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 identify 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.

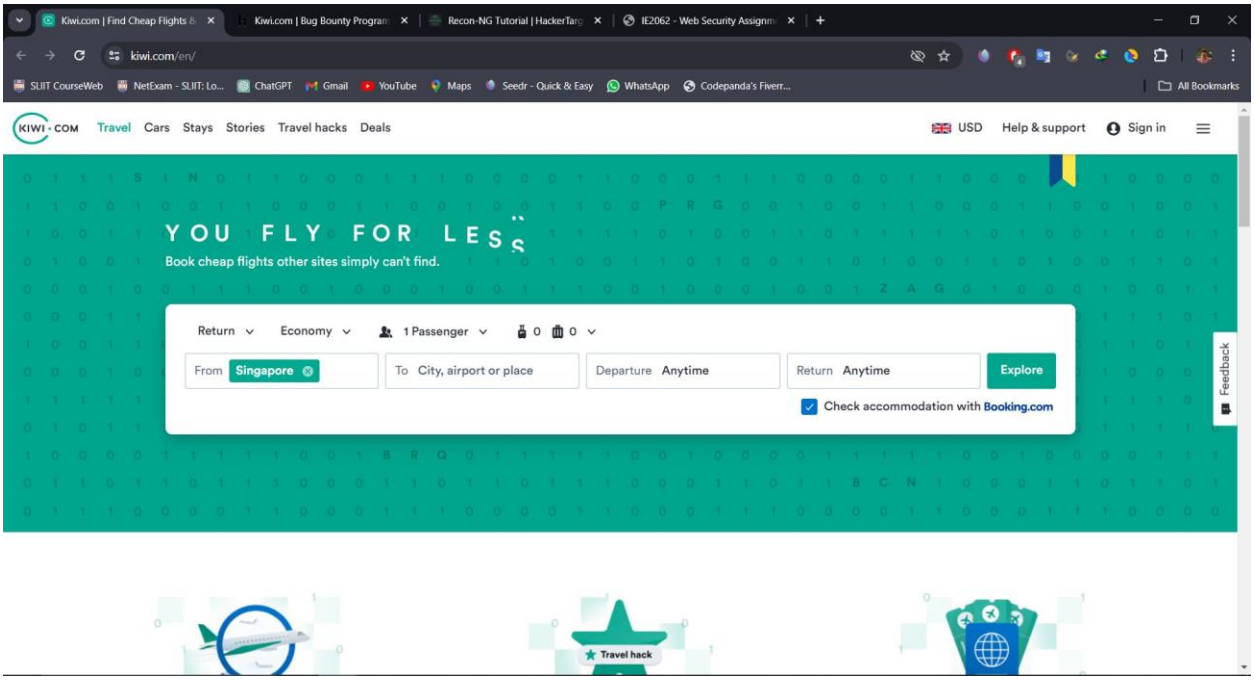
The importance of scanning websites and web apps for security issues is examined in this study. We will observe how these security measures follow the law and reduce the risk of cyberattacks. We can determine how successful these safeguards are by examining actual cases and industry standards. Our aim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

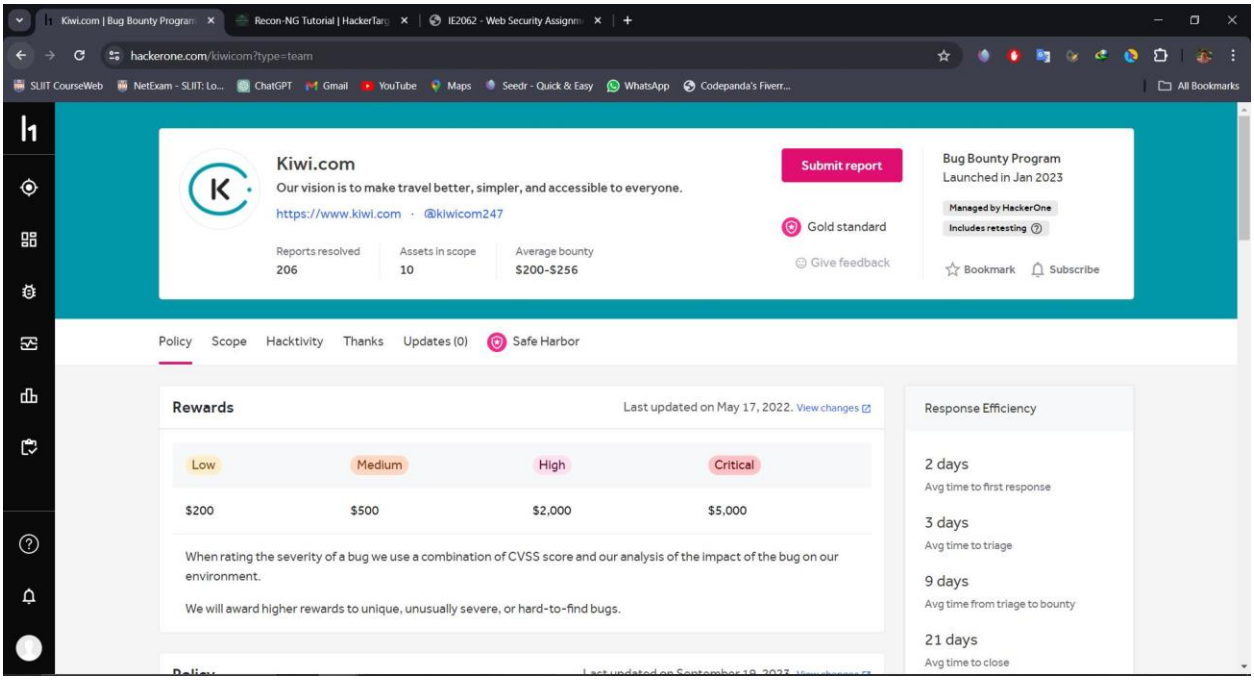
Target domain – https://www.kiwi.com/



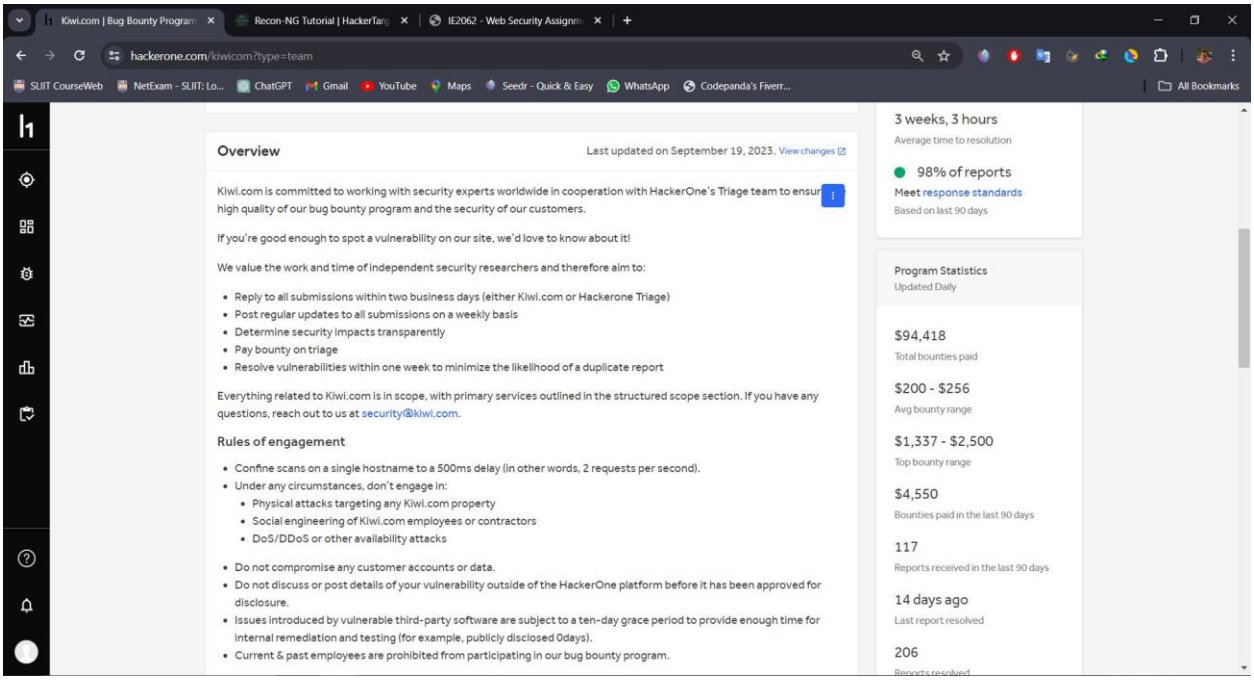
Kiwi.com, formerly known as skypicker.com is a digital travel agency founded in 2012 by Oliver Dlouhý and Jozef Képesi, with its headquarters located in the Czech Republic. Kiwi.com acts as a middleman website that makes it easier to look for and book flights and ground transportation. One unique feature 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

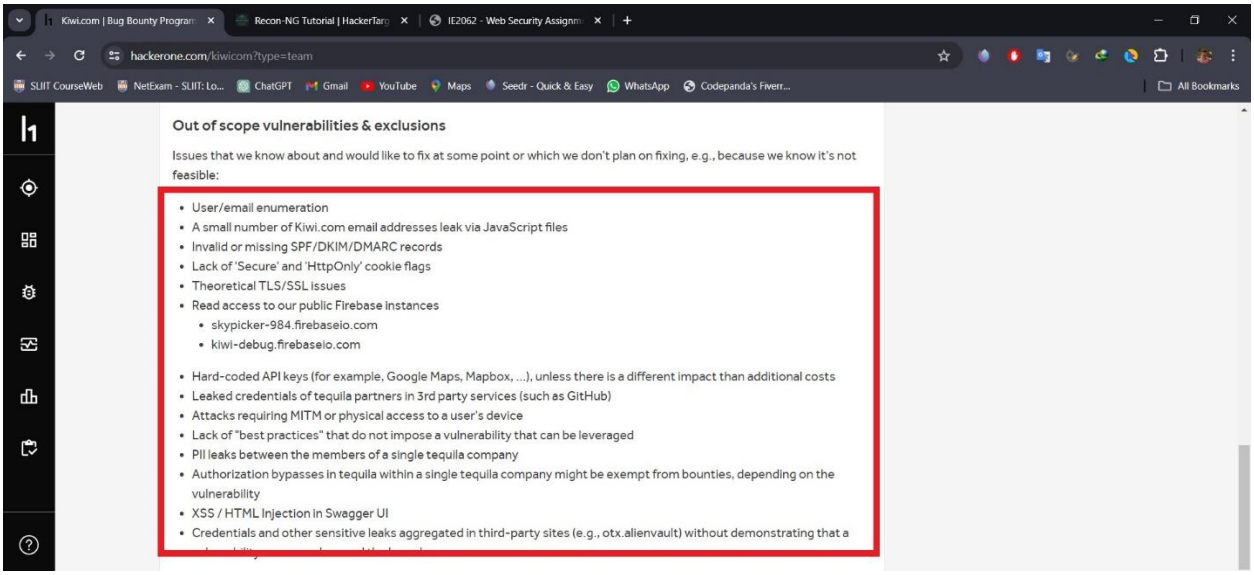
Kiwi.com offers a comprehensive reward plan to encourage security researchers to take part in their bug bounty program. kiwi.com is dedicated to creating a secure online space, so it appreciates the help researchers provide in identifying and correcting such security vulnerabilities. Researchers who 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.



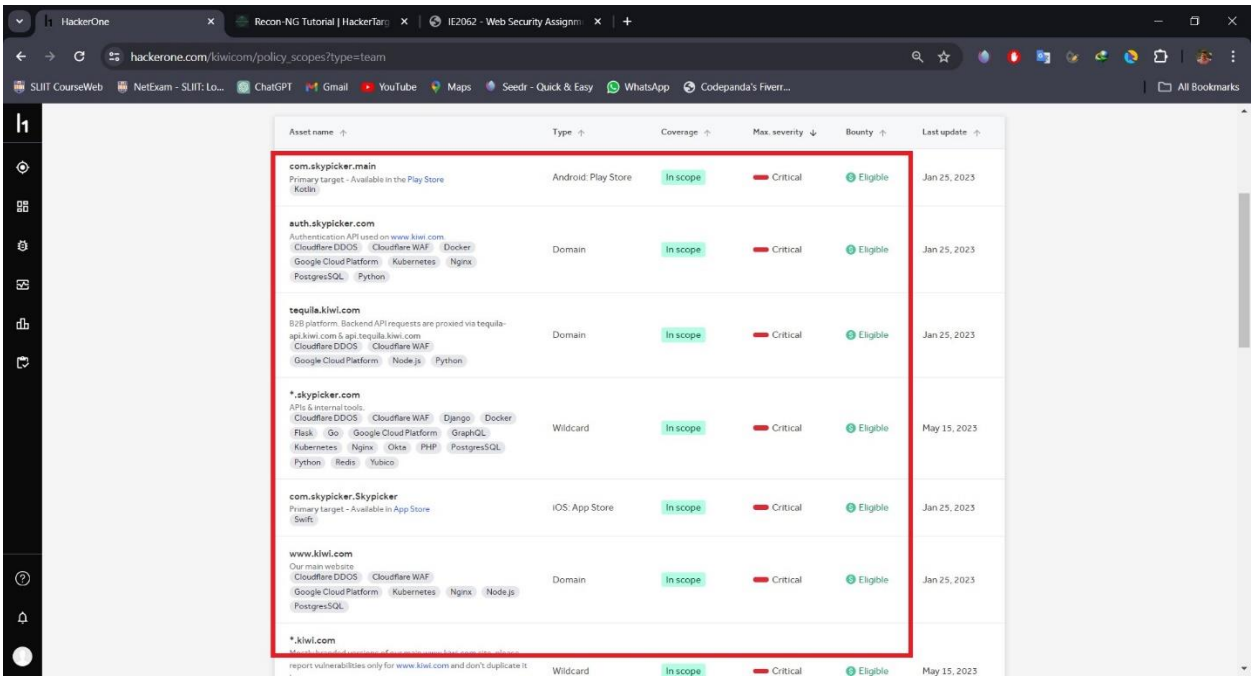
It's important to know the privacy policies before initiating a bug bounty. These guidelines specify how information will be managed, guaranteeing its confidentiality and security. They also go through how security researchers should respect people's right to privacy while reporting vulnerabilities.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



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.



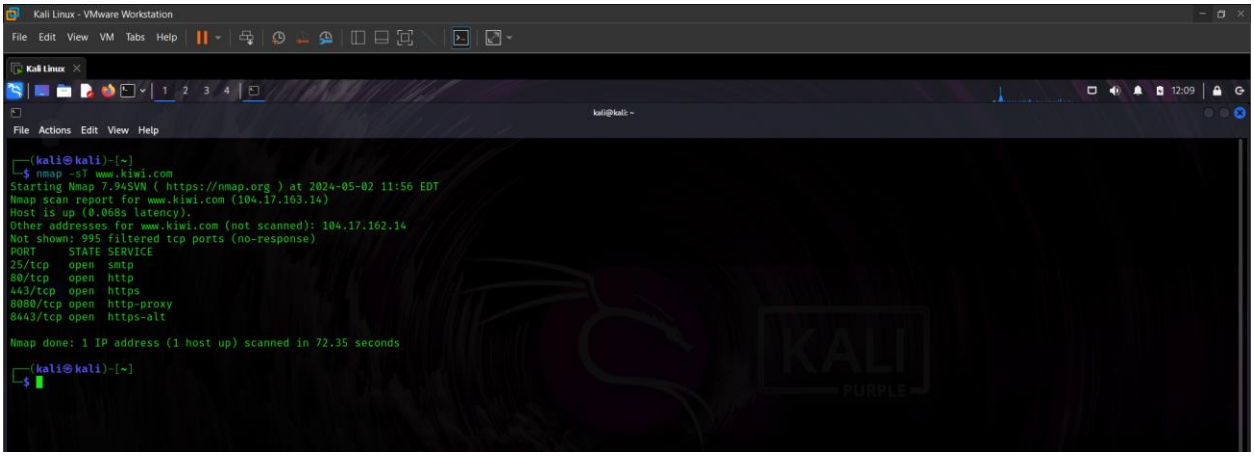
When searching for bugs that eligible for bounties, the "In scope" domain is critical. Our scanning procedures only look for regions which are under this specified range. In the case that events fail to proceed as planned, we predict several difficulties.



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.

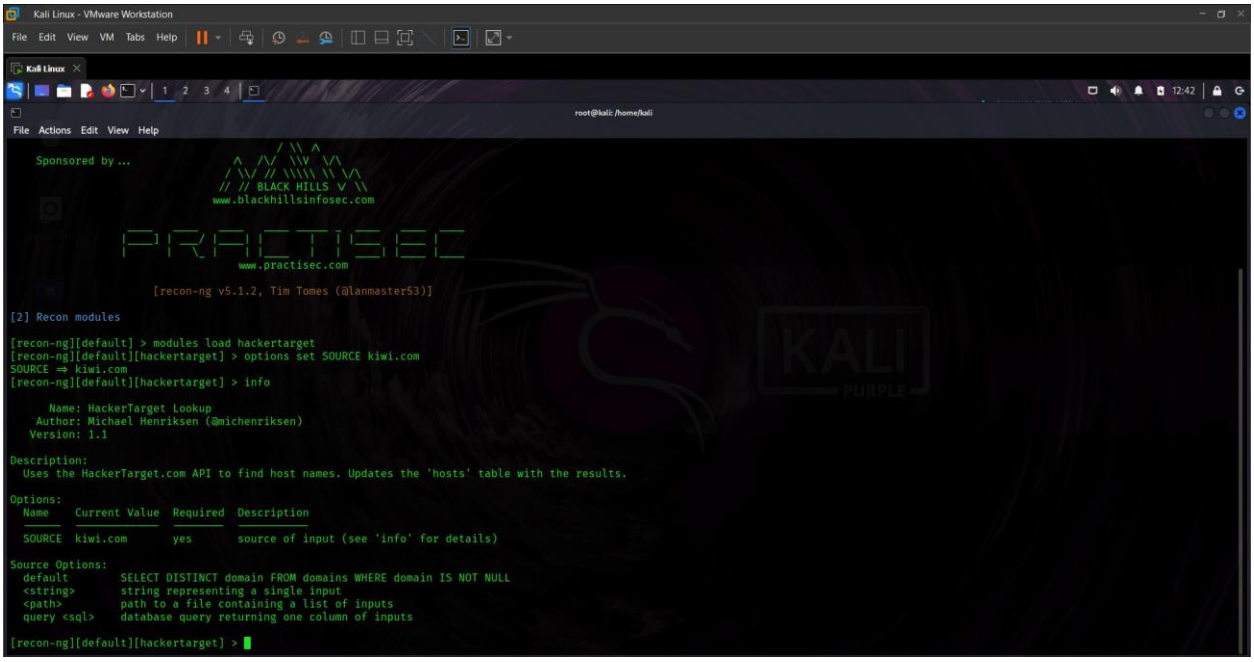


After carefully scanning the website's ports with nmap, I did not find any vulnerable ports or services running on this root domain. It seems like the website is well-protected and does not have vulnerable ports hackers to exploit. This means the website has good security and is less likely to be attacked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

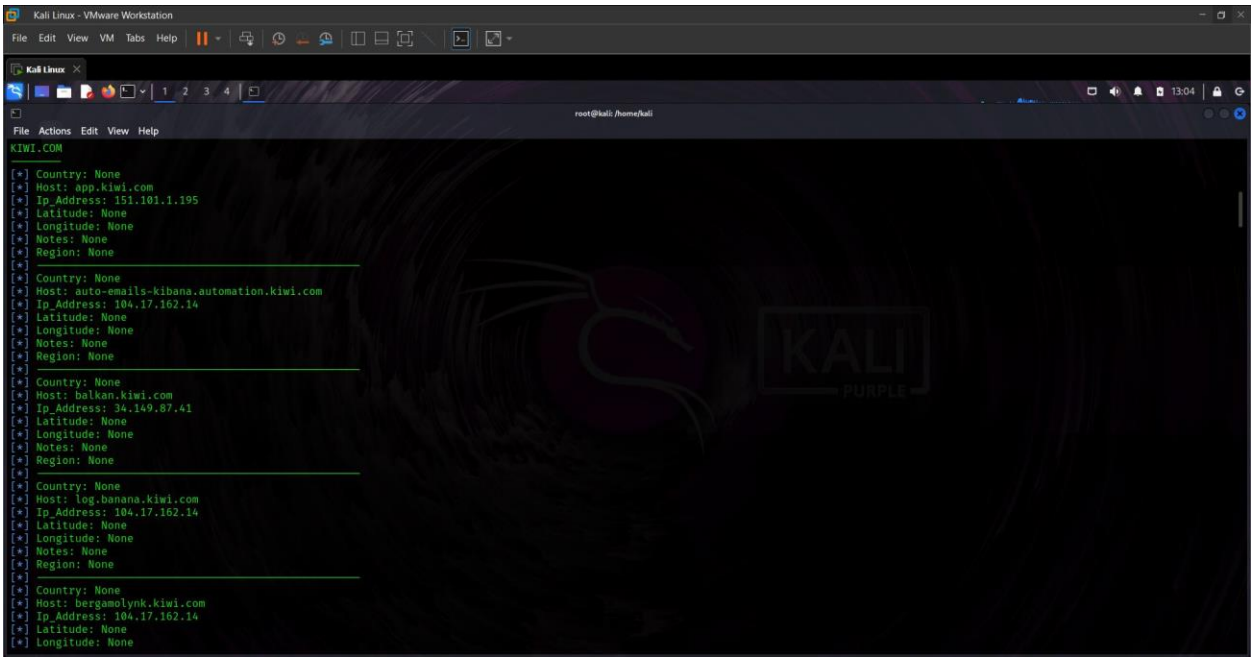
Using recon-ng framework to find subdomains of this root domain.

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.



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
Kali Linux
1 2 3 4
13:04
root@kali: /home/kali
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-emails-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: geoip-api-cr.kiwi.com
[*] Ip_Address: 104.17.162.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ——
[*] Country: None
[*] Host: goopt1.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.

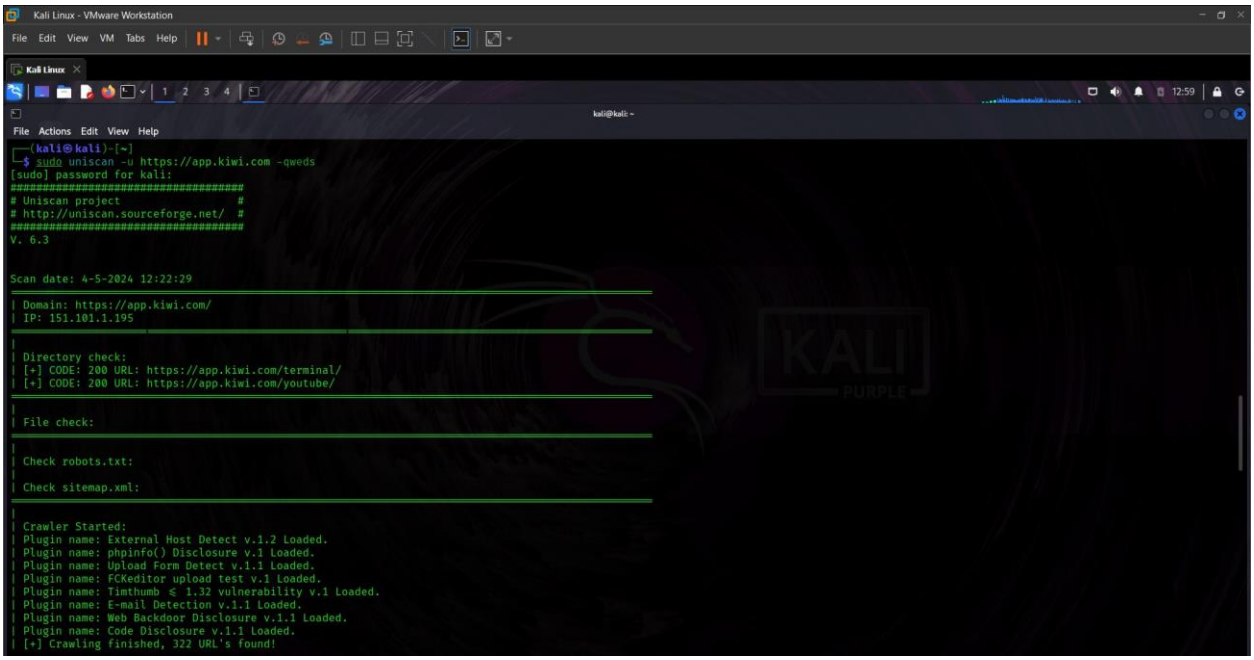
Report 01

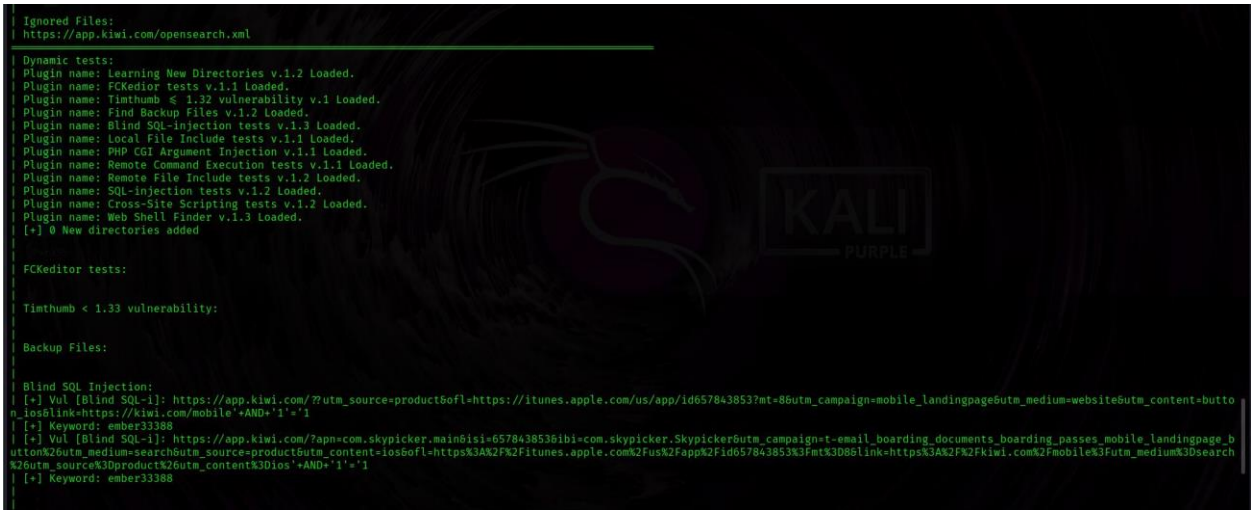
Target domain: http://app.kiwi.com/

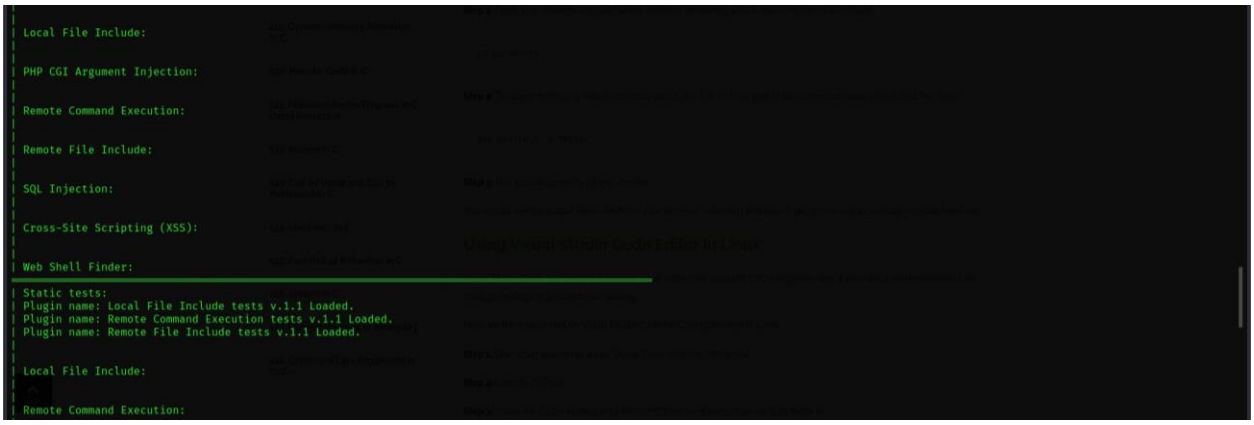
Scan using uniscan tool.

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:





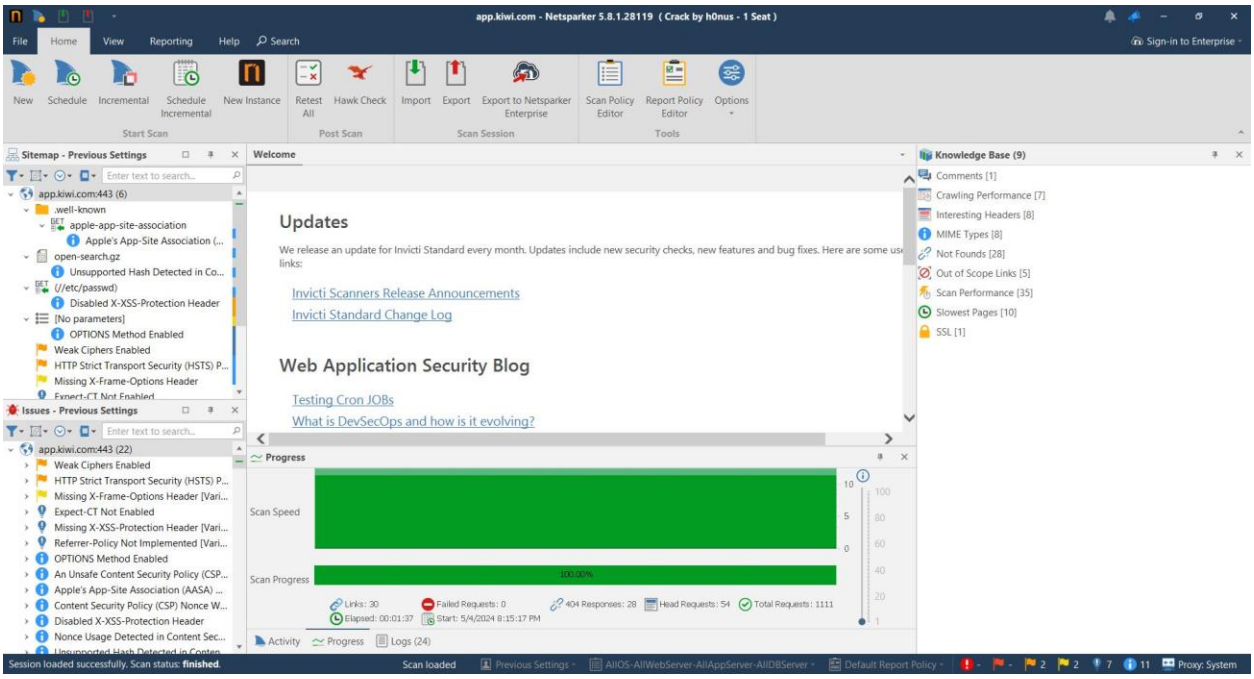


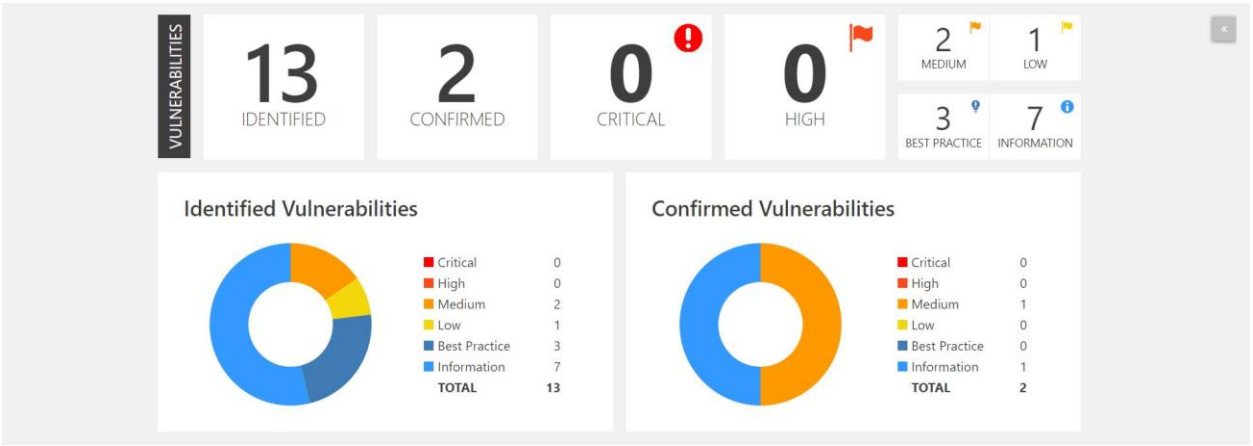
Even though it didn't seem promising at first, running the "uniscan –u app.kiwi.com -qweds" command uncovered two blind SQL injection vulnerabilities on the kiwi.com website.

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

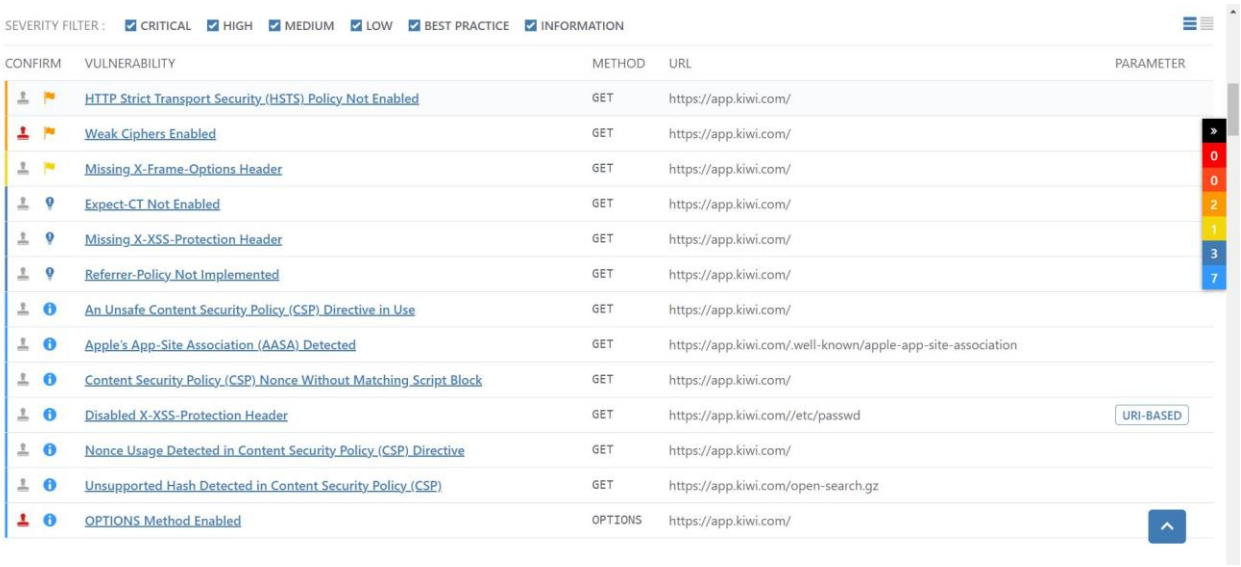
Scan using Netsparker

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**.**





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



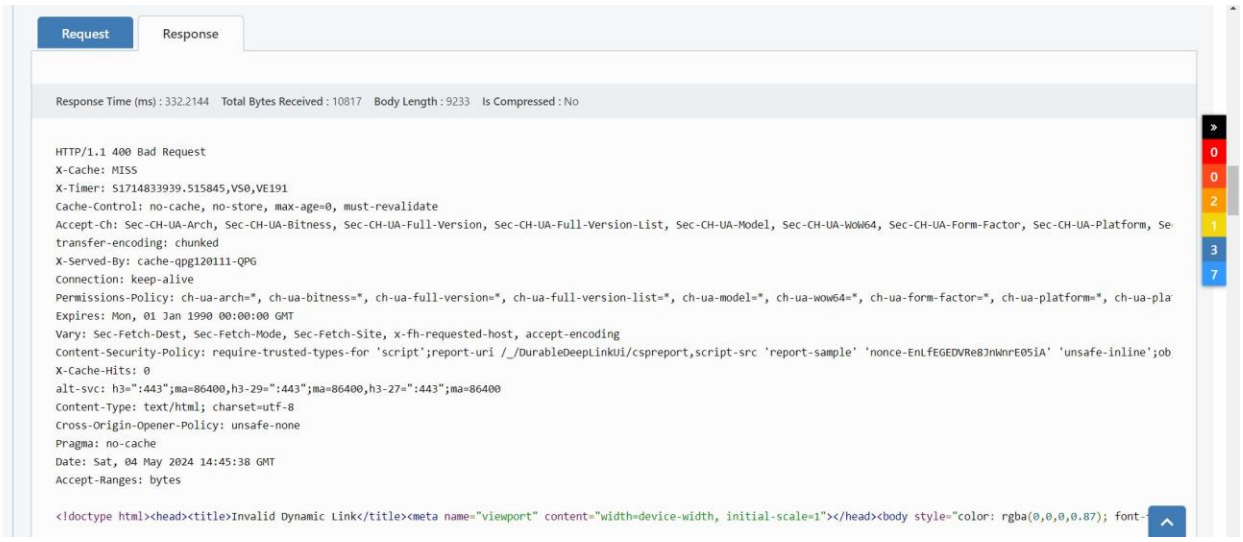
Vulnerability 1:

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.

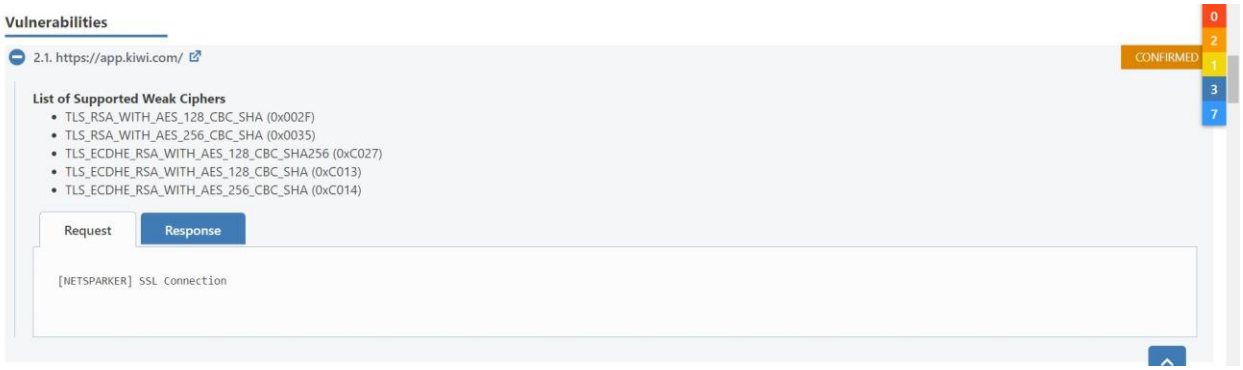
HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response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



Vulnerability 2:

Weak Ciphers Enabled

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



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 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

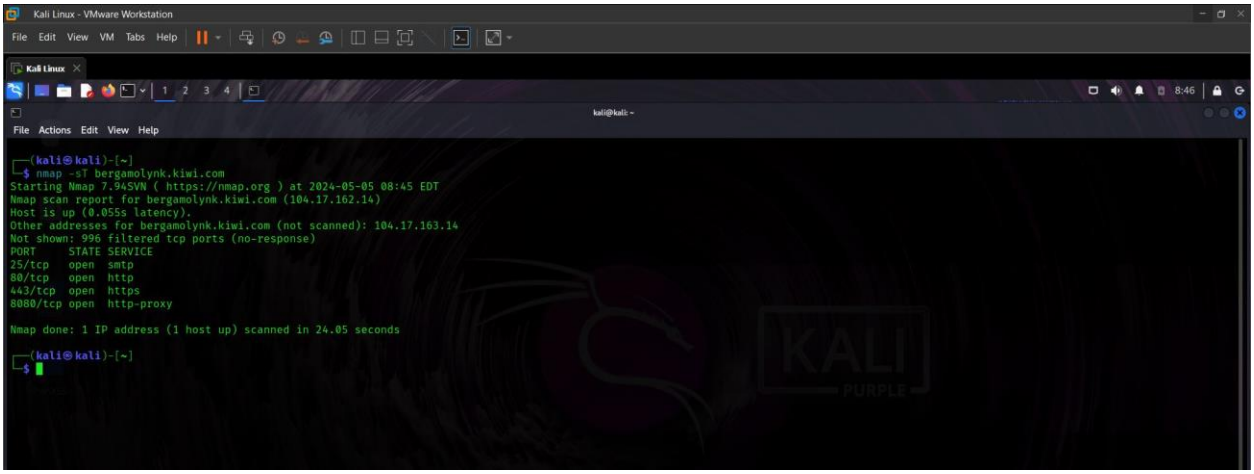
In summary, the security assessment of http://app.kiwi.com/ using Uniscan and Netsparker revealed significant vulnerabilities. Uniscan identified two blind SQL injection flaws in the mobile app while Netsparker uncovered 13 vulnerabilities in the app.kiwi.com subdomain including two medium-risk issues. 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.

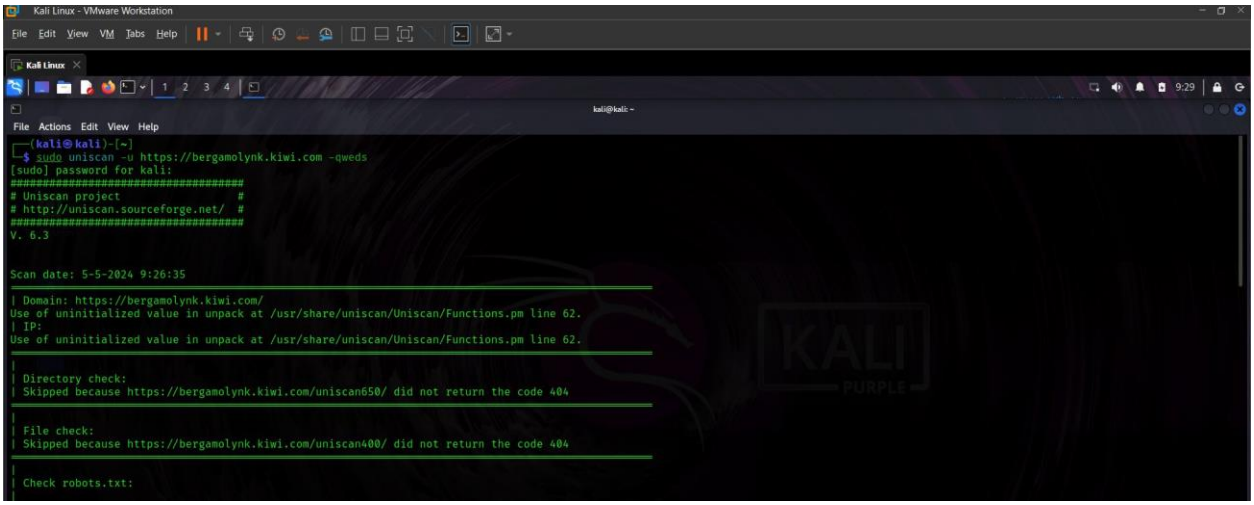
First, I used the nmap tool to check for any vulnerable ports or services on this subdomain.

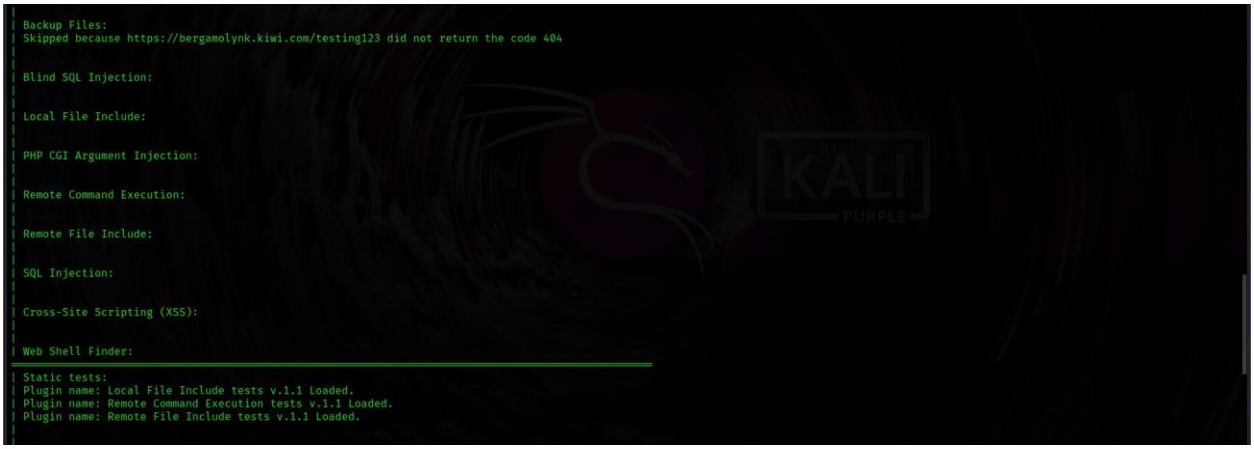


The Nmap scan results did not reveal any vulnerable ports or services.

Scan using uniscan tool.

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

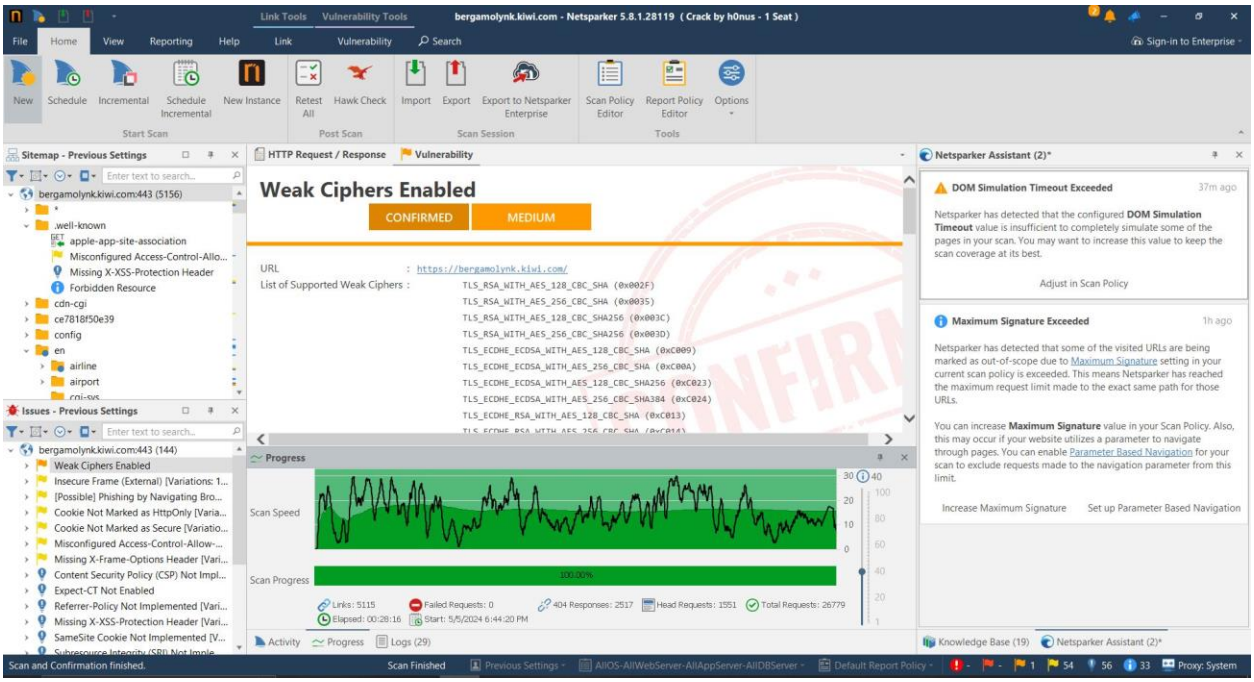


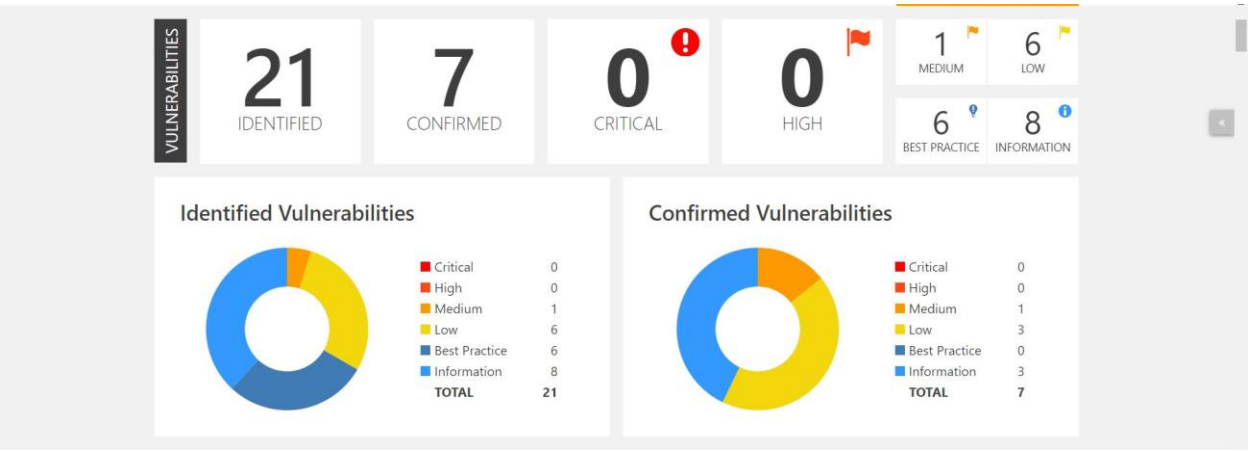


I did not find any useful information or vulnerabilities in the current subdomain on uniscan.

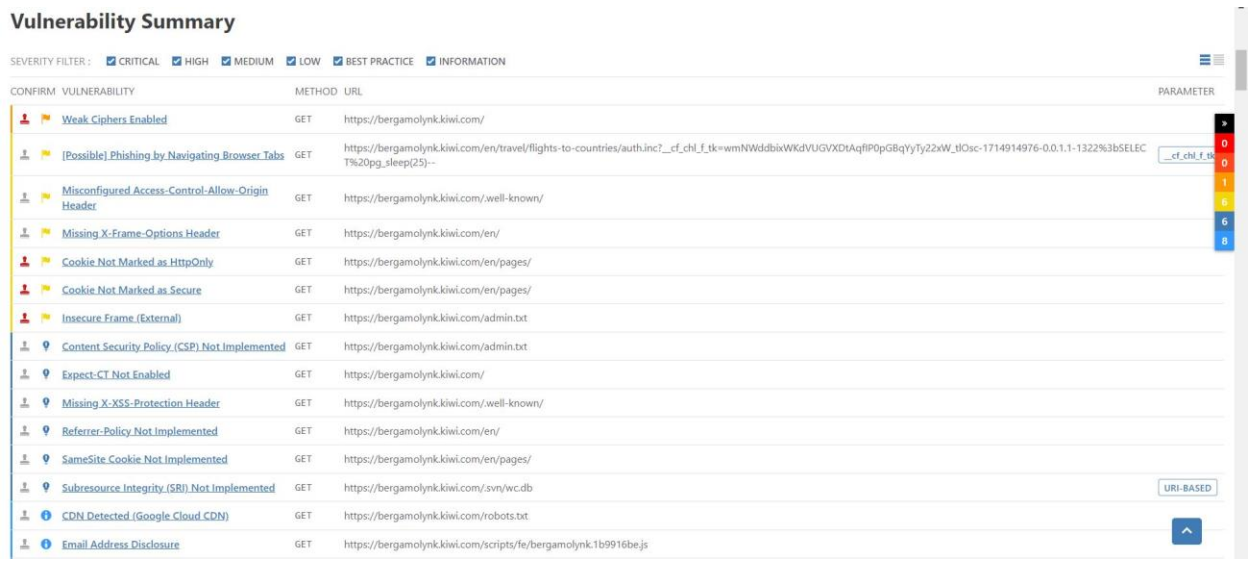
Scan using Netsparker.

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





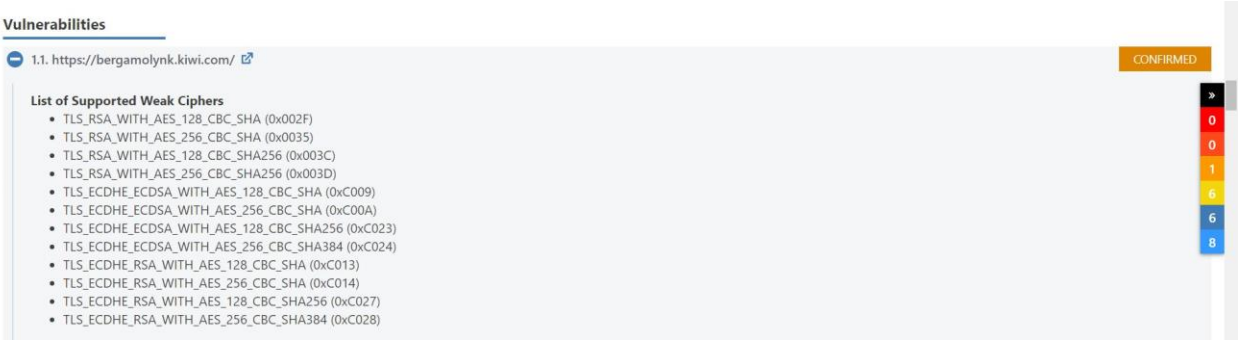
I identified a total of 13 vulnerabilities associated with app.kiwi.com subdomain. Among these, two vulnerabilities pose a medium level of risk.



Vulnerability:

Weak Ciphers Enabled

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



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 regedt32or 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

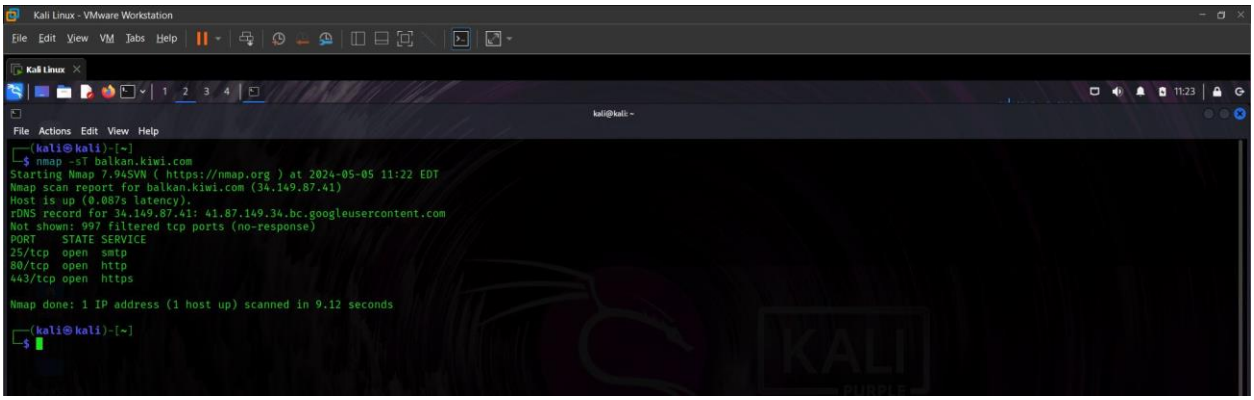
In conclusion, the security assessment of bergamolynk.kiwi.com revealed no vulnerabilities through Nmap and Uniscan scans. However, Netsparker detected weak ciphers during SSL communication posing a potential risk of SSL traffic decryption. Addressing this vulnerability is crucial to bolster the subdomain's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

Report 03

Target domain: balkan.kiwi.com

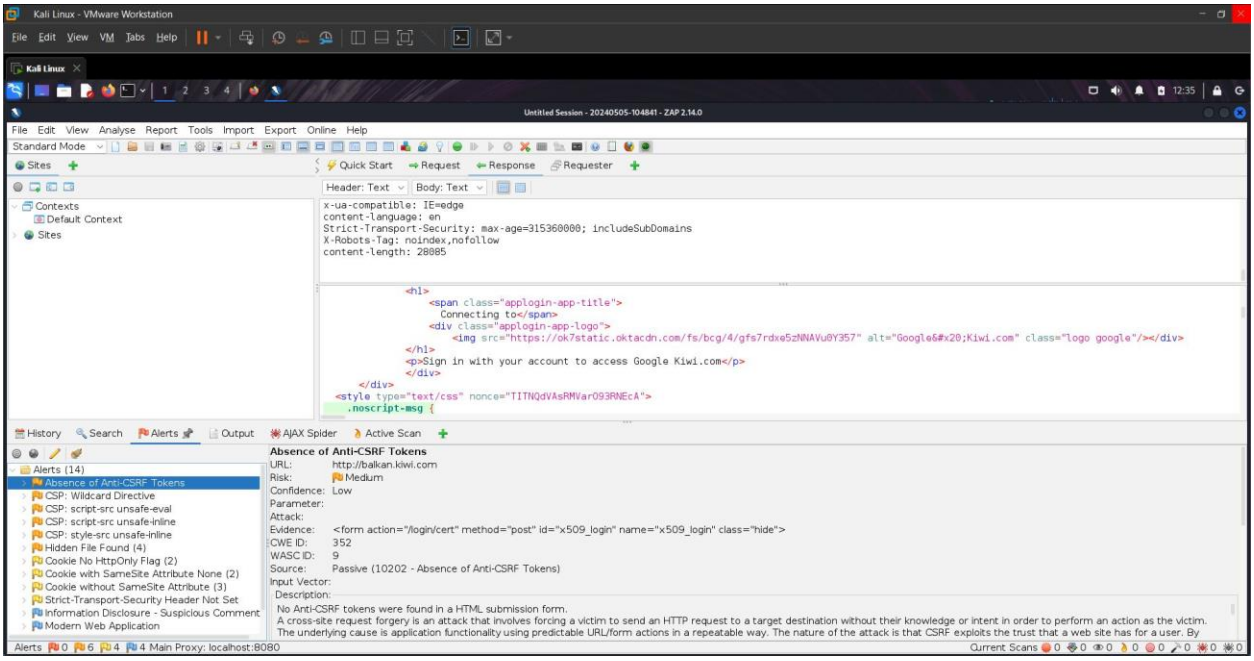
Scan using nmap tool.

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



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

Scan using OWASP-Zap tool.



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

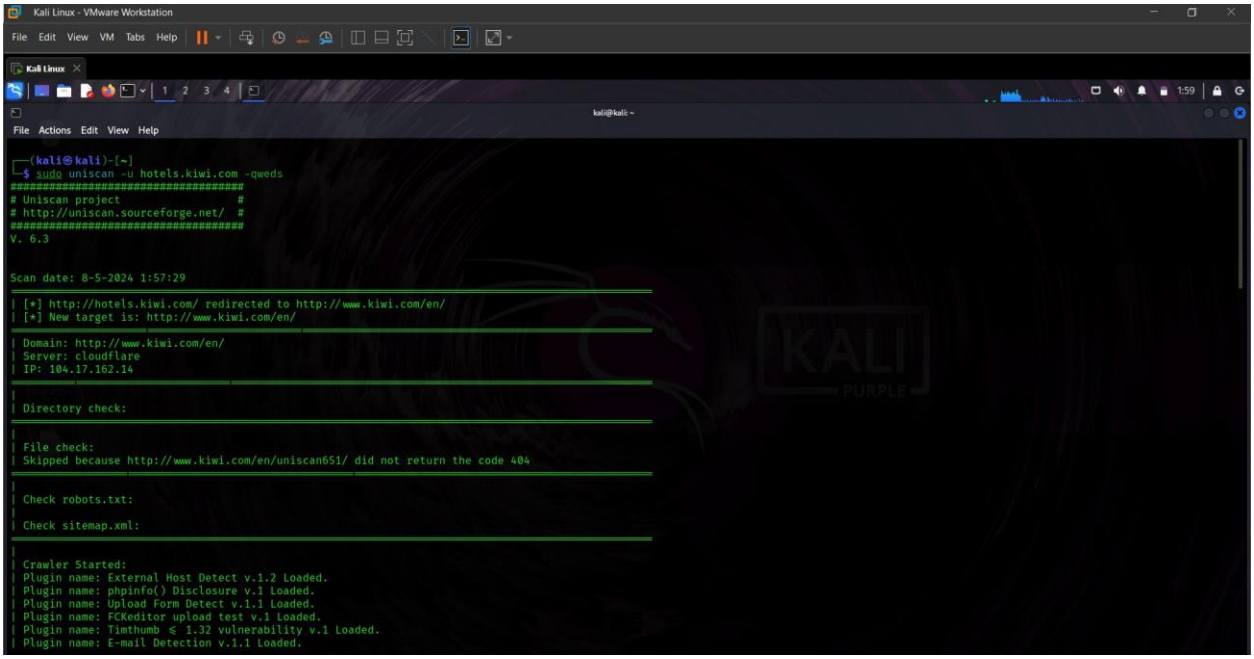
To summarize, the security assessment of balkan.kiwi.com found no susceptible ports or services based on Nmap. OWASP-Zap identified 14 alerts, specifically noting the lack of Anti-CSRF Tokens in the HTML form utilized on the website. This vulnerability has the potential to result in Cross-Site Request 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.

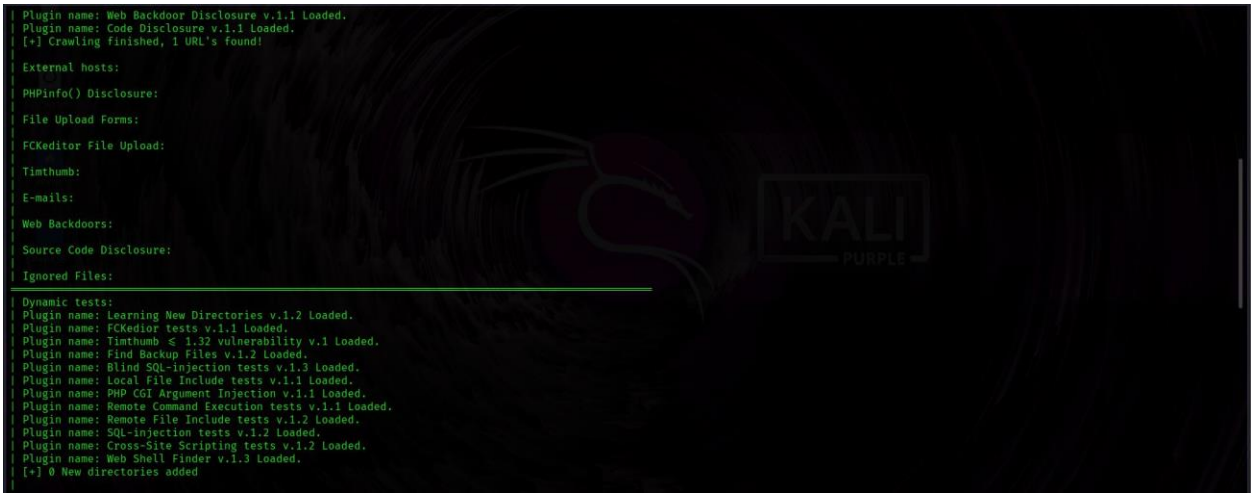
Report 04

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:





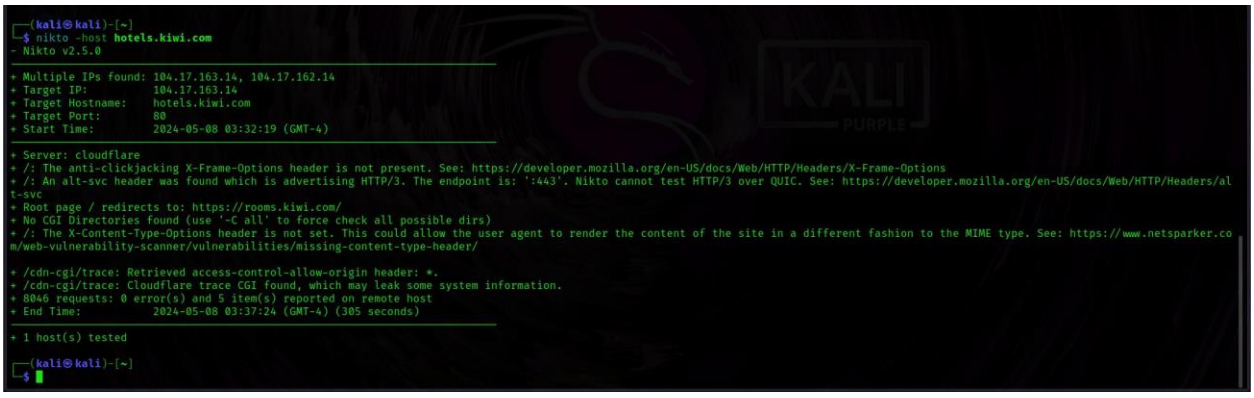
Uniscan report did not contains any interesting information about the subdomain.

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.

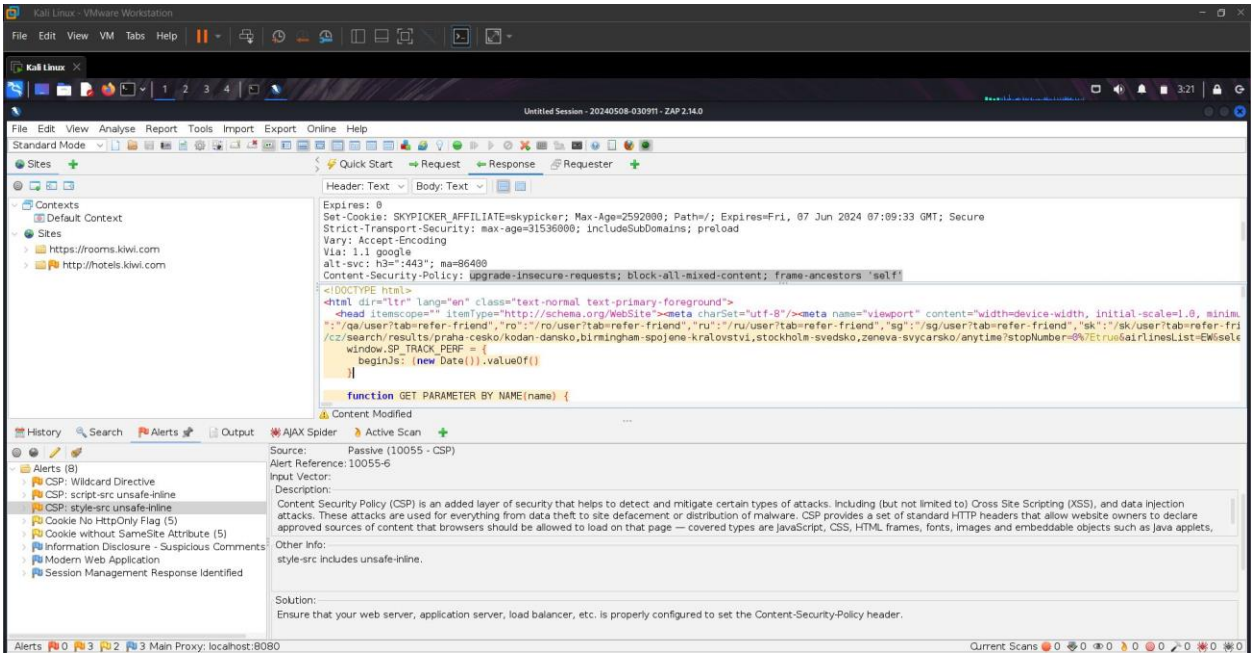
Scan results of the target subdomain as follows:



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:



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.

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:

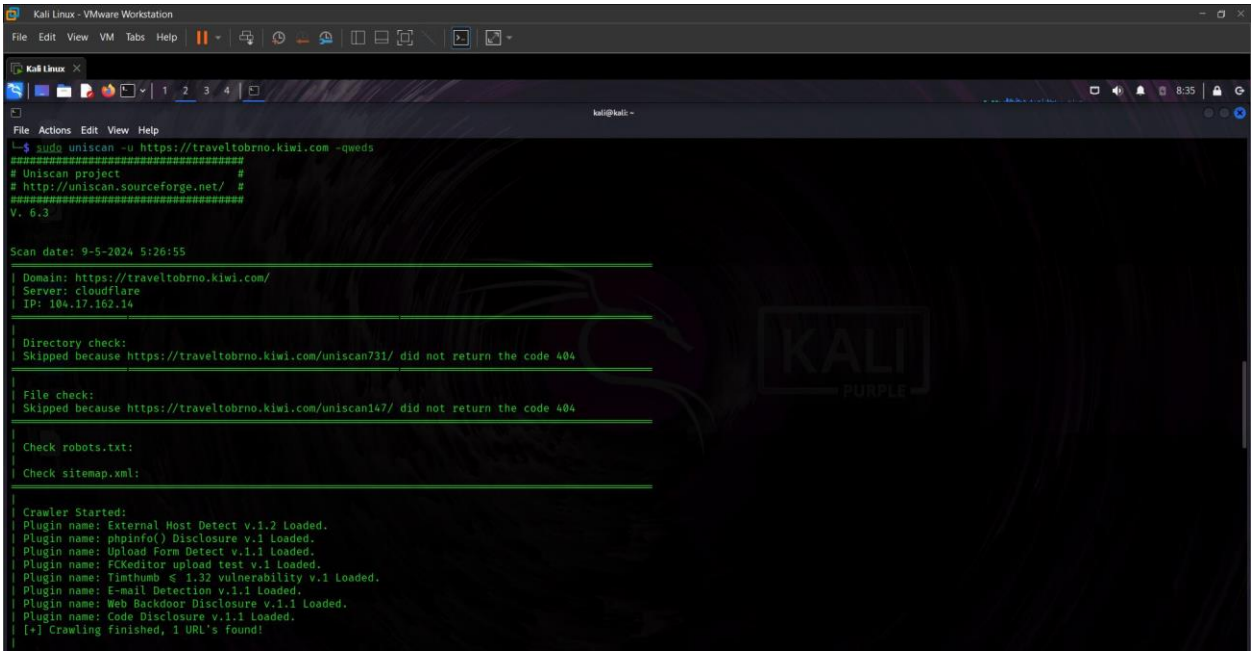
As a result of Uniscan, Nikto, and OWASP-Zap examinations, the security evaluation of hotel.kiwi.com produced negligible results. Although OWASP-Zap detected a script-src vulnerability related to unsafe-inline content in the Content Security Policy (CSP), Uniscan and Nikto did not report any significant 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.

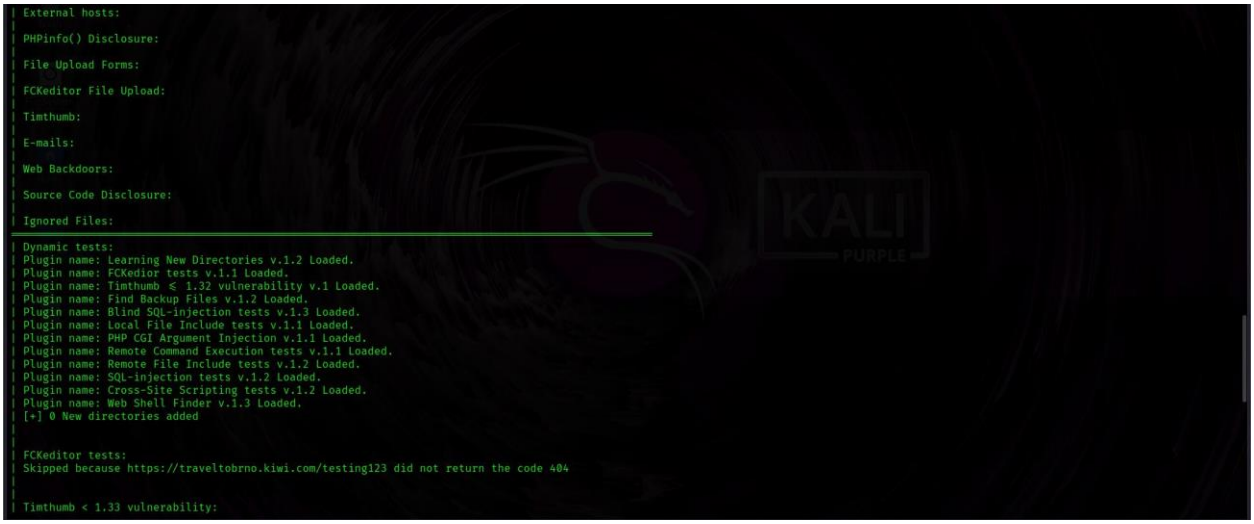
Report 05

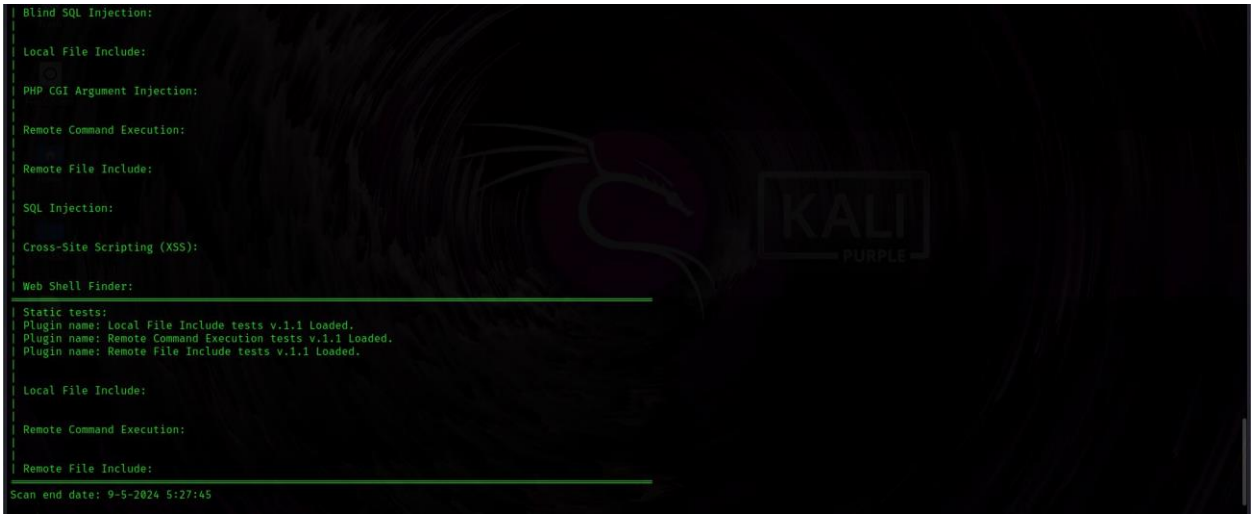
Target domain: https://traveltobrno.kiwi.com

Scan using uniscan tool.

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

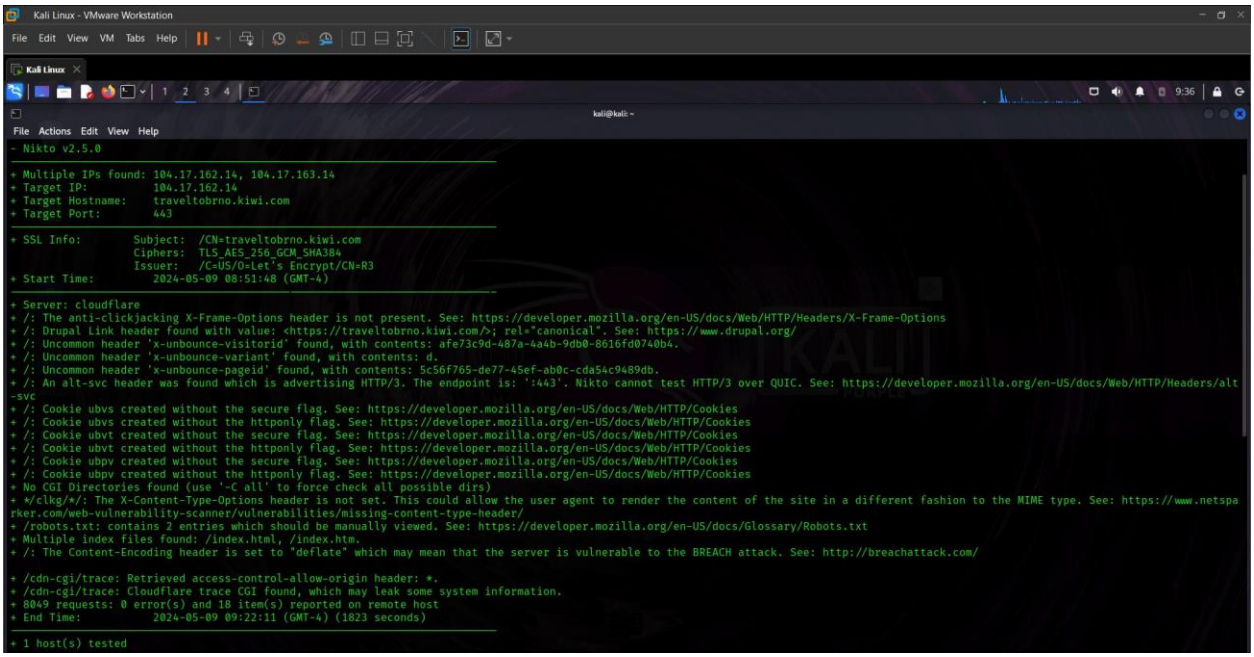






Uniscan report did not contains any interesting information about the subdomain.

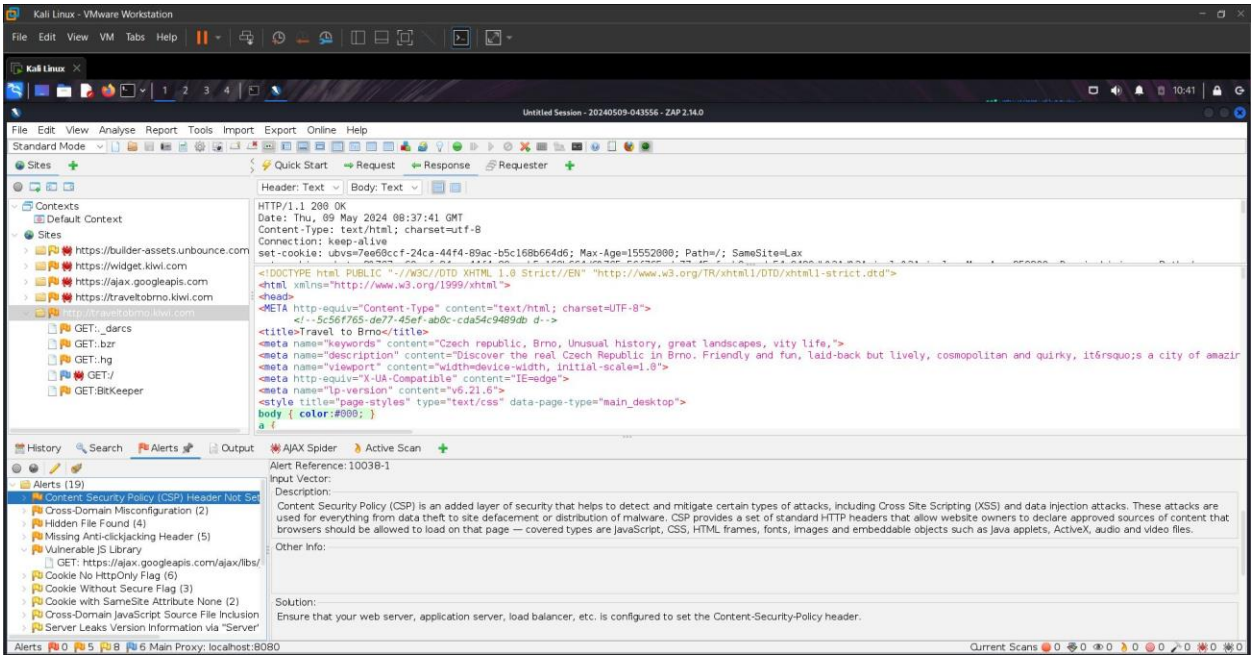
Scan using Nikto tool.



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

Scan using OWASP-Zap tool.

Automated zap scan results as follows:



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

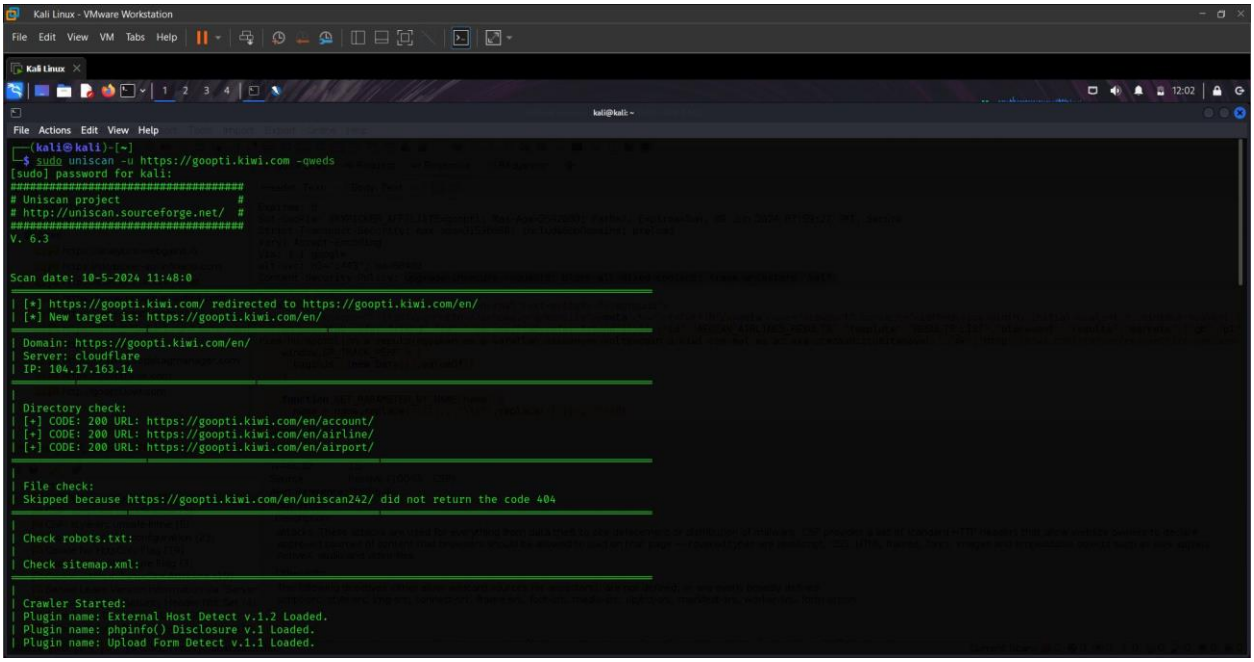
All things considered, the security evaluation of https://traveltobrno.kiwi.com turned up serious flaws even though the first scans produced nothing particularly interesting. Risks are high when there is no Content Security Policy (CSP) header and Cross-Origin Resource Sharing (CORS) settings are incorrect; 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.

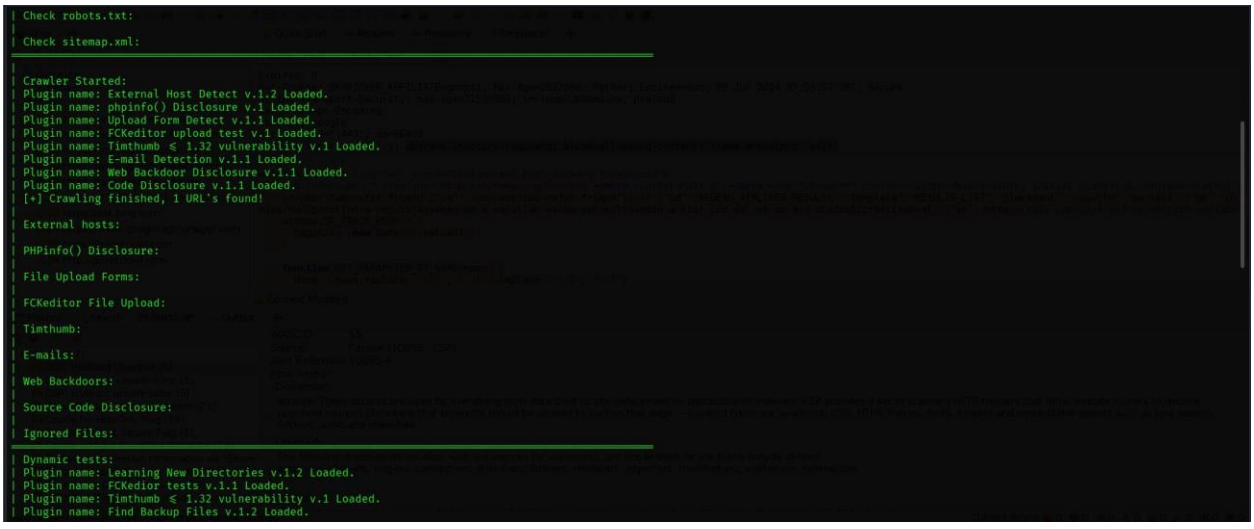
Report 06

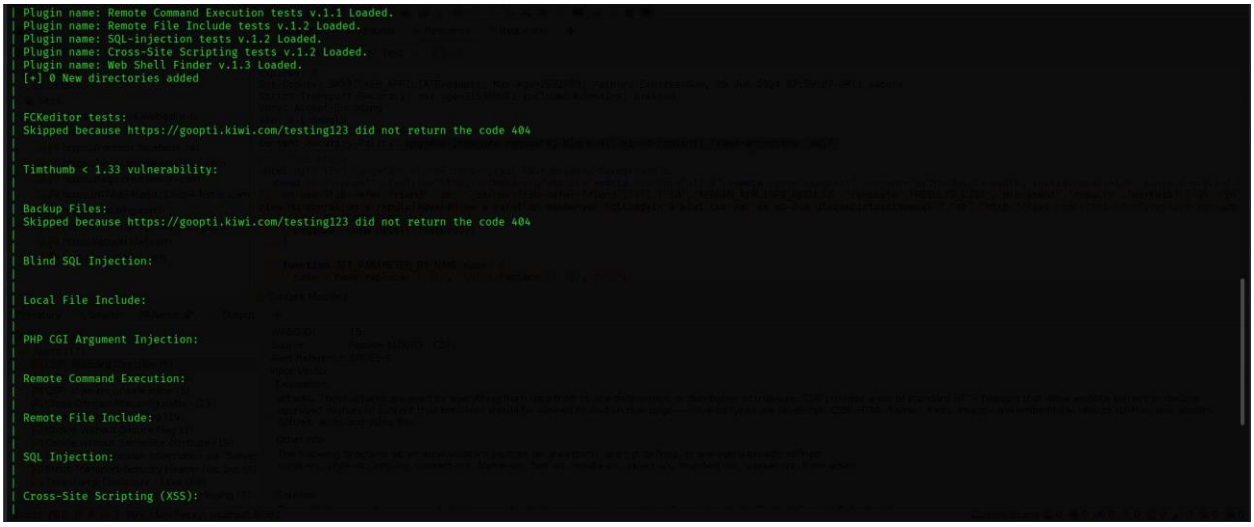
Target domain: https://goopti.kiwi.com

Scan using uniscan tool.

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

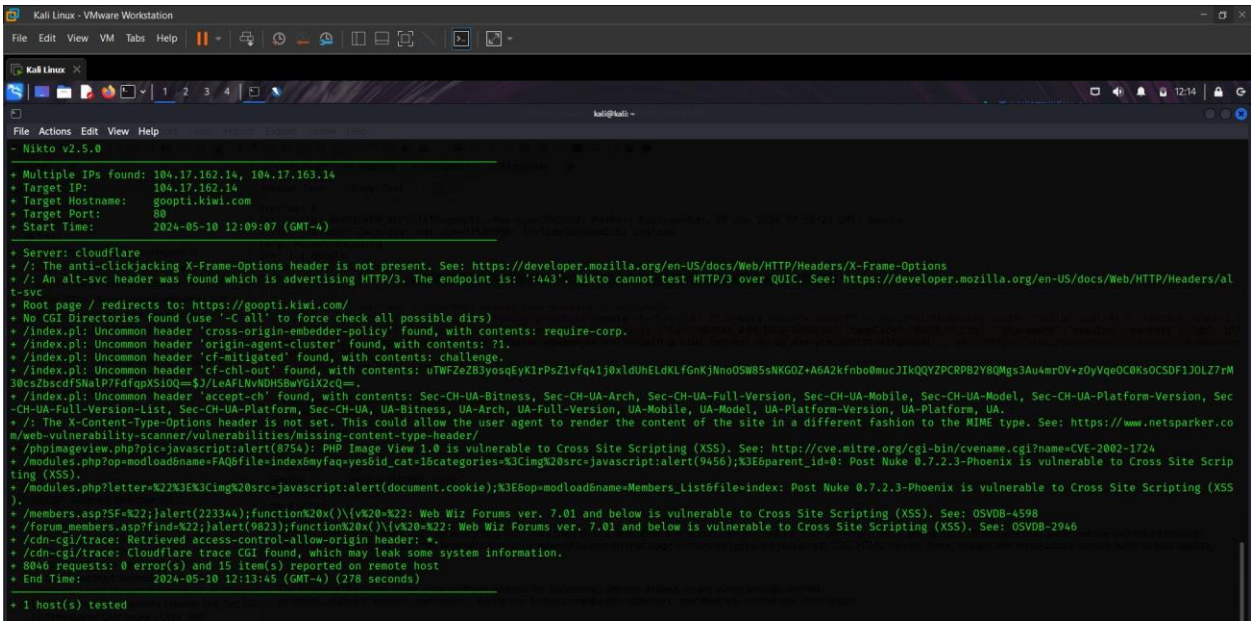






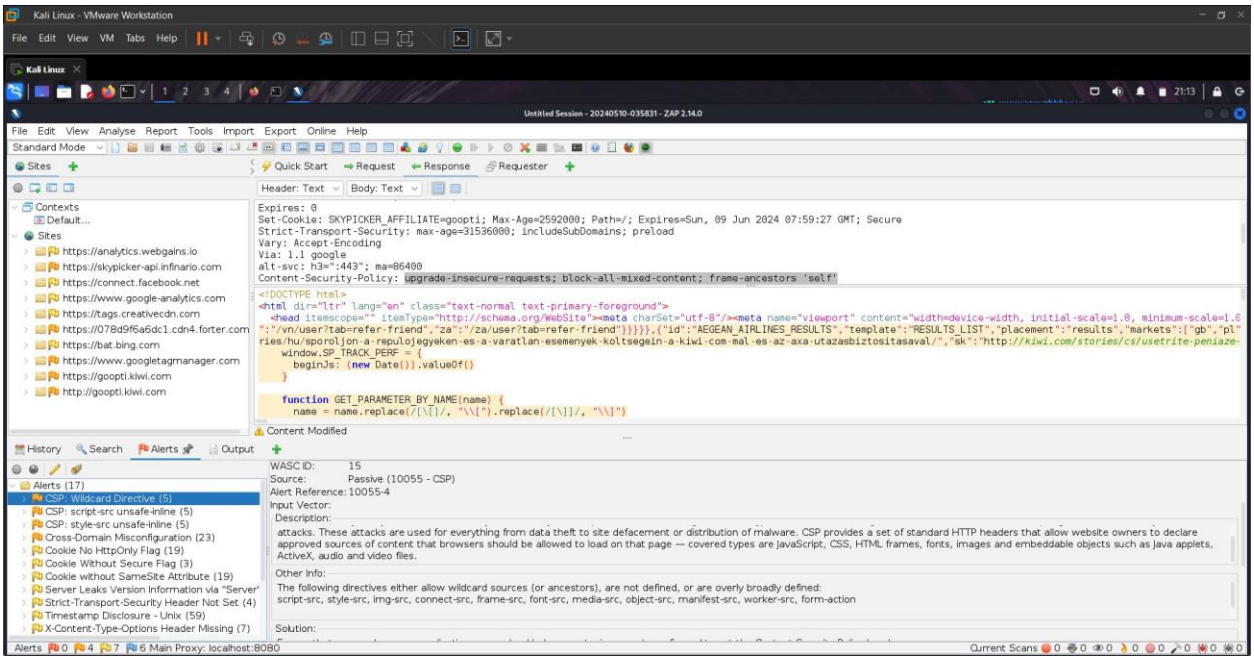
Uniscan report returned some directories, but those directories are already visible in the system. There is not any interesting information about vulnerabilities found.

Scan using Nikto tool.



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.



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

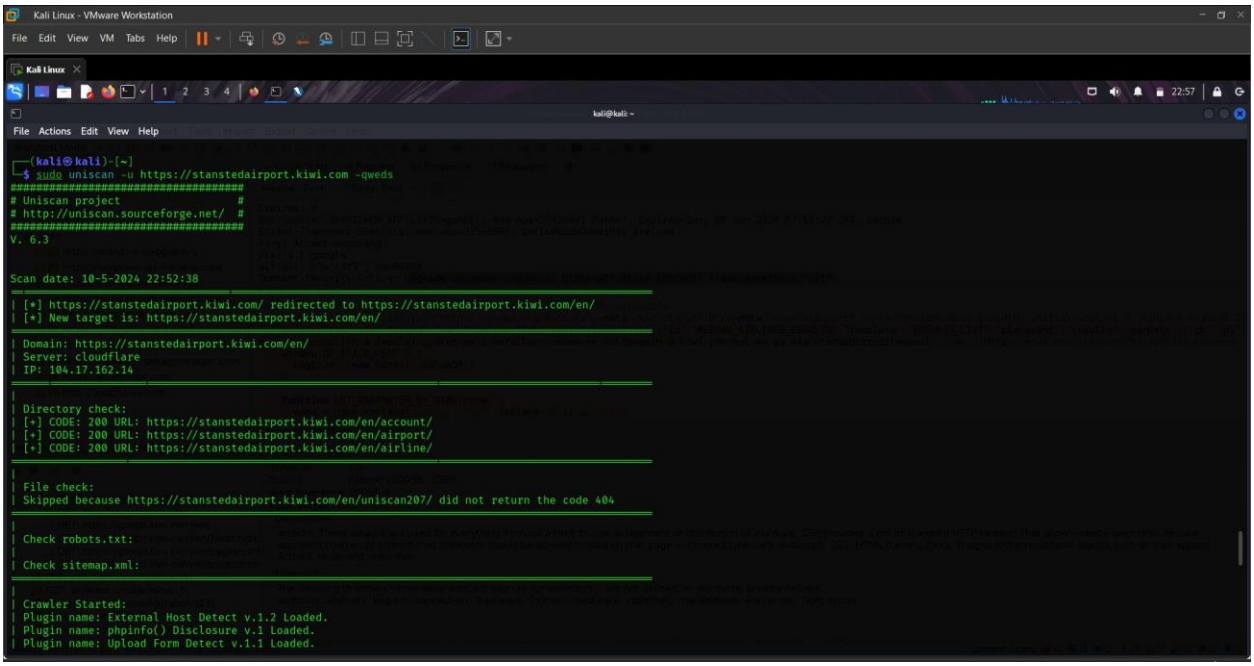
In conclusion, the security assessment of https://goopti.kiwi.com demonstrated various results generated by different security scanning applications. Although significant vulnerabilities were not detected by Uniscan and Nikto, OWASP-Zap produced seventeen alerts including the violation of the content 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

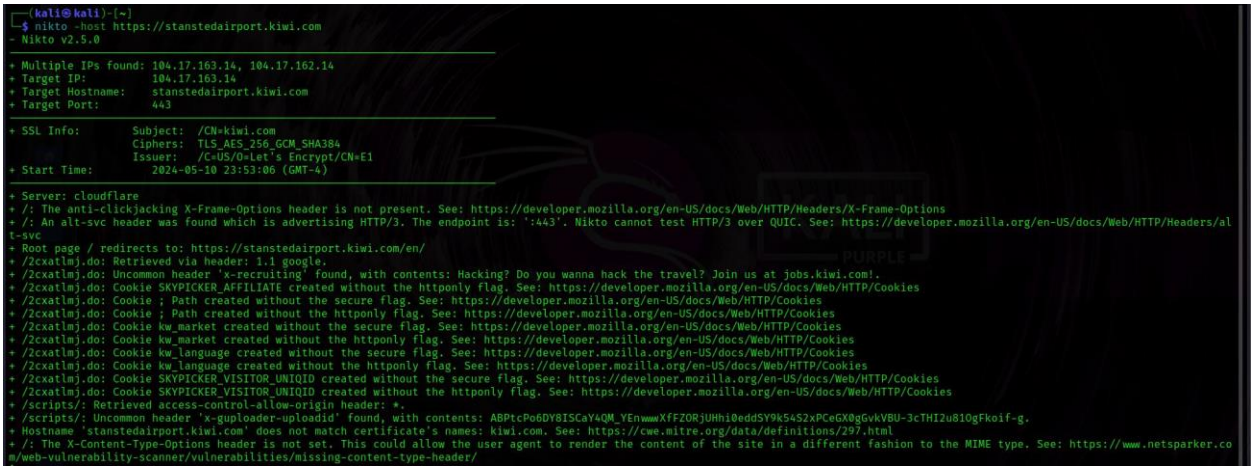
Scan using uniscan tool.

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



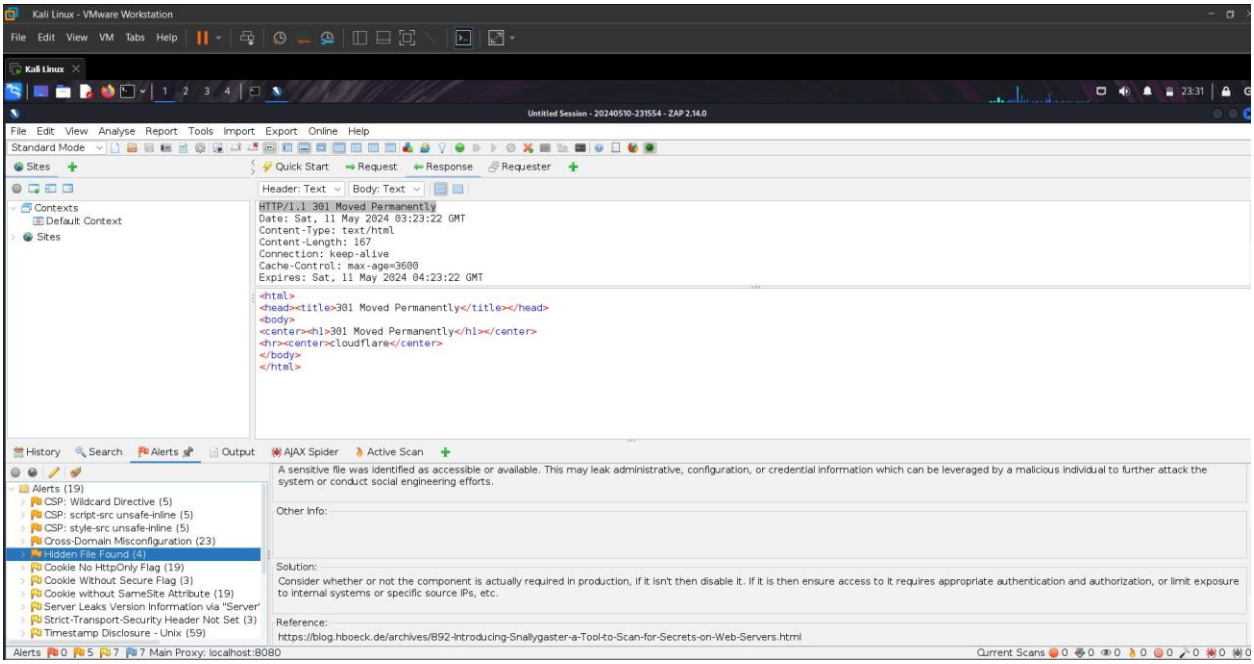
Found some common directories but those directories are already visible in the system. There is not any interesting information about vulnerabilities found.

Scan using Nikto tool.



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

Scan using OWASP-Zap tool.



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:

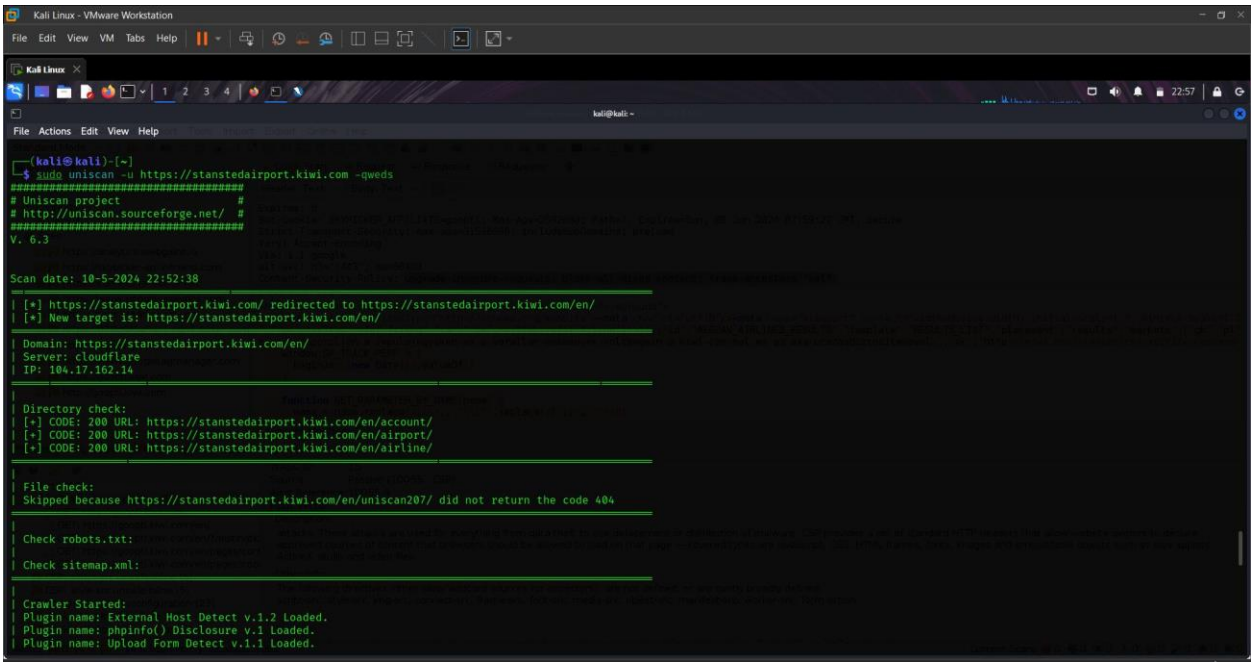
All these risk factors from "style-src 'unsafe-inline'" are prevented by the setting of the Content-Security-Policy header uniformly across the web server, application server, load balancer, and relevant components. This should then be extended to tighter CSP policies where unsafe-inline is absolutely 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.

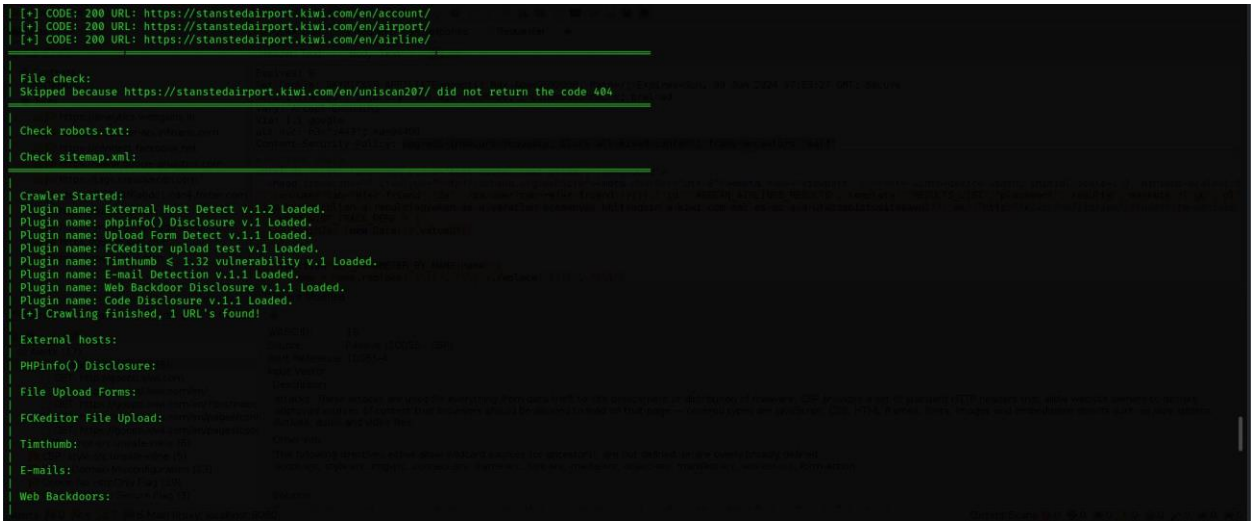
Report 08

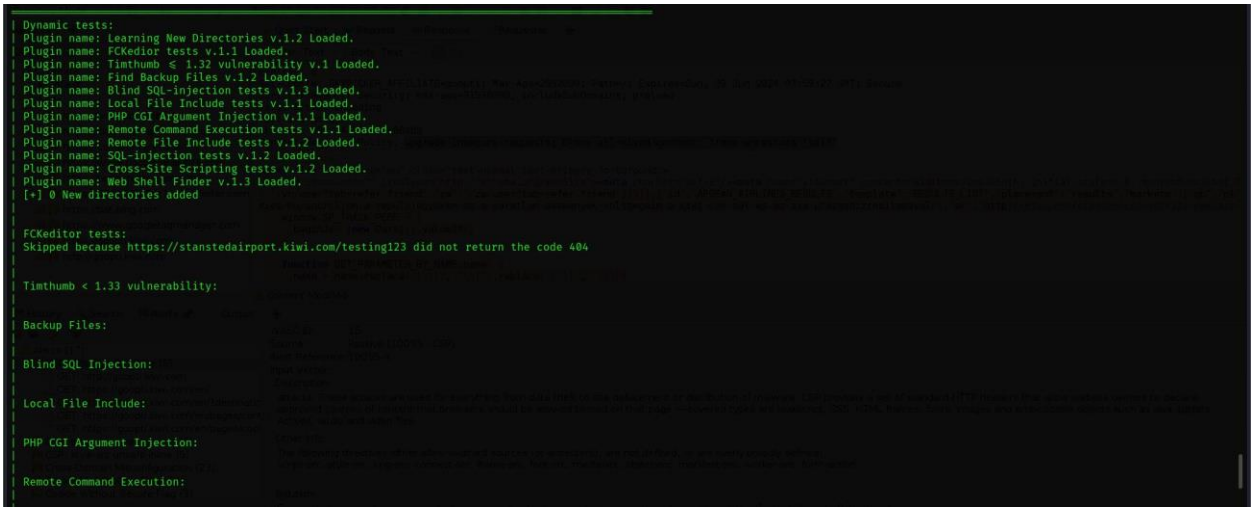
Target domain: https://platform-api.skypicker.com/

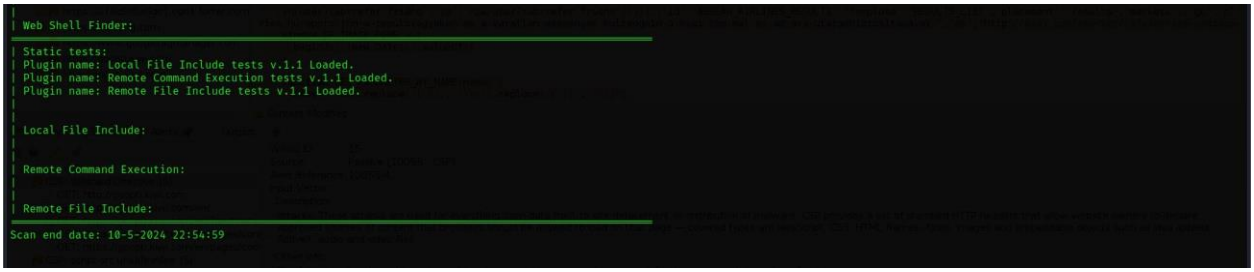
Scan using uniscan tool.

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









Uniscan report neither returned any valuable information nor any vulnerabilities.

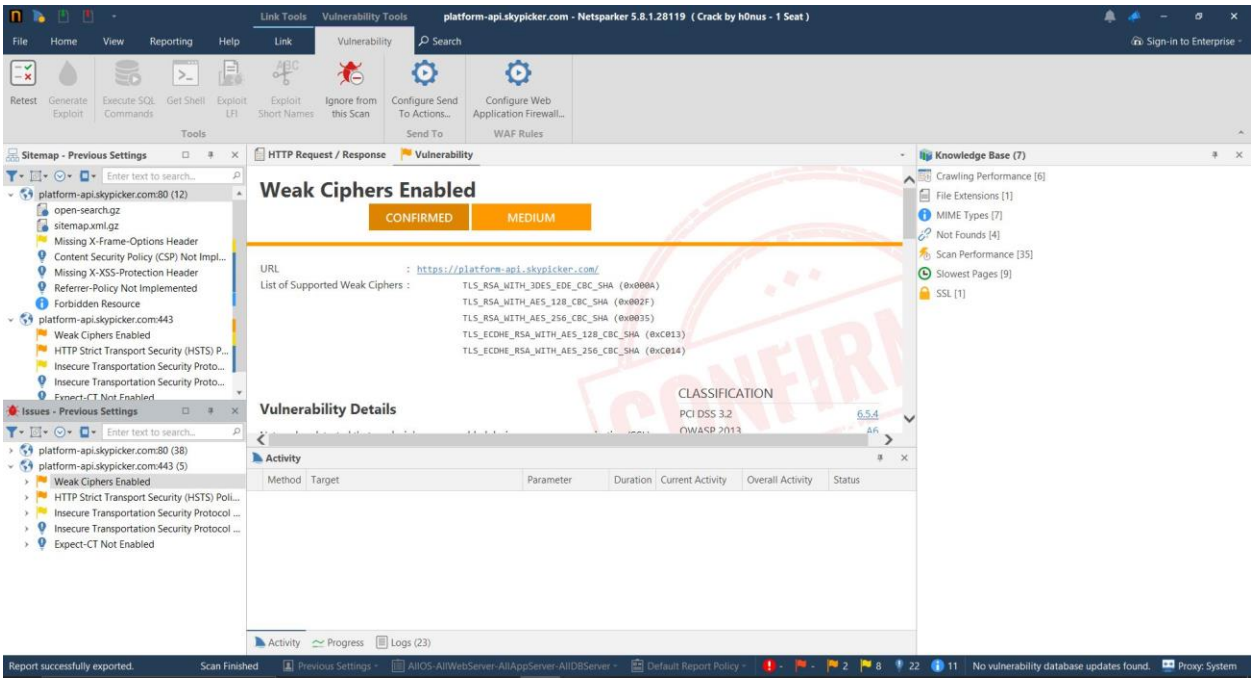
Scan using Nikto tool.

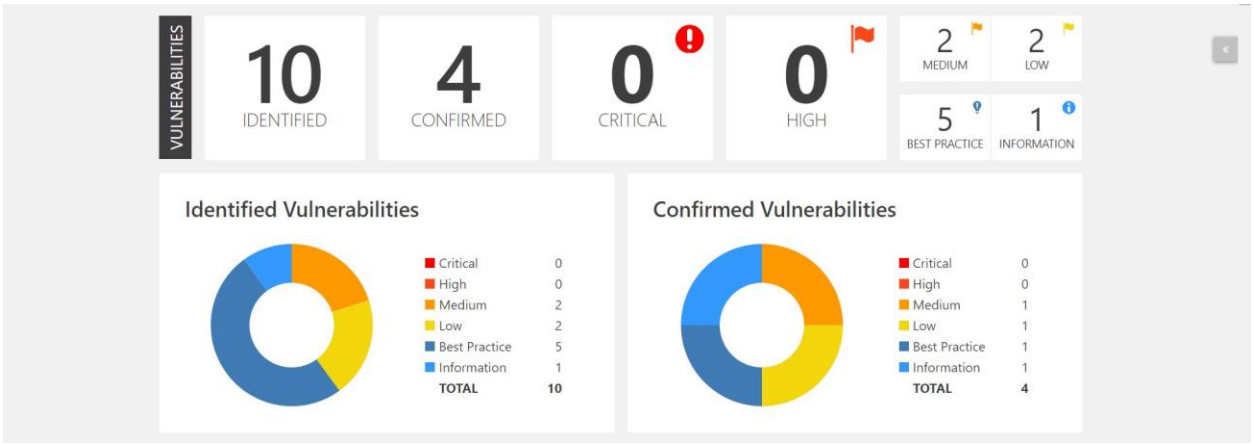
Found nothing with the Nikto scan.

Scan using Netsparker.

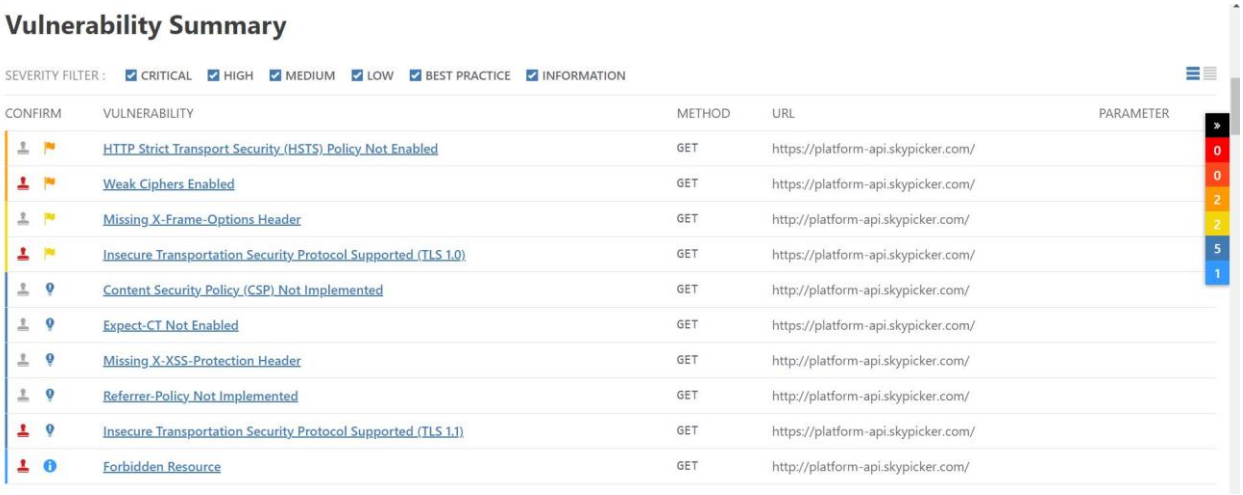
Finally, after having exercised several security evaluations using the Uniscan, Nikto, and OWASP ZAP tools, it was concluded that there were no vulnerabilities in the given subdomain. Even after running these in-depth vulnerability scans, since nothing showed up, this either proves that the security 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.



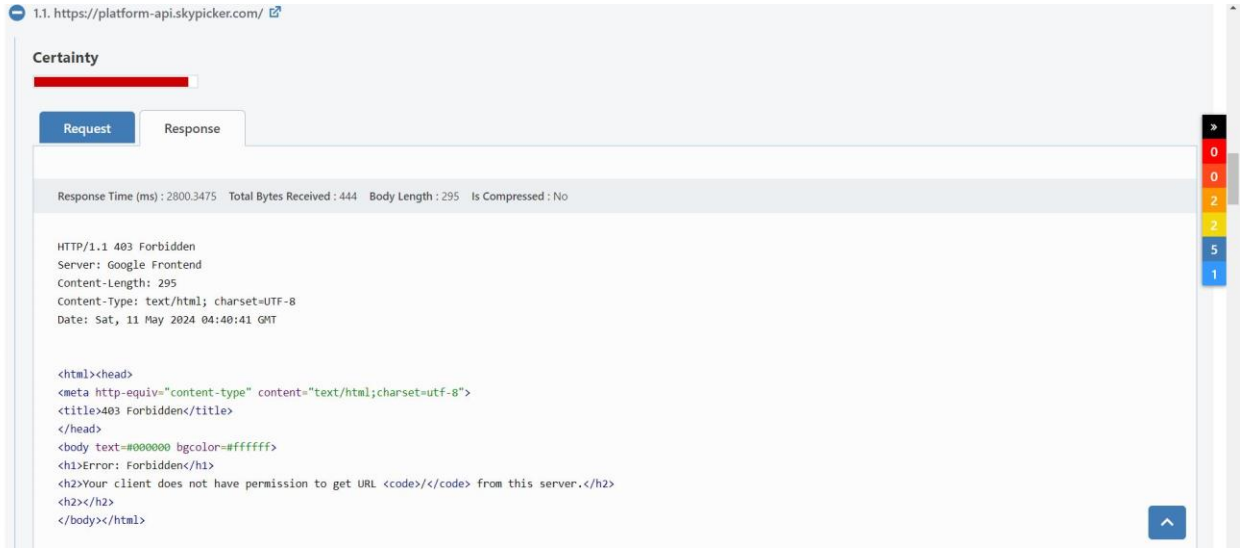
Vulnerability 01:

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.

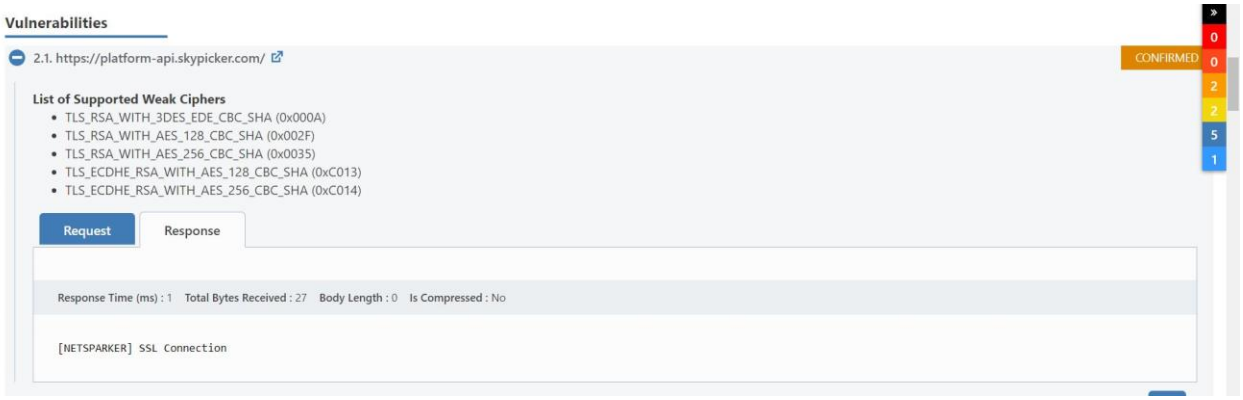
HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response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



Vulnerability 2:

Weak Ciphers Enabled

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



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 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

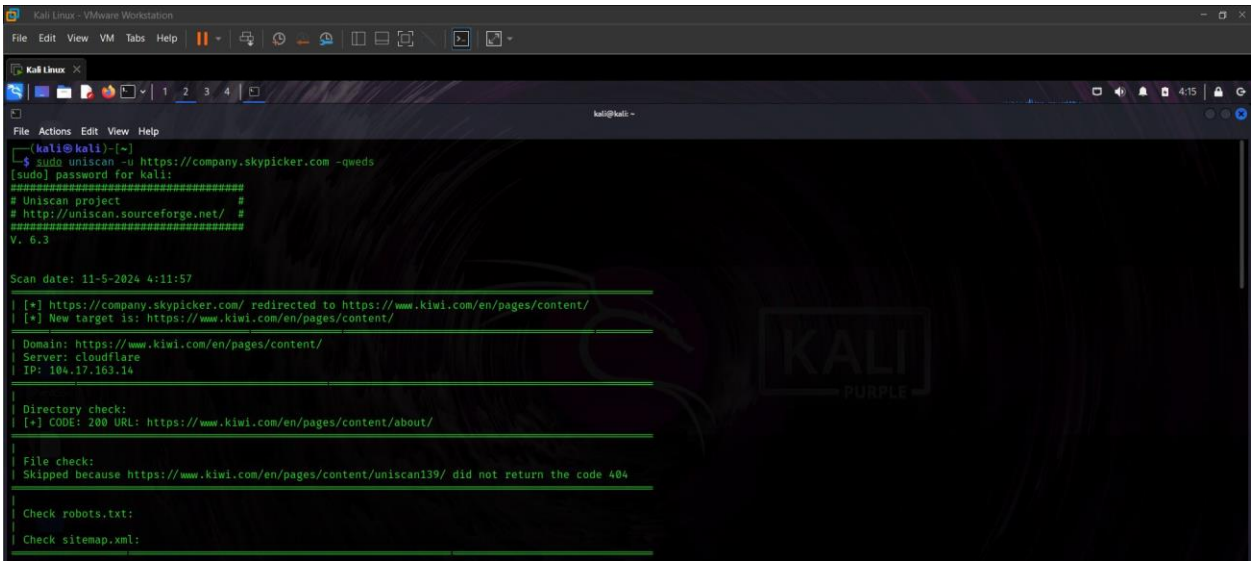
Security testing on the domain https://platform-api.skypicker.com/ was performed using Uniscan, Nikto, and OWASP ZAP; thus, no outstanding issues were found. Ten more were found in a scan using Netsparker, out of which two were with medium risk ratings. Most of the weaknesses found are that HSTS is enabled, 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.

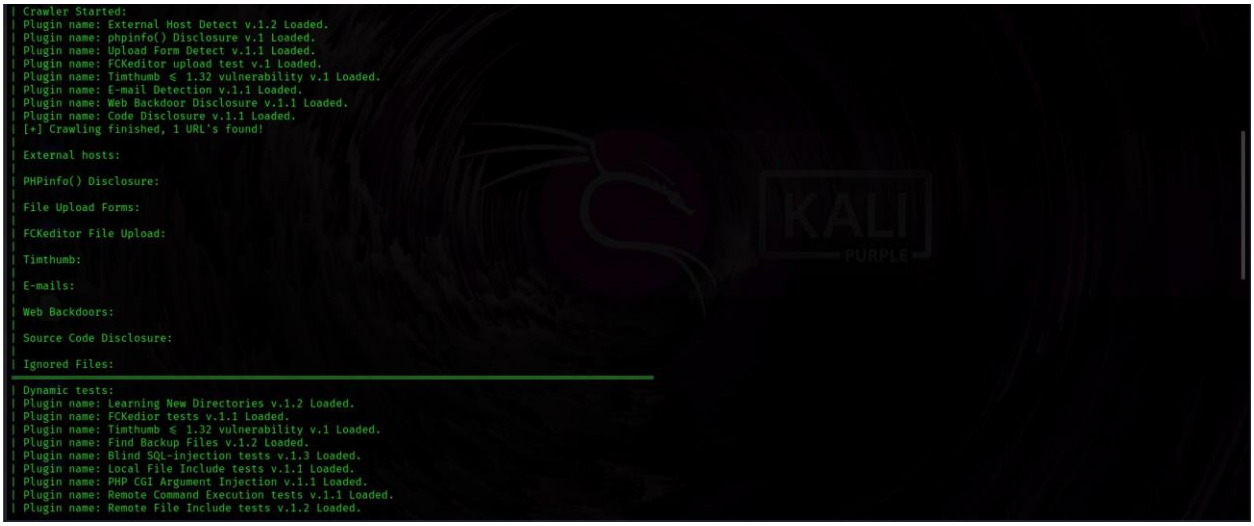
Report 09

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:

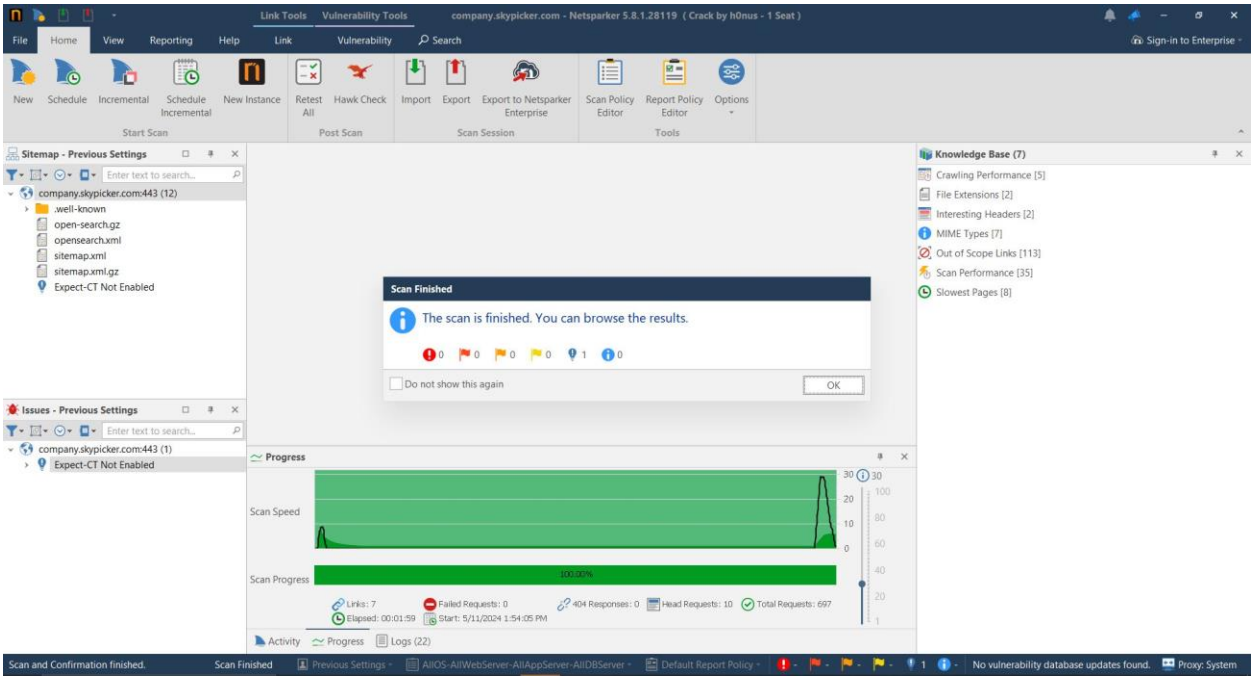


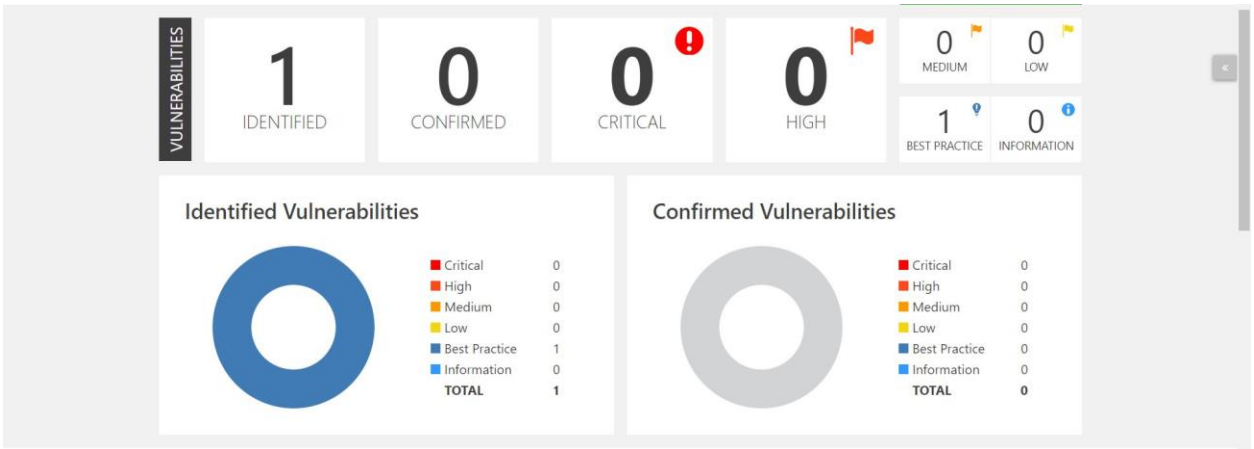


```
| FCKeditor tests:
| Skipped because https://www.kiwi.com/testing123 did not return the code 404
|
| Timthumb < 1.33 vulnerability:
|
|
| Backup Files:
| Skipped because https://www.kiwi.com/testing123 did not return the code 404
|
| Blind SQL Injection:
|
| Local File Include:
|
| PHP CGI Argument Injection:
|
|
| Remote Command Execution:
|
| Remote File Include:
|
| SQL Injection:
|
| Cross-Site Scripting (XSS):
```

Uniscan report neither returned any valuable information nor any vulnerabilities.

Scan using Netsparker.





Conclusion

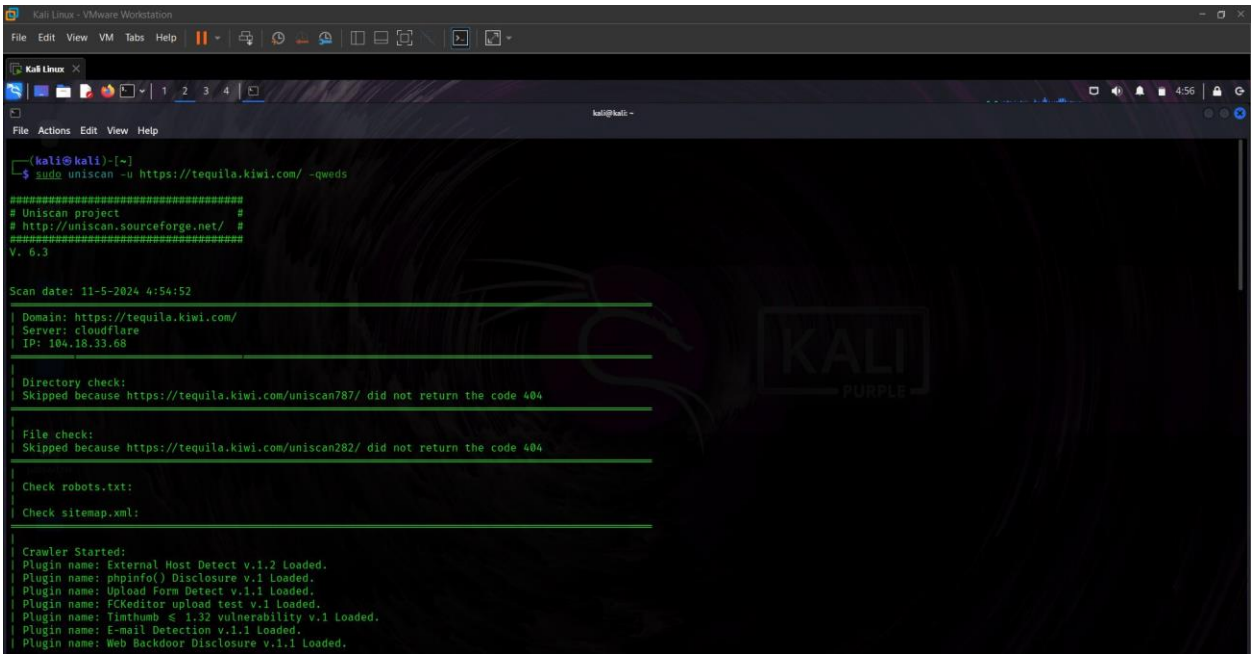
Netsparker ran complete security scans on the subdomain company.skypicker.com without finding any vulnerabilities. Such an outcome might seem to indicate a very strong security posture, but consideration should be given to possible constraints that might be forced on the scope and, therefore, methodology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

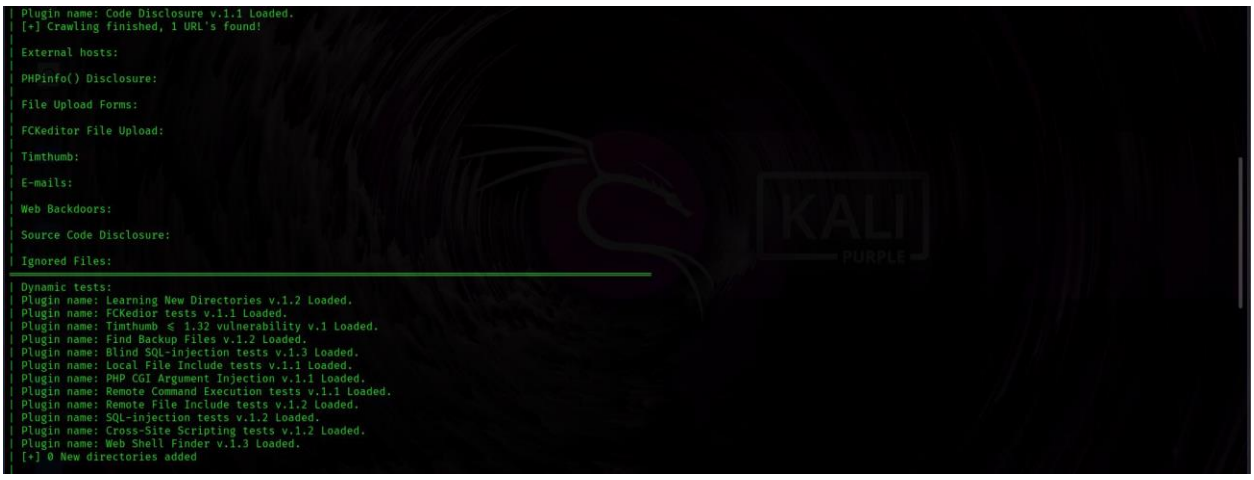
Report 10

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:

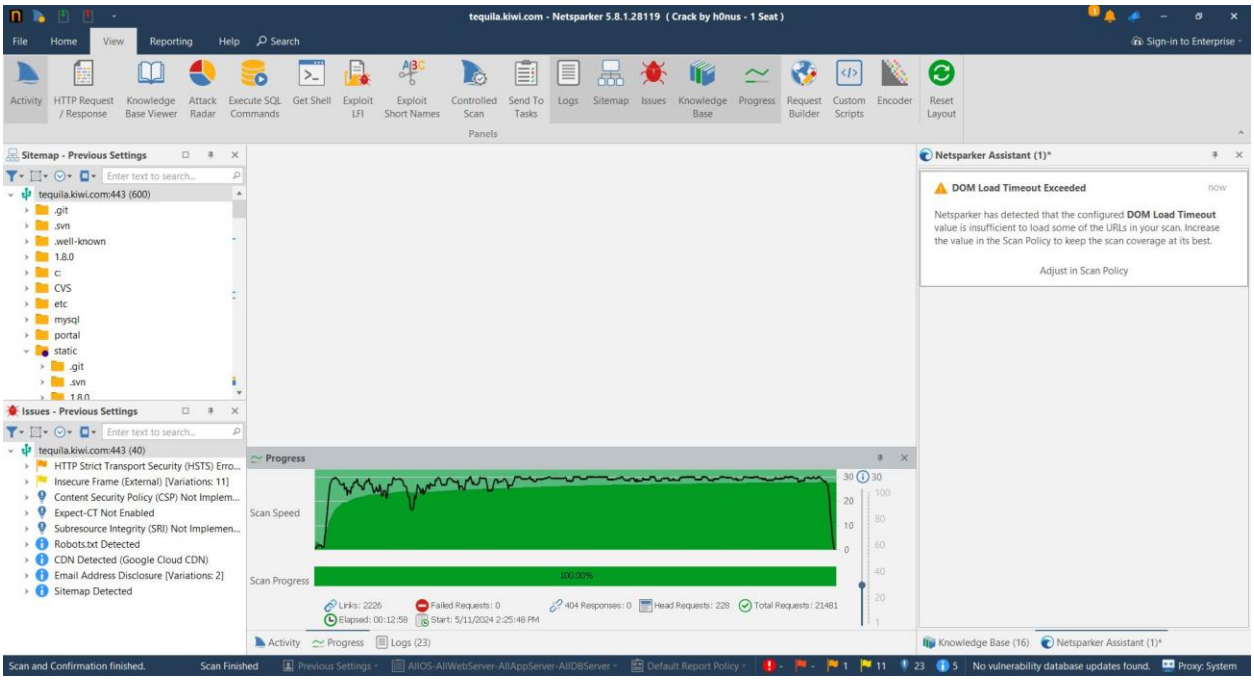




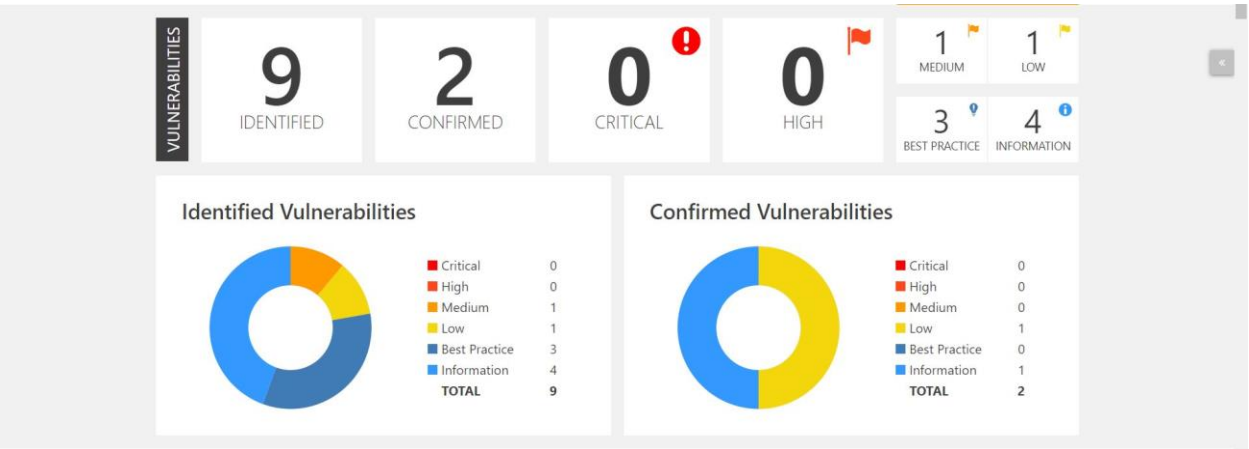
```
FCKeditor tests:
Skipped because https://tequila.kiwi.com/testing123 did not return the code 404

Timthumb < 1.33 vulnerability:

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):
```

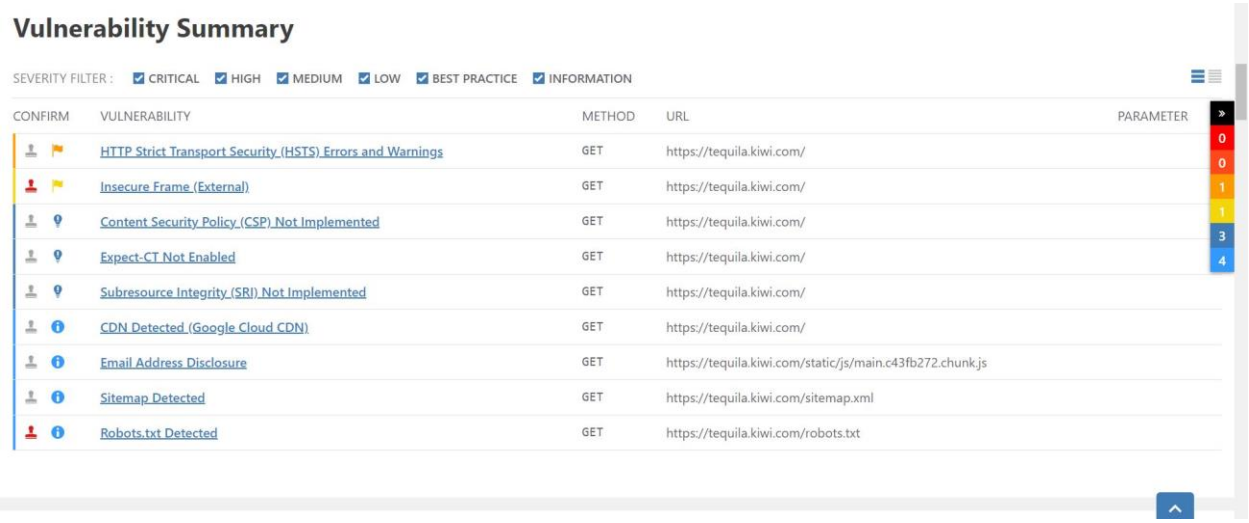
Uniscan report neither returned any valuable information nor any vulnerabilities.

Scan using Netsparker.



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

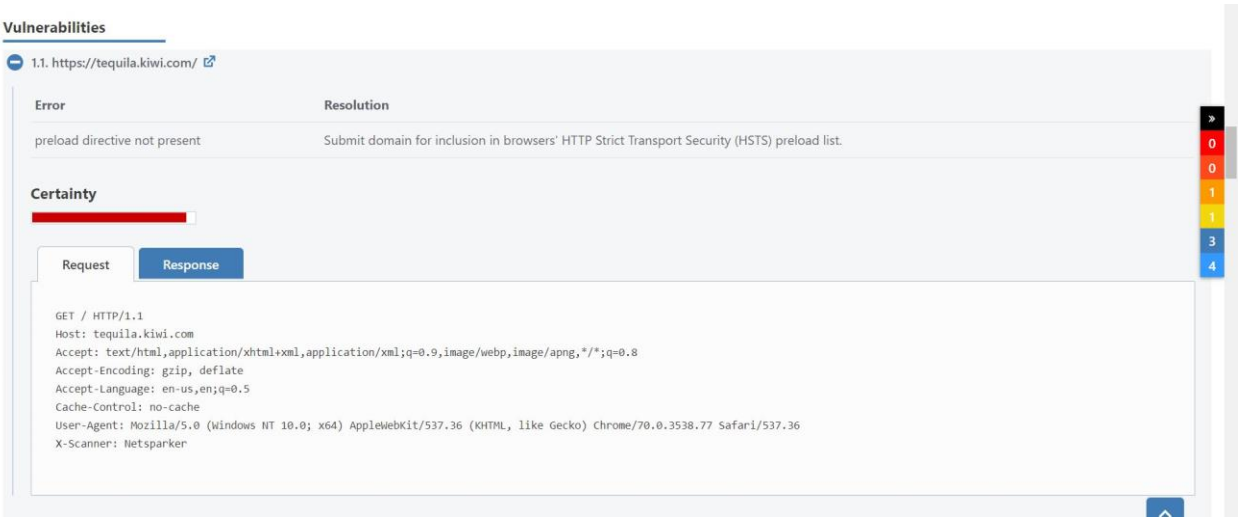


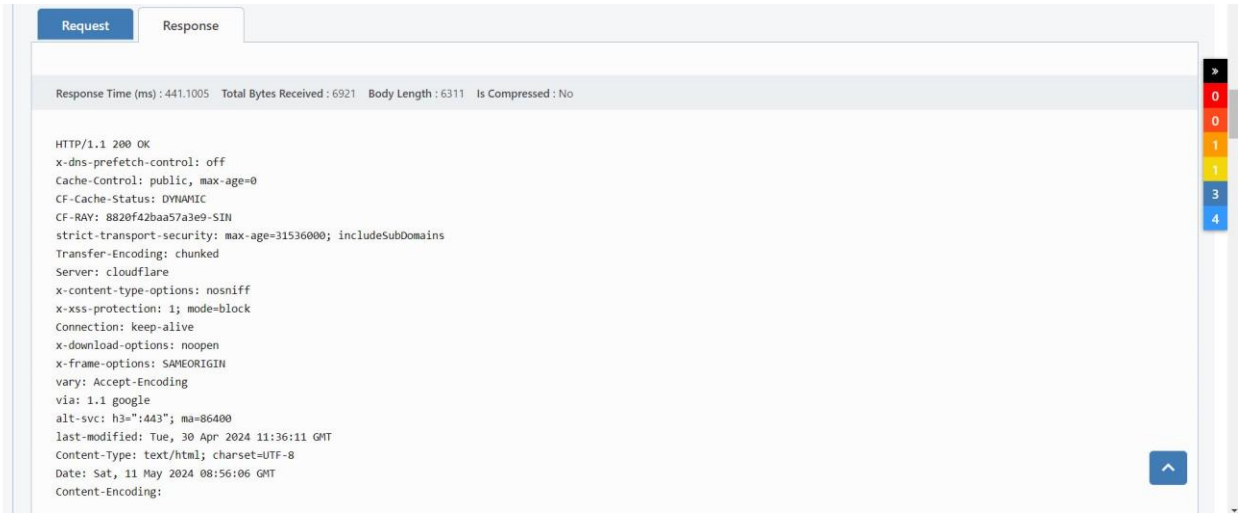


Vulnerability:

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.

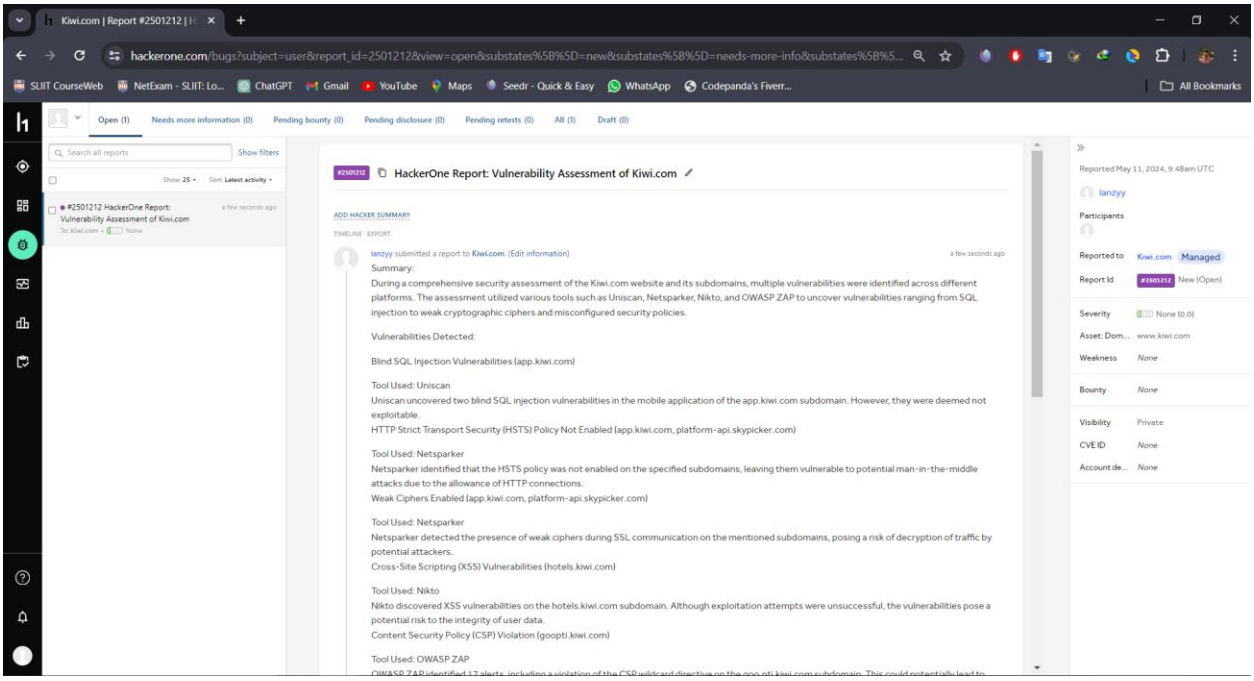




Conclusion

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



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]