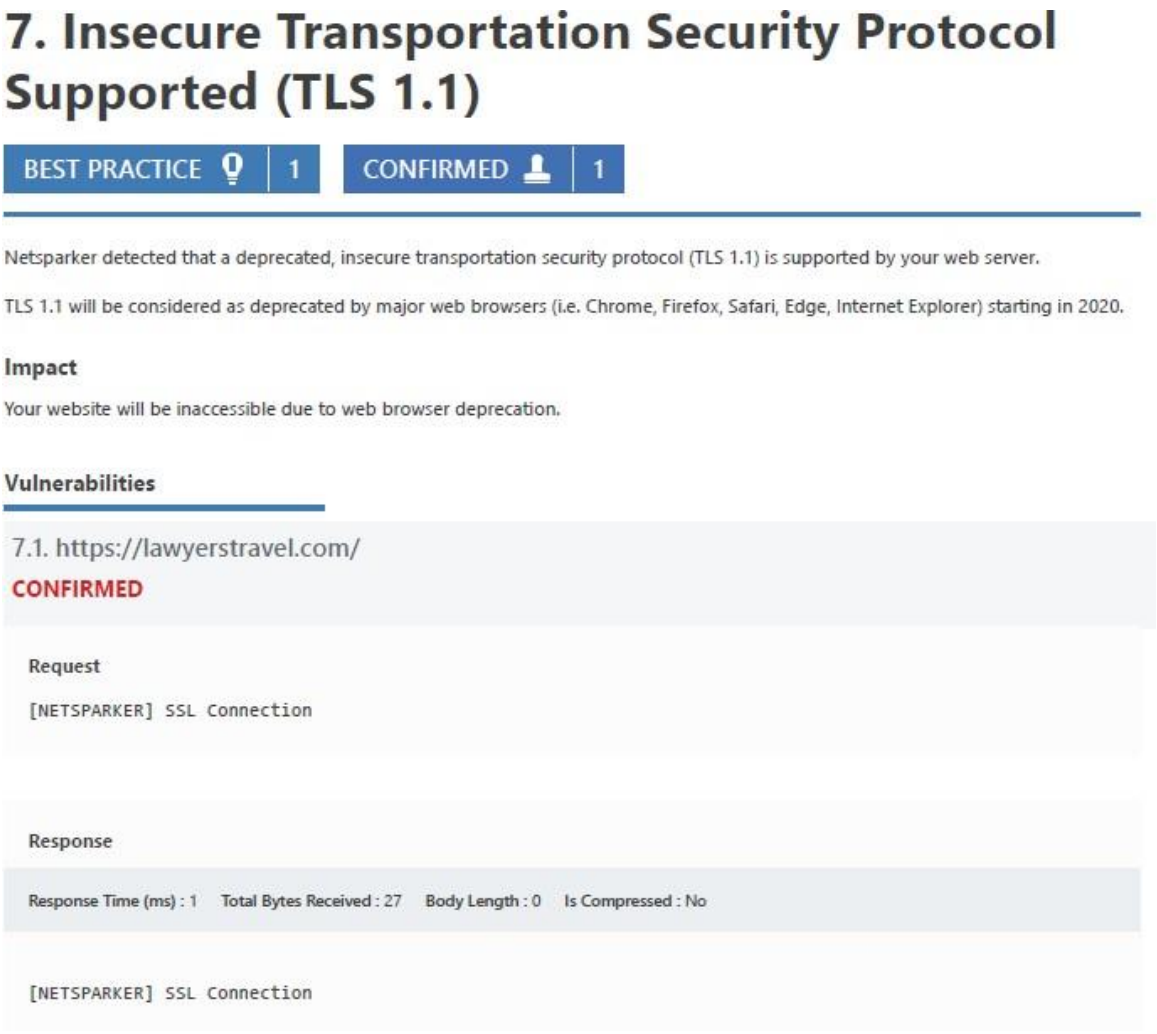
Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Actions to take in this kind of situation, I have mentioned under the same vulnerability in previous subdomain.

Remedy

Configure the web server to refuse use of weak ciphers.



7. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE | 1 | CONFIRMED | 1

Netsparker detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge, Internet Explorer) starting in 2020.

Impact

Your website will be inaccessible due to web browser deprecation.

Vulnerabilities

7.1. https://lawyerstravel.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Actions to take

- Replace TLS 1.1 with TLS 1.2 or later version.

Remedy

(Mentioned previously also. Rewrote this for easy access)

Disallow to use weak ciphers by configuring the web server. To enable the changes that are applied, need to restart the web server.

- The SSLProtocol directive which provide by mod_ssl module for the Apache server should be adjust. SSLProtocal directive can be configure in virtual host or at server level.

```
SSLProtocol +TLSv1.2
```

- Detect any operate of directive ssl_protocols in nginx.conf file and disconnect TLSv1.1 for Nginx.

```
ssl_protocols TLSv1.2;
```

- Do few changes in system registry for Microsoft IIS. Configuring system registry in a wrong way is harmful to the system. Anyway prior to making changes, backing up of important data on the computer is important.

1. Click on Start and then Run, type `regedt32`or `regedit`, and then click OK.
2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

3. Locate a key named `Server`or create if it doesn't exist.
4. Under the `Server`key, locate a DWORD value named `Enabled`or create if it doesn't exist and set its value to "0".

- Put the below lines in to the configuration file for lighttpd.

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

Unconfirmed Critical Vulnerabilities

1. Out-of-date Version (Nginx)

CRITICAL 1

Netsparker identified you are using an out-of-date version of Nginx.

Impact

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

Nginx Off-by-one Error Vulnerability

A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

Affected Versions

1.7.4 to 1.20.0

External References

- CVE-2021-23017

Vulnerabilities

1.1. https://lawyerstravel.com/opensearch

Identified Version

- 1.18.0

Latest Version

- 1.21.3 (in this branch)

Vulnerability Database

- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Request

```
HEAD /opensearch HTTP/1.1
Host: lawyerstravel.com
Accept: netsparker/check
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 812.8782 Total Bytes Received : 172 Body Length : 0 Is Compressed : No

```
HTTP/1.1 503 Service Temporarily Unavailable
Server: nginx/1.18.0
Connection: close
Content-Length: 599
Content-Type: text/html
Date: Wed, 13 Oct 2021 05:00:57 GMT
```

Remedy

Nginx installation should upgrade to the stable latest version.

Manual Scans

SSLyze Scan to inspect cipher strength

```
└─$ sslyze --regular lawyerstravel.com

CHECKING HOST(S) AVAILABILITY
-----------------------------

  lawyerstravel.com:443                       => 96.45.83.43



SCAN RESULTS FOR LAWYERSTRAVEL.COM:443 - 96.45.83.43
---------------------------------------------------

* Deflate Compression:
                                     OK - Compression disabled

* OpenSSL Heartbleed:
                                     OK - Not vulnerable to Heartbleed

* TLS 1.3 Cipher Suites:
    Attempted to connect using 5 cipher suites; the server rejected all cipher suites.

* SSL 3.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* Downgrade Attacks:
      TLS_FALLBACK_SCSV:             OK - Supported

* TLS 1.2 Session Resumption Support:
     With Session IDs: OK - Supported (5 successful resumptions out of 5 attempts).
```

```
* TLS 1.2 Session Resumption Support:
     With Session IDs: OK - Supported (5 successful resumptions out of 5 attempts).
     With TLS Tickets: OK - Supported.

* OpenSSL CCS Injection:
                                       OK - Not vulnerable to OpenSSL CCS injection

* TLS 1.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites.

    The server accepted the following 27 cipher suites:
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256              256
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 256
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256              128
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 128
       TLS_RSA_WITH_ARIA_256_GCM_SHA384                  256
       TLS_RSA_WITH_ARIA_128_GCM_SHA256                  128
       TLS_RSA_WITH_AES_256_GCM_SHA384                   256
       TLS_RSA_WITH_AES_256_CCM_8                        128
       TLS_RSA_WITH_AES_256_CCM                          256
       TLS_RSA_WITH_AES_256_CBC_SHA256                   256
       TLS_RSA_WITH_AES_256_CBC_SHA                      256
       TLS_RSA_WITH_AES_128_GCM_SHA256                   128
       TLS_RSA_WITH_AES_128_CCM_8                        128
       TLS_RSA_WITH_AES_128_CCM                          128
       TLS_RSA_WITH_AES_128_CBC_SHA256                   128
       TLS_RSA_WITH_AES_128_CBC_SHA                      128
       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256       256       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384        256       ECDH: X25519 (253 bits)
```

```
       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256       256       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384        256       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256        128       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384            256       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256            128       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384             256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384             256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256             128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256             128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1 (256 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                   OK - Supported
      Legacy RC4 Algorithm              OK - Not Supported


* Session Renegotiation:
      Client Renegotiation DoS Attack:   OK - Not vulnerable
      Secure Renegotiation:              OK - Supported

* ROBOT Attack:
                                        OK - Not vulnerable.

* TLS 1.1 Cipher Suites:
    Attempted to connect using 80 cipher suites.

    The server accepted the following 6 cipher suites:
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 256
       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 128
       TLS_RSA_WITH_AES_256_CBC_SHA                      256
       TLS_RSA_WITH_AES_128_CBC_SHA                      128
```

```
       TLS_RSA_WITH_AES_256_CBC_SHA                    256
       TLS_RSA_WITH_AES_128_CBC_SHA                    128
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA              256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA              128       ECDH: prime256v1 (256 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                   OK - Supported
      Legacy RC4 Algorithm              OK - Not Supported


* Certificates Information:
      Hostname sent for SNI:            lawyerstravel.com
      Number of certificates detected:  1


    Certificate #0 ( _RSAPublicKey )
      SHA1 Fingerprint:                 50a9a2fbe8644882c612b8dadc8ded67e3feecd8
      Common Name:                      *.dnsmadeeasy.com
      Issuer:                           Sectigo RSA Domain Validation Secure Server CA
      Serial Number:                    128674998968921170630697350153431975050
      Not Before:                       2020-03-23
      Not After:                        2022-06-25
      Public Key Algorithm:             _RSAPublicKey
      Signature Algorithm:              sha256
      Key Size:                         2048
      Exponent:                         65537
      DNS Subject Alternative Names:    ['*.dnsmadeeasy.com', 'dnsmadeeasy.com']

    Certificate #0 - Trust
      Hostname Validation:              FAILED - Certificate does NOT match server hostname
      Android CA Store (9.0.0_r9):      OK - Certificate is trusted
      Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is trusted
```

```
      Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is trusted
      Java CA Store (jdk-13.0.2):       OK - Certificate is trusted
      Mozilla CA Store (2021-01-24):    OK - Certificate is trusted
      Windows CA Store (2021-02-08):    OK - Certificate is trusted
      Symantec 2018 Deprecation:        OK - Not a Symantec-issued certificate
      Received Chain:                   *.dnsmadeeasy.com --> USERTrust RSA Certification Authority --> S
ectigo RSA Domain Validation Secure Server CA --> AddTrust External CA Root
      Verified Chain:                   *.dnsmadeeasy.com --> Sectigo RSA Domain Validation Secure Server
 CA --> USERTrust RSA Certification Authority
      Received Chain Contains Anchor:   OK - Anchor certificate not sent
      Received Chain Order:             FAILED - Certificate chain out of order!
      Verified Chain contains SHA1:     OK - No SHA1-signed certificate in the verified certificate chain

    Certificate #0 - Extensions
      OCSP Must-Staple:                 NOT SUPPORTED - Extension not found
      Certificate Transparency:         OK - 4 SCTs included

    Certificate #0 - OCSP Stapling
                                        NOT SUPPORTED - Server did not send back an OCSP response

 * Elliptic Curve Key Exchange:
      Supported curves:                 X25519, X448, prime256v1, secp384r1, secp521r1
      Rejected curves:                  prime192v1, secp160k1, secp160r1, secp160r2, secp192k1, secp224k1
, secp224r1, secp256k1, sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1, sect233r1, sect23
9k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1

 * SSL 2.0 Cipher Suites:
    Attempted to connect using 7 cipher suites; the server rejected all cipher suites.


 SCAN COMPLETED IN 65.13 S
 -------------------------
```

Not Vulnerable to ROBOT Attack, Session Renegotiation, OpenSSL CCS Injection, Downgrade Attacks, and OpenSSL Heartbeat.

CORS Misconfiguration test

No CORS misconfiguration detected.

Open Redirection Vulnerability testing.

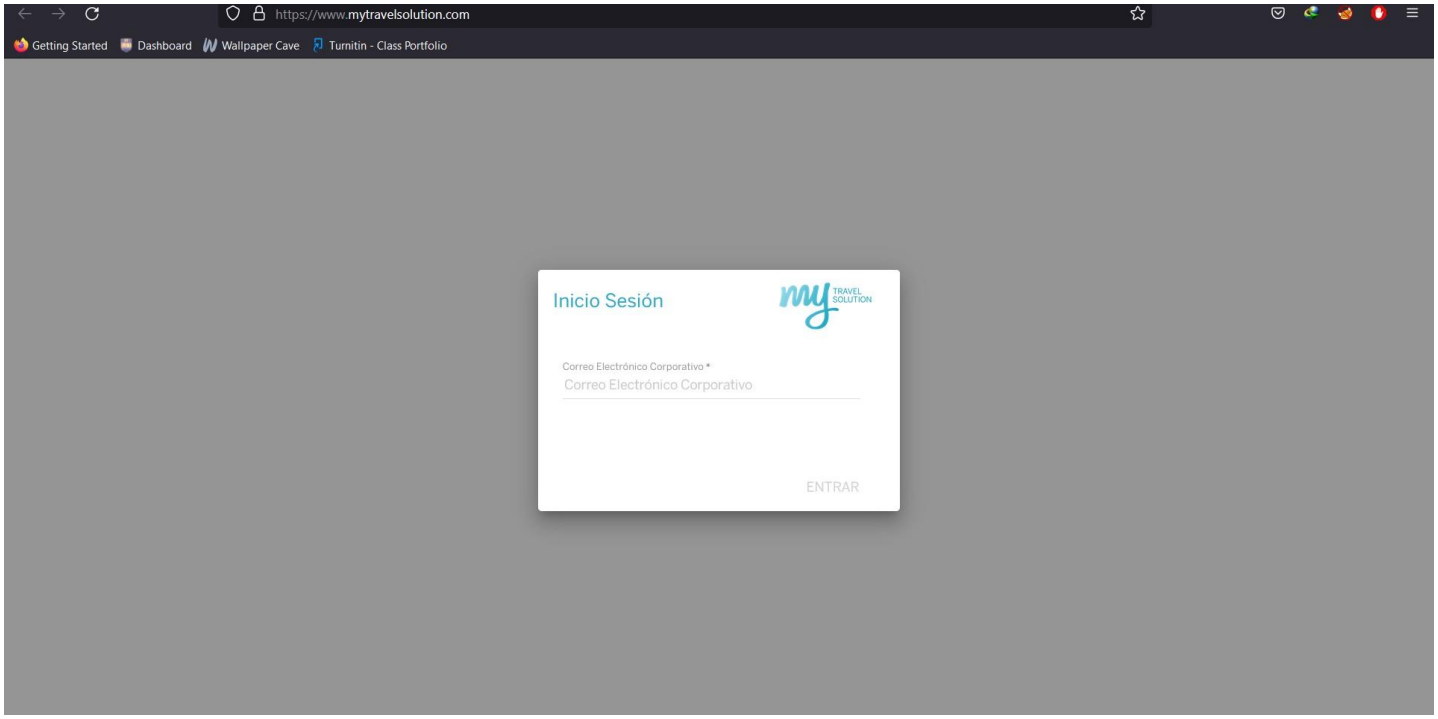
```
└─$ python3 oralyzer.py -u https://www.lawyerstravel.com/

[•] Appending payloads just after the URL
[•] Infusing payloads
[•] https://www.lawyerstravel.com/http://www.google.com [404]
[•] https://www.lawyerstravel.com/http%3A%2F%2Fwww.google.com [404]
[•] https://www.lawyerstravel.com/https%3A%2F%2Fwww.google.com [404]
[•] https://www.lawyerstravel.com///www.google.com [404]
[•] https://www.lawyerstravel.com/https:www.google.com [404]
[•] https://www.lawyerstravel.com/google.com [404]
[•] https://www.lawyerstravel.com//%5C/%5Cgoogle.com [404]
[•] https://www.lawyerstravel.com//%5C/google.com [404]
[•] https://www.lawyerstravel.com/////google.com [404]
[•] https://www.lawyerstravel.com/HtTP://google.com [404]
[•] https://www.lawyerstravel.com/HTTP://google.com [404]
[•] https://www.lawyerstravel.com/hTTp://google.com [404]
[•] https://www.lawyerstravel.com/HtTPs://google.com [404]
[•] https://www.lawyerstravel.com/hthttp://tp://google.com [404]
[•] https://www.lawyerstravel.com/x00http://google.com [404]
[•] https://www.lawyerstravel.com/%5Cx20http://google.com [404]
[•] https://www.lawyerstravel.com/216.58.214.206 [404]
[•] https://www.lawyerstravel.com/172.217.167.46 [404]
[•] https://www.lawyerstravel.com//216.58.214.206 [404]
[•] https://www.lawyerstravel.com/////216.58.214.206 [404]
[•] https://www.lawyerstravel.com//%5C216.58.214.206 [404]
```

```
[•] https://www.lawyerstravel.com///216.58.214.206 [404]
[•] https://www.lawyerstravel.com////216.58.214.206 [404]
[•] https://www.lawyerstravel.com///google%E3%80%82com [404]
[•] https://www.lawyerstravel.com///google%E3%80%82com [404]
[•] https://www.lawyerstravel.com/http%5Cx3A%5Cx2F%5Cx2Fgoogle.com [404]
[•] https://www.lawyerstravel.com/http://%5B::ffff:216.58.214.206%5D [404]
[•] https://www.lawyerstravel.com/http:%5B::ffff:216.58.214.206%5D [404]
[•] https://www.lawyerstravel.com/http://00330.00072.0000326.00000316 [404]
[•] https://www.lawyerstravel.com/http:00330.00072.0000326.00000316 [404]
[•] https://www.lawyerstravel.com/http://00330.0x3a.54990 [404]
[•] https://www.lawyerstravel.com/http:00330.0x3a.54990 [404]
[•] https://www.lawyerstravel.com/http://00330.3856078 [404]
[•] https://www.lawyerstravel.com/http:00330.3856078 [404]
[•] https://www.lawyerstravel.com/http://0330.072.0326.0316 [404]
[•] https://www.lawyerstravel.com/http:0330.072.0326.0316 [404]
[•] https://www.lawyerstravel.com/http:%0A%0D%E2%93%81%F0%9D%90%A8%F0%9D%97%B0%EF%BF%BD%F0%9D%95%9D%E2%85%8
6%F0%9D%93%B8%E2%93%9C%E2%82%90%E2%84%B9%E2%93%83%EF%BD%A1%EF%BC%B0%E2%93%A6 [404]
[•] https://www.lawyerstravel.com/http:%0A%0Dgoogle.com [404]
[•] https://www.lawyerstravel.com/http://0xd8.072.54990 [404]
[•] https://www.lawyerstravel.com/http:0xd8.072.54990 [404]
[•] https://www.lawyerstravel.com/http://0xd8.0x3a.0xd6.0xce [404]
[•] https://www.lawyerstravel.com/http:0xd8.0x3a.0xd6.0xce [404]
[•] https://www.lawyerstravel.com/http://0xd8.3856078 [404]
[•] https://www.lawyerstravel.com/http:0xd8.3856078 [404]
[•] https://www.lawyerstravel.com/http://0xd83ad6ce [404]
[•] https://www.lawyerstravel.com/http:0xd83ad6ce [404]
[•] https://www.lawyerstravel.com/http://%5B::216.58.214.206%5D [404]
[•] https://www.lawyerstravel.com/http:%5B::216.58.214.206%5D [404]
```

The website is not vulnerable to Open Redirection vulnerability.

Subdomain 5

https://www.mytravelsolution.com/



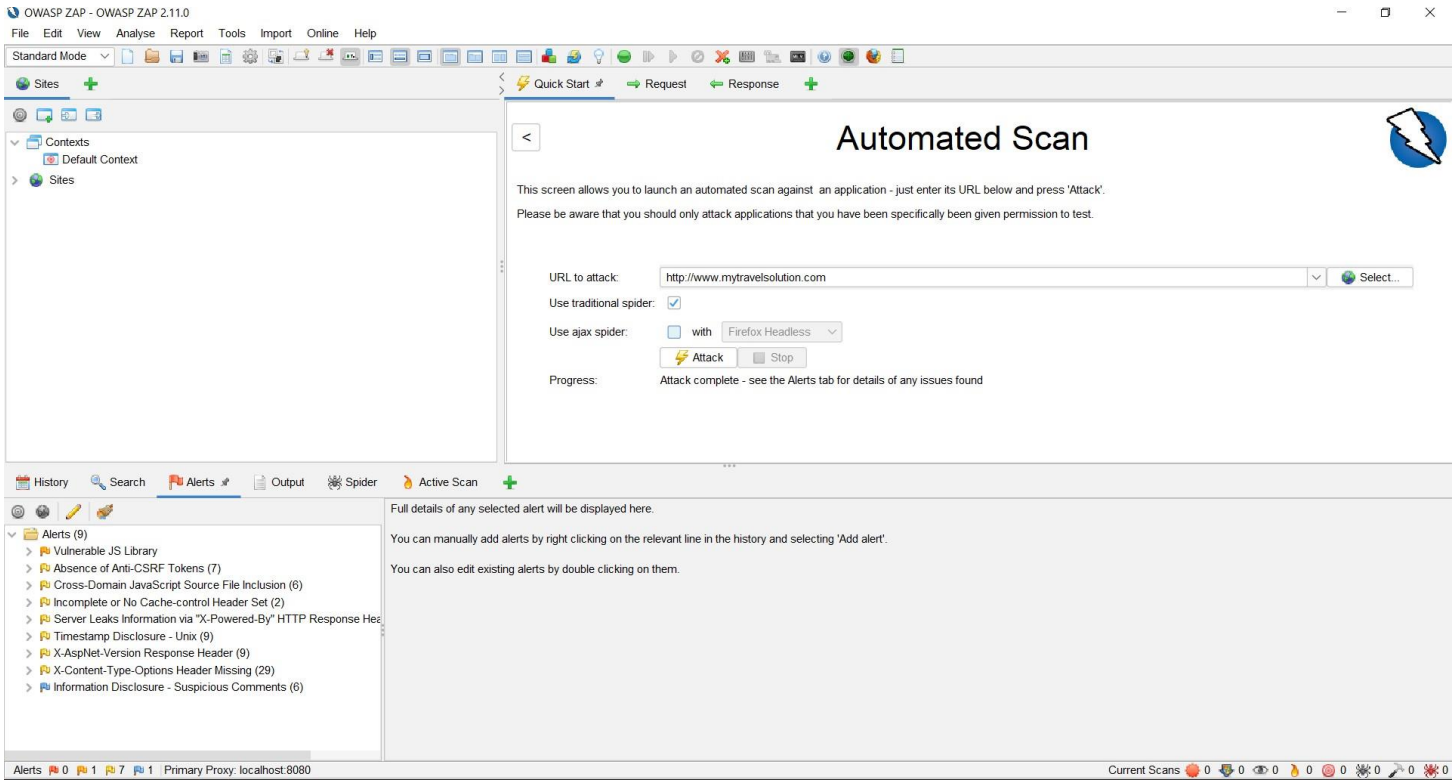
Automated Scans

Nmap Scan

```
└─$ sudo nmap -sS www.mytravelsolution.com
[sudo] password for aviano:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-14 12:55 EDT
Nmap scan report for www.mytravelsolution.com (40.119.158.171)
Host is up (0.24s latency).
Not shown: 995 filtered ports
PORT      STATE  SERVICE
25/tcp    open   smtp
80/tcp    open   http
443/tcp   open   https
990/tcp   closed ftps
50500/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 16.22 seconds
```

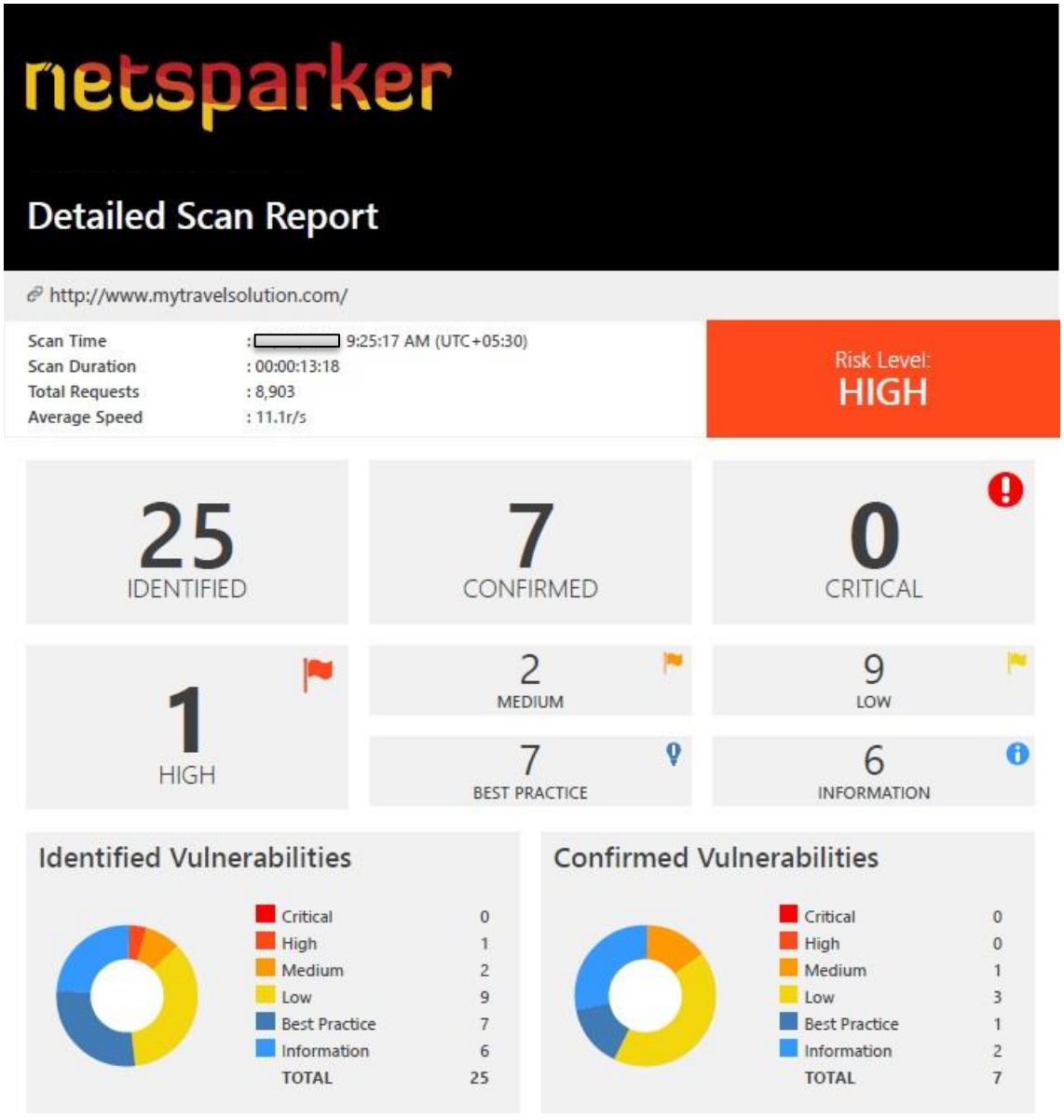
- I found three open ports (smtp, http, https) and two closed ports (ftps, unknown) using Nmap scanning.

OWASP ZAP Scan



According to the automated scan done by OWASP ZAP, I found 9 types of vulnerabilities withing the subdomain https://www.mytravelsolution.com/ . Furthermore, I did another automated scan for the same subdoain using Netsparker and it gave me a well detailed report as shown below.

Netsparker Scan



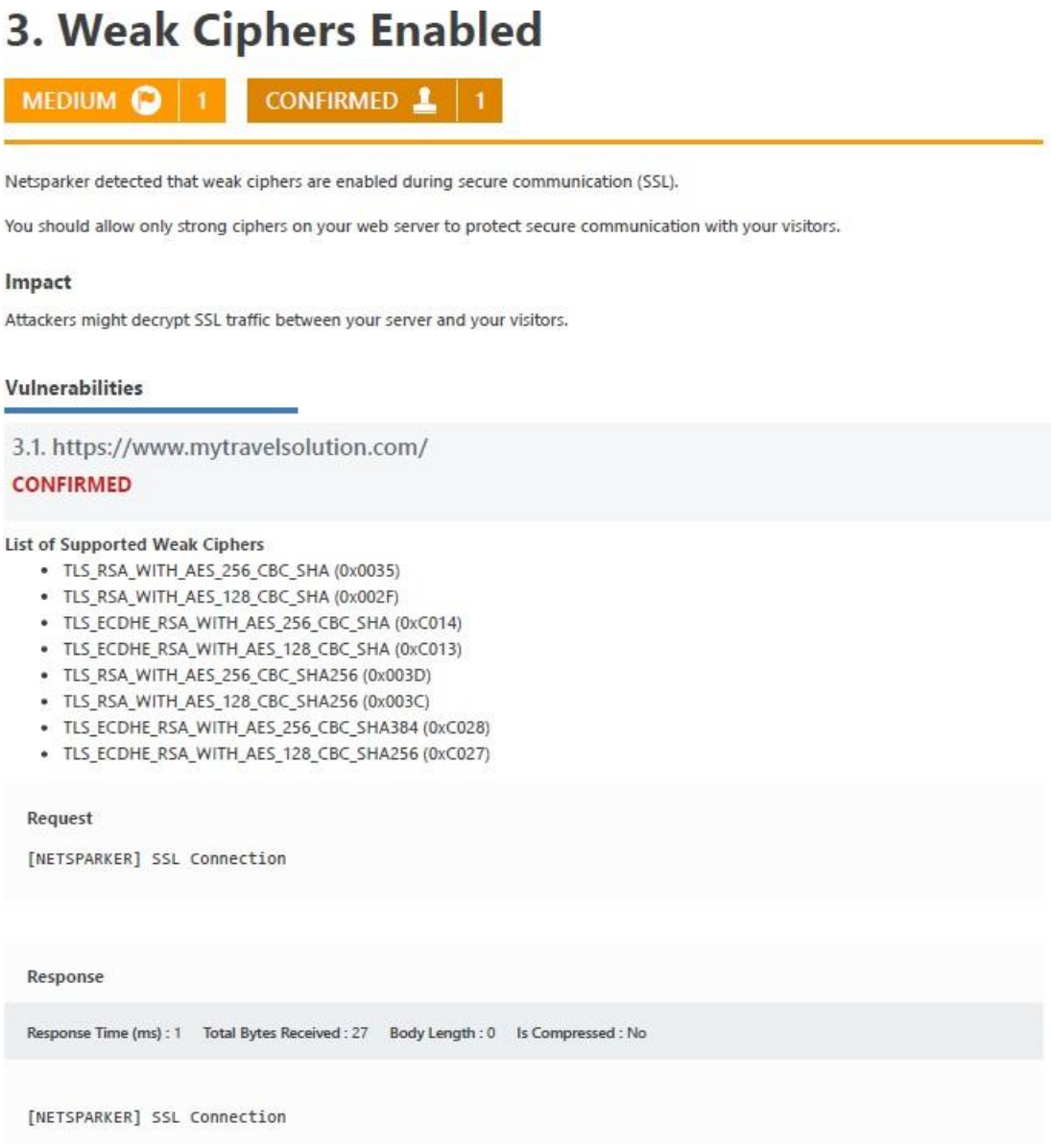
As shown in the image by performing a Netsparker scan on https://www.mytravelsolution.com/ website, it identified total of 25 vulnerabilities. Seven of them are confirmed vulnerabilities and the overall risk severity levels is high.

Vulnerability Summery

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (AngularJS)	GET	https://www.mytravelsolution.com/	
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://www.mytravelsolution.com/	
	Weak Ciphers Enabled	GET	https://www.mytravelsolution.com/	
	[Possible] Cross-site Request Forgery	GET	https://www.mytravelsolution.com/	
	[Possible] Cross-site Request Forgery in Login Form	GET	https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/	
	Programming Error Message	GET	http://www.mytravelsolution.com/trace.axd	URI-BASED
	Stack Trace Disclosure (ASP.NET)	GET	http://www.mytravelsolution.com/c:/boot.ini	URI-BASED
	Version Disclosure (ASP.NET)	GET	http://www.mytravelsolution.com/c:/boot.ini	URI-BASED
	Autocomplete is Enabled	GET	https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/	
	Cookie Not Marked as Secure	GET	https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/	
	Internal Server Error	GET	https://www.mytravelsolution.com/?%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%20src%3d%22%2f%2fuc0npbdxkmlxuwe-4ptlnbi-ti58qlwi9vj9cap1xm0%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscRipt%3e	
	Content Security Policy (CSP) Not Implemented	GET	http://www.mytravelsolution.com/.well-known	
	Expect-CT Not Enabled	GET	https://www.mytravelsolution.com/img/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Missing X-XSS-Protection Header	GET	http://www.mytravelsolution.com/.well-known	
	Referrer-Policy Not Implemented	GET	http://www.mytravelsolution.com/.well-known	
	SameSite Cookie Not Implemented	GET	https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/	
	Subresource Integrity (SRI) Not Implemented	GET	http://www.mytravelsolution.com/.well-known	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://www.mytravelsolution.com/	
	[Possible] Login Page Identified	GET	https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/	
	ASP.NET Identified	GET	http://www.mytravelsolution.com/	
	Out-of-date Version (jQuery)	GET	https://www.mytravelsolution.com/	
	Version Disclosure (IIS)	GET	http://www.mytravelsolution.com/	
	Autocomplete Enabled (Password Field)	GET	https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/	
	Forbidden Resource	GET	https://www.mytravelsolution.com/img/	

Confirmed Vulnerabilities in details.



3. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

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.

Vulnerabilities

3.1. https://www.mytravelsolution.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Both Action to take and Remedy are explained by me for the exact same vulnerability in previous subdomains.

7. Autocomplete is Enabled

LOW 1 CONFIRMED 1

Netsparker detected that Autocomplete is Enabled in one or more of the form fields which might contain sensitive information like "username", "credit card" or "CVV".

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Vulnerabilities

7.1. https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/

CONFIRMED

Method	Parameter	Value
GET	ReturnUrl	/Sitefinity/

Identified Field Name

- LoginFormControl$UserName

Request

```
GET /Sitefinity/Login?ReturnUrl=/Sitefinity/ HTTP/1.1
Host: www.mytravelsolution.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://www.mytravelsolution.com/Sitefinity/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1176.4178 Total Bytes Received : 18527 Body Length : 18190 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: .SFLOG-MTSv01=; expires=Mon, 11-Oct-1999 22:00:00 GMT; path=/; HttpOnly
Server: Microsoft-IIS/10.0
Content-Length: 18190
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Date: Wed, 13 Oct 2021 03:56:09 GMT
Cache-C
…
Login to manage the site
</h2>

<ol>

<li>
<label for="LoginFormControl_UserName" id="LoginFormControl_UserNameLabel" class="sfTxtLbl">Email / Use
rname</label>
<input name="LoginFormControl$UserName" type="text" id="LoginFormControl_UserName" accesskey="u" class
="sfTxt" />
<span id="LoginFormControl_UserNameRequired" class="sfValidator" style="display:none;">
<strong>Enter your email / username</strong>
</span>
</li>
<li>
<l
…
```

Action to take

- Set the attribute “autocomplete = off” to the individual “input” fields or to the form tag. Anyhow, browsers do not respect this directive and offer users to stock their passwords internally since early 2014.
- For all inputs which store sensitive data should disable the autocomplete. Sensitive data like credit card numbers, CCV etc. data should not be saved under cached.
- Rescan the web application to check whether the issues are fixed after addressing them all.

8. Cookie Not Marked as Secure

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Vulnerabilities

8.1. https://www.mytravelsolution.com/Sitefinity/Login?ReturnUrl=/Sitefinity/

CONFIRMED

Method	Parameter	Value
GET	ReturnUrl	/Sitefinity/

Identified Cookie(s)

- .SFLOG-MTSv01

Cookie Source

- HTTP Header

Request

```
GET /Sitefinity/Login?ReturnUrl=/Sitefinity/ HTTP/1.1
Host: www.mytravelsolution.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://www.mytravelsolution.com/Sitefinity/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 976.14 Total Bytes Received : 18527 Body Length : 18190 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: .SFLOG-MTSv01=; expires=Mon, 11-Oct-1999 22:00:00 GMT; path=/; HttpOnly
Server: Microsoft-IIS/10.0
Content-Length: 18190
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Date: Wed, 13 Oct 2021 03:55:29 GMT
Cache-CHTTP/1.1 200 OK
Set-Cookie: .SFLOG-MTSv01=; expires=Mon, 11-Oct-1999 22:00:00 GMT; path=/; HttpOnly

Server: Microsoft-IIS/10.0
Content-Length: 18190
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Date: Wed, 13 Oct 2021 03:5
```

Remedy

Make sure to mark all the cookies secure that use withing the application.

9. Internal Server Error

LOW 1 CONFIRMED 1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Vulnerabilities

9.1. https://www.mytravelsolution.com/?%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%20src%3d%22%2f%2fuc0npbdxkmlxuwe-4ptlnbi-ti58qlwi9vj9cap1xm0%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Value
GET	%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt+src%3d%22%2f%2fuc0npbdxkmlxuwe-4ptlnbi-ti58qlwi9vj9cap1xm0%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscRipt%3e	

Request

```
GET /?%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%20src%3d%22%2f%2fuc0npbdxkmlxuwe-4ptlnbi-ti58ql
wi9vj9cap1xm0%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscRipt%3e HTTP/1.1
Host: www.mytravelsolution.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://www.mytravelsolution.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 286.8466 Total Bytes Received : 6283 Body Length : 6013 Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/10.0
Content-Length: 6013
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Date: Wed, 13 Oct 2021 03HTTP/1.1 500 Internal Server Error

Server: Microsoft-IIS/10.0
Content-Length: 6013
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Date: Wed, 13 Oct 2021 03:55
…
```

Remedy

To handle the unpredicted errors by inspecting and review the web application. All the errors should handle in server-side only.

Unconfirmed Critical Vulnerabilities

1. Out-of-date Version (AngularJS)

HIGH | 1

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

Impact

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

AngularJS Improper Input Validation Vulnerability

In AngularJS before 1.7.9 the function `merge()` could be tricked into adding or modifying properties of `Object.prototype` using a `__proto__` payload.

Affected Versions

0.9.0 to 1.7.8

External References

- CVE-2019-10768

AngularJS Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

There is a vulnerability in all angular versions before 1.5.0-beta.0, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.

Affected Versions

1.0.0 to 1.4.14

External References

- CVE-2019-14863

AngularJS Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

angular.js prior to 1.8.0 allows cross site scripting. The regex-based input HTML replacement may turn sanitized code into unsanitized one. Wrapping "<option>" elements in "<select>" ones changes parsing behavior, leading to possibly unsanitizing code.

Affected Versions

0.9.0 to 1.7.9

External References

- CVE-2020-7676

AngularJS Denial of Service (DoS)

AngularJS.Core is a AngularJS.* package for other Angular modules within .NET. Affected versions of this package are vulnerable to Denial of Service (DoS). https://snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-471886

Affected Versions

0.9.0 to 1.6.2

AngularJS Cross-site Scripting (XSS) Vulnerability

AngularJS.Core is an AngularJS.* package for other Angular modules within .NET. Affected versions of this package are vulnerable to Cross-site Scripting (XSS) https://snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-471883

Affected Versions

0.9.0 to 1.6.4

External References

- -

Vulnerabilities

1.1. https://www.mytravelsolution.com/

Identified Version

- 1.4.7

Latest Version

- 1.8.2 (in this branch)

Vulnerability Database

- Result is based on 10/06/2021 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: www.mytravelsolution.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://www.mytravelsolution.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 482.709 Total Bytes Received : 20867 Body Length : 20583 Is Compressed : No

```
HTTP/1.1 200 OK
Expires: -1
Content-Length: 20583
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Pragma: no-cache
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Date: Wed, 13 Oct 2021 03:55:25 GMT
Cache-Control: no-cache



<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1"><title>
Home
</title><meta http-equiv="content-type" content="text/html; charset=utf-8" /><meta http-equiv="Content-
Security-Policy: script-src &#39;self&#39;" /><meta http-equiv="Cache-control" content="no-cache" /><me
ta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.
0, user-scalable=no" /><link rel="apple-touch-icon" sizes="57x57" href="/img/favicons/apple-touch-icon-
57x57.png" /><link rel="apple-touch-icon" sizes="60x60" href="/img/favicons/apple-touch-icon-60x60.png"
 /><link rel="apple-touch-icon" sizes="72x72" href="/img/favicons/apple-touch-icon-72x72.png" /><link r
el="apple-touch-icon" sizes="76x76" href="/img/favicons/apple-touch-icon-76x76.png" /><link rel="apple-
touch-icon" sizes="114x114" href="/img/favicons/apple-touch-icon-114x114.png" /><link rel="apple-touch-
icon" sizes="120x120" href="/img/favicons/apple-touch-icon-120x120.png" /><link rel="apple-touch-icon"
 sizes="144x144" href="/img/favicons/apple-touch-icon-144x144.png" /><link rel="apple-touch-icon" sizes
="152x152" href="/img/favicons/apple-touch-icon-152x152.png" /><link rel="apple-touch-icon" sizes="180x
180" href="/img/favicons/apple-touch-icon-180x180.png" /><link rel="icon" type="image/png" href="/img/f
avicons/favicon-32x32.png" sizes="32x32" /><link rel="icon" type="image/png" href="/img/favicons/androi
d-chrome-192x192.png" sizes="192x192" /><link rel="icon" type="image/png" href="/img/favicons/favicon-9
6x96.png" sizes="96x96" /><link rel="icon" type="image/png" href="/img/favicons/favicon-16x16.png" size
s="16x16" />


<!--jQuery-->
<script type="text/javascript
—
```

Remedy

AngularJs installation should be upgraded to stable latest version.

Manual Scans

SSLyze Scan to inspect cipher strength

```
└─$ sslyze --regular mytravelsolution.com

CHECKING HOST(S) AVAILABILITY
-----------------------------

  mytravelsolution.com:443                      => 40.119.158.171



SCAN RESULTS FOR MYTRAVELSOLUTION.COM:443 - 40.119.158.171
----------------------------------------------------------

* Certificates Information:
      Hostname sent for SNI:             mytravelsolution.com
      Number of certificates detected:   1


    Certificate #0 ( _RSAPublicKey )
      SHA1 Fingerprint:                  b38c07c174d1c6a0813507252d29448affb3860a
      Common Name:                       *.mytravelsolution.com
      Issuer:                            Sectigo RSA Domain Validation Secure Server CA
      Serial Number:                     84942613795006262395249841850772469 58
      Not Before:                        2021-10-04
      Not After:                         2022-10-04
      Public Key Algorithm:              _RSAPublicKey
      Signature Algorithm:               sha256
      Key Size:                          2048
      Exponent:                          65537
      DNS Subject Alternative Names:     ['*.mytravelsolution.com', 'mytravelsolution.com']
```

```
    Certificate #0 - Trust
      Hostname Validation:              OK - Certificate matches server hostname
      Android CA Store (9.0.0_r9):      OK - Certificate is trusted
      Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is trusted
      Java CA Store (jdk-13.0.2):       OK - Certificate is trusted
      Mozilla CA Store (2021-01-24):    OK - Certificate is trusted
      Windows CA Store (2021-02-08):    OK - Certificate is trusted
      Symantec 2018 Deprecation:        OK - Not a Symantec-issued certificate
      Received Chain:                   *.mytravelsolution.com --> Sectigo RSA Domain Validation Secure S
erver CA
      Verified Chain:                   *.mytravelsolution.com --> Sectigo RSA Domain Validation Secure S
erver CA --> USERTrust RSA Certification Authority
      Received Chain Contains Anchor:   OK - Anchor certificate not sent
      Received Chain Order:             OK - Order is valid
      Verified Chain contains SHA1:     OK - No SHA1-signed certificate in the verified certificate chain

    Certificate #0 - Extensions
      OCSP Must-Staple:                 NOT SUPPORTED - Extension not found
      Certificate Transparency:         OK - 3 SCTs included

    Certificate #0 - OCSP Stapling
      OCSP Response Status:             SUCCESSFUL
      Validation w/ Mozilla Store:      OK - Response is trusted
      Responder Key Hash:               b'\x8d\x8c^\xc4T\xad\x8a\xe1w\xe9\x9b\xf9\x9b\x05\xe1\xb8\x01\x8d
a\xe1'
      Cert Status:                      GOOD
      Cert Serial Number:               84942613795006262395249841850772469 58
      This Update:                      2021-10-14
      Next Update:                      2021-10-21

 * TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites.
```

```
    The server accepted the following 12 cipher suites:
       TLS_RSA_WITH_AES_256_GCM_SHA384                 256
       TLS_RSA_WITH_AES_256_CBC_SHA256                 256
       TLS_RSA_WITH_AES_256_CBC_SHA                    256
       TLS_RSA_WITH_AES_128_GCM_SHA256                 128
       TLS_RSA_WITH_AES_128_CBC_SHA256                 128
       TLS_RSA_WITH_AES_128_CBC_SHA                    128
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384           256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384           256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA              256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256           128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256           128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA              128       ECDH: prime256v1 (256 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                   OK - Supported
      Legacy RC4 Algorithm              OK - Not Supported


 * SSL 3.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 * TLS 1.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 * Deflate Compression:
                                     OK - Compression disabled

 * OpenSSL CCS Injection:
                                     OK - Not vulnerable to OpenSSL CCS injection

 * TLS 1.3 Cipher Suites:
```

```
 * TLS 1.3 Cipher Suites:
     Attempted to connect using 5 cipher suites; the server rejected all cipher suites.

 * SSL 2.0 Cipher Suites:
     Attempted to connect using 7 cipher suites; the server rejected all cipher suites.

 * TLS 1.1 Cipher Suites:
     Attempted to connect using 80 cipher suites.

     The server accepted the following 4 cipher suites:
        TLS_RSA_WITH_AES_256_CBC_SHA                    256
        TLS_RSA_WITH_AES_128_CBC_SHA                    128
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA              256       ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA              128       ECDH: prime256v1 (256 bits)

     The group of cipher suites supported by the server has the following properties:
       Forward Secrecy                  OK - Supported
       Legacy RC4 Algorithm             OK - Not Supported


 * OpenSSL Heartbleed:
                                        OK - Not vulnerable to Heartbleed

 * TLS 1.2 Session Resumption Support:
      With Session IDs: OK - Supported (5 successful resumptions out of 5 attempts).
      With TLS Tickets: NOT SUPPORTED - Server did not return a TLS ticket.

 * Elliptic Curve Key Exchange:
       Supported curves:                X25519, prime256v1, secp384r1
       Rejected curves:                 X448, prime192v1, secp160k1, secp160r1, secp160r2, secp192k1, sec
p224k1, secp224r1, secp256k1, secp521r1, sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1,
```

```
 * Downgrade Attacks:
       TLS_FALLBACK_SCSV:               VULNERABLE - Signaling cipher suite not supported

 * Session Renegotiation:
       Client Renegotiation DoS Attack:   OK - Not vulnerable
       Secure Renegotiation:              OK - Supported

 * ROBOT Attack:
                                        OK - Not vulnerable.


 SCAN COMPLETED IN 58.23 S
 -------------------------
```

The website is not vulnerable to ROBOT Attack, Session Renegotiation, Downgrade Attacks, OpenSSL Heartbleed, OpenSSL CCS Injection.

CORS Misconfiguration test

```
└─$ python3 corsy.py -u https://www.mytravelsolution.com/

    C O R S Y   {v1.0-beta}

 - No misconfigurations found.
```

No CORS misconfiguration found on the website.

Open Redirection Vulnerability testing.

```
└─$ python3 oralyzer.py -u https://www.mytravelsolution.com/
  ____                  __
 / __ \_____ _____ _/ /_ _____ ___ ____
/ /_/ / __/ _ `/ / // /_ // -_) __/
\____/_/  \_,_/_/\_, //__/\__/_/
                /___/

[•] Appending payloads just after the URL
[•] Infusing payloads
[•] https://www.mytravelsolution.com/http://www.google.com [400]
[•] https://www.mytravelsolution.com/http%3A%2F%2Fwww.google.com [400]
[•] https://www.mytravelsolution.com/https%3A%2F%2Fwww.google.com [400]
[•] https://www.mytravelsolution.com/https:www.google.com [400]
[•] https://www.mytravelsolution.com/HtTP://google.com [400]
[•] https://www.mytravelsolution.com/HTTP://google.com [400]
[•] https://www.mytravelsolution.com/hTTp://google.com [400]
[•] https://www.mytravelsolution.com/HtTPs://google.com [400]
[•] https://www.mytravelsolution.com/hthttp://tp://google.com [400]
[•] https://www.mytravelsolution.com/x00http://google.com [400]
[•] https://www.mytravelsolution.com/%5Cx20http://google.com [400]
[•] https://www.mytravelsolution.com/http://%5B::ffff:216.58.214.206%5D [400]
[•] https://www.mytravelsolution.com/http:%5B::ffff:216.58.214.206%5D [400]
[•] https://www.mytravelsolution.com/http://00330.00072.0000326.00000316 [400]
[•] https://www.mytravelsolution.com/http:00330.00072.0000326.00000316 [400]
[•] https://www.mytravelsolution.com/http://00330.0x3a.54990 [400]
[•] https://www.mytravelsolution.com/http:00330.0x3a.54990 [400]
[•] https://www.mytravelsolution.com/http://00330.3856078 [400]
[•] https://www.mytravelsolution.com/http:00330.3856078 [400]
[•] https://www.mytravelsolution.com/http://0330.072.0326.0316 [400]
[•] https://www.mytravelsolution.com/http:0330.072.0326.0316 [400]
```

```
[•] https://www.mytravelsolution.com/http:%0A%0D%E2%93%81%F0%9D%90%A8%F0%9D%97%B0%EF%BF%BD%F0%9D%95%9D%E2%85%86%F0%9D%93%B8%E2%93%9C%E2%82%90%E2%84%B9%E2%93%83%EF%BD%A1%EF%BC%B0%E2%93%A6 [400]
[•] https://www.mytravelsolution.com/http:%0A%0Dgoogle.com [400]
[•] https://www.mytravelsolution.com/http://0xd8.072.54990 [400]
[•] https://www.mytravelsolution.com/http:0xd8.072.54990 [400]
[•] https://www.mytravelsolution.com/http://0xd8.0x3a.0xd6.0xce [400]
[•] https://www.mytravelsolution.com/http:0xd8.0x3a.0xd6.0xce [400]
[•] https://www.mytravelsolution.com/http://0xd8.3856078 [400]
[•] https://www.mytravelsolution.com/http:0xd8.3856078 [400]
[•] https://www.mytravelsolution.com/http://0xd83ad6ce [400]
[•] https://www.mytravelsolution.com/http:0xd83ad6ce [400]
[•] https://www.mytravelsolution.com/http://%5B::216.58.214.206%5D [400]
[•] https://www.mytravelsolution.com/http:%5B::216.58.214.206%5D [400]
```

The website is not vulnerable to Open Redirection Vulnerability.

Conclusion

In https://www.amexglobalbusinesstravel.com website, I found number of vulnerabilities with critical, high, medium and low risk levels. To obtain the details and the vulnerabilities of the target, I did both automated scans and manual scans using different tools. At last, I was able to find a few confirm vulnerabilities with high, medium, and low risk levels. However, there are few unconfirmed vulnerabilities of out-of-date versions with critical risk level which can be a target of attackers. For each and every confirmed vulnerability and critical level vulnerabilities I gave the remedy/solution under the topic.

When it comes to manual scanning, I tried to test for three types of selected OWASP Top 10 vulnerabilities. But unfortunately, I was not succeeded.

To sum up, in https://www.amexglobalbusinesstravel.com the overall risk level of the subdomains under the main domain is medium. However, my point of view is, it is important to take actions against vulnerabilities currently available under each subdomain. That will develop the security level of both the domain and the sub domains.

References

[1] "SYNOPSYS," Synopsys technology, 2021. [Online]. Available: https://www.synopsys.com/glossary/what-is-owasp-top-10.html#1. [Accessed 01 10 2021].

[2] "OWASP," OWASP Foundation, 2021. [Online]. Available: https://owasp.org/www-project-top-ten/#. [Accessed 1 10 2021].

[3] O. T. 1. team, "A01:2021 – Broken Access Control," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/. [Accessed 10 2021].

[4] 2. -. O. T. 1. team, "A02:2021 – Cryptographic Failures," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/. [Accessed 10 2021].

[5] 2. -. O. T. 1. team, "A03:2021 – Injection," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A03_2021-Injection/. [Accessed 10 2021].

[6] 2. -. O. T. 1. team, "A04:2021 – Insecure Design," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A04_2021-Insecure_Design/. [Accessed 10 2021].

[7] 2. -. O. T. 1. team, "A05:2021 – Security Misconfiguration," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/. [Accessed 10 2021].

[8] 2. -. O. T. 1. team, "A06 Vulnerable and Outdated Components," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/. [Accessed 10 2021].

[9] S. Bathla, "A06:2021-Vulnerable and Outdated Components," Medium, 22 September 2021. [Online]. Available: https://medium.com/@shivam_bathla/a06-2021-vulnerable-and-outdated-components-a5d96017049c. [Accessed 10 2021].

[10] 2. -. O. T. 1. team, "A07 Identification and Authentication Failures," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/. [Accessed 10 2021].

[11] 2. -. O. T. 1. team, "A08 Software and Data Integrity Failures," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/. [Accessed 10 2021].

[12] 2. -. O. T. 1. team, "A09 Security Logging and Monitoring Failures," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/. [Accessed 10 2021].

[13] 2. -. O. T. 1. team, "A10:2021 – Server-Side Request Forgery (SSRF)," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/. [Accessed 10 2021].

[14] "Vulnerability Severity Levels," Netsparker, [Online]. Available: https://www.netsparker.com/support/vulnerability-severity-levels-netsparker/. [Accessed 10 2021].

[15] "Information Gathering Techniques," W3 schools, [Online]. Available: https://www.w3schools.in/ethical-hacking/information-gathering-techniques/. [Accessed 10 2021].

[16] "Enumeration and its Types," GreyCampus, [Online]. Available: https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types. [Accessed 10 2021].