Sri Lanka Institute of Information Technology

IE2062 – Web Security

Journal Book

IT22589668

Jayasekara J K C D

Y2-S2-CS WD

Abstract

This Bug Bounty Assessment Journal summarizes an engaged security researcher's dynamic journey into the world of vulnerability assessment under the Bug Bounty program. Every aspect of the phases, from the selection of the platform to the exploration of the target, is recorded, elaborating on the challenges, successes, and learnings in every step along the way. Using HackerOne, the leading platform for hosting Bug Bounty activities, and www.kiwi.com, one of the leading platforms in the field of travel, this journal lays out all the details of cybersecurity reconnaissance and vulnerability identification. With a focus on step-by-step exploration, usage of tools, and detailed documentation, this journal represents the relentless pursuit of digital security and the spirit of collaboration inherent in Bug Bounty projects.

Introduction

Bug Bounty programs are the pillars of proactive cybersecurity in that they stand for collaboration in enhancing digital landscapes against threats which keep on evolving in the digital space. Such initiatives, at their core, incentivize security researchers worldwide to seek out vulnerabilities lurking in the organizations' digital assets and, in the process, foster a symbiotic relationship between defenders and those who seek to protect them. At the very heart of this realm of digital vigilantism, HackerOne stands as the beacon of collaboration the platform at which security researchers and organizations merge to safeguard digital infrastructures.

In this Bug Bounty Assessment Journal, we take a journey of finding, documenting, and all that is in between within the dynamic confines of a Bug Bounty program. Choosing HackerOne as our conduit, we will explore how to carry out vulnerability assessment using an amalgamation of tools and methodologies to detect weaknesses in the digital realm. We shall be focusing on www.kiwi.com, the titan of the travel industry, whose digital footprint shall be used as the canvas on which our investigative prowess shall be tried and tested.

In this paper, we explore the various phases that this Bug Bounty assessment goes through, from the first selection of the platform and target domain to the meticulous documentation of our findings. The journal is a firsthand account of the challenges, successes, and lessons learned along the way. We use HackerOne and www.kiwi.com to put into perspective the intricacies of cybersecurity reconnaissance, identification of vulnerabilities, and the cooperative spirit underpinning Bug Bounty initiatives.

Come with us on this journey into the digital frontier as we unravel the mysteries of www.kiwi.com's digital ecosystem, armed with determination, ingenuity, and a commitment to securing the digital landscape for future generations.

My Bug Bounty Journey is divided into four phases.

Phase 1:

Overview of Bug Bounty

A bug bounty program entails proactive organizational measures towards detecting and mitigating security vulnerabilities among their digital assets. It goes ahead to encourage security researchers, known as bug bounty hunters, in the discovery and reporting of vulnerabilities for a reward, monetary compensation, recognition, or both. The overall objective of a bug bounty program is to increase the security posture of an organization leveraging the aggregate expertise of security researchers worldwide.

Salient features of a bug bounty program:

Incentivization:

This is the act of giving incentives to security researchers for discovering and reporting vulnerabilities. The incentives take the form of monetary incentives, swag, invitations to private programs, or public recognition.

Scope:

The bug bounty programs define the scope of eligible assets for testing, among them being the web applications, mobile applications, APIs, and network infrastructure. The scope serves as a guideline for the researchers on the areas to focus on that are of high priority.

Rules of Engagement:

The bug bounty programs list the rules of engagement that guide and stipulate what acceptable and forbidden actions are for participating researchers. These rules commonly are composed of guidelines for vulnerability disclosure, reporting procedure, and ethical considerations.

Vulnerability Severity Tiers:

Most bug bounty programs grade the vulnerabilities based on their impact and exploitability into respective tiers of severity. The significance of severity tiers is to prioritize remediation and the magnitude of rewards.

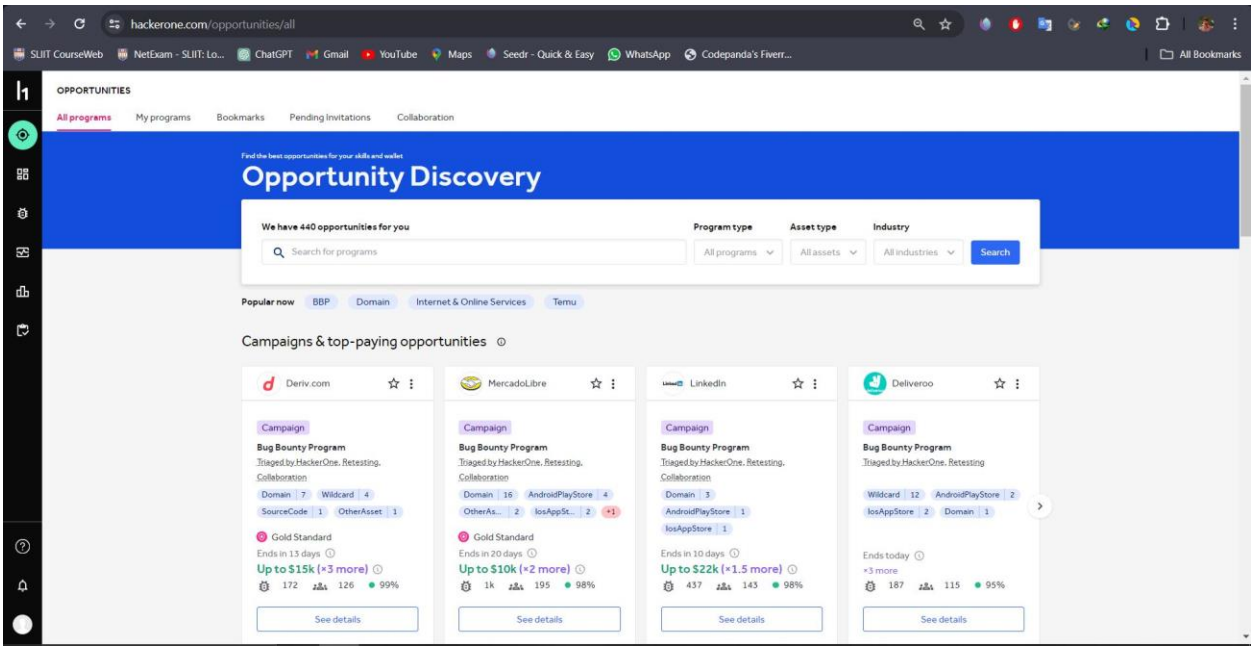
Reporting and Remediation:

The bug bounty program comprises mechanisms whereby the researchers report vulnerabilities securely and confidentially. When a report is received from the researchers, the organizations usually follow established procedures for the validation, prioritization, and remediation of the vulnerabilities.

The basics of the bug bounty programs are very important for the researchers engaged in the assessment of bug bounty. They provide a framework within which ethical hacking activities should be conducted, ensure compliance with the guidelines of the programs, and cooperate between researchers and organizations in pursuit of better cybersecurity.

What is HackerOne?

HackerOne is a leading platform that facilitates Bug Bounty programs, serving as a central hub where security researchers and organizations converge to identify, report, and remediate vulnerabilities in digital assets. As a pioneer in the Bug Bounty space, HackerOne has revolutionized the way organizations approach cybersecurity by harnessing the collective intelligence of a global community of security researchers.



Target Selection

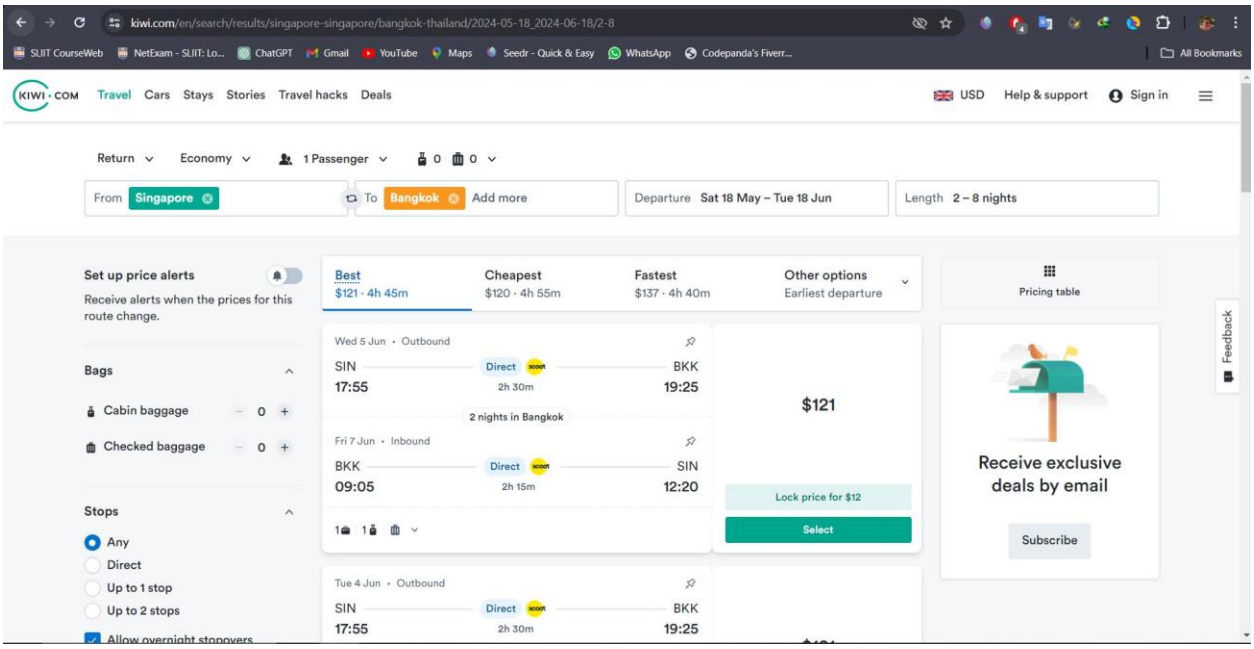
The appropriate target domain is of crucial importance for the success and effectiveness of the Bug Bounty assessment. In our assessment, www.kiwi.com has been chosen as the target domain, a well-known major player in the travel industry. Our choice was guided by the following factors: the complexity of the digital infrastructure of www.kiwi.com, its importance in the travel sector, and the potential impact of vulnerabilities on its users and stakeholders.

Complex Digital Infrastructure: www.kiwi.com maintains a very complex digital ecosystem comprising web applications, mobile applications, APIs, and backend systems. This complexity provides an extremely rich and diversified vulnerability landscape to study, with many potential attack surfaces to be explored.

Significance within the Travel Sector: As a major player in the travel sector, www.kiwi.com deals with a lot of sensitive information related to personal and financial information regarding travelers. Discovering vulnerabilities within the digital assets of www.kiwi.com may have serious consequences for the organization and its customers.

Potential Impact of Vulnerabilities: Vulnerabilities in www.kiwi.com's digital infrastructure can lead to many security risks for its users: for example, data breaches, compromise of accounts, fraud, and a lot more. Due to the nature of the information www.kiwi.com handles, vulnerability identification and remediation are of utmost importance to safeguard the reputation of the organization and maintain customer trust.

In selecting www.kiwi.com as the target domain for our Bug Bounty assessment, we aim to add to the improvement of its cybersecurity posture while gaining many valuable insights into the complexities of vulnerability identification and remediation within a complex digital ecosystem. Guided by ethical hacking, collaboration with the security team of www.kiwi.com, and the shared vision of creating a safer and more secure online environment for all stakeholders, our efforts will focus on putting the above into practice.



Phase 2:

Tool Exploration

Our evaluation of the Bug Bounty begins with large-scale exploration of various tools at the frontier of cybersecurity for the accomplishment of effective reconnaissance and vulnerability assessment. This stage is defined by curiosity, experimentation, and the thirst for knowledge about the capabilities and limitations of various tools.

Purpose:

This will, for the most part, focus on the determination of a diversified set of tools that will be useful in reconnaissance, vulnerability scanning, and exploitation. Each tool will be judged by its functionality, ease of use, accuracy, and relevance toward the Bug Bounty assessment objectives.

Tool Selection Criteria:

We select our tools based on a wide range of factors, including reputation among the cybersecurity community, user reviews and recommendations, compatibility with our operating environment, and alignment to the scope of our Bug Bounty assessment.

Categories:

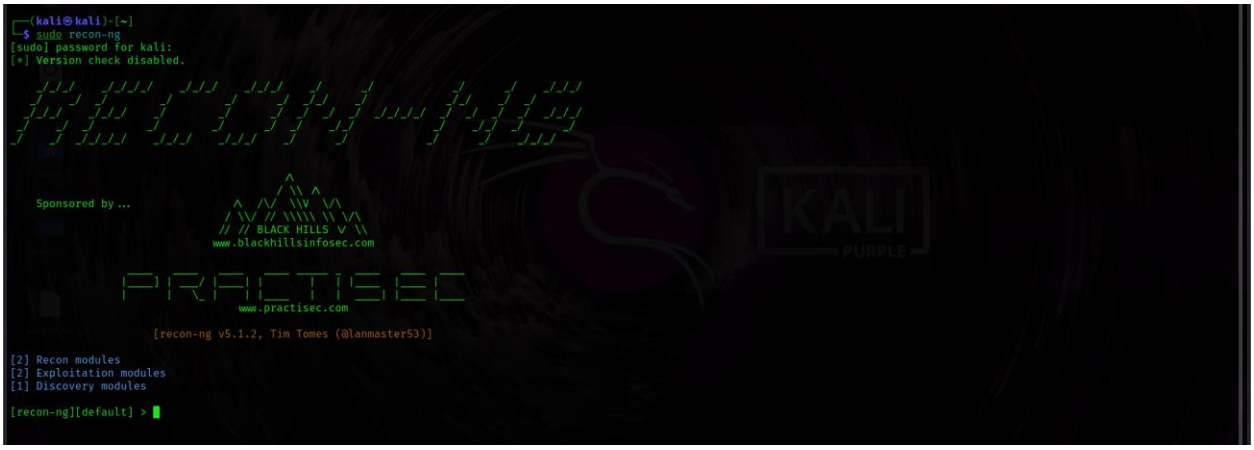
Our exploration would range from a wide spectrum of tool categories, including:

- **Reconnaissance Tools:**

Tools designed to gather information about the target domain, such as its subdomains, IP addresses, open ports, and network topology.

Nmap

Recon-ng

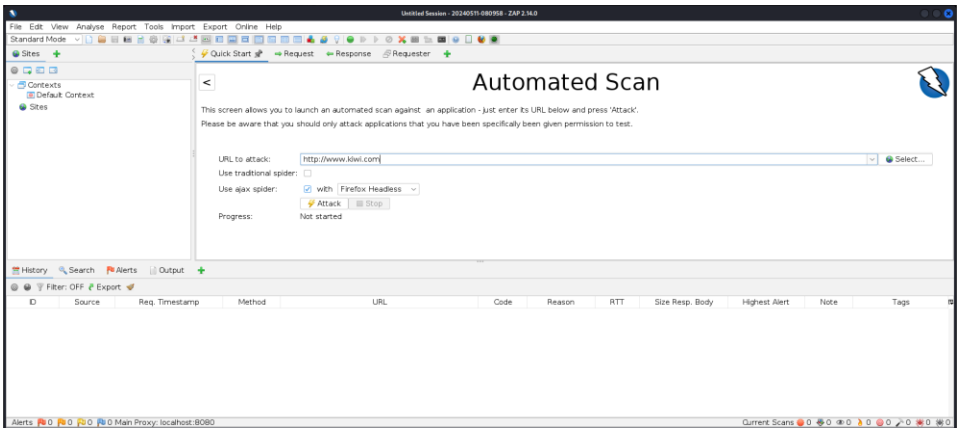


Uniscan

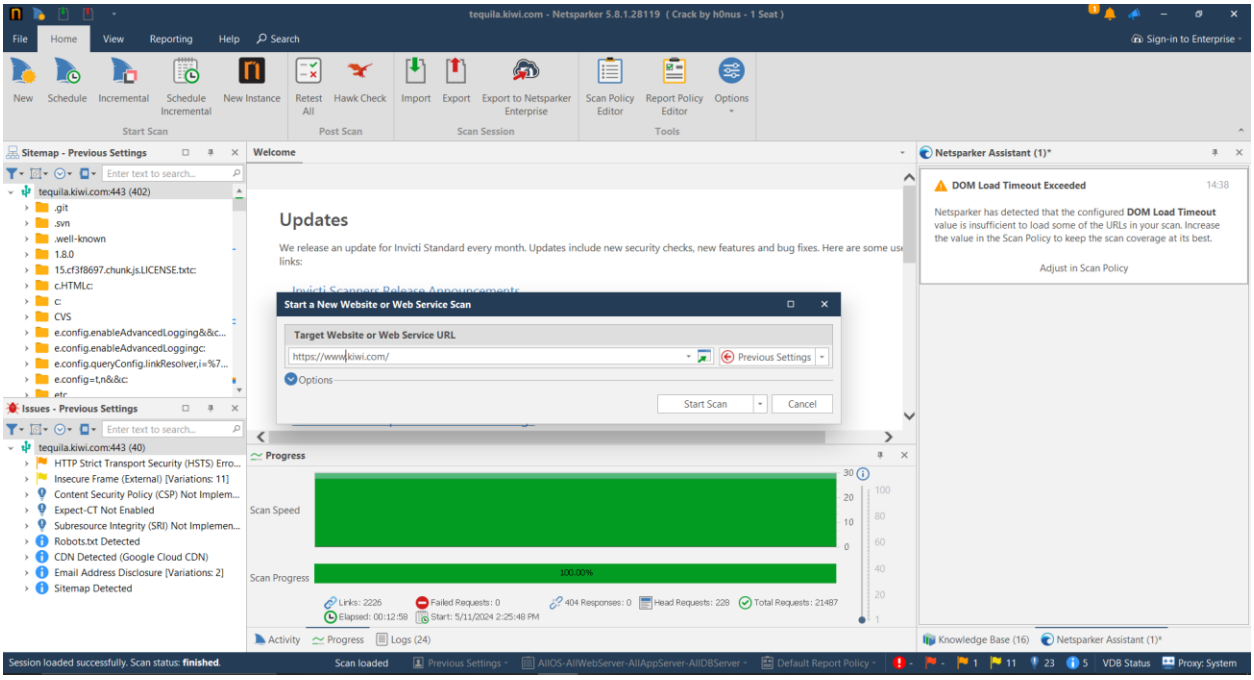
- **Vulnerability Scanning Tools:**

Tools that automate the process of identifying potential security vulnerabilities within the target domain, including web application vulnerabilities, misconfigurations, and outdated software versions.

OWASP-Zap



Netsparker



In this way, through this investment of time and effort into exploring tools, we lay down the groundwork for successful reconnaissance and vulnerability assessment in further phases of a Bug Bounty assessment. We work to put together the all-inclusive toolkit that shall enable identification of vulnerabilities, reduction of security risks, and generally working towards the betterment of cybersecurity across any given domain.

Tool Limitations and Challenges

Limitations of Tools and Challenges:

In going through this process of building an effective toolkit for Bug Bounty assessment, we shall inevitably find several limitations and challenges in the tools under consideration. This phase is the critical review of how the functionality of tools, their reliability, and applicability to our assessment objectives pan out.

Compatibility Issues:

Many of the challenges that are built into the process of tool exploration are related to compatibility issues with our operating environment or target domain. Some tools might not be compatible with operating systems, programming languages, or network configurations, and therefore produce errors or unreliable results.

Inaccurate Results:

Another challenge would be the possibility of tools returning wrong or misleading results. This can be caused by outdated databases of vulnerabilities, incorrect settings for the tools, or false positives/negatives coming out of the scan. It is, therefore, very important to scrutinize tool outputs carefully and validate findings through manual verification wherever possible.

Limited Functionality:

Some tools may suffer from limited functionality or just support one specific category of vulnerabilities and vectors of attack. These limitations of tool functionality render them useful only in specific scenarios, and other tools or manual techniques must be used to supplement functionality.

Resource Constraints:

Some tools may have resource constraints like limitations on memory or CPU usage while running scans or exploitation activities. Such constraints may affect the scalability and performance of the tool and bring a necessity for careful optimization and resource management to mitigate such an impact.

Ethical Considerations:

Ethical considerations should lead through all this tool exploration. Some tools may have certain functions that might become harmful if used without any responsibility. Extreme caution is therefore necessitated in such a case, and the use of tools is required to remain within legal and ethical bounds.

We are professional and honest about our process of doing the Bug Bounty assessment when we acknowledge the limitations and challenges of using tools and do our best to handle them. Through such experiences, we are bound to learn and innovate, forever trying to do cybersecurity reconnaissance and vulnerability assessment in a better way.

Reliable tools

In our effort to equip ourselves with a powerful armament for conducting bug bounty assessment, we identify and validate a set of dependable tools that are effective, reliable, and versatile in the realm of reconnaissance and vulnerability assessment. It will elaborate on enhancing our toolkit to equip it with tools that will meet our objectives of assessment and provide actionable insight in identifying and mitigating security vulnerabilities. Those tools I already mentioned above.

Phase 3:

Unraveling the Domain

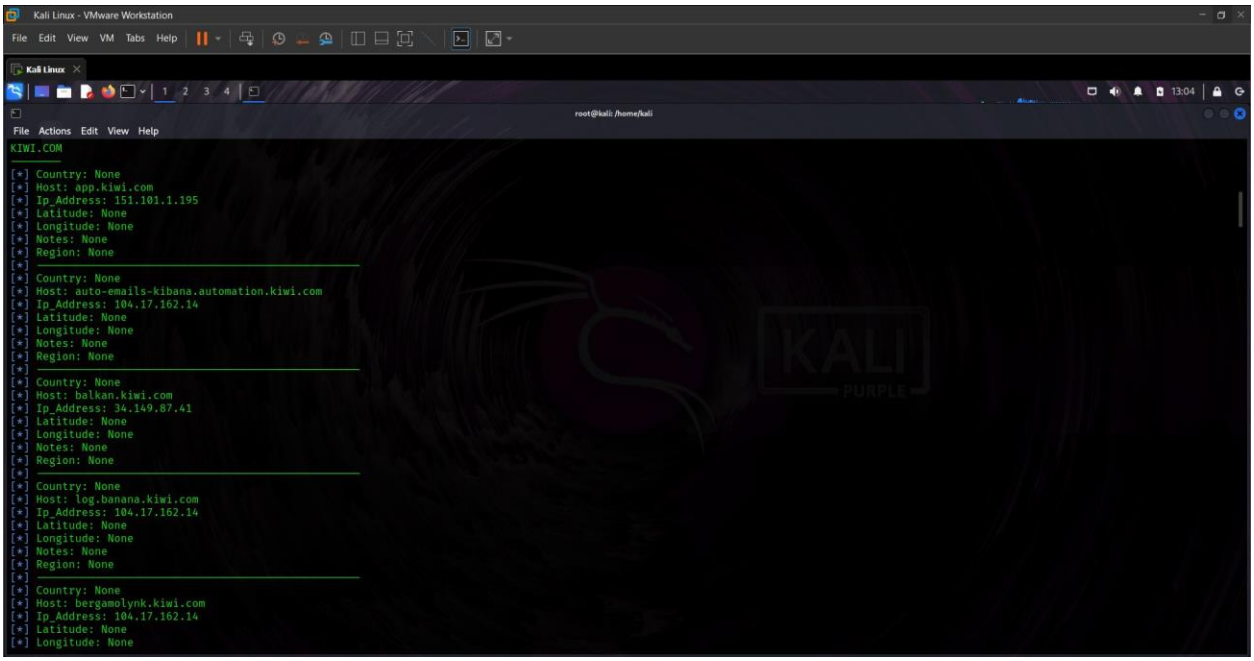
Bug Bounty Assessment delves into the meticulous process of uncovering vulnerabilities within the target domain, www.kiwi.com. This phase is characterized by comprehensive reconnaissance, meticulous subdomain enumeration, and the identification of potential attack surfaces for vulnerability assessment.

Subdomain Enumeration.

Challenges were met from tools during our phase of tool exploration, such as Knockpy and Sublist3r, which did not work as expected and finally proved to be duds. For example, Knockpy, which is a subdomain enumeration tool, had some limitations that impeded it from the identification of subdomains belonging to www.kiwi.com. This was based on its dependency on external APIs and, at the same time, outdated databases for discovering subdomains. Also, Sublist3r, which is another subdomain enumeration tool, gave out inconsistent results in discovering all the relevant subdomains of the target domain. In a nutshell, these limitations impeded our reconnaissance effort by compelling us to seek other solutions and adjust our approach in subdomain enumeration. On the other hand, our experience with both Knockpy and Sublist3r reminded us that resilience and flexibility are very important in overcoming the challenging hurdles in conducting a Bug Bounty assessment. It pushed us to investigate other tools and methodologies that would make our goals feasible.

Discovery of the recon-ng 'hackertarget' Module

Our persistence pays off in the finding of the recon-ng 'hackertarget' module, which happens to be a pretty useful tool in easing the task of subdomain enumeration and enhancing our reconnaissance capabilities. It is with this module that we get to intensively scan the subdomains on www.kiwi.com, hence uncovering hidden assets that widen our attack surface.


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

Selected subdomains after recon-ng scan

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

Having enumerated the list of important subdomains, we now proceed to the next phase:

full testing of each one of the chosen subdomains. This will be a step where the identified subdomains are tested against a battery of rigorous testing by using a combination of automated scanning tools, manual testing techniques, and web application testing frameworks.

Vulnerability Scanning:

Running against the chosen subdomains are automated vulnerability scanning tools like Nikto, OWASP ZAP, and Netsparker, scanning for common security vulnerabilities like injection flaws, cross-site scripting (XSS) vulnerabilities, insecure server configurations, and out-of-date software versions. This is meant to identify possible weaknesses and security gaps that might be exploited by malicious actors.

Web Application Testing Frameworks:

On top of the automated scanning tools, in-depth analysis of web applications hosted on the chosen subdomains will be done using web application testing frameworks like OWASP ZAP and Burp Suite. These frameworks enable us to simulate real-world attack scenarios, analyze application

behavior, intercept and manipulate HTTP requests, and identify vulnerabilities such as input validation errors, session management flaws, and access control issues.

Risk Prioritization:

The identified vulnerabilities through testing are then evaluated against severity, impact, and exploitability to prioritize remediation efforts effectively. In other words, vulnerabilities with the highest risk to www.kiwi.com security posture and the integrity of user data are prioritized, and resources are put in place to address the most critical security issues first.

It would uncover vulnerabilities from comprehensive testing of chosen subdomains, estimate possible consequences, and give actionable insight to the security team at www.kiwi.com for remediation. This step would then form an important part of our evaluation as part of the Bug Bounty where compilation of the reconnaissance, vulnerability scanning, and manual testing efforts is channeled in delivering constructive findings and contributing to the continuous enrichment of cybersecurity defenses of www.kiwi.com.

Phase 4:

Documenting and Analyzing Findings

The bug bounty evaluation goes on in the consolidation phase, which is the fourth and final one, ending today. It is the consolidation phase of all the findings that have been collected during the reconnaissance and vulnerability assessment phase. Of course, documenting what I found and providing the www.kiwi.com security team with actionable insights is the most important thing to do.

Review of Findings:

This basically involves the detailed review of the security vulnerabilities or issues discovered in the assessment. Each discovery would be weighed on several factors, the level of the severity of the vulnerability, the extent of the possible impact, and the ease of exploitation. In this way, I am confident and fully aware of the potential dangers that might lay bare the assets of www.kiwi.com and its users.

Submission of Evidence:

I attach evidence in the form of screenshots, exploit code, or proof-of-concept demonstrations to prove the severity of the identified vulnerabilities. The supplementary information adds validity to my conclusions and helps security personnel from www.kiwi.com understand the potential dangers in every weakness.

Summary of Findings and Recommendations:

I document the compilation and results of the analysis and documentation in a comprehensive report. The report is written with clarity and conciseness to make the reading easy and to enable prioritization of remediation efforts by the security team of www.kiwi.com.

Collaboration:

To ensure collaboration and the veracity of findings are not wasted, the www.kiwi.com Security Team will not close the door on any inquiries or need for clarity that might have arisen via the HackerOne platform.

I fulfill my duty to the www.kiwi.com security team and the www.kiwi.com Bug Bounty program through the submission of a diligently written and actionable report at the end of phase 4. The insights gained from this documentation and analysis allow the organization to effectively mitigate the vulnerability and enhance its cybersecurity resilience with respect to the security posture of www.kiwi.com.

Conclusion

The Bug Bounty Assessment Journal represents this relentless pursuit and collaboration in the cybersecurity domain. From the selection of the platform to the exploration of the target domain, every aspect of the bug bounty assessment has been chronicled in detail, thus revealing the challenges, successes, and learning from the journey traveled.

This has been an exercise in which we have gone through all the details of the vulnerability assessment by using tools and methodologies and collaborative efforts to bring into visibility the weaknesses hidden within www.kiwi.com's digital ecosystem. We have been resilient, ingenious, and committed, thus enhancing cybersecurity resilience toward emerging threats.

This journal is the very essence of how to collaborate with a global community of security researchers for the identification and fixation of vulnerabilities that will empower organizations like www.kiwi.com to empower themselves against existing vulnerabilities and finally protect their digital assets while preserving trust in this digital landscape.

Moving forward, we remember the power of collaboration, innovation, and ethical hacking in digital security driving us onward. With an ever-changing threat landscape to grapple with, may we never forget our commitment to securing the digital frontier and to building a safer online environment for all.

This Bug Bounty Assessment Journal celebrates the spirit of collaboration, exploration, and continuous improvement in cybersecurity, including all the challenges and opportunities that go into the pursuit of a safer digital future.