Sri Lanka Institute of Information Technology

2024

Web Security - IE2062

Assignment

Year 2, Semester 2

IT22562074
JAYARATHNA K.P.G.C.M
Y2.S2.WE.CS.01
MALABE CAMPUS

Contents

Introduction

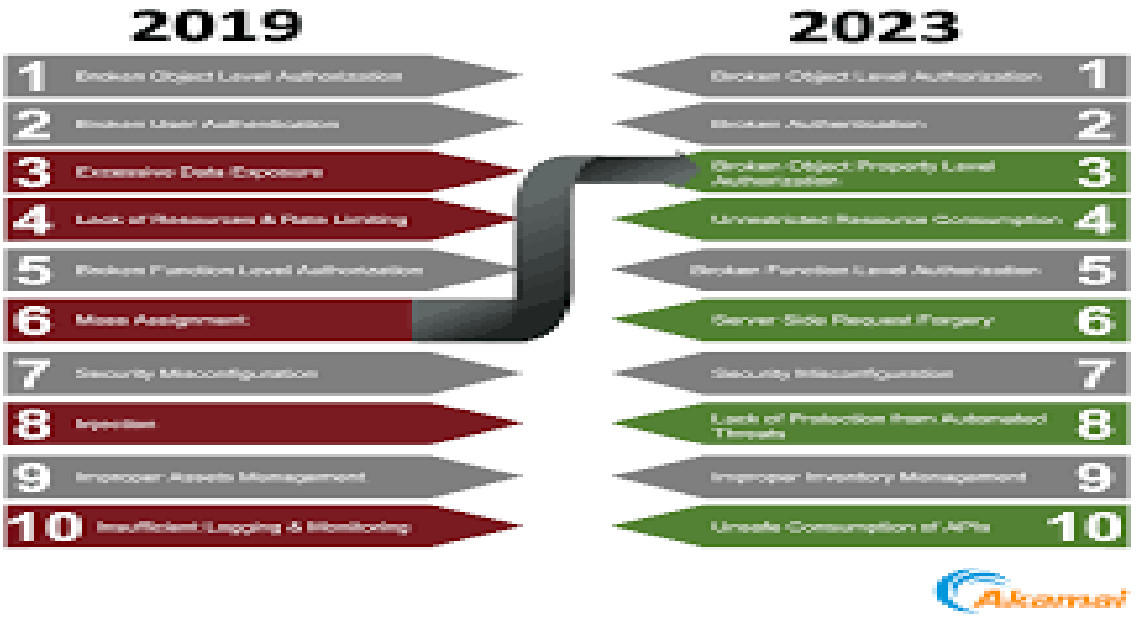
I carefully record all of my daily activities, discoveries, difficulties, and lessons learned while performing web security assessments in this journal. Every day offers me a chance to learn more about the complex field of cybersecurity. I investigate security holes in web applications and create efficient defenses against possible attacks.Every task helps me learn more about cybersecurity principles and practices, from examining subdomains for security flaws to interpreting intricate vulnerability reports produced by security assessment tools like Legion, Nikto, Wapiti, and Netsparker. I face a variety of obstacles as I work through each assessment, which calls for ingenuity in solving problems and a voracious appetite for information.

This journal serves as a chronicle of my journey, providing insights into the vulnerabilities uncovered, the strategies employed to mitigate them, and the invaluable lessons learned along the way. It underscores the importance of continuous learning and adaptation in the ever-evolving landscape of web security, reinforcing the notion that vigilance and proactive measures are essential to fortify digital defenses against cyber threats.

Date 04/04/2024

Summary of the day's activities

Today marked the beginning of my journey into understanding cybersecurity vulnerabilities, focusing particularly on the OWASP Top 10 Security Risks and Vulnerabilities. I went into great detail about the relevance of OWASP, how it directs cybersecurity initiatives, and how critical it is to counter these major risks in web applications.



Vulnerabilities discovered or explored:

I explored the OWASP Top 10 vulnerabilities in detail, gaining insights into the various threats that can compromise the security of web applications. The OWASP Top 10 vulnerabilities, including broken access control, cryptographic failures, injection attacks, insecure design, security misconfiguration, authentication failures, software and data integrity failures, and server-side request forgery, are extensively studied

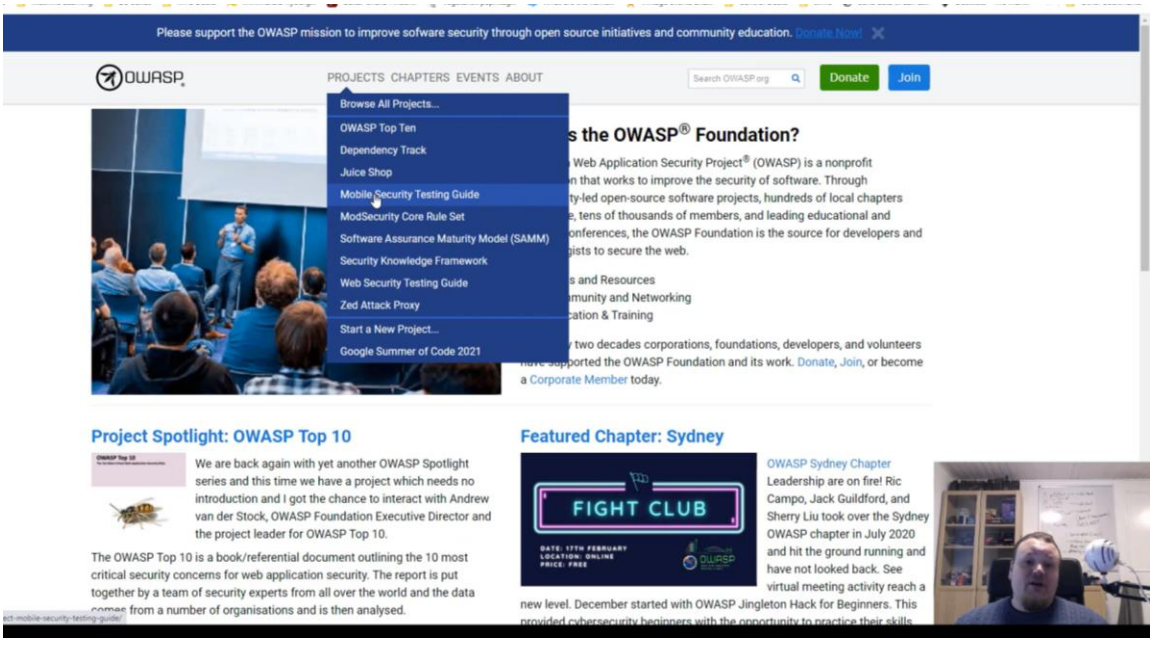
Challenges faced and how they were overcome:

- The main challenge I encountered today was my initial unfamiliarity with structuring a journal entry. However, I tackled this by breaking down the required sections and gradually organizing my thoughts under each category.

- Some concepts within the OWASP Top 10 were initially difficult to grasp. To overcome this, I engaged in further research, seeking clarification through online resources and tutorials. This allowed me to deepen my understanding of each vulnerability and its implications.

New tools, techniques, or concepts learned:

Today, I learned about various security risks and vulnerabilities outlined by OWASP, including preventive measures to mitigate these risks.



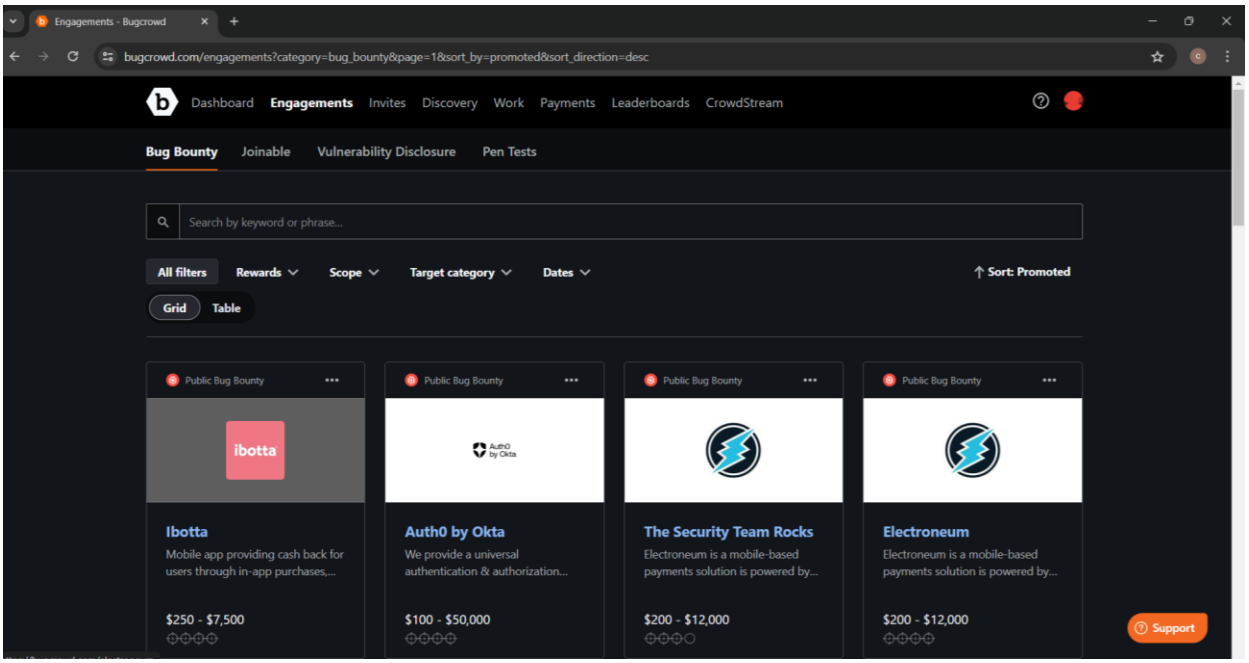
Reflections and takeaways:

As I reflect on today's learning, I realize the critical role that understanding cybersecurity vulnerabilities plays in ensuring the safety and integrity of web applications. The OWASP Top 10 provides a comprehensive framework for identifying and addressing common security threats, empowering developers and security professionals to proactively safeguard digital assets against potential attacks. Moving forward, I am excited to continue exploring cybersecurity concepts and enhancing my knowledge in this field.

Date 05/04/2024

Summary of the day's activities

Today, I gained valuable insights into the process of selecting a bug bounty platform and choosing a suitable bug bounty program. I also learned about the importance of thoroughly understanding the scope and policies of bug bounty programs to ensure compliance and maximize the chances of successful bug discoveries.



Vulnerabilities discovered or explored:

While I didn't directly explore vulnerabilities today, I did engage in researching bug bounty platforms and programs, which indirectly contributes to my understanding of cybersecurity vulnerabilities and their mitigation

Challenges faced and how they were overcome:

- One of the primary challenges I faced today was determining which bug bounty platform to choose. To overcome this, I conducted thorough research on various platforms, considering factors such as reputation, user feedback

and available programs.After careful consideration, I selected a reputable bug bounty platform

- Another challenge I encountered was understanding the scope and policies of bug bounty programs. To address this challenge, I meticulously reviewed the documentation provided by the bug bounty platform and carefully studied the scope and policies of the selected program.

New tools, techniques, or concepts learned:

Today, I gained valuable insights into the process of selecting a bug bounty platform and choosing a suitable bug bounty program. I also learned about the importance of thoroughly understanding the scope and policies of bug bounty programs to ensure compliance and maximize the chances of successful bug discoveries.

Reflections and takeaways:

As I reflect on today's activities, I recognize the importance of thorough research and attention to detail when selecting a bug bounty platform and program. By overcoming the challenges encountered today, I have taken a significant step forward in my bug bounty journey. Moving forward, I am excited to begin actively participating in the selected bug bounty program and further honing my skills in identifying and reporting security vulnerabilities.

Date 06/04/2024

Summary of the day's activities

Today, I focused on learning about bug bounty methodologies and tools, particularly those related to reconnaissance, subdomain searching, port scanning, vulnerability scanning, and information gathering. I explored both passive and active information gathering techniques and familiarized myself with various tools used for these purposes

Vulnerabilities discovered or explored:

While I didn't directly discover vulnerabilities today, I gained valuable knowledge about the initial stages of bug bounty hunting, which lay the groundwork for identifying potential security issues in web applications.

Challenges faced and how they were overcome:

- Some tools do not work in Kali Linux no matter how much you try.To address this, I update my kali linux and troubleshooting methods to resolve compatibility issues.
- Additionally, I faced difficulties in understanding the functionality of some tools, which hindered my progress in using them effectively. To overcome this challenge, I dedicated time to studying documentation, tutorials, and online resources related to these tools.

New tools, techniques, or concepts learned:

Today, I expanded my knowledge of bug bounty methodologies and tools, particularly in the realm of reconnaissance and information gathering. I familiarized myself with a variety of passive and active information gathering tools, each serving specific purposes in the initial phase of bug hunting.
Passive information gathering tools

- Sublist3r
- nslookup
- whois
- whatweb
- whoislookup
- netcarft
- wayback machine

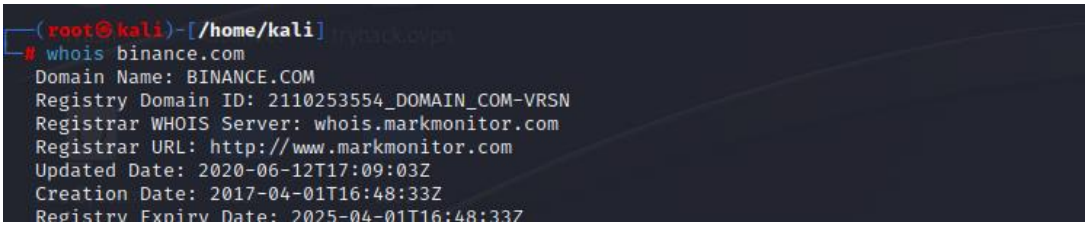
Active information gathering tools

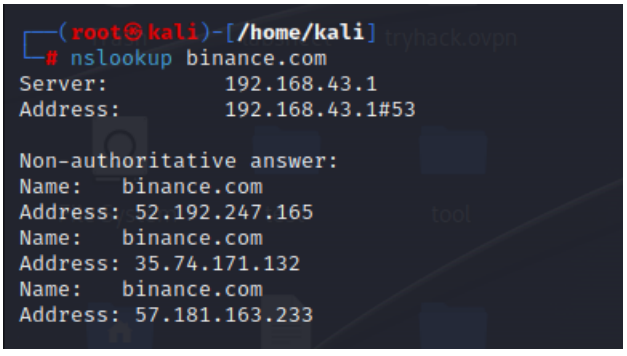
- nmap
- recon-ng
- sodan

Date 07/04/2024

Summary of the day's activities

Today, I focused on actively gathering information about my target domain using tools such as Sublist3r, nslookup, and whois. These tools helped me in identifying subdomains, retrieving DNS information, and obtaining registration details about the target domain





Vulnerabilities discovered or explored:

While I didn't directly discover vulnerabilities today, the information gathered using these tools lays the groundwork for further exploration and potential discovery of security weaknesses in the target domain.

Challenges faced and how they were overcome:

- One of the primary challenges I encountered today was intermittent connection problems, which hindered the smooth execution of scanning processes.To address this issue, I ensured that my internet connection was stable and optimized.

- Another challenge I faced was the extended scan time, particularly with Sublist3r, which significantly slowed down the information-gathering process. To mitigate this challenge, I optimized the scan parameters, such as adjusting the timeout settings and limiting the depth of subdomain enumeration. This helped in reducing the overall scan time while still capturing relevant information about the target domain.

New tools, techniques, or concepts learned:

Today, I gained hands-on experience with Sublist3r, nslookup, and whois, which are valuable tools for reconnaissance and information gathering in bug bounty hunting. I learned various techniques for identifying subdomains, retrieving DNS records, and obtaining domain registration details, enhancing my skill set in this aspect of cybersecurity.

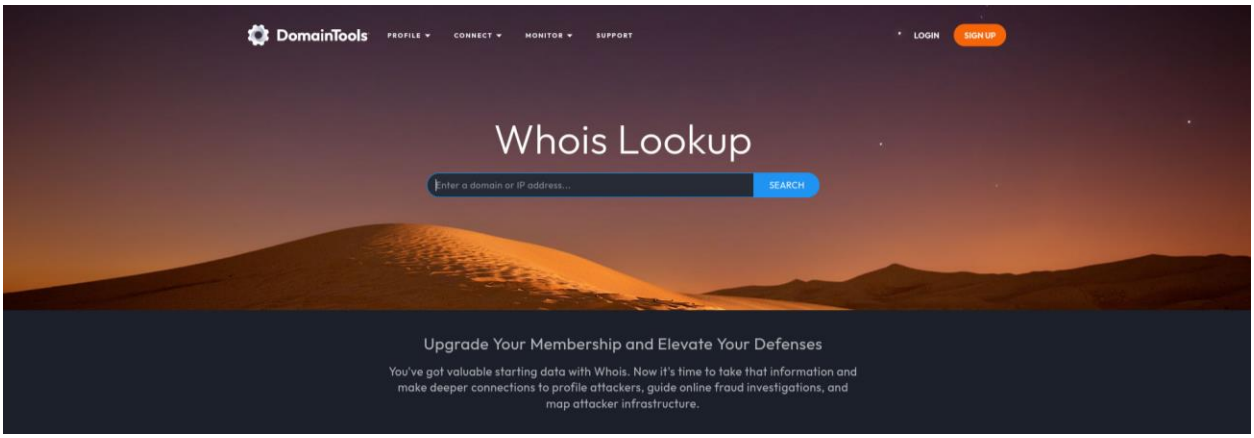
Reflections and takeaways:

As I reflect on today's activities, I recognize the importance of patience and perseverance when dealing with challenges in bug bounty hunting. Despite encountering obstacles such as connection problems and prolonged scan times, I remained persistent and employed troubleshooting techniques to overcome these challenges. Moving forward, I am committed to further refining my skills in reconnaissance and information gathering, as they form the foundation for successful vulnerability discovery in bug bounty programs.

Date 08/04/2024

Summary of the day's activities

Today, I continued my information-gathering process on the target domain using additional tools such as WhatWeb, whoislookup, netcarft, and the Wayback Machine. These tools provided valuable insights into the technologies used by the target domain, its network infrastructure, domain registration details, and historical snapshots of the website.



Vulnerabilities discovered or explored:

The focus today was on gathering information rather than directly discovering vulnerabilities, but the data from these tools serves as a foundation for further analysis and potential security weaknesses.

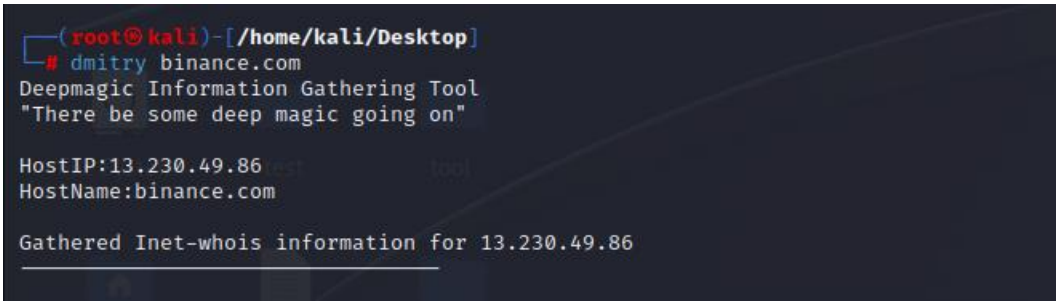
New tools, techniques, or concepts learned:

Today, I gained hands-on experience with WhatWeb, whoislookup, netcarft, and the Wayback Machine, expanding my repertoire of tools for reconnaissance and information gathering in bug bounty hunting. These tools provided unique functionalities, allowing me to gather diverse sets of information about the target domain.

Date 09/04/2024

Summary of the day's activities

Today, I focused on active information gathering using tools such as Nmap, Recon-ng, Dmitry, and Shodan. These tools provided insights into the status of ports, domain information, and potential vulnerabilities of the target domain, www.binance.com.



Vulnerabilities discovered or explored:

While the primary focus was on gathering information rather than directly discovering vulnerabilities, the data obtained from these tools can help in identifying potential security weaknesses in the target domain, which can be further explored in subsequent stages of bug bounty hunting

Challenges faced and how they were overcome:

- I encountered challenges with some tools not supporting my environment or operating system. To address this, I explored alternative tools

- Another challenge I faced today was a power outage in my area, which disrupted my workflow and hindered the progress of my activities. To overcome this challenge, I went to my friend's house and ensured continuity in my work.

New tools, techniques, or concepts learned:

Today, I gained hands-on experience with active information gathering tools such as Nmap, Recon-ng, Dmitry, and Shodan, expanding my skill set in conducting reconnaissance and vulnerability assessment tasks in bug bounty hunting. These tools provided unique functionalities for gathering diverse sets of information about the target domain.

Reflections and takeaways:

As I reflect on today's activities, I realize the importance of adaptability and resilience in overcoming challenges encountered during bug bounty hunting. Despite facing obstacles such as tool compatibility issues and power outages, I remained committed to the information gathering process, leveraging alternative solutions and backup resources to ensure progress. Moving forward, I am excited to analyze the data obtained today and explore potential security vulnerabilities in the target domain as part of my bug bounty hunting efforts.

Date 21/04/2024

Summary of the day's activities

Today, I focused on planning and analysis following the information gathering phase in preparation for vulnerability detection. I categorized the gathered data based on technical specifications, including details about the web server, application server, database server, DNS information, open ports, and HTTP security measures. This analysis served as the foundation for selecting appropriate tools and scheduling vulnerability scanning processes.

Vulnerabilities discovered or explored:

the primary focus today was on planning and analysis

Challenges faced and how they were overcome:

- I encountered challenges in fully understanding some of the gathered information, which hindered the planning and analysis process. To address this, I revisited the documentation provided by the information gathering tools and sought clarification through online resources and tutorials

New tools, techniques, or concepts learned:

Today, I gained insights into the importance of planning and analysis in vulnerability detection, as well as the process of categorizing gathered data to guide the selection of appropriate tools and scheduling of vulnerability scanning processes. This approach helps in saving time and carrying out vulnerability detection effectively.

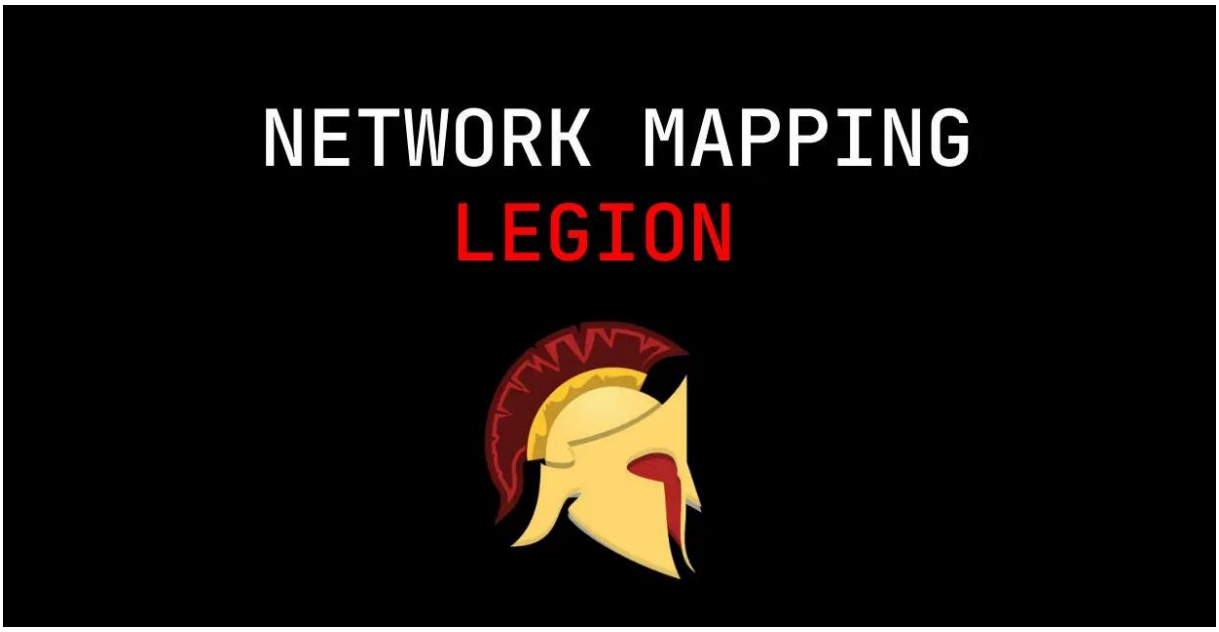
Reflections and takeaways:

As I reflect on today's activities, I realize the critical role that planning and analysis play in the bug bounty hunting process. By systematically categorizing and analyzing the gathered information, I can prioritize areas of focus and tailor vulnerability scanning processes accordingly. Despite encountering challenges in understanding some of the gathered information, I remained proactive in seeking clarification and leveraging resources to enhance my understanding. Moving forward, I am excited to proceed with vulnerability scanning based on the insights gained from today's planning and analysis phase.

Date 22/04/2024

Summary of the day's activities

Today, I focused on vulnerability detection, a crucial stage in bug bounty assessment aimed at identifying weaknesses in software, hardware, networks, or systems that could be exploited by attackers. I explored both automated and manual scanning techniques using vulnerability detection tools such as Legion and UniScan to scan for vulnerabilities in the target domain, www.binance.com.



Vulnerabilities discovered or explored:

the scanning results did not reveal any specific vulnerabilities in the target domain

Challenges faced and how they were overcome:

- the main challenge I encountered today was the absence of identified vulnerabilities in the target domain despite conducting thorough scans using vulnerability detection tools.

New tools, techniques, or concepts learned:

Today, I gained practical experience with vulnerability detection tools such as Legion and UniScan, expanding my knowledge of automated and manual scanning techniques in bug bounty assessment. While specific vulnerabilities were not identified, the scanning process enhanced my understanding of network vulnerabilities and their detection methods.

Reflections and takeaways:

As I reflect on today's activities, I recognize the inherent challenges in vulnerability detection, particularly in complex network environments such as those found in bug bounty assessments. While specific vulnerabilities were not discovered, the scanning process provided valuable insights into the security posture of the target domain. Moving forward, I remain committed to refining my skills in vulnerability detection and exploring alternative approaches to uncover potential security weaknesses. Additionally, I understand the importance of persistence and continuous learning in the dynamic field of cybersecurity.

Date 24/04/2024

Summary of the day's activities

Today, I focused on vulnerability detection using tools such as Nikto and Wapiti to scan the target domain, www.binance.com, for potential security vulnerabilities. These tools provided insights into various security headers, missing content security policies, and other vulnerabilities present in the web application.

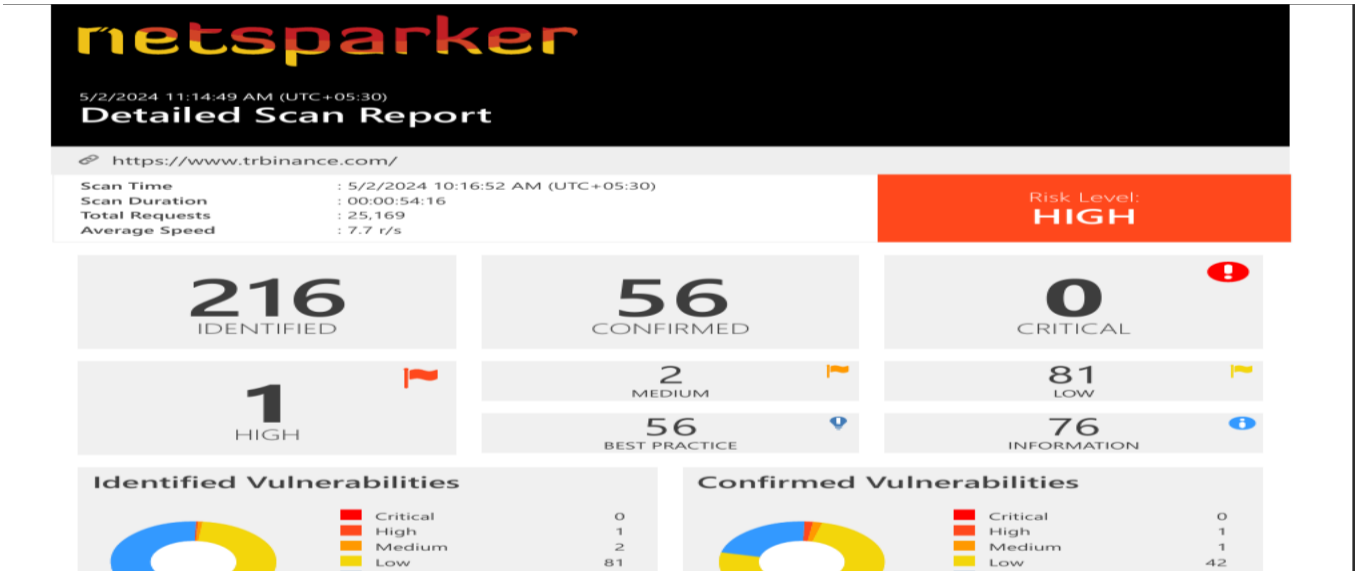
Vulnerabilities discovered or explored:

Nikto Scan:

- Missing X-Frame-Options Header: This vulnerability indicates that the website may be vulnerable to clickjacking attacks.
- Missing X-Content-Type-Options Header: This vulnerability could lead to MIME-sniffing attacks and potentially cross-site scripting (XSS) vulnerabilities.

Wapiti Scan:

- Missing Content Security Policy (CSP): This vulnerability leaves the website susceptible to various attacks such as XSS and data injection.
- Missing Security Headers: The absence of security headers like X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, and Strict-Transport-Security exposes the website to clickjacking, XSS, MIME type sniffing, and protocol downgrade attacks.
- SSRF (Server-Side Request Forgery): This vulnerability indicates that the website may allow attackers to make unauthorized requests from the server, potentially leading to data access or further exploitation.



Challenges faced and how they were overcome:

- I encountered challenges in fully understanding some of the vulnerabilities detected by the scanning tools. To address this, I referred to documentation provided by the tools, online resources, and tutorials to gain a better understanding of each vulnerability and its potential impact on the website's security.

New tools, techniques, or concepts learned:

Learnd ho to work wapiti nd nikto tool

Date 25/04/2024

Summary of the day's activities

Today, I utilized Netsparker, a web application security scanner, to conduct a comprehensive scan of the target domain, www.binance.com. Netsparker identified a medium-risk vulnerability related to weak ciphers enabled during secure communication (SSL). This vulnerability could potentially allow attackers to decrypt SSL traffic between the server and visitors, compromising the security of the web application.

Vulnerabilities discovered or explored:

Weak Ciphers Enabled during SSL Communication:

- Netsparker detected that weak ciphers are enabled during secure communication (SSL), posing a medium risk to the security of the web application. This vulnerability could allow attackers to decrypt SSL traffic between the server and visitors.

Challenges faced and how they were overcome:

- Conducting a thorough scan using Netsparker proved to be time-consuming. To address this challenge, I optimized the scan parameters and utilized parallel processing capabilities where available to expedite the scanning process.

New tools, techniques, or concepts learned:

Today, I learned about Netsparker, a powerful web application security scanner designed to automatically identify vulnerabilities in web applications. Netsparker's ability to analyze the structure and behavior of web applications enables it to detect various security issues, including SQL injection, cross-site scripting (XSS), and weak cipher vulnerabilities in SSL communication.

Date 26/04/2024

Summary of the day's activities

Today, I focused on gathering information about subdomains associated with the main domain, www.binance.com. By identifying and analyzing these subdomains, I aimed to gain a comprehensive understanding of the domain's ecosystem and potential attack surface.

Subdomains identified:

- trbinance.com
- academy.binance.com
- info.binance.com
- coinmarketcap.com
- pro.coinmarketcap.com
- *.binance.us
- account.binance.com
- c2c.binance.com
- support.binance.com

Challenges faced and how they were overcome:

- The information gathering tools were unable to support certain subdomains, causing limitations in comprehensive data collection. Alternative methods were explored to address this issue.

New tools, techniques, or concepts learned:

Today's activities reinforced the importance of thoroughly mapping out subdomains associated with a main domain to gain a comprehensive understanding of the web application's attack surface.

Reflections and takeaways:

The process of gathering information about subdomains highlighted the complexity of web application infrastructure and the need for thorough reconnaissance in bug bounty assessments. Despite encountering challenges with certain subdomains, I persevered in finding alternative methods for information gathering, ultimately enhancing my skills in reconnaissance and expanding my knowledge of web application security. Moving forward, I am better equipped to conduct comprehensive assessments of web applications and identify potential vulnerabilities more effectively.

Date 27/04/2024

Summary of the day's activities

Today, I conducted vulnerability assessments on the target subdomain, https://www.trbinance.com/, using various security scanning tools, including Legion, Nikto, Wapiti, and Netsparker. These assessments aimed to identify potential security vulnerabilities within the web application, allowing for proactive mitigation to enhance its overall security posture.

Vulnerabilities discovered or explored:

Nikto Scan:

- Missing X-Frame-Options Header: Leaves the website vulnerable to clickjacking attacks.
- Missing Strict-Transport-Security Header: Exposes users to risks related to protocol downgrade attacks.
- Missing X-Content-Type-Options Header: Allows potential content-type sniffing attacks.
- Content-Encoding Header Vulnerability: Indicates vulnerability to the BREACH attack, which can extract sensitive information from encrypted web traffic.

Wapiti Scan:

- Potential SSRF (Server-Side Request Forgery) Vulnerability: Indicates susceptibility to allowing attackers to make unauthorized requests from the server, potentially leading to unauthorized data access or further exploitation.

Netsparker Scan:

- Session Cookie Not Marked as Secure: The session cookie is transmitted over HTTPS but not marked as secure, potentially allowing attackers to intercept it and hijack a victim's session.

Challenges faced and how they were overcome:

Vulnerability found by nikto Because connection problem ,so kali linux did not loading much time

Date 30/04/2024

Summary of the day's activities

Today, I conducted vulnerability assessments on two target subdomains: https://academy.binance.com/en and https://www.binance.com/en/price. I utilized various tools including Legion, Nikto, Wapiti, and Netsparker to identify potential security vulnerabilities in the web applications.

Vulnerabilities discovered or explored:

For Subdomain 03 (https://academy.binance.com/en):

- Nikto Scan:
  - Missing security headers such as X-Frame-Options, Strict-Transport-Security, and X-Content-Type-Options.
  - Content-Encoding header vulnerability indicating a potential susceptibility to the BREACH attack.

- Wapiti Scan:
  - Missing Content Security Policy (CSP).
  - Missing security headers (X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Strict-Transport-Security).
  - Potential SSRF (Server-Side Request Forgery) vulnerability.

- Netsparker Scan:
  - Detected a possible BREACH attack vulnerability due to HTTP-level compression and reflection of user-input in HTTP response bodies.

For Subdomain 04 (https://www.binance.com/en/price):

- Nikto Scan:
  - Insecure cookie attributes for cookies such as "theme" lacking secure and httponly flags.
  - Content-Encoding header vulnerability indicating potential susceptibility to the BREACH attack.

- Wapiti Scan:
    - Missing security headers (X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Strict-Transport-Security).
- Netsparker Scan:
    - Detected a possible BREACH attack vulnerability due to HTTP-level compression and reflection of user-input in HTTP response bodies.

Date 01/05/2024

Summary of the day's activities

Today, I conducted vulnerability assessments on two subdomains: https://coinmarketcap.com/ and https://pro.coinmarketcap.com/. Using tools such as Legion, Nikto, Netsparker, and Wapiti, I identified security vulnerabilities in the web applications.

Vulnerabilities discovered or explored:

For Subdomain 05 (https://coinmarketcap.com/):

- Nikto Scan:
  - Missing X-Content-Type-Options Header.
  - Content-Encoding header vulnerability indicating potential susceptibility to the BREACH attack.
- Netsparker Scan:
  - Weak ciphers enabled during secure communication (SSL), which could allow attackers to decrypt SSL traffic between the server and visitors.

For Subdomain 06 (https://pro.coinmarketcap.com/):

- Nikto Scan:
  - Missing X-Content-Type-Options Header.
  - Content-Encoding header vulnerability indicating potential susceptibility to the BREACH attack.
  - Uncommon Headers (x-traefik-route, x-envoy-decorator-operation, x-envoy-upstream-service-time), which may reveal sensitive server information.
- Wapiti Scan:
  - Missing Content Security Policy (CSP), exposing the website to various content injection attacks such as XSS.

Challenges faced and how they were overcome:

- The main challenge encountered today was the discovery of similar vulnerabilities across different scans for both subdomains. This indicates a consistent pattern of security weaknesses that need to be addressed promptly to enhance the overall security posture of the web applications.

Date 03/05/2024

Summary of the day's activities

Today's focus was on conducting vulnerability assessments for two subdomains: https://www.binance.us/ and https://c2c.binance.com/en. Utilizing tools such as Legion, Nikto, and Wapiti, I identified various security vulnerabilities present in these web applications.

Vulnerabilities discovered or explored:

For Subdomain 07 (https://www.binance.us/):

- Legion and Nikto Scan:
  - Missing X-Frame-Options Header, leaving the website vulnerable to clickjacking attacks.
  - Missing Strict-Transport-Security Header, exposing users to risks related to protocol downgrade attacks.
  - Missing X-Content-Type-Options Header, potentially allowing content rendering inconsistencies.
  - Content-Encoding header vulnerability indicating potential susceptibility to the BREACH attack.

For Subdomain 08 (https://c2c.binance.com/en):

- Legion and Nikto Scan:
  - Missing X-Content-Type-Options Header, potentially leading to XSS vulnerabilities or other types of attacks.
  - Content-Encoding header vulnerability indicating potential susceptibility to the BREACH attack.
  - Insecure Cookie Attributes, where cookies such as "theme" are created without the secure and httponly flags, making them vulnerable to interception and manipulation.

Wapiti Scan for Subdomain 07 and Subdomain 08:

  - Identified similar vulnerabilities as Legion and Nikto scans, including:
  - Missing X-Frame-Options Header.
  - Missing Strict-Transport-Security Header.
  - Missing X-Content-Type-Options Header.
  - Missing X-XSS-Protection Header.

Date 04/05/2024

Summary of the day's activities

Today, I conducted vulnerability assessments for two subdomains: https://support.binance.com/ and https://account.binance.com/. The assessments involved using various tools such as Legion, Nikto, and Wapiti to identify potential security vulnerabilities within these web applications.

Vulnerabilities discovered or explored:

For Subdomain 09 (https://support.binance.com/):

- Legion and Nikto Scan:
    - Missing X-Content-Type-Options Header, which could lead to content interpretation manipulation and XSS vulnerabilities.

For Subdomain 10 (https://account.binance.com/):

- Legion and Nikto Scan:
    - Missing X-Frame-Options Header, leaving the website vulnerable to clickjacking attacks.
    - Missing Strict-Transport-Security Header, which exposes users to risks related to protocol downgrade attacks.
    - Missing X-Content-Type-Options Header, potentially allowing content rendering inconsistencies.
    - Content-Encoding header vulnerability indicating potential susceptibility to the BREACH attack.

Wapiti Scan for Subdomain 09 and Subdomain 10:

- Identified similar vulnerabilities as Legion and Nikto scans, including:
- Missing X-Frame-Options Header.
- Missing Strict-Transport-Security Header.
- Missing X-Content-Type-Options Header.
- sMissing X-XSS-Protection Header.

Date 09/05/2024

Summary of the day's activities

Today, I focused on devising mitigation strategies for the vulnerabilities identified in the past few days' assessments. It involved understanding each vulnerability's impact and implementing appropriate measures to address them effectively.

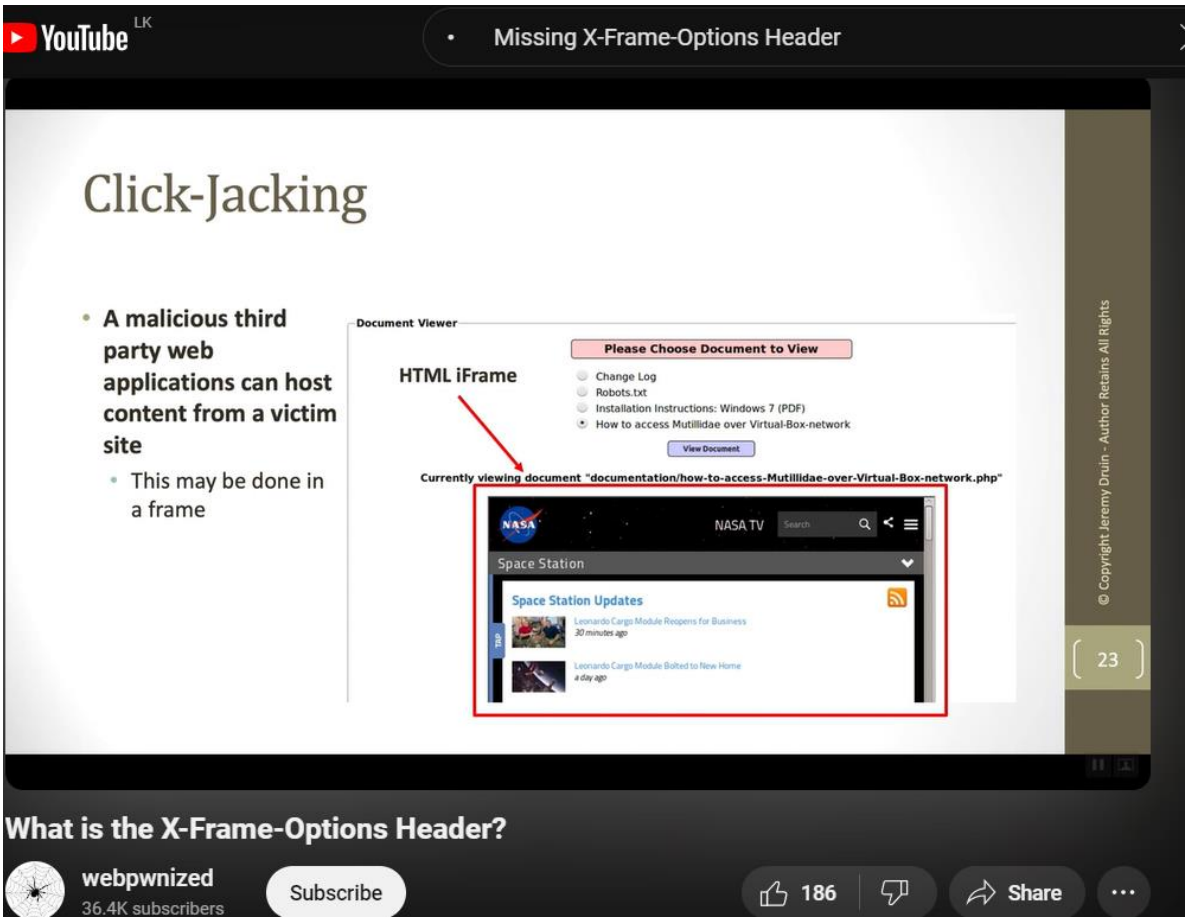
Vulnerabilities discovered or explored:

The vulnerabilities identified in previous assessments include:

- Missing X-Frame-Options Header
- Missing X-Content-Type-Options Header
- SSRF (Server-Side Request Forgery)
- Content-Encoding Header Vulnerability
- Missing Content Security Policy (CSP)
- Uncommon Headers (x-traefik-route, x-envoy-decorator-operation, x-envoy-upstream-service-time)
- Insecure Cookie Attributes
- Missing Security Headers (X-XSS-Protection, Strict-Transport-Security)

Challenges faced and how they were overcome:

- The main challenge faced was a lack of in-depth knowledge of some mitigation techniques for certain vulnerabilities. To overcome this, I researched each vulnerability extensively, consulted documentation, and sought advice from peers experienced in web security.



New tools, techniques, or concepts learned:

- Missing X-Frame-Options Header:
  - Add X-Frame-Options header with the value DENY or SAMEORIGIN to prevent clickjacking attacks.

- Missing X-Content-Type-Options Header:
  - Set the X-Content-Type-Options header to "nosniff" to prevent content-type sniffing attacks.

- SSRF (Server-Side Request Forgery):
  - Implement input validation and sanitization, whitelist allowed domains, and use DNS resolution to ensure safe resource points.

- Content-Encoding Header Vulnerability:
  - Disable compression algorithms like "deflate" and implement additional security controls like data encryption, input validation, and rate limiting.

- Missing Content Security Policy (CSP):
  - Implement a strict Content Security Policy (CSP) to whitelist trusted content sources and scripts.

- Uncommon Headers:
  - Regularly review uncommon headers, configure web servers and reverse proxies to strip unnecessary ones, and use appropriate security headers to mitigate common attack vectors.

- Insecure Cookie Attributes:
  - Set the "secure" attribute on cookies for secure HTTPS connections and "httponly" to prevent client-side script access.

- Missing Security Headers:
  - Implement additional security headers in web server configuration or application code, including X-XSS-Protection and Strict-Transport-Security.

Conclusion

As I conclude this journal documenting my daily experiences in the realm of web security assessments, I reflect on the myriad lessons learned and challenges overcome. Each day presented unique opportunities to delve deeper into the intricacies of web application vulnerabilities and explore effective mitigation strategies to bolster defenses against potential threats.

The analysis of security vulnerability reports and subdomains provided valuable insights into web application security weaknesses, enhancing understanding of cybersecurity principles and best practices.Despite encountering challenges along the way, such as the need for deeper knowledge in vulnerability mitigation strategies, I persevered, leveraging each obstacle as an opportunity for growth and learning. The journey reaffirmed the critical importance of continuous education and adaptation in the face of ever-evolving cyber threats. I carry with me a wealth of knowledge, insights, and experiences that will undoubtedly inform and shape my future endeavors in the field of cybersecurity.