

Sri Lanka Institute of Information Technology



IE2062 – Web Security

Bug Bounty Reports

IT22589668

Jayasekara J K C D

Y2-S2-CS WD

Acknowledgement

Bug bounty programs have gained popularity in the constantly changing field of cybersecurity. These large-scale corporations' initiatives enable "white hat" hackers or ethical hackers to search for weaknesses in their technological infrastructure. White hats assist businesses in strengthening their defenses and receive reward for finding and reporting these bugs. Because of the increase in bug bounty programs, ethical hackers now have plenty of options to explore, making this a rewarding and fascinating subject. After delving deeper into the resources required for effective bug bounty hunting. I will continue with over ten informative reports that cover everything from the basics to web application security.

Objective

The goal of this effort is to locate vulnerabilities on a well-known website. Attackers could potentially take advantage of these vulnerabilities. Undergraduate students studying cyber security can close the knowledge gap between theory and practice with this practical exercise. The website's security posture will be carefully evaluated using both automated and manual testing techniques. The first vulnerability scan will use automated tools such as nmap, uniscan, recon-ng, Nikto, OWASP ZAP, Netsparker.

Introduction

These days, bug bounty programs are crucial for organizations trying to reinforce their cybersecurity safeguards. These efforts urge users to identify and resolve vulnerabilities before hackers may take advantage of them. Businesses can identify and resolve these problems more quickly by collaborating with security researchers. This kind of cooperation additionally encourages mutual learning.

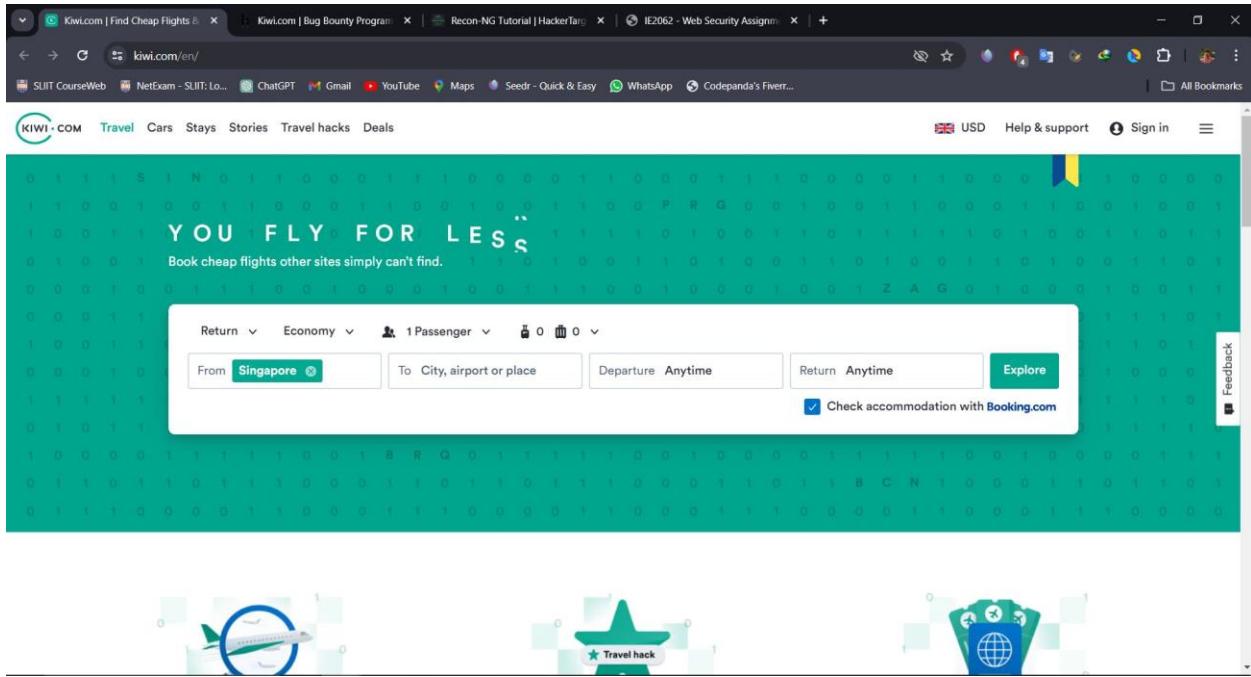
The importance of scanning websites and web apps for security issues is examined in this study. We will observe how these security measures follow the law and reduce the risk of cyberattacks. We can determine how successful these safeguards are by examining actual cases and industry standards. Our aim is to demonstrate the significance of these routine inspections for businesses.

We are aware that a data breach can cost an organization an incredible amount of wealth. They risk losing money and having their reputation harmed. The expense of doing routine security audits is significantly less than this. Preventive maintenance and repair are made possible by these inspections. They also assist organizations in adhering to the recommended practices for internet safety.

Security audits and bug bounty programs are critical to an organization's security on the internet. We can use the internet in a safer environment if we cooperate and follow the rules. Organizations must always learn to stay one step ahead of attackers as cyber threats evolve.

Bug bounty Reports

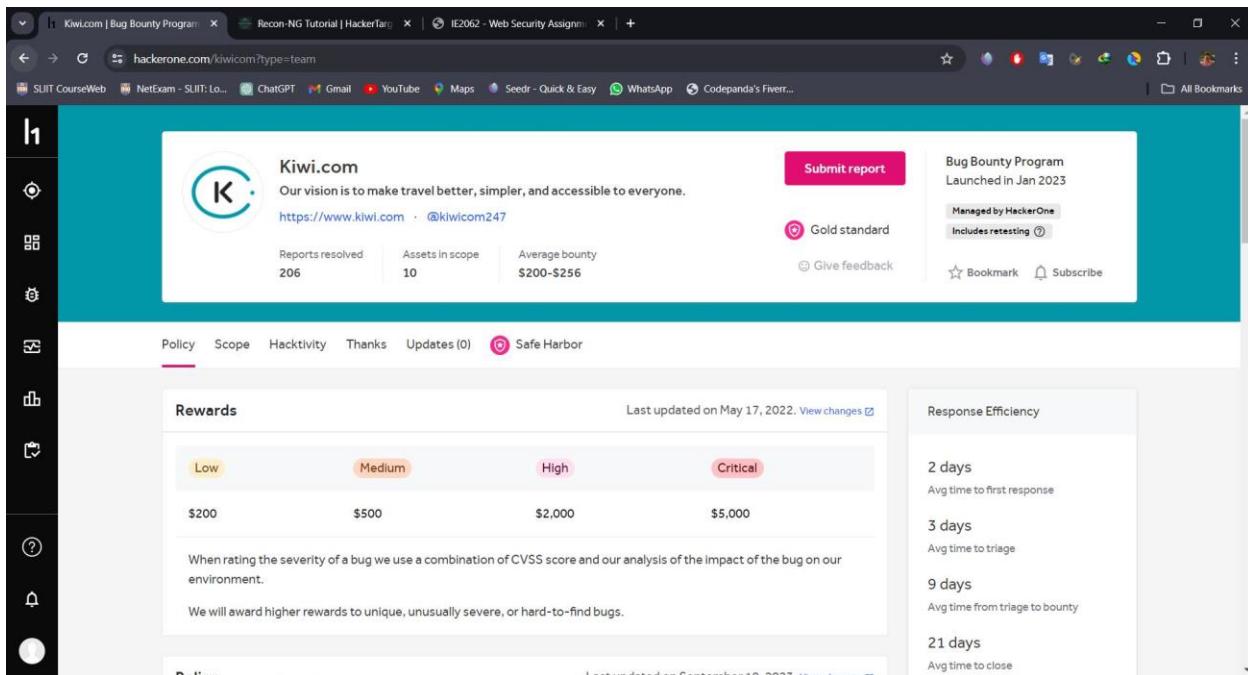
Target domain – <https://www.kiwi.com/>



Kiwi.com, formerly known as skypicker.com is a digital travel agency founded in 2012 by Oliver Dlouhý and Jozef Képesi, with its headquarters located in the Czech Republic. Kiwi.com acts as a middleman website that makes it easier to look for and book flights and ground transportation. One unique feature of kiwi.com's operation is its innovative "virtual interlining" system. With the help of this modern technology, consumers may create custom travel plans by combining routes from over 750 different carriers. It is noteworthy that this group includes airlines that typically do not participate in joint ventures in the internet reservation space. By means of this technological development, Kiwi.com aims to provide its customers with increased flexibility and more options for travel, ultimately optimizing the booking experience.

Overview

Kiwi.com offers a comprehensive reward plan to encourage security researchers to take part in their bug bounty program. kiwi.com is dedicated to creating a secure online space, so it appreciates the help researchers provide in identifying and correcting such security vulnerabilities. Researchers who identify vulnerabilities with low severity can be eligible for a \$200 incentive. A \$500 incentive is appropriate for medium severity vulnerabilities because of their greater impact on security. Significant risks associated with high severity vulnerabilities are rewarded with \$2,000, whereas the most serious dangers associated with critical vulnerabilities are rewarded with \$5,000. This structured method encourages researchers to do thorough and meticulous security assessments by paying them according to the severity and potential effect of the vulnerabilities they find.



The screenshot shows the Kiwi.com Bug Bounty Program page. At the top, there's a navigation bar with tabs for 'Kiwi.com | Bug Bounty Program', 'Recon-NG Tutorial | HackerOne', and 'IE2062 - Web Security Assignment'. Below the navigation is a header with the Kiwi.com logo, a 'Submit report' button, and information about the 'Bug Bounty Program' launched in Jan 2023, managed by HackerOne, and including retesting. The main content area has a sidebar with various icons and a central panel for 'Rewards' and 'Response Efficiency'. The 'Rewards' section shows a scale from 'Low' to 'Critical' with corresponding monetary values: \$200, \$500, \$2,000, and \$5,000. It also includes a note about rating bugs based on CVSS score and impact. The 'Response Efficiency' section lists average times for response, triage, and closing bugs.

Rewards	Last updated on May 17, 2022. View changes
Low	\$200
Medium	\$500
High	\$2,000
Critical	\$5,000

When rating the severity of a bug we use a combination of CVSS score and our analysis of the impact of the bug on our environment.
We will award higher rewards to unique, unusually severe, or hard-to-find bugs.

Response Efficiency
2 days Avg time to first response
3 days Avg time to triage
9 days Avg time from triage to bounty
21 days Avg time to close

It's important to know the privacy policies before initiating a bug bounty. These guidelines specify how information will be managed, guaranteeing its confidentiality and security. They also go through how security researchers should respect people's right to privacy while reporting vulnerabilities. In the end, it comes down to securing private data and establishing mutual trust between all parties involved.

Kiwi.com is committed to working with security experts worldwide in cooperation with HackerOne's Triage team to ensure high quality of our bug bounty program and the security of our customers.

If you're good enough to spot a vulnerability on our site, we'd love to know about it!

We value the work and time of independent security researchers and therefore aim to:

- Reply to all submissions within two business days (either Kiwi.com or HackerOne Triage)
- Post regular updates to all submissions on a weekly basis
- Determine security impacts transparently
- Pay bounty on triage
- Resolve vulnerabilities within one week to minimize the likelihood of a duplicate report

Everything related to Kiwi.com is in scope, with primary services outlined in the structured scope section. If you have any questions, reach out to us at security@kiwi.com.

Rules of engagement

- Confine scans on a single hostname to a 500ms delay (in other words, 2 requests per second).
- Under any circumstances, don't engage in:
 - Physical attacks targeting any Kiwi.com property
 - Social engineering of Kiwi.com employees or contractors
 - DoS/DDoS or other availability attacks
- Do not compromise any customer accounts or data.
- Do not discuss or post details of your vulnerability outside of the HackerOne platform before it has been approved for disclosure.
- Issues introduced by vulnerable third-party software are subject to a ten-day grace period to provide enough time for internal remediation and testing (for example, publicly disclosed 0days).
- Current & past employees are prohibited from participating in our bug bounty program.

Program Statistics

Metric	Value
Total bounties paid	\$94,418
Avg bounty range	\$200 - \$256
Top bounty range	\$1,337 - \$2,500
Bounties paid in the last 90 days	\$4,550
Reports received in the last 90 days	117
Last report resolved	14 days ago
Reports resolved	206

There are certain actions or areas that are out of the scope of any bug bounty program. These are defined as behaviors, systems or vulnerabilities that are not acceptable for program consideration. For example, some security vulnerabilities or systems might not be included in the specified scope. It is crucial that the companies performing the program and security researchers participating understand these exclusions.

Out of scope vulnerabilities & exclusions

Issues that we know about and would like to fix at some point or which we don't plan on fixing, e.g., because we know it's not feasible:

- User/email enumeration
- A small number of Kiwi.com email addresses leak via JavaScript files
- Invalid or missing SPF/DKIM/DMARC records
- Lack of 'Secure' and 'HttpOnly' cookie flags
- Theoretical TLS/SSL Issues
- Read access to our public Firebase instances
 - skypicker-984.firebaseio.com
 - kiwi-debug.firebaseio.com
- Hard-coded API keys (for example, Google Maps, Mapbox, ...), unless there is a different impact than additional costs
- Leaked credentials of tequila partners in 3rd party services (such as GitHub)
- Attacks requiring MITM or physical access to a user's device
- Lack of "best practices" that do not impose a vulnerability that can be leveraged
- PII leaks between the members of a single tequila company
- Authorization bypasses in tequila within a single tequila company might be exempt from bounties, depending on the vulnerability
- XSS / HTML Injection in Swagger UI
- Credentials and other sensitive leaks aggregated in third-party sites (e.g., otx.alienvault) without demonstrating that a

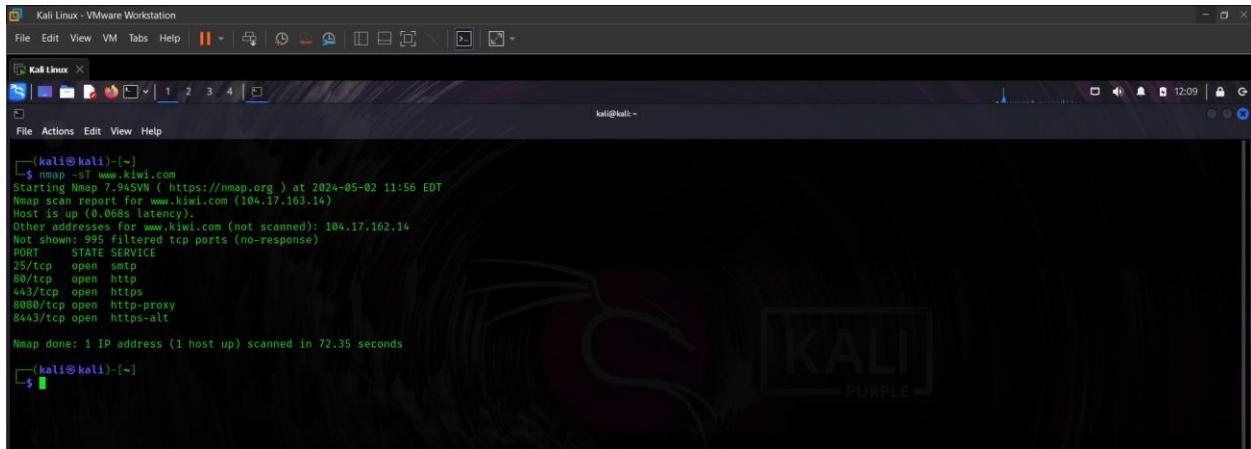
When searching for bugs that eligible for bounties, the "In scope" domain is critical. Our scanning procedures only look for regions which are under this specified range. In the case that events fail to proceed as planned, we predict several difficulties.

Asset name	Type	Coverage	Max. severity	Bounty	Last update
com.skypicker.main	Android: Play Store	In scope	Critical	Eligible	Jan 25, 2023
auth.skypicker.com	Domain	In scope	Critical	Eligible	Jan 25, 2023
tequila.kiwi.com	Domain	In scope	Critical	Eligible	Jan 25, 2023
*.skypicker.com	Wildcard	In scope	Critical	Eligible	May 15, 2023
com.skypicker.skypicker	iOS: App Store	In scope	Critical	Eligible	Jan 25, 2023
www.kiwi.com	Domain	In scope	Critical	Eligible	Jan 25, 2023
*.kiwi.com	Wildcard	In scope	Critical	Eligible	May 15, 2023

Information gathering for root Domain.

Using nmap

Firstly, I use the network exploration utility nmap to perform a port scanning process. The target website's infrastructure may be thoroughly evaluated thanks to this methodical procedure, which also offers priceless insights on the variety of running services and ports it hosts. I hope to gain a deeper comprehension of the website's technological architecture and the variety of services it offers by following this methodical approach. This will enable me to analyze the website's digital footprint and potential vulnerabilities more intelligently.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running an nmap scan against the host www.kiwi.com. The output shows the following details:

```
(kali㉿kali)-[~]
$ nmap -sT www.kiwi.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 11:56 EDT
Nmap scan report for www.kiwi.com (104.17.163.14)
Host is up (0.068s latency).
Other addresses for www.kiwi.com (not scanned): 104.17.162.14
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 72.35 seconds
(kali㉿kali)-[~]
```

After carefully scanning the website's ports with nmap, I did not find any vulnerable ports or services running on this root domain. It seems like the website is well-protected and does not have vulnerable ports hackers to exploit. This means the website has good security and is less likely to be attacked or hacked.

Using recon-ng framework to find subdomains of this root domain.

One effective tool for cybersecurity reconnaissance is the Recon-*ng* framework. To assist in the detection of potential vulnerabilities, it helps gather information about targets such as websites, networks, or organizations. By using numerous modules and approaches, Recon-*ng* streamlines the process of information collection, making it efficient and accurate.

Here, I'm searching for subdomains using the Hackertarget module in the Recon-`ng` framework. This module offers important insights into the website's broader digital footprint by focusing on finding subdomains connected to a target domain. This scan allows me to find more web resources associated with the target domain, which improves my knowledge of its online presence and possible attack surface.

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| 1 2 3 4 | X

[+] Kali Linux X 12:42
File Actions Edit View Help
Sponsored by ...

www.blackhillsinfosec.com

PRACTISEE
www.practise.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[2] Recon modules

[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > options set SOURCE kiwi.com
SOURCE = kiwi.com
[recon-ng][default][hackertarget] > info

    Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
    Version: 1.1

Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
    Name      Current Value  Required  Description
    _____
    SOURCE    kiwi.com       yes        source of input (see 'info' for details)

Source Options:
    default   SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>  string representing a single input
    <path>    path to a file containing a list of inputs
    query <sql> database query returning one column of inputs

[recon-ng][default][hackertarget] > |
```

I discovered that kiwi.com is related to 59 subdomains after utilizing the module. I'm going to concentrate on the top ten subdomains at this point and examine each one for vulnerabilities. This methodical approach will assist me in identifying any weaknesses that require attention, hence enhancing the security of kiwi.com's online environment.

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| 1 2 3 4 | X
Kali Linux
File Actions Edit View Help
KIWI.COM
[*] Country: None
[*] Host: app.kiwi.com
[*] Ip Address: 151.101.1.195
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: auto-mails-kibana.automation.kiwi.com
[*] Ip Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: balkan.kiwi.com
[*] Ip Address: 34.149.87.41
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: log.banana.kiwi.com
[*] Ip Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: bergamolynk.kiwi.com
[*] Ip Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
```

```
[*] Country: None
[*] Host: beta-balkan.kiwi.com
[*] Ip_Address: 34.149.87.41
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: code.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: confluence.kiwi.com
[*] Ip_Address: 104.17.163.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: coupons.kiwi.com
[*] Ip_Address: 35.241.34.48
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: docs.kiwi.com
[*] Ip_Address: 104.17.163.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] Country: None
[*] Host: fe-cloudrun.kiwi.com
[*] Ip_Address: 104.18.15.219
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: fe-search-cloud-run.kiwi.com
[*] Ip_Address: 104.17.163.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: fluggesellschaft.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: geopl-api-cr.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: goopti.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*]
[*] Country: None
[*] Host: graphql-cr.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: hamburgairport.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: help-graphql.kiwi.com
[*] Ip_Address: 104.17.163.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: holidaypirates.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: hotels.kiwi.com
[*] Ip_Address: 104.17.163.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*]
[*] Host: images.kiwi.com
[*] Ip_Address: 104.17.163.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: jamesvillasflights.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: jobs.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: kiwibase.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: kiwistore.kiwi.com
[*] Ip_Address: 23.227.38.65
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

These are the subdomains that I have chosen for further enumeration.

app.kiwi.com

bergamolynk.kiwi.com

balkan.kiwi.com

hotels.kiwi.com

stanstedairport.kiwi.com

platform-api.skypicker.com

traveltobrno.kiwi.com

goopti.kiwi.com

images.skypicker.com

tequila-api.kiwi.com

By choosing these subdomains for further enumeration, the focus now turns to doing a thorough investigation of each one separately to discover any possible vulnerabilities. This systematic technique seeks to methodically evaluate the security status of the selected subdomains, investigating any vulnerabilities or exploitable areas that could potentially undermine the integrity of kiwi.com's digital infrastructure. To enhance the overall resilience and security of kiwi.com's online presence, proactive measures can be taken by running comprehensive vulnerability scans and analyses on each subdomain. This allows for the identification and mitigation of any discovered issues. By following this rigorous procedure, any possible risks may be swiftly dealt with, ensuring the security and accessibility of kiwi.com's services and data.

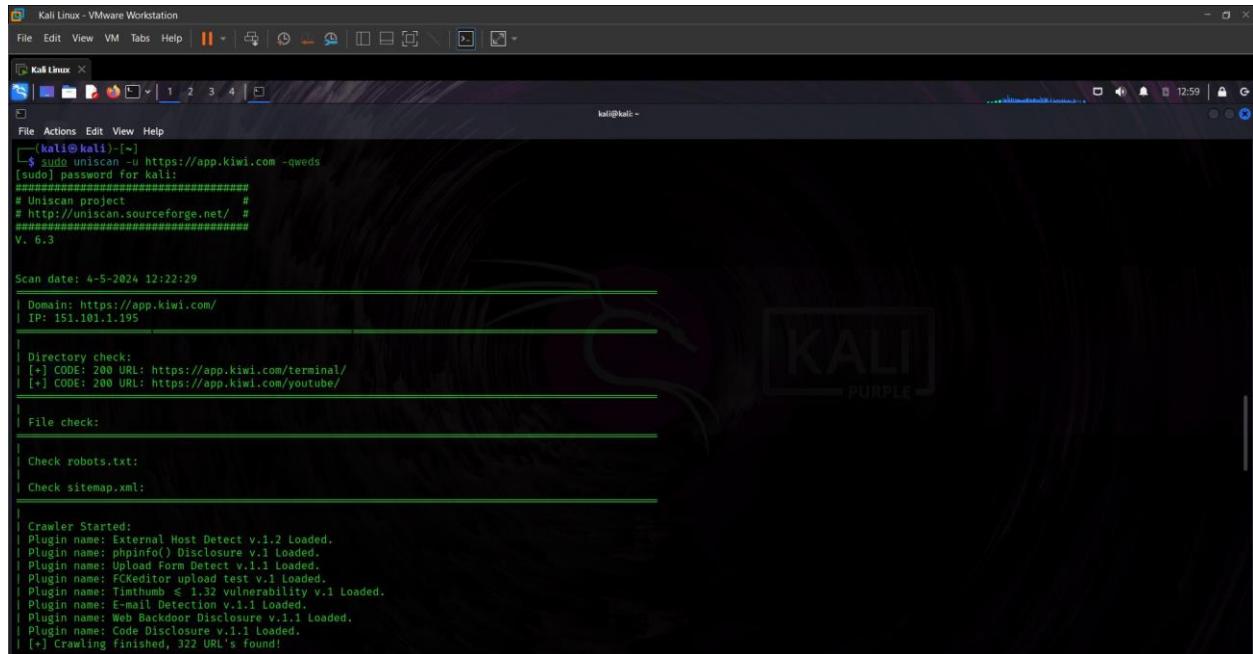
Report 01

Target domain: <http://app.kiwi.com/>

Scan using uniscan tool.

Uniscan is an online security tool designed to detect vulnerabilities such as SQL injection and Cross-Site Scripting in web applications. Security experts recommend this tool for its comprehensive scans and user-friendly interface, which greatly contributes to its effectiveness in assuring the security of web applications.

The command "uniscan -u app.kiwi.com -qweds" was executed as follows:



```
(kali㉿kali)-[~]
$ sudo uniscan -u https://app.kiwi.com -qweds
[sudo] password for kali:
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 4-5-2024 12:22:29
| Domain: https://app.kiwi.com/
| IP: 151.101.1.195

| Directory check:
| [+] CODE: 200 URL: https://app.kiwi.com/terminal/
| [+] CODE: 200 URL: https://app.kiwi.com/youtube/
|
| File check:
|
| Check robots.txt:
| Check sitemap.xml:

Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
Plugin name: Upload Form Detect v.1.3 Loaded.
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
[+] Crawling Finished, 322 URL's Found!
```

```

ignored Files:
https://app.kiwi.com/opensearch.xml

Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.1 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 0 New directories added

FCKeditor tests:

Timthumb < 1.33 vulnerability:

Backup Files:

Blind SQL Injection:
[+] Vul [Blind SQL-1]: https://app.kiwi.com/?utm_source=product&ofl=https://itunes.apple.com/us/app/id657843853?mt=8&utm_campaign=mobile_landingpage&utm_medium=website&utm_content=button_&ioslink=https://kiwi.com/mobile"&AND+'1'='1
[+] Keyword: ember33388
[+] Vul [Blind SQL-1]: https://app.kiwi.com/?apn=com.skypicker.main&isi=657843853&ibi=com.skypicker.Skypicker&utm_campaign=t-email_boarding_documents_boarding_passes_mobile_landingpage_b
utton%26utm_medium=search&utm_source=product&utm_content=ioslink=https%3A%2F%2Fapp%2Fid657843853%3Fmt%3D8&link=https%3A%2F%2Fkiwi.com%2Fmobile%3Futm_medium%3Dsearch
[+] Keyword: ember33388

```

```

Local File Include:                               http://
[+] Dynamic directory disclosure
[+] Local File Include in C

PHP CGI Argument Injection:                     http://
[+] Local Header Code in C

Remote Command Execution:                      http://
[+] Local Header Code in C

Remote File Include:                           http://
[+] Local Header Code in C

SQL Injection:                                 http://
[+] Local Header Code in C

Cross-Site Scripting (XSS):                   http://
[+] Local Header Code in C

Web Shell Finder:                             http://
[+] Local Header Code in C

Static tests:
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.1 Loaded.

Local File Include:                           http://
[+] Local Header Code in C

Remote Command Execution:                    http://
[+] Local Header Code in C

```

Even though it didn't seem promising at first, running the "uniscan -u app.kiwi.com -qweds" command uncovered two blind SQL injection vulnerabilities on the kiwi.com website.

These vulnerabilities were found in mobile application, and I was unable to take advantage of these vulnerabilities.

Scan using Netsparker

Netsparker (Invicti) is an automated online security scanner. It helps scan websites, web applications and services for vulnerabilities. Netsparker is versatile, working with various platforms and programming languages used in web applications.

The screenshot shows the Netsparker 5.8.1.28119 interface. The top navigation bar includes File, Home, View, Reporting, Help, and a search bar. The main menu bar has options like New, Schedule, Incremental, Schedule Incremental, New Instance, Restest All, Hawk Check, Import, Export, Export to Netsparker Enterprise, Scan Policy Editor, Report Policy Editor, Options, and Tools. On the left, there's a Sitemap - Previous Settings panel and an Issues - Previous Settings panel. The central area displays the 'Welcome' page with sections for 'Updates', 'Web Application Security Blog', and 'Testing Cron JOBS'. A progress bar at the bottom indicates the scan speed and progress. The bottom status bar shows session details like Links: 30, Failed Requests: 0, 404 Requests: 29, Head Requests: 54, Total Requests: 1111, and activity logs. A message at the bottom says 'Session loaded successfully. Scan status: finished.'



I identified a total of 13 vulnerabilities associated with app.kiwi.com subdomain. Among these, two vulnerabilities pose a medium level of risk.

CONFIRM VULNERABILITY		METHOD	URL	PARAMETER
		GET	https://app.kiwi.com/	
		GET	https://app.kiwi.com/well-known/apple-app-site-association	
		GET	https://app.kiwi.com/	
		GET	https://app.kiwi.com/etc/passwd	URI-BASED
		GET	https://app.kiwi.com/	
		GET	https://app.kiwi.com/open-search.gz	
		OPTIONS	https://app.kiwi.com/	

Vulnerability 1:

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period during which the user agent shall access the server in only secure fashion.

Vulnerabilities

1.1. https://app.kiwi.com/

Certainty

Request **Response**

```

GET / HTTP/1.1
Host: app.kiwi.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

```

Request Response

Response Time (ms) : 332.2144 Total Bytes Received : 10817 Body Length : 9233 Is Compressed : No

```

HTTP/1.1 400 Bad Request
X-Cache: MISS
X-Timer: S1714833939.515845,VS0,VE191
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Accept-Ch: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Form-Factor, Sec-CH-UA-Platform, Se
transfer-encoding: chunked
X-Served-By: cache-qpp120111-QP6
Connection: keep-alive
Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-form-factor=*, ch-ua-platform=*, ch-ua-pla
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site, x-fh-requested-host, accept-encoding
Content-Security-Policy: require-trusted-types-for 'script';report-uri /_DurableDeepLinkUi/cspreport,script-src 'report-sample' 'nonce-EnLfEGEDVRc8JNmrE05iA' 'unsafe-inline';obj
X-Cache-Hits: 0
alt-svc: h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400
Content-Type: text/html; charset=utf-8
Cross-Origin-Opener-Policy: unsafe-none
Pragma: no-cache
Date: Sat, 04 May 2024 14:45:38 GMT
Accept-Ranges: bytes
<!doctype html><head><title>Invalid Dynamic Link</title><meta name="viewport" content="width=device-width, initial-scale=1"></head><body style="color: rgba(0,0,0,0.87); font-size: 1em; font-family: sans-serif; margin: 0; padding: 0;">

```

Vulnerability 2: Weak Ciphers Enabled

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

Vulnerabilities

2.1. https://app.kiwi.com/ CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

Request Response

[NETSPARKER] SSL Connection

Impact:

Attackers might decrypt SSL traffic between the server and site visitors.

Solution:

For Apache, you should modify the SSLCipherSuite directive in httpd.conf.

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

Lighttpd:

```
ssl.honor-cipher-order = "enable"
```

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

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type regedit32 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

Conclusion

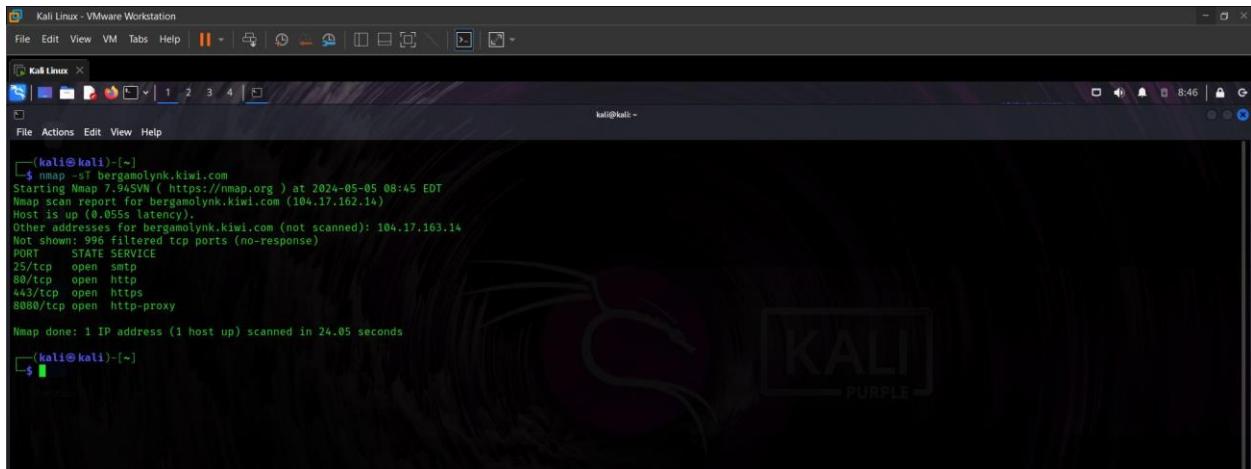
In summary, the security assessment of <http://app.kiwi.com/> using Uniscan and Netsparker revealed significant vulnerabilities. Uniscan identified two blind SQL injection flaws in the mobile app while Netsparker uncovered 13 vulnerabilities in the app.kiwi.com subdomain including two medium-risk issues. These vulnerabilities, such as the absence of HTTP Strict Transport Security (HSTS) and weak ciphers during SSL communication pose potential risks to user security.

Report 02

Target domain: bergamolynk.kiwi.com

Scan using nmap tool.

First, I used the nmap tool to check for any vulnerable ports or services on this subdomain.



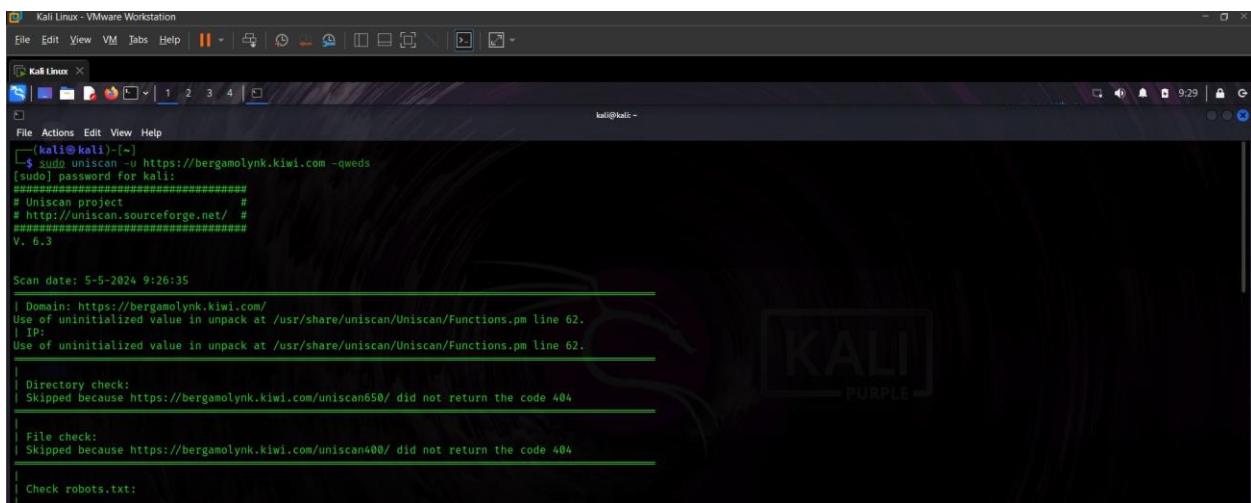
```
(kali㉿kali)-[~]
└$ nmap -sT bergamolynk.kiwi.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-05 08:45 EDT
Nmap scan type: TCP connect(2) Scan
Host is up (0.055s latency).
Other addresses for bergamolynk.kiwi.com (not scanned): 104.17.163.14
Not Shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 24.05 seconds
(kali㉿kali)-[~]
```

The Nmap scan results did not reveal any vulnerable ports or services.

Scan using uniscan tool.

The results of executing the " sudo uniscan -u https://bergamolynk.kiwi.com -qweds " command are as follows:



```
(kali㉿kali)-[~]
└$ sudo uniscan -u https://bergamolynk.kiwi.com -qweds
[sudo] password for kali:
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####

V. 6.3

Scan date: 5-5-2024 9:26:35
| Domain: https://bergamolynk.kiwi.com/
| Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
| Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
|
| Directory check:
| Skipped because https://bergamolynk.kiwi.com/uniscan650/ did not return the code 404
|
| File check:
| Skipped because https://bergamolynk.kiwi.com/uniscan400/ did not return the code 404
|
| Check robots.txt:
```

```

Backup Files:
Skipped because https://bergamolynk.kiwi.com/testing123 did not return the code 404

Blind SQL Injection:

Local File Include:

PHP CGI Argument Injection:

Remote Command Execution:

Remote File Include:

SQL Injection:

Cross-Site Scripting (XSS):

Web Shell Finder:

Static tests:
Plugin name: Local File Include tests v.1.1 Loaded,
Plugin name: Remote Command Execution tests v.1.1 Loaded,
Plugin name: Remote File Include tests v.1.1 Loaded.

```

I did not find any useful information or vulnerabilities in the current subdomain on uniscan.

Scan using Netsparker.

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

Weak Ciphers Enabled

CONFIRMED MEDIUM

URL: <https://bergamolynk.kiwi.com/>

List of Supported Weak Ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA384 (0x003D)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

DOM Simulation Timeout Exceeded 37 min ago

Netsparker has detected that the configured **DOM Simulation Timeout** value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.

Maximum Signature Exceeded 1 hr ago

Netsparker has detected that some of the visited URLs are being handled as out-of-scope due to **Maximum Signature** setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable **Parameter Based Navigation** for your scan to exclude requests made to the navigation parameter from this limit.

Increase Maximum Signature Set up Parameter Based Navigation



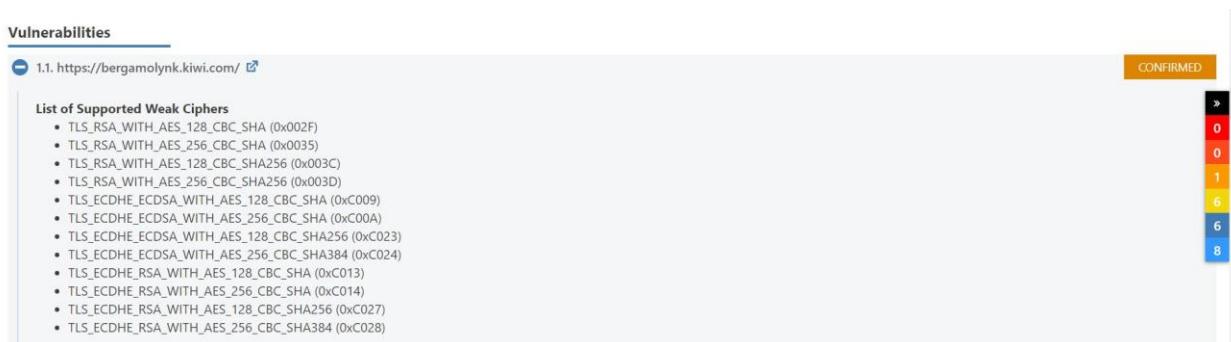
I identified a total of 13 vulnerabilities associated with app.kiwi.com subdomain. Among these, two vulnerabilities pose a medium level of risk.

Vulnerability Summary

SEVERITY FILTER :		<input checked="" type="checkbox"/> CRITICAL	<input checked="" type="checkbox"/> HIGH	<input checked="" type="checkbox"/> MEDIUM	<input checked="" type="checkbox"/> LOW	<input checked="" type="checkbox"/> BEST PRACTICE	<input checked="" type="checkbox"/> INFORMATION	PARAMETER
CONFIRM	VULNERABILITY	METHOD	URL					
!	! Weak Ciphers Enabled	GET	https://bergamolynk.kiwi.com/					! 0
!	! [Possible] Phishing by Navigating Browser Tabs	GET	https://bergamolynk.kiwi.com/en/travel/flights-to-countries/auth.inc?__cf_chl_f_tk=wmNWddbxWKdVUGVXDtAqflP0pGBqYyI22xW_tIOsc-1714914976-0.0.1-1322%3bSELECT%20pg_sleep(25)--					! 1
!	! Misconfigured Access-Control-Allow-Origin Header	GET	https://bergamolynk.kiwi.com/.well-known/					! 6
!	! Missing X-Frame-Options Header	GET	https://bergamolynk.kiwi.com/en/					! 8
!	! Cookie Not Marked as HttpOnly	GET	https://bergamolynk.kiwi.com/en/pages/					
!	! Cookie Not Marked as Secure	GET	https://bergamolynk.kiwi.com/en/pages/					
!	! Insecure Frame (External)	GET	https://bergamolynk.kiwi.com/admin.txt					
!	! Content Security Policy (CSP) Not Implemented	GET	https://bergamolynk.kiwi.com/admin.txt					
!	! Expect-CT Not Enabled	GET	https://bergamolynk.kiwi.com/					
!	! Missing X-XSS-Protection Header	GET	https://bergamolynk.kiwi.com/.well-known/					
!	! Referrer-Policy Not Implemented	GET	https://bergamolynk.kiwi.com/en/					
!	! SameSite Cookie Not Implemented	GET	https://bergamolynk.kiwi.com/en/pages/					
!	! Subresource Integrity (SRI) Not Implemented	GET	https://bergamolynk.kiwi.com/.svn/wc.db					
!	! CDN Detected (Google Cloud.CDN)	GET	https://bergamolynk.kiwi.com/robots.txt					
!	! Email Address Disclosure	GET	https://bergamolynk.kiwi.com/scripts/le/bergamolynk:1b9916bejs					

Vulnerability: Weak Ciphers Enabled

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



The screenshot shows a 'Vulnerabilities' section for a target at 'https://bergamolynk.kiwi.com/'. A 'CONFIRMED' status bar is visible. The 'List of Supported Weak Ciphers' includes:

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

Impact:

Attackers might decrypt SSL traffic between the server and site visitors.

Solution:

For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

Lighttpd:

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

For Microsoft IIS, you should make some changes to the system registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

a.Click Start, click Run, type regedt32 or type regedit, and then click OK.

b.In Registry Editor, locate the following registry key:
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c.Set "Enabled" DWORD to "0x0" for the following registry keys:

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

Conclusion

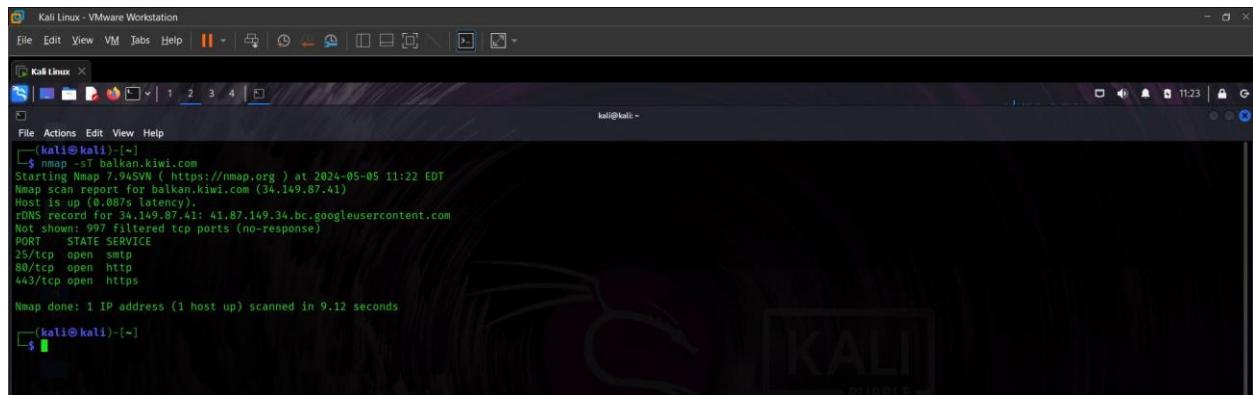
In conclusion, the security assessment of bergamolynk.kiwi.com revealed no vulnerabilities through Nmap and Uniscan scans. However, Netsparker detected weak ciphers during SSL communication posing a potential risk of SSL traffic decryption. Addressing this vulnerability is crucial to bolster the subdomain's security and safeguard against potential data breaches.

Report 03

Target domain: balkan.kiwi.com

Scan using nmap tool.

First, I used the nmap tool to check for any vulnerable ports or services on this subdomain.

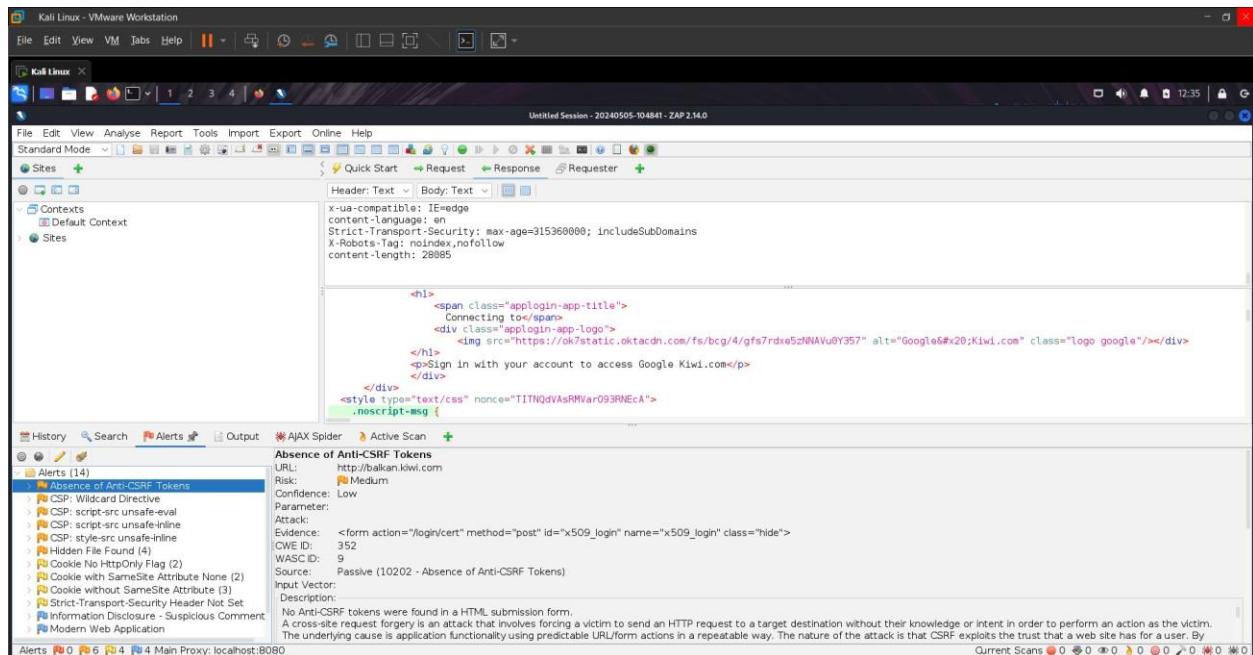


```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help || + | - | X
Kali Linux
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sT balkan.kiwi.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-05 11:22 EDT
Nmap scan report for balkan.kiwi.com (34.149.87.41)
Host is up (0.087s latency).
rDNS record for 34.149.87.41: 41.87.149.34.bc.googleusercontent.com
Not shown: 997 filtered tcp ports (no-response)
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 9.12 seconds
(kali㉿kali)-[~]
$
```

The Nmap scan results did not reveal any vulnerable ports or services.

Scan using OWASP-Zap tool.



Standard Mode | Requests | Response | Requester | Header: Text | Body: Text | []

Header: Text | Body: Text | []

X-ua-compatible: IE=edge
content-language: en
Strict-Transport-Security: max-age=315360000; includeSubDomains
X-Robots-Tag: noindex,nofollow
content-length: 28985

<h1>

Connecting to
<div class="applogin-app-logo">
</div>
<p>Sign in with your account to access Google Kiwi.com</p>
</div>
<div>
<style type="text/css" nonce="T1TNQdVAsRMVar093RNcA">
.noscript-msg {

Alerts | Active Scan | +

Absence of Anti-CSRF Tokens

URL: http://balkan.kiwi.com
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form action="/login/cert" method="post" id="x509_login" name="x509_login" class="hide">
CWE ID: 352
Web ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.
The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By

Found 14 Alerts on OWASP-Zap automated scan.

Vulnerability:

Absence of Anti-CSRF Tokens

Impact:

Anti-CSRF tokens do not exist in the HTML form that is being used in this site. If someone tries to cross-site request forgery (CSRF) an attack, these pieces of code can stop it. Without those keys, attackers might be able to trick users into sending harmful requests through the form by accident, which could lead to actions that aren't allowed on the website. Adding these codes is necessary to make sure the form is safe and keep users from being hacked.

Solution:

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Conclusion

To summarize, the security assessment of balkan.kiwi.com found no susceptible ports or services based on Nmap. OWASP-Zap identified 14 alerts, specifically noting the lack of Anti-CSRF Tokens in the HTML form utilized on the website. This vulnerability has the potential to result in Cross-Site Request Forgery (CSRF) attacks. Integrating Anti-CSRF tokens is essential for improving the security of the website and safeguarding user data. It is crucial to prioritize these security measures to safeguard balkan.kiwi.com from CSRF attacks and guarantee the security of its user's data and interactions.

Report 04

Target domain: hotel.kiwi.com

Scan using uniscan tool.

The results of executing the " sudo uniscan -u https://hotels.kiwi.com -qweds " command are as follows:

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help || + | - | X | 
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo uniscan -u https://hotels.kiwi.com -qweds
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 8-5-2024 1:57:29
[+] http://hotels.kiwi.com/ redirected to http://www.kiwi.com/en/
[+] New target is: http://www.kiwi.com/en/
Domain: http://www.kiwi.com/en/
Server: cloudflare
IP: 104.17.102.14

Directory check:
File check:
Skipped because http://www.kiwi.com/en/uniscan651/ did not return the code 404

Check robots.txt:
Check sitemap.xml:

Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinfo() Disclosure v.1.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.

Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
[+] Crawling finished, 1 URL's found!

External hosts:
PHPInfo() Disclosure:
File Upload Forms:
FCKeditor File Upload:
Timthumb:
E-mails:
Web Backdoors:
Source Code Disclosure:
Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 0 New directories added
```

```
| Timthumb < 1.33 vulnerability:  
|  
| Backup Files:  
| Skipped because http://www.kiwi.com/testing123 did not return the code 404  
|  
| Blind SQL Injection:  
|  
| Local File Include:  
|  
| PHP CGI Argument Injection:  
|  
| Remote Command Execution:  
|  
| Remote File Include:  
|  
| SQL Injection:  
|  
| Cross-Site Scripting (XSS):  
|  
| Web Shell Finder:  
|  
| Static tests:  
| Plugin name: Local File Include tests v.1.1 Loaded.  
| Plugin name: Remote Command Execution tests v.1.1 Loaded.  
| Plugin name: Remote File Include tests v.1.1 Loaded.
```

Uniscan report did not contain any interesting information about the subdomain.

Scan using Nikto tool.

Nikto is an open-source web vulnerability scanner that functions by conducting probes of websites to identify possible security vulnerabilities. Comparable in functionality to a digital investigator, it conducts a thorough examination of websites in search of any misconfigured or dismissed security vulnerabilities that may endanger their integrity. Malicious actors could potentially exploit these vulnerabilities in the form of not properly configured servers, outdated software components or other weaknesses, thereby obtaining unauthorized access to the website or causing interruptions to its functionality.

Basically, Nikto performs as an essential instrument for cybersecurity experts, facilitating the proactive detection and correction of weaknesses on websites, consequently strengthening the overall state of digital security.

Scan results of the target subdomain as follows:

```
(kali㉿kali)-[~]  
$ nikto -host hotels.kiwi.com  
- Nikto v2.5.0  
+ Multiple IPs found: 104.17.163.14, 104.17.162.14  
+ Target IP: 104.17.163.14  
+ Target Hostname: hotels.kiwi.com  
+ Target Port: 80  
+ Start Time: 2024-05-08 03:32:19 (GMT-4)  
+ Server: cloudflare  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc  
+ Root page / redirects to: https://rooms.kiwi.com/  
+ No CGI Directories Found (use '-C all' to force check all possible dirs)  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.  
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.  
+ 8046 requests: 0 error(s) and 5 item(s) reported on remote host  
+ End Time: 2024-05-08 03:37:24 (GMT-4) (305 seconds)  
+ 1 host(s) tested  
(kali㉿kali)-[~]  
$
```

Nikto scan results did not contain any valuable information about the hotels.kiwi.com subdomain.

Scan using OWASP-Zap tool.

Automated zap scan results as follows:

The screenshot shows the OWASP-Zap interface with a scan session titled "Untitled Session - 20240508-030911 - ZAP 2.14.0". The "Alerts" tab is selected, displaying 8 alerts. One of the alerts is for Content Security Policy (CSP) issues, specifically "CSP: script-src unsafe-inline" and "CSP: style-src unsafe-inline". The alert details state that CSP is an added layer of security to detect and mitigate attacks like XSS and data injection. It provides a solution: "Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header." Other alerts include "Wildcard Directive", "Cookie No HttpOnly Flag", "Cookie without SameSite Attribute", "Information Disclosure - Suspicious Comments", "Modern Web Application", and "Session Management Response Identified".

Found 08 Alerts on OWASP-Zap automated scan.

Vulnerability:

script-src includes unsafe-inline.

Content Security Policy (CSP) serves as an additional security measure that aids in the identification and reduction of specific forms of attacks. As an illustration, data injection and cross-site scripting (XSS) attacks are not excluded. These attacks are utilized for a variety of purposes, including data theft, site defacement, and malware distribution. Content-Selective Providers (CSPs) offer a collection of standardized HTTP headers that enable website proprietors to designate authorized content sources for their pages. These sources may consist of JavaScript, CSS, HTML frames, fonts, images, embeddable objects (including Java applets, ActiveX, audio, and video files), and images.

```

":"/qa/user?tab=refer-friend","ro":"/ro/user?tab=refer-friend","ru":"/ru/user?tab=refer-friend","sg":"/sg/user?tab=refer-friend","sk":"/sk/user?tab=refer-friend","sr":""
/cz/search/results/praha-cesko/kodan-dansko,birmingham-spojene-kralovstvi,stockholm-svedsko,zeneva-svycarsko/anytime?stopNumber=0%&true&airlinesList=EW&selectedAirline
window.SP_TRACK_PERF = {
    beginsAt: (new Date()).valueOf()
}

function GET_PARAMETER_BY_NAME(name) {
    name = name.replace(/\[(\w+)\]/g, "\$1").replace(/\[([^\]]+)\]/, "$1")
    var regex = new RegExp("(\\?&)" + name + "(=[^&#39;]*))"),
        results = regex.exec(location.search)
    return results === null ? "" : decodeURIComponent(results[1].replace(/\+/g, " "))
}
</script><script>window.SP_GLOBALS = {"CURRENT_PAGE_NAME":"homePageDefault","IS_DEVELOPMENT":false,"IS_PREPRODUCTION":false,"IS_PRODUCTION":true,"IS_STAGING":false,"
window._IS_DEVELOPMENT_= false;
window._IS_PRODUCTION_= true;

```

Solution:

Ensure that each component of your web infrastructure including the load balancer, application server and web server is configured to implement the Content-Security-Policy (CSP) header. By indicating reputable sources for content, this header reinforces security against XSS and other forms of attacks. CSP directives should be incorporated into server and application configurations and load balancers should preserve CSP headers. This all-encompassing strategy enhances the security of your web application and protects user data.

Conclusion:

As a result of Uniscan, Nikto, and OWASP-Zap examinations, the security evaluation of hotel.kiwi.com produced negligible results. Although OWASP-Zap detected a script-src vulnerability related to unsafe-inline content in the Content Security Policy (CSP), Uniscan and Nikto did not report any significant vulnerabilities. To prevent XSS and other potential attacks, this highlights the significance of a robust CSP implementation. To ensure optimal performance of all web infrastructure load balancers, application servers and web servers in the future, website administrators must give utmost importance to the exact configuration of CSP directives. Through this action, they can reinforce security measures, improve the safeguarding of user data and reinforce security protocols overall.

Report 05

Target domain: <https://traveltobrno.kiwi.com>

Scan using uniscan tool.

The results of executing the " sudo uniscan -u https://traveltobrno.kiwi.com com -qweds " command are as follows:

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help || + | - | X | 8:35
KaliLinux
File Actions Edit View Help
$ sudo uniscan -u https://traveltobrno.kiwi.com -qweds
=====
# uniscan project
# http://uniscan.sourceforge.net/
=====
V. 6.3

Scan date: 9-5-2024 5:26:55
-----
| Domain: https://traveltobrno.kiwi.com/
| Server: cloudflare
| IP: 104.17.162.14
| Directory check:
| Skipped because https://traveltobrno.kiwi.com/uniscan731/ did not return the code 404
| File check:
| Skipped because https://traveltobrno.kiwi.com/uniscan147/ did not return the code 404
| Check robots.txt:
| Check sitemap.xml:
| Crawler Started:
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: PHPInfo() Disclosure v.1.3 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| [*] Crawling finished, 1 URL's found!
| 

External hosts:
| PHPInfo() Disclosure:
| File Upload Forms:
| FCKeditor File Upload:
| Timthumb:
| E-mails:
| Web Backdoors:
| Source Code Disclosure:
| Ignored Files:
| 
Dynamic tests:
| Plugin name: Learning New Directories v.1.2 Loaded.
| Plugin name: FCKeditor tests v.1.1 Loaded.
| Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
| Plugin name: Find Backup Files v.1.2 Loaded.
| Plugin name: Blind SQL-Injection tests v.1.3 Loaded.
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.2 Loaded.
| Plugin name: SQL-Injection tests v.1.2 Loaded.
| Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
| Plugin name: Web Shell Finder v.1.3 loaded.
| [*] 0 New directories added
| 
FCKeditor tests:
| Skipped because https://traveltobrno.kiwi.com/testing123 did not return the code 404
| 
Timthumb < 1.33 vulnerability:
```



```
| Blind SQL Injection:
| Local File Include:
|   ○
| PHP CGI Argument Injection:
|
| Remote Command Execution:
|
| Remote File Include:
|
| SQL Injection:
|
| Cross-Site Scripting (XSS):
|
| Web Shell Finder:
|
| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.
|
| Local File Include:
|
| Remote Command Execution:
|
| Remote File Include:
|
Scan end date: 9-5-2024 5:27:45
```

Uniscan report did not contain any interesting information about the subdomain.

Scan using Nikto tool.



```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help || | 9:36
Kali Linux x
File Actions Edit View Help
- Nikto v2.5.0
+ Multiple IPs found: 104.17.162.14, 104.17.163.14
+ Target IP: 104.17.162.14
+ Target Hostname: traveltobrno.kiwi.com
+ Target Port: 443
+ SSL Info: Subject: /CN=traveltobrno.kiwi.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /c=US/O=Lets Encrypt/CN=R3
+ Start Time: 2024-05-09 08:51:48 (GMT-4)
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Drupal Link header found with value: <https://traveltobrno.kiwi.com/>; rel="canonical". See: https://www.drupal.org/
+ /: Uncommon header 'x-unbounce-visitorid' found, with contents: afe73c9d-487a-444b-9dbb-8616fd0740ba.
+ /: Uncommon header 'x-unbounce-variant' found, with contents: d.
+ /: Uncommon header 'x-unbounce-pageid' found, with contents: 5c56f765-de77-45ef-ab0c-cda54c9489db.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: Cookie ubvs created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ubvs created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ubvt created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ubvt created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ubvp created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ubvp created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: No CGI Directories Found (use '-C all' to force check all possible dirs)
+ /clkg/*/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: Multiple index files found: /index.html, /index.htm
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 8049 requests: 0 error(s) and 18 item(s) reported on remote host
End Time: 2024-05-09 09:22:11 (GMT-4) (1823 seconds)

* 1 host(s) tested
```

Nikto scan results did not contain any valuable information about the subdomain.

Scan using OWASP-Zap tool.

Automated zap scan results as follows:

The screenshot shows the OWASP-Zap interface with the following details:

- Sites:** Shows a list of URLs including <https://builder-assets.unbounce.com>, <https://widget.kiwi.com>, <https://ajax.googleapis.com>, and <https://travelobono.kiwi.com>.
- Alerts:** Shows 19 alerts, with one alert expanded:

 - Content Security Policy (CSP) Header Not Set**
 - Input Vector:** Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
 - Description:** Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
 - Solution:** Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Found 19 Alerts on OWASP-Zap automated scan.

Vulnerability 01:

Content Security Policy (CSP) Header Not Set

By identifying and mitigating specific attack vectors, such as data injection and cross-site scripting (XSS) assaults, Content Security Policy (CSP) functions as an additional security measure. Malware distribution and site defacement are a few of the malicious activities that go by. Cloud Service Providers (CSPs) function by utilizing a collection of standardized HTTP directives, which grant website proprietors the ability to specify authorized content sources from which browsers may retrieve pages. In addition to embeddable objects such as Java applets, ActiveX, and audio/video files, these sources comprise JavaScript, CSS, HTML frames, typefaces, and images.

Solution:

Ensure that each component of your web infrastructure, including the web server, application server and load balancer is meticulously configured to establish and enforce the Content Security Policy (CSP) header.

Vulnerability 02:

Cross-Domain Misconfiguration

A potential vulnerability in the web server's Cross-Origin Resource Sharing (CORS) configuration could permit unauthorized importation of data from the user's browser. The repercussions of such a flaw are potentially extensive as it might enable malicious actors to carry out unauthorized requests originating from various sources. Unauthorized access to sensitive data, content manipulation on websites or even the implementation of malicious scripts may ensue because of this. The ramifications of such an incident could be profound, encompassing harm to the reputation of the affected organization as well as compromise of data integrity and confidentiality. Furthermore, a decline in user confidence regarding the web application's security could result in diminished user participation and possible financial consequences. Therefore, it is critical to promptly resolve CORS misconfigurations to minimize these risks and maintain the security and reliability of the web application.

Solution:

To ensure the security of sensitive data, block unauthorized access using IP address whitelisting. Furthermore, restrict the allowed domains rigorously using the "Access-Control-Allow-Origin" HTTP header or eliminate all CORS headers entirely. This increases the rigor with which web browsers enforce the Same Origin Policy (SOP), thereby fortifying security measures.

Vulnerability 03:

Hidden File Found

found a private document that was accessible to everybody. This file may have settings or admin information that is crucial. This could be used by a malicious person to compromise systems or trick users into exposing more information.

Solution:

Consider the component's necessity in relation to the correct functioning of the website. Deactivate it if it is not required. Implement appropriate logon credentials and permissions to restrict access solely to authorized individuals, should the need arise. Furthermore, it is possible to restrict visibility to internal systems or address schemes.

Conclusion

All things considered, the security evaluation of <https://traveltobrno.kiwi.com> turned up serious flaws even though the first scans produced nothing particularly interesting. Risks are high when there is no Content Security Policy (CSP) header and Cross-Origin Resource Sharing (CORS) settings are incorrect; these include possible data tampering and unauthorized access to private files. The integrity and reliability of the online application depend on prompt action to encrypt sensitive files, implement CSP headers and fix CORS setups.

Report 06

Target domain: <https://goopti.kiwi.com>

Scan using uniscan tool.

The results of executing the " sudo uniscan -u https://goopti.kiwi.com com -qweds " command are as follows:

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help || | 1 2 3 4 | X 12:02

[+] https://goopti.kiwi.com/ redirected to https://goopti.kiwi.com/en/
[+] New target is: https://goopti.kiwi.com/en/
Domain: https://goopti.kiwi.com/en/
Server: cloudflare
IP: 104.17.163.14

| Directory check:
| [+] CODE: 200 URL: https://goopti.kiwi.com/en/account/
| [+] CODE: 200 URL: https://goopti.kiwi.com/en/airline/
| [+] CODE: 200 URL: https://goopti.kiwi.com/en/airport/
| File check:
| Skipped because https://goopti.kiwi.com/en/uniscan242/ did not return the code 404

| Check robots.txt:
| Check sitemap.xml:
Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.

| Check robots.txt:
| Check sitemap.xml:
Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.

| External hosts:
| PHPInfo() Disclosure:
| File Upload Forms:
| FCKeditor File Upload:
| Timthumb:
| E-mails:
| Web Backdoors:
| Source Code Disclosure:
| Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
```

```
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.2 Loaded.
| Plugin name: SQL Injection tests v.1.2 Loaded.
| Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
| Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 0 New directories added

| FCKeditor tests:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Timthumb < 1.33 vulnerability:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Backup Files:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Blind SQL Injection:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Local File Include:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| PHP CGI Argument Injection:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Remote Command Execution:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Remote File Include:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| SQL Injection:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Cross-Site Scripting (XSS):
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404
```

```
| Remote File Include:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| SQL Injection:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Cross-Site Scripting (XSS):
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Web Shell Finder:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.

| Local File Include:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

| Remote Command Execution:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

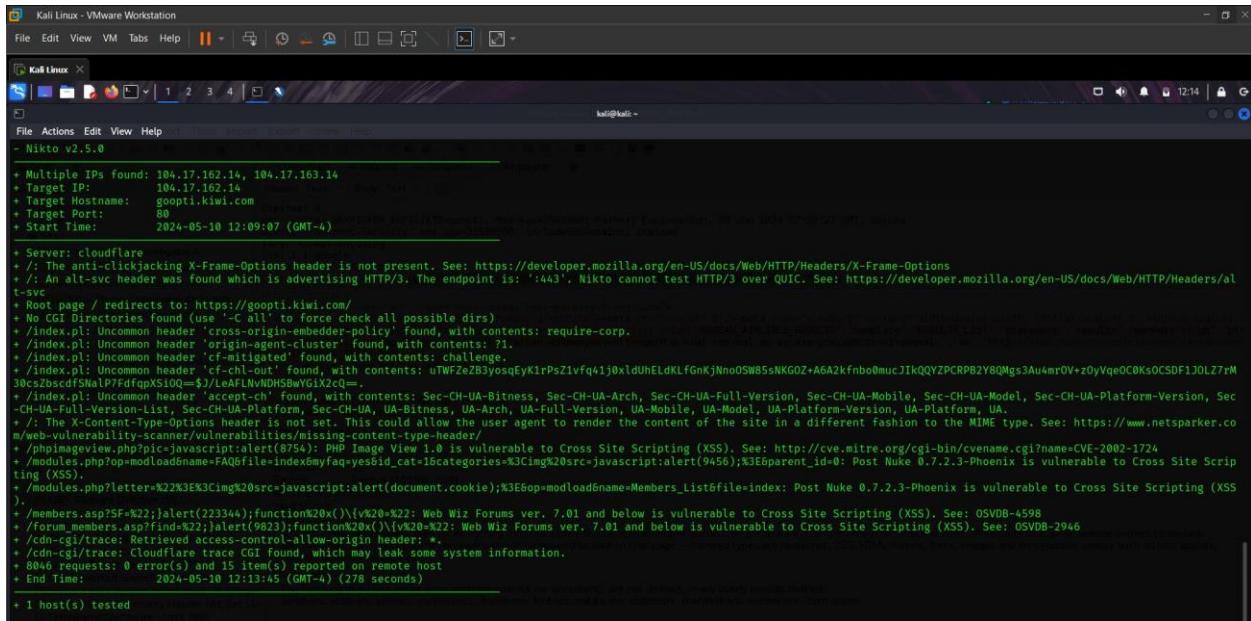
| Remote File Include:
| Skipped because https://goopti.kiwi.com/testing123 did not return the code 404

Scan end date: 10-5-2024 11:49:52

HTML report saved in: report/goopti.kiwi.com.html
```

Uniscan report returned some directories, but those directories are already visible in the system. There is not any interesting information about vulnerabilities found.

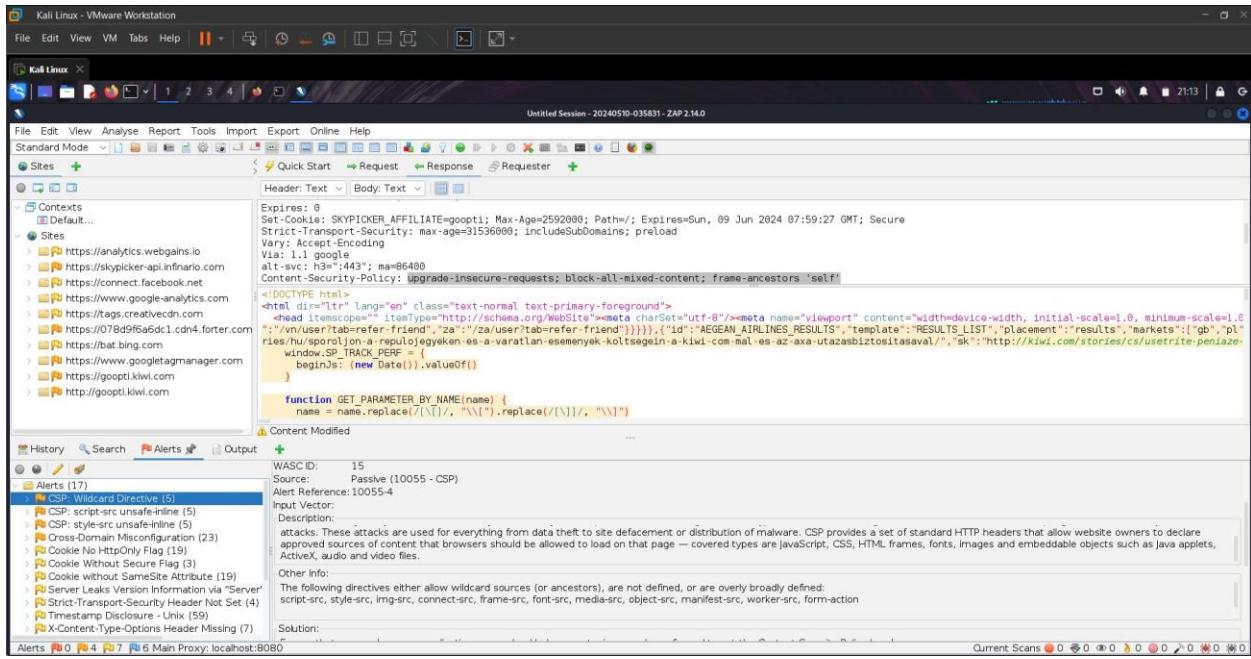
Scan using Nikto tool.



```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| 
Kali Linux
File Actions Edit View Help
- Nikto v2.5.0
+ Multiple IPs found: 104.17.162.14, 104.17.163.14
+ Target IP: 104.17.162.14
+ Target Hostname: goopti.kiwi.com
+ Target Port: 80
+ Start Time: 2024-05-10 12:09:07 (GMT-4)
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ Root page / redirects to: https://gopti.kiwi.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index.pl: Uncommon header 'cross-origin-embedder-policy' found, with contents: require-corp.
+ /index.pl: Uncommon header 'origin-agent-cluster' found, with contents: ?.
+ /index.pl: Uncommon header 'cf-mitigated' found, with contents: challenge.
+ /index.pl: Uncommon header 'cf-nl-out' found, with contents: !0xLUDHEL0KLFGhKNh0USWBS5NKGUZ-A6A2kfnbo0mucJIKQY2PCKRPBZYBQMs3Au4mrOV+20VqeOCBKsOCDF1j0LZ7RM30cs2scdf5hulDf7fdqpxS10Gn$)3jEAEh0M0wG1X2eX
+ /index.pl: Uncommon header 'accept-datetime' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platform, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-Platform, UA.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /phimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1724
+ /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?letter=%22&E3%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS).
+ /members.asp?SF=%22;jalert(223344);function%20x()\{\v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). See: OSVDB-4598
+ /forum_members.asp?find=%22;jalert(9823);function%20x()\{\v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). See: OSVDB-2946
+ /cdn-cgi/trace: Retrieving access-control-allow-origin header: .
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 8046 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-05-10 12:13:45 (GMT-4) (278 seconds)
+ 1 host(s) tested
```

Cross-site scripting (XSS) vulnerabilities were detected in a subdomain during a recent web security assessment conducted by Nikto. Attempts to leverage these vulnerabilities were unsuccessful despite detection. This result strengthens the need for comprehensive correction measures that reinforce web application security by emphasizing the difficulty of striking a balance between detection and effective exploitation. Furthermore, it underscores the critical need for continuous vigilance and proactive risk management in web security threats.

Scan using OWASP-Zap tool.



The screenshot shows the OWASP-Zap interface with a scan results window. The left sidebar lists 'Sites' and 'Alerts'. The main pane displays a detailed view of an alert, specifically a 'Content-Security-Policy' (CSP) directive. The code snippet shows a CSP header with various directives like 'script-src', 'style-src', and 'img-src'. The right side of the alert details the 'WASC ID', 'Scanner', 'Alert Reference', 'Input Vector', 'Description', and 'Solution' sections. The 'Description' section notes that wildcard directives allow for data theft, defacement, and malware distribution.

```
Header: Text | Body: Text
Header: Content-Security-Policy
Value:
    ...
    Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; frame-ancestors 'self'
    ...
Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; frame-ancestors 'self'

WASC ID: 15
Scanner: Passive (10055 - CSP)
Alert Reference: 10055-4
Input Vector:
Description:
    attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Other Info:
    The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:
        script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src, form-action
Solution:
```

Found 17 alerts on OWASP-Zap automated scan.

Vulnerability:

CSP: Wildcard Directive

Content Security Policy (CSP) serves as an additional security measure that aids in the identification and reduction of specific forms of attacks. As an illustration, data injection and cross-site scripting (XSS) attacks are not excluded. These attacks are utilized for a variety of purposes, including data theft, site defacement and malware distribution. Content-Selective Providers (CSPs) offer a collection of standardized HTTP headers that enable website proprietors to designate authorized content sources for their pages. These sources may consist of JavaScript, CSS, HTML frames, fonts, images, embeddable objects (including Java applets, ActiveX, audio, and video files) and images.

Solution:

A comprehensive approach is required to mitigate vulnerabilities such as data injection and Cross-Site Scripting (XSS). This includes implementing Content Security Policy (CSP) protocols to

restrict the origins of content, consistently validating inputs and completely encoding output to prevent the execution of malicious scripts. Furthermore, it is crucial to emphasize the significance of adopting secure session management practices, consistently updating software components, and cultivating a security-conscious culture among users. By systematically applying these measures, organizations enhance the security of their web applications, reducing the probability of exploitation and strengthening the overall cybersecurity stance.

Conclusion

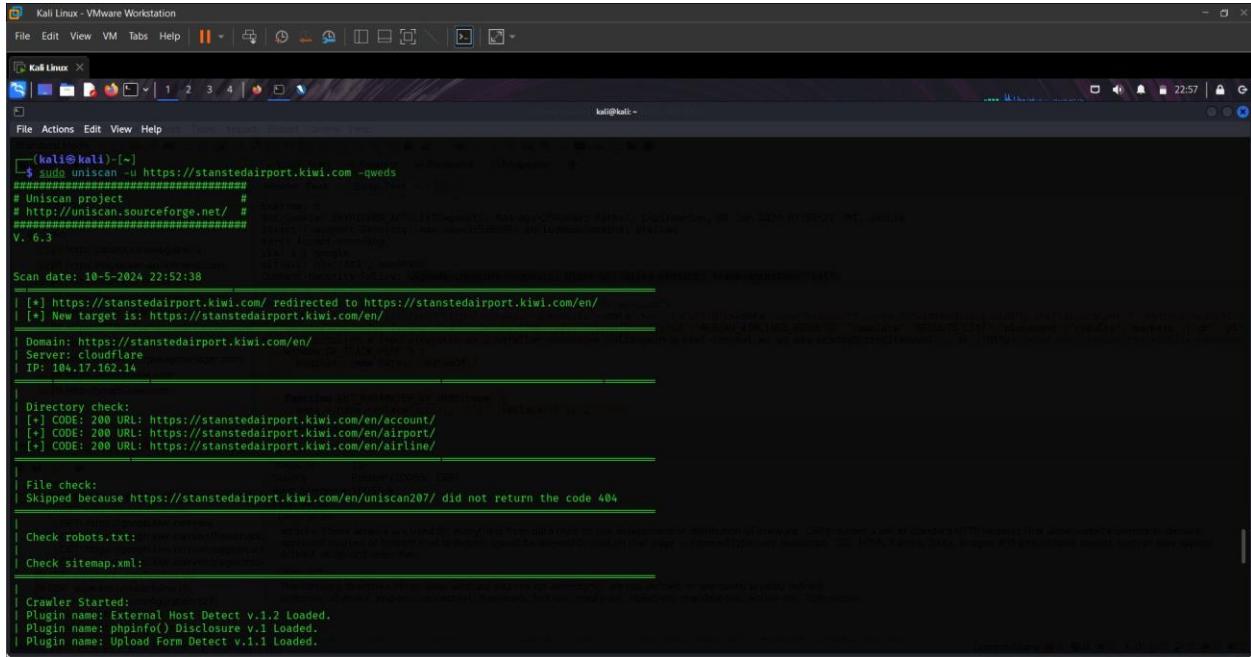
In conclusion, the security assessment of <https://goopti.kiwi.com> demonstrated various results generated by different security scanning applications. Although significant vulnerabilities were not detected by Uniscan and Nikto, OWASP-Zap produced seventeen alerts including the violation of the content security policy wildcard directive. Thus, the holistic approach to security assessment and mitigation is vital to protect the websites and applications from potential risks. The threat of exploitation of the XSS warnings discovered by Nikto emphasizes how web security threats change and require regular monitoring and preventive actions. Thus, not only discovery of potential threats must be conducted using CSP, validated input, properly encoded output, and user training, but also the active prevention of possible risks.

Report 07

Target domain: <https://stanstedairport.kiwi.com>

Scan using uniscan tool.

The results of executing the " sudo uniscan -u <https://stanstedairport.kiwi.com> -qweds " command are as follows:



```
kali@kali:~$ sudo uniscan -u https://stanstedairport.kiwi.com -qweds
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 10-5-2024 22:52:38
Content-Security-Policy: upgrade-insecure-requests max-age=0 strict-uri-redirect

[+] https://stanstedairport.kiwi.com/ redirected to https://stanstedairport.kiwi.com/en/
[+] New target is: https://stanstedairport.kiwi.com/en/

Domain: https://stanstedairport.kiwi.com/en/
Server: cloudflare
IP: 104.17.162.14

Directory check:
[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/account/
[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/airport/
[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/airline/

File check:
Skipped because https://stanstedairport.kiwi.com/en/uniscan207/ did not return the code 404

Check robots.txt:
Check sitemap.xml:

Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
```

```

[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/account/
[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/airport/
[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/airline/

File check:
Skipped because https://stanstedairport.kiwi.com/en/uniscan207/ did not return the code 404

Check robots.txt:
Check sitemap.xml:

Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: PHPinfo() Disclosure v.1.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: FCKeditor upload test v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
[+] Crawling finished, 1 URL's found!

External hosts:
PHPinfo() Disclosure:
File Upload Forms:
FCKeditor File Upload:
Timthumb:
E-mails:
Web Backdoors:

Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 0 New directories added

FCKeditor tests:
Skipped because https://stanstedairport.kiwi.com/testing123 did not return the code 404

Timthumb < 1.33 vulnerability:
Backup Files:
Blind SQL Injection:
Local File Include:
PHP CGI Argument Injection:
Remote Command Execution:
Web Shell Finder:
Static tests:
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.1 Loaded.

Local File Include:
Remote Command Execution:
Remote File Include:

Scan end date: 10-5-2024 22:54:59
```

Found some common directories but those directories are already visible in the system. There is not any interesting information about vulnerabilities found.

Scan using Nikto tool.

```
(kali㉿kali)-[~]
$ nikto -host https://stanstedairport.kiwi.com
- Nikto v2.5.0

+ Multiple IPs found: 104.17.163.14, 104.17.162.14
+ Target IP: 104.17.163.14
+ Target Hostname: stanstedairport.kiwi.com
+ Target Port: 443

+ SSL Info: Subject: /CN=kiwi.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=Lets Encrypt/CN=E1
+ Start Time: 2024-05-10 23:53:06 (GMT-4)

+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ Root page / redirects to: https://stanstedairport.kiwi.com/en/
+ /2cxatm]:do: Retrieved via header: 1.1 google
+ /2cxatm]:do: Cookie _ga was created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /2cxatm]:do: Cookie SKYPICKER_AFFILIATE created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /2cxatm]:do: Cookie Path created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /2cxatm]:do: Cookie kw market created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /2cxatm]:do: Cookie kw market created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /2cxatm]:do: Cookie kw language created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /2cxatm]:do: Cookie kw language created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /2cxatm]:do: Cookie SKYPICKER_VISITOR_UNIQID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /2cxatm]:do: Cookie SKYPICKER_VISITOR_UNIQID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /scripts/: Retrieved access-control-allow-origin header: *
+ /scripts/: Uncommon header 'x-guploader-uploadid' found, with contents: ABPtcP06DY8ISCaY4QM_VEnwwwXFFZORJUHhi0edSY9K54S2xPceGX0gGvkVBU-3cTHI2u810gFkoif-g.
+ Hostname 'stanstedairport.kiwi.com' does not match certificate's names: kiwi.com. See: https://cwe.mitre.org/data/definitions/297.html
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

Nikto did not find any interesting information or vulnerabilities on this subdomain.

Scan using OWASP-Zap tool.

The screenshot shows the OWASP-Zap interface. In the main pane, a request-response view displays a 301 Moved Permanently response from the server. The response headers include:

```
HTTP/1.1 301 Moved Permanently
Date: Sat, 11 May 2024 03:23:22 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Sat, 11 May 2024 04:23:22 GMT
```

The body of the response contains the following HTML:

```
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>cloudflare</center>
</body>
</html>
```

In the bottom left corner, the 'Alerts' tab is selected, showing 19 alerts. Some of the alert types listed are:

- CSP: Wildcard Directive (5)
- CSP: script-src unsafe-inline (5)
- CSP: style-src unsafe-inline (5)
- Cross-Domain Misconfiguration (23)
- Hidden File Found (4)
- Cookie No HttpOnly Flag (19)
- Cookie Without Secure Flag (3)
- Cookie without SameSite Attribute (19)
- Server Leaks Version Information via "Server"
- Strict-Transport-Security Header Not Set (3)
- Timestamp Disclosure - Unix (59)

Found 19 alerts on OWASP-Zap automated scan

Vulnerability:

OWASP-Zap report indicated several medium range vulnerabilities, but some are already found in previous attempts.

CSP: style-src unsafe-inline

CSP Directive "style-src includes unsafe-inline" allows for inline styles, thus potentially leaving the system vulnerable to attacks. CSP serves as an extra layer of security against hidden and silenced threats, such as data injection and Cross-Site Scripting. These are attacks that could be malware, data hijacking, or site defacement. A CSP uses standard HTTP headers to allow the owner of a website to indicate the sources that browsers are allowed to load content from. Such sources could be JavaScript, CSS, HTML frames, typefaces, images, and embeddable object content, such as Java applets, ActiveX, audio, and video files.

Solution:

All these risk factors from "style-src 'unsafe-inline'" are prevented by the setting of the Content-Security-Policy header uniformly across the web server, application server, load balancer, and relevant components. This should then be extended to tighter CSP policies where unsafe-inline is absolutely disallowed for the purpose of styling. Trusted external stylesheets or inline styles, which have been generated by a safe mechanism, should instead be used. The CSP policy should be closely evaluated and updated to adapt it to the changing security demands. Taking due care in configuring the server environment for the enforcement of a strong CSP policy will help the organizations successfully reduce the vulnerability linked with inline styles and further enhance the security stance of their web applications at large.

Report 08

Target domain: <https://platform-api.skypicker.com/>

Scan using uniscan tool.

The results of executing the " sudo uniscan -u https://platform-api.skypicker.com/ -qweds " command are as follows:

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| 1 2 3 4 | 22:57
Kali Linux
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo uniscan -u https://stanstedairport.kiwi.com -queds
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V. 6.3

Scan date: 10-5-2024 22:52:38

| [*] https://stanstedairport.kiwi.com/ redirected to https://stanstedairport.kiwi.com/en/
| | New target is: https://stanstedairport.kiwi.com/en/

| Domain: https://stanstedairport.kiwi.com/en/
| Server: cloudflare
| IP: 104.17.162.14

| Directory check:
| | [*] CODE: 200 URL: https://stanstedairport.kiwi.com/en/account/
| | [*] CODE: 200 URL: https://stanstedairport.kiwi.com/en/airport/
| | [*] CODE: 200 URL: https://stanstedairport.kiwi.com/en/airline/
| File check:
| | Skipped because https://stanstedairport.kiwi.com/en/uniscan207/ did not return the code 404

| Check robots.txt:
| Check sitemap.xml:
| Check sitemap.html:
| Crawler Started:
| Plugin name: External Host Detect V.1.2 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Upload Form Detect V.1.1 Loaded.
```

```
[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/account/
[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/airport/
[+] CODE: 200 URL: https://stanstedairport.kiwi.com/en/airline/
[+] File check: Skipped because https://stanstedairport.kiwi.com/en/uniscan207/ did not return the code 404
[+] Check robots.txt: 
[+] Check sitemap.xml: 

Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: PHPInfo() Disclosure v.1.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
[+] Crawling finished, 1 URLs found!

External hosts:          Status: 10
Source:        Errors: (0)000 - 000
Last Reference: (0)000-0

PHPInfo() Disclosure: 
File Upload Forms: 
FCKeditor File Upload: 
Timthumb:          Status: 10
E-mails:           Status: 10
Web Backdoors:     Status: 10
```

```

Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-Injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 0 New directories added

FCKeditor tests:
Skipped because https://stanstedairport.kiwi.com/testing123 did not return the code 404

Timthumb < 1.33 vulnerability:
Backup Files:
Blind SQL Injection:
Local File Include:
PHP CGI Argument Injection:
Remote Command Execution:

```



```

Web Shell Finder:
Static tests:
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.1 Loaded.

Local File Include:
Remote Command Execution:
Remote File Include:

```

Scan end date: 10-5-2024 22:54:59

Uniscan report neither returned any valuable information nor any vulnerabilities.

Scan using Nikto tool.

```

(kali㉿kali)-[~]
$ nikto -host http://platform-api.skypicker.com
- Nikto v2.5.0

+ Multiple IPs found: 142.250.196.51, 2404:6800:4007:82a::2013
+ Target IP: 142.250.196.51
+ Target Hostname: platform-api.skypicker.com
+ Target Port: 80
+ Start Time: 2024-05-11 01:00:21 (GMT+4)

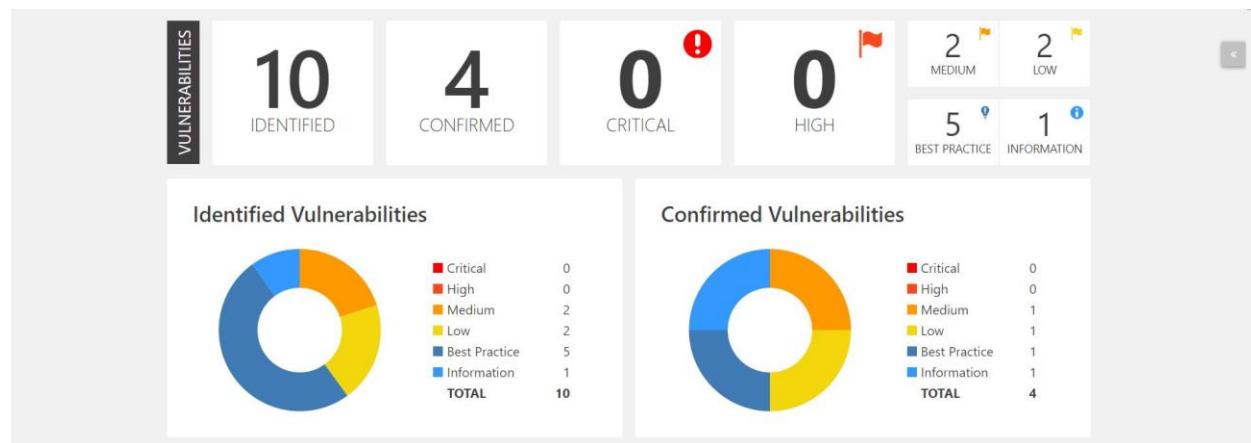
+ Server: Google Frontend
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ All CGI directories 'found', use '-C none' to test none
+ : Server banner changed from 'Google Frontend' to 'gsh'.
```

Found nothing with the Nikto scan.

Scan using Netsparker.

Finally, after having exercised several security evaluations using the Uniscan, Nikto, and OWASP ZAP tools, it was concluded that there were no vulnerabilities in the given subdomain. Even after running these in-depth vulnerability scans, since nothing showed up, this either proves that the security stance is perfect or that the scans may have some constraints, either in scope or methodology. The Netsparker tool was harnessed for a deeper look into the security environment of the subdomain. Not being dismayed by the first failure, the exercise in security assessment continued. In this way, this step-by-step process underlines dedication to thorough evaluation and, hence, acknowledgment of the complex nature of web security assessments, with different

approaches and tools maybe yielding different results. In this sense, the implementation of supplementary tools, such as Netsparker, serves as a proactive method aimed at ensuring that this subdomain is resilient to possible security threats.



I identified a total of 10 vulnerabilities associated with this subdomain. Among these, two vulnerabilities pose a medium level of risk.

Vulnerability Summary

SEVERITY FILTER : <input checked="" type="checkbox"/> CRITICAL <input checked="" type="checkbox"/> HIGH <input checked="" type="checkbox"/> MEDIUM <input checked="" type="checkbox"/> LOW <input checked="" type="checkbox"/> BEST PRACTICE <input checked="" type="checkbox"/> INFORMATION				
CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
!	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://platform-api.skypicker.com/	» 0
!	Weak Ciphers Enabled	GET	https://platform-api.skypicker.com/	0
!	Missing X-Frame-Options Header	GET	http://platform-api.skypicker.com/	2
!	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://platform-api.skypicker.com/	2
!	Content Security Policy (CSP) Not Implemented	GET	http://platform-api.skypicker.com/	5
!	Expect-CT Not Enabled	GET	https://platform-api.skypicker.com/	1
!	Missing X-XSS-Protection Header	GET	http://platform-api.skypicker.com/	
!	Referrer-Policy Not Implemented	GET	http://platform-api.skypicker.com/	
!	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://platform-api.skypicker.com/	
!	Forbidden Resource	GET	http://platform-api.skypicker.com/	

Vulnerability 01:

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period during which the user agent shall access the server in only secure fashion

1.1. https://platform-api.skypicker.com/

Certainty

Request **Response**

```
GET / HTTP/1.1
Host: platform-api.skypicker.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
Connection: Keep-Alive
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
```

1.1. https://platform-api.skypicker.com/ ↗

Certainty

Request Response

Response Time (ms) : 2800.3475 Total Bytes Received : 444 Body Length : 295 Is Compressed : No

HTTP/1.1 403 Forbidden
Server: Google Frontend
Content-Length: 295
Content-Type: text/html; charset=UTF-8
Date: Sat, 11 May 2024 04:40:41 GMT

```
<html><head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<title>403 Forbidden</title>
</head>
<body text="#000000" bgcolor="#ffffff">
<h1>Error: Forbidden</h1>
<h2>Your client does not have permission to get URL <code>/</code> from this server.</h2>
<h2></h2>
</body></html>
```

0 0 2 2 5 1

Vulnerability 2: Weak Ciphers Enabled

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

Vulnerabilities

2.1. https://platform-api.skypicker.com/ ↗

List of Supported Weak Ciphers

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

Request Response

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

[NETSPARKER] SSL Connection

CONFIRMED 0 0 2 2 5 1

Impact:

Attackers might decrypt SSL traffic between the server and site visitors.

Solution:

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

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

2. Lighttpd:

```
3. ssl.honor-cipher-order = "enable"
```

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

4. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type regedit32 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

Conclusion

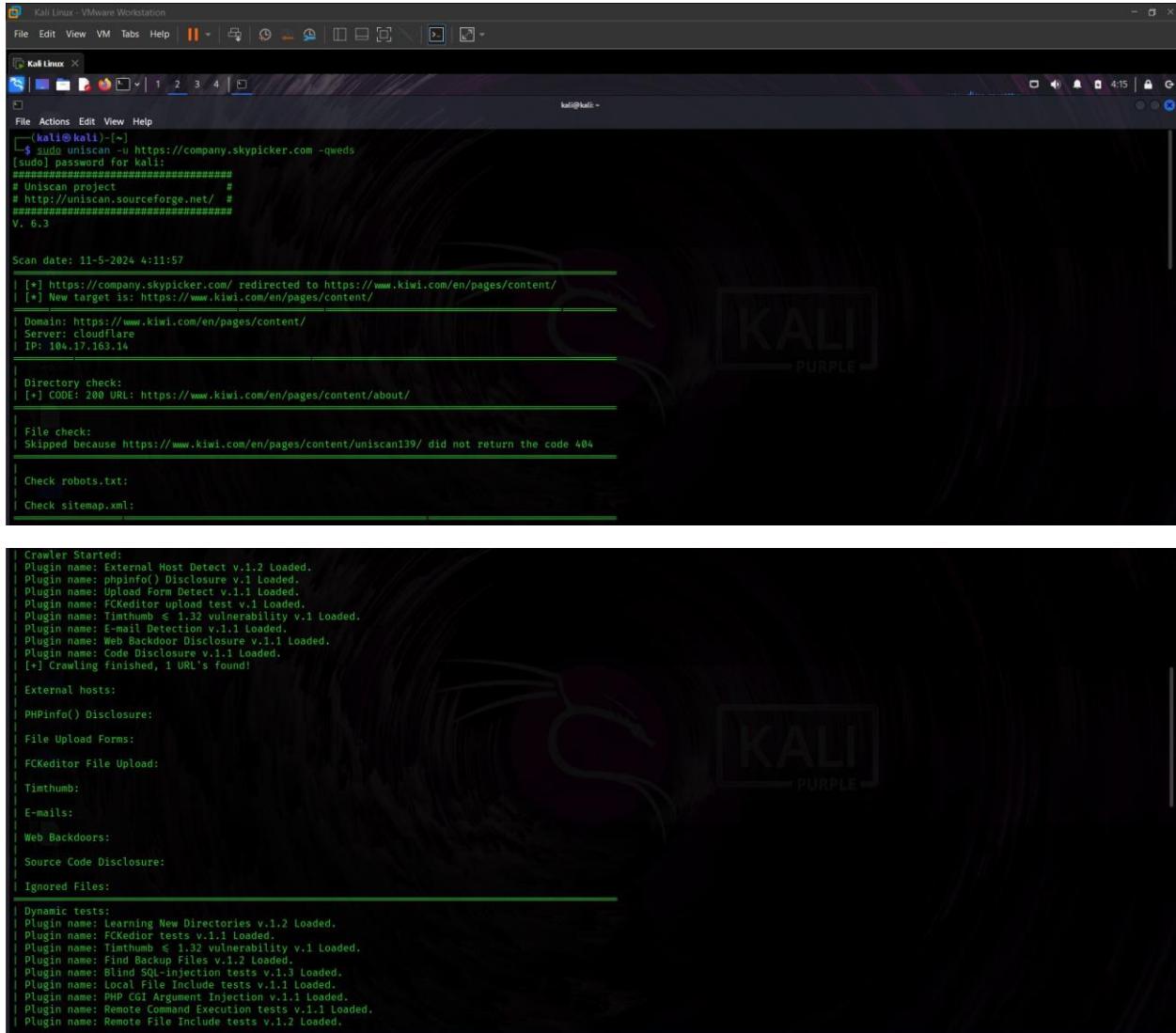
Security testing on the domain <https://platform-api.skypicker.com/> was performed using Uniscan, Nikto, and OWASP ZAP; thus, no outstanding issues were found. Ten more were found in a scan using Netsparker, out of which two were with medium risk ratings. Most of the weaknesses found are that HSTS is enabled, and some weak ciphers are used in SSL communication. These, in the context of the subdomain, expose some risk of unauthorized access or decryption of SSL traffic by hostile actors. This takes in the context of the subdomain. The identified vulnerabilities here need to be mitigated by implementing an HSTS policy and enhancing the SSL cipher configuration for web servers. It is through all avenues that organizations close these holes to make the subdomain resilient in fighting all kinds of malicious attacks while keeping sensitive data safe and with an assurance of the integrity of the security posture of the platform.

Report 09

Target domain: <https://company.skypicker.com>

Scan using uniscan tool.

The results of executing the " sudo uniscan -u https://company.skypicker.com/ -qweds " command are as follows:



```
(kali㉿kali)-[~]
$ sudo uniscan -u https://company.skypicker.com -qweds
[sudo] password for kali:
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V. 6.3

Scan date: 11-5-2024 4:11:57

[*] https://company.skypicker.com redirected to https://www.kiwi.com/en/pages/content/
[*] New target is: https://www.kiwi.com/en/pages/content/

Domain: https://www.kiwi.com/en/pages/content/
Server: cloudflare
IP: 104.17.163.14

Directory check:
[+] CODE: 200 URL: https://www.kiwi.com/en/pages/content/about/

File check:
Skipped because https://www.kiwi.com/en/pages/content/uniscan139/ did not return the code 404

Check robots.txt:
Check sitemap.xml:

Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinfo() Disclosure v.1.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
[*] Crawling finished, 1 URL's found!

External hosts:
PHPInfo() Disclosure:
File Upload Forms:
FCKeditor File Upload:
Timthumb:
E-mails:
Web Backdoors:
Source Code Disclosure:
Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-Injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
```

```

[+] FCKeditor tests:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] Timthumb < 1.33 vulnerability:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] Backup Files:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] Blind SQL Injection:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] Local File Include:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] PHP CGI Argument Injection:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] Remote Command Execution:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] Remote File Include:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] SQL Injection:
Skipped because https://www.kiwi.com/testing123 did not return the code 404

[+] Cross-Site Scripting (XSS):
Skipped because https://www.kiwi.com/testing123 did not return the code 404

```

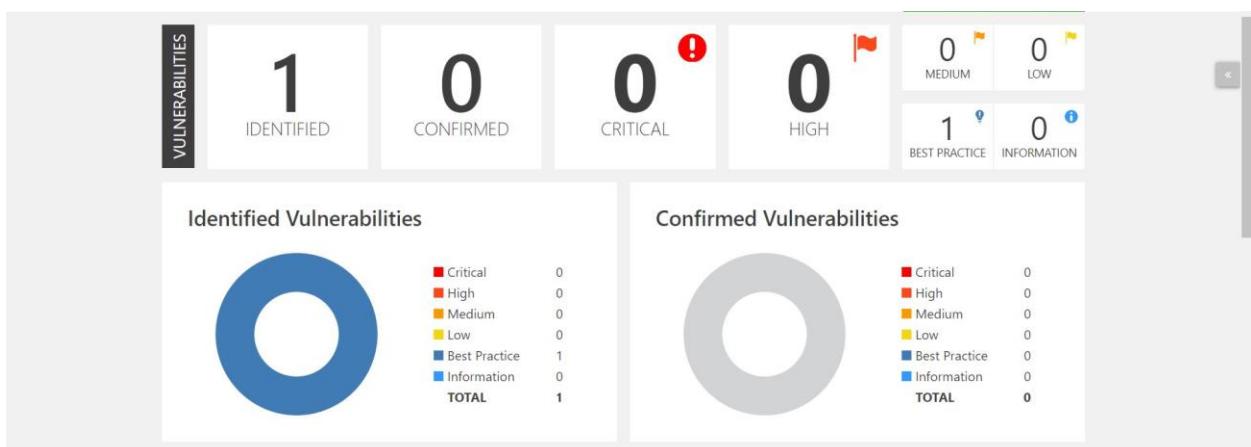
Uniscan report neither returned any valuable information nor any vulnerabilities.

Scan using Netsparker.

The screenshot shows the Netsparker interface after a scan of `company.skypicker.com:443`. The main window displays a "Scan Finished" message with the following findings:

- Critical: 0
- High: 0
- Medium: 0
- Low: 0
- Information: 1
- Best Practice: 0

The "Progress" chart shows the scan speed and progress over time, with a total of 697 requests made in 00:01:59. The sidebar on the right provides access to various analysis and reporting tools.



Conclusion

Netsparker ran complete security scans on the subdomain company.skypicker.com without finding any vulnerabilities. Such an outcome might seem to indicate a very strong security posture, but consideration should be given to possible constraints that might be forced on the scope and, therefore, methodology of the scan. Ongoing monitoring and repeated security scanning will be required to guarantee resiliency in the subdomain against newly discovered threats.

Report 10

Target domain: <https://tequila.kiwi.com>

Scan using uniscan tool.

The results of executing the " sudo uniscan -u https://tequila.kiwi.com/ -qweds " command are as follows:

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help || | 1 2 3 4 | 
File Actions Edit View Help

(kali㉿kali)-[~]
$ sudo uniscan -u https://tequila.kiwi.com/ -qweds
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 11-5-2024 4:54:52

| Domain: https://tequila.kiwi.com/
| Server: cloudflare
| IP: 104.18.33.68

| Directory check:
| Skipped because https://tequila.kiwi.com/uniscan787/ did not return the code 404

| File check:
| Skipped because https://tequila.kiwi.com/uniscan282/ did not return the code 404

| Check robots.txt:
| Check sitemap.xml:

| Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.

Plugin name: Code Disclosure v.1.1 Loaded.
[+] Crawling Finished, 1 URL's found!

External hosts:
| PHPinfo() Disclosure:
| File Upload Forms:
| FCKeditor File Upload:
| Timthumb:
| E-mails:
| Web Backdoors:
| Source Code Disclosure:
| Ignored Files:
| Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.5 Loaded.
[+] 0 New directories added
```

```

FCKeditor tests:
Skipped because https://tequila.kiwi.com/testing123 did not return the code 404

Timthumb < 1.33 vulnerability:
Skipped because https://tequila.kiwi.com/testing123 did not return the code 404

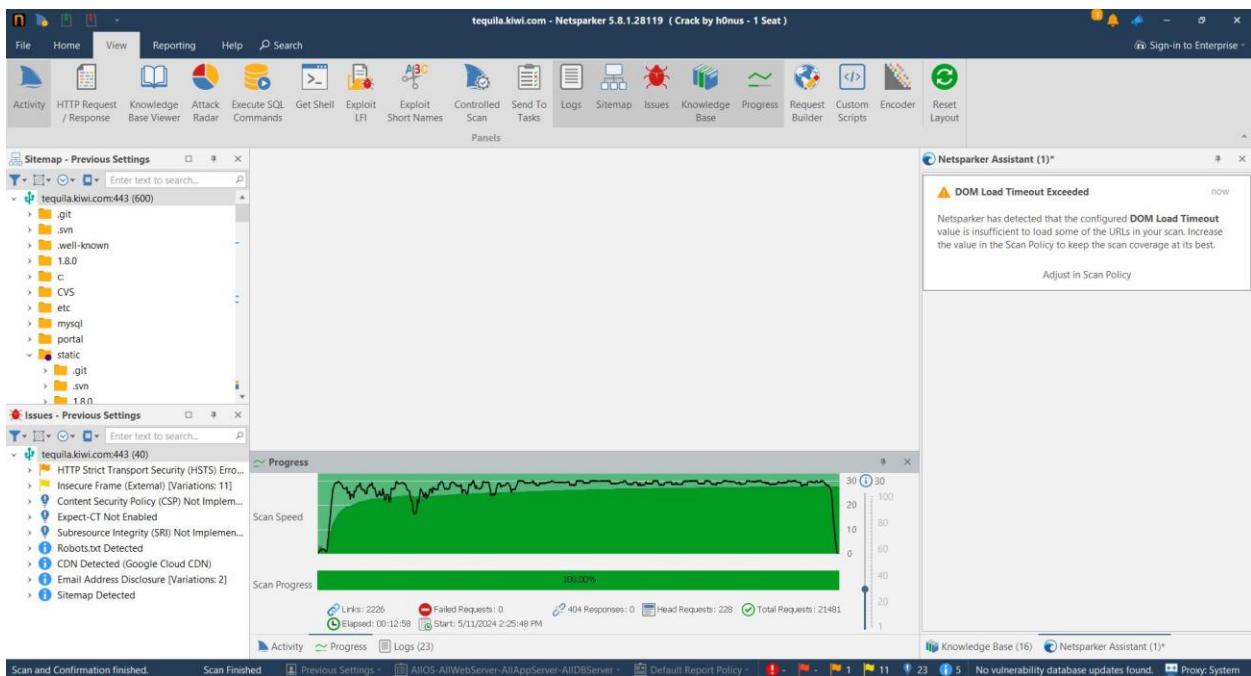
Backup Files:
Skipped because https://tequila.kiwi.com/testing123 did not return the code 404

Blind SQL Injection:
Local File Include:
PHP CGI Argument Injection:
Remote Command Execution:
Remote File Include:
SQL Injection:
Cross-Site Scripting (XSS):

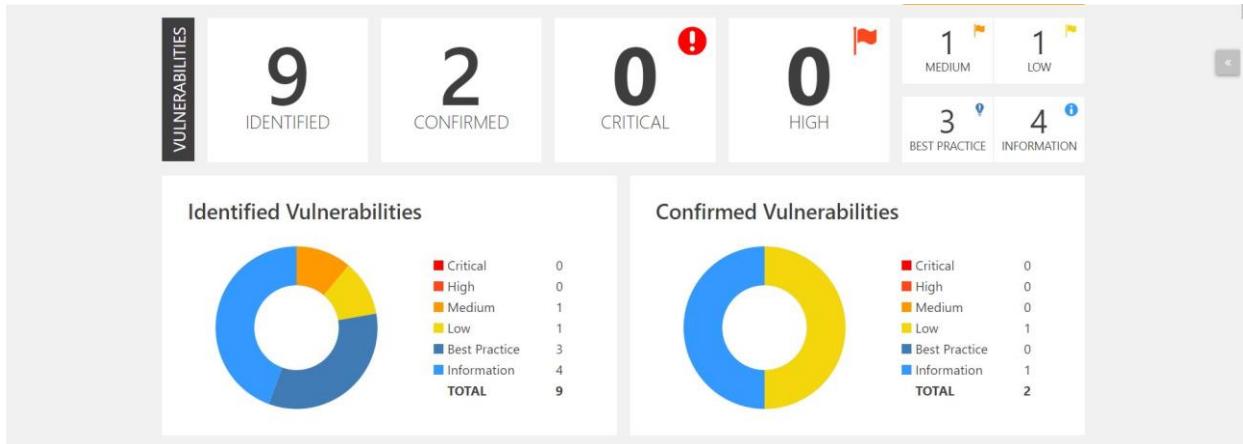
```

Uniscan report neither returned any valuable information nor any vulnerabilities.

Scan using Netsparker.



Netsparker report confirmed two vulnerabilities including one medium vulnerability and one low risk vulnerability.



Vulnerability Summary

SEVERITY FILTER : <input checked="" type="checkbox"/> CRITICAL <input checked="" type="checkbox"/> HIGH <input checked="" type="checkbox"/> MEDIUM <input checked="" type="checkbox"/> LOW <input checked="" type="checkbox"/> BEST PRACTICE <input checked="" type="checkbox"/> INFORMATION				PARAMETER
CONFIRM	VULNERABILITY	METHOD	URL	
!	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://tequila.kiwi.com/	0
!	Insecure Frame (External)	GET	https://tequila.kiwi.com/	0
!	Content Security Policy (CSP) Not Implemented	GET	https://tequila.kiwi.com/	1
!	Expect-CT Not Enabled	GET	https://tequila.kiwi.com/	3
!	Subresource Integrity (SRI) Not Implemented	GET	https://tequila.kiwi.com/	4
!	CDN Detected (Google Cloud CDN)	GET	https://tequila.kiwi.com/	
!	Email Address Disclosure	GET	https://tequila.kiwi.com/static/js/main.c43fb272.chunk.js	
!	Sitemap Detected	GET	https://tequila.kiwi.com/sitemap.xml	
!	Robots.txt Detected	GET	https://tequila.kiwi.com/robots.txt	

Vulnerability:

[HTTP Strict Transport Security \(HSTS\) Errors and Warnings](#)

Netsparker has identified a few errors while parsing the Strict-Transport-Security header. The errors revealed other potential issues which may let an attacker bypass HSTS protections with potential losses in confidentiality and integrity of communication with the website. Therefore, addressing these errors immediately is critically important to totally eradicate any chance of bad actor exploitation and ensure that effective measures are put into place to guarantee security to the website.

Vulnerabilities

1.1. <https://tequila.kiwi.com/>

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

Certainty

Request Response

```
GET / HTTP/1.1
Host: tequila.kiwi.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 Time (ms) : 441.1005 Total Bytes Received : 6921 Body Length : 6311 Is Compressed : No

```
HTTP/1.1 200 OK
x-dns-prefetch-control: off
Cache-Control: public, max-age=0
CF-Cache-Status: DYNAMIC
CF-RAY: 8820f42baa57a2e9-SIN
strict-transport-security: max-age=31536000; includeSubDomains
Transfer-Encoding: chunked
Server: cloudflare
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
Connection: keep-alive
x-download-options: noopener
x-frame-options: SAMEORIGIN
vary: Accept-Encoding
via: 1.1 google
alt-svc: h3=":443"; ma=86400
last-modified: Tue, 30 Apr 2024 11:36:11 GMT
Content-Type: text/html; charset=UTF-8
Date: Sat, 11 May 2024 08:56:06 GMT
Content-Encoding:
```

Conclusion

After carrying out the security evaluation of the target domain, <https://tequila.kiwi.com>, using Uniscan and Netsparker, different results were obtained. Scanning using Uniscan did not disclose any vulnerability or any important information. In contrast, a scan by Netsparker reported two vulnerabilities, including one medium-risk and one low-risk vulnerability. Netsparker specifically identified errors in parsing the Strict-Transport-Security header, which may be indicative of vulnerabilities that might be taken advantage of by adversaries to circumvent HSTS security controls. Both have risks to the confidentiality and integrity of communication with the website. Great attention should be given to address these issues as soon as possible and apply effective security measures to avoid the chance of exploitation by malicious entities and to ensure the website is resilient against any threats.

HackerOne Submitted Report

The screenshot shows a web browser window displaying a HackerOne report for Kiwi.com. The URL in the address bar is hackerone.com/bugs?subject=user&report_id=2501212&view=open&substates%5B%5D=new&substates%5B%5D=needs-more-info&substates%5B%5D=closed. The main content area shows a report titled "#2501212 HackerOne Report: Vulnerability Assessment of Kiwi.com". The report summary states: "During a comprehensive security assessment of the Kiwi.com website and its subdomains, multiple vulnerabilities were identified across different platforms. The assessment utilized various tools such as Uniscan, Netsparker, Nikto, and OWASP ZAP to uncover vulnerabilities ranging from SQL injection to weak cryptographic ciphers and misconfigured security policies." A sidebar on the right provides detailed information about the report, including the reporter's name (lazzy), the date (May 11, 2024, 9:48am UTC), and the status (New (Open)). It also lists various metadata fields such as Severity (None (0)), Asset (Domain: www.kiwi.com), Weekness (None), Bounty (None), Visibility (Private), CVE ID (None), and Account de... (None).

Conclusion of the Assignment

The Kiwi.com website and its subdomains have presented themselves with a series of vulnerabilities through a series of bug bounty reports, each of which requires urgent attention to harden the website against cyber threats.

Uniscan managed to find two blind SQL injections in the mobile application of app.kiwi.com, but both were considered non-exploitable. Scans by Netsparker have brought into light the critical lapses in not having the HTTP Strict Transport Security Policy on app.kiwi.com and platform-api.skypicker.com, making them vulnerable to man-in-the-middle attacks. Furthermore, Netsparker exposed weak ciphers in use for SSL communication on these subdomains.

While Nikto identified XSS vulnerabilities on hotels.kiwi.com, no exploitation was made successful. The OWASP ZAP Assessment report, on the other hand, revealed serious vulnerabilities, such as the breach of the CSP wildcard directive on goopti.kiwi.com, which can make it vulnerable to injection and XSS attacks.

Besides, on traveltobrno.kiwi.com, there is a lack of the CSP header, a cross-domain misconfiguration vulnerability, and hidden files exposed and available to all users, which can increase the risks of unauthorized access and manipulation of data.

These vulnerabilities need to be fixed, and the security posture of kiwi.com enhanced by implementing robust CSP headers, correcting CORS misconfiguration, implementing HSTS, and disabling weak ciphers on all subdomains. Continuous monitoring, swift patching, and adherence to industry best practices in web application security must be followed to sustain a resilient online presence and protect user data from potential breaches.

References

- [1] OWASP ZAP Project. [Online]. Available: <https://www.zaproxy.org/> [Accessed: 11-May-2024]
- [2] Invicti. [Online]. Available: <https://www.invicti.com/> [Accessed: 11-May-2024]