



IE2062 [2023/JUL]- Web Security

Web Security Bug Bounty Assignment

Journal

Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

Contents

1. Introduction	4
2. Acknowledgement	5
3. Abstract.....	6
4. OWSAP Vulnerabilities.	7
4.1. Broken access Control.....	7
4.2. Cryptographic Failures	7
4.3. Injection.....	7
4.4. Insecure Design	7
4.5. Security Misconfigure	8
4.6. Vulnerable and Outdated Components	8
4.7. Identification and Authentication Failures	8
4.8. Software and Data integrity Failures.....	8
4.9. Security logging and monitoring failures.....	8
4.10. Server-side request forgery SSRF	8
5. Bug Bounty Programs	9
5.1. Bugcrowd	9
5.2. Hackerone.....	10
5.3. Microsoft BB program	10
5.4. Intigriti.com.....	11
6. Methodology and tools	14
6.1. Reconnaissance:	14
6.2. Scanning:	14
6.3. Exploitation:	14
6.4. Traffic interception and manipulation:.....	14
6.5. Automation:.....	14
6.6. Kali-Linux	15
6.7. Amass	15
6.8. Sublist3r	16
6.9. Knock.py	16
6.10. Dmitry.....	17
6.11. Burp suite.....	17
6.12. Nikto	18

6.13.	Nmap	18
6.14.	Recon-ng.....	19
6.15.	RapidScan.....	20
6.16.	Wapiti	20
6.17.	Exploit-DB.....	21
6.18.	Metasploit	21
6.19.	SQL Map	22
6.20.	XSSer.....	22
7.	Report Journal.....	23
7.1.	First Step	23
7.2.	Reports 1	25
7.3.	Reports 2	28
7.4.	Reports 3	29
7.5.	Reports 4	31
7.6.	Reports 5	34
7.7.	Reports 6	36
7.8.	Reports 7	38
7.9.	Report 8.....	40
7.10.	Report 9	42
7.11.	Report 10	44
7.12.	End.....	46
8.	Summary.....	47
9.	References	48

1. Introduction.

In our ever-evolving digital landscape, cybersecurity has become more than just a critical component; it's now a foundational pillar of the modern world. Bug bounty programs, within the vast realm of cybersecurity, have emerged as a crucial battleground where enthusiasts and organizations come together to safeguard our digital realm.

Bug bounty programs are of paramount importance because they provide a transformative defense against malicious threats and vulnerabilities. This ecosystem showcases the remarkable synergy between ethical hackers, organizations, and the broader cybersecurity community. It's a space where technology, ethics, and collaborative efforts converge to enhance digital security.

As the Assignment for the web security module in Year 2 Semester 2 cybersecurity Undergraduate, I had the opportunity to do the bug bounty programs and journal them in my own experience. This journal explores the process that I had gone through under a month, things I have learned and much more knowledge.

In these pages, we'll delve into a comprehensive exploration, revealing the profound processes, knowledge, and insights gained in this brief but impactful period, with a commitment to sharing this newfound expertise.

2. Acknowledgement.

I am profoundly grateful to the following individuals and organizations for their unwavering support, invaluable guidance, and significant contributions that have played a pivotal role in the creation of this cybersecurity journal on bug bounty programs.

First and foremost, I extend my heartfelt appreciation to the lecturer in charge of the web security module, Ms. Chethana Liyanapathirana, and the lab assistants for their unwavering guidance. Their expertise and mentorship were instrumental in sharpening my assignment to achieve its success.

Furthermore, I extend my sincere gratitude to the organizations and companies that have embraced bug bounty programs as an integral component of their security strategy. Their collaborative spirit and willingness to engage with the cybersecurity community are truly inspiring.

I would also like to express my deepest appreciation to the dedicated and skilled ethical hackers who tirelessly seek out vulnerabilities, thus contributing to the fortification of our digital landscape. Their commitment to the field of cybersecurity serves as the driving force behind this journal.

Last but not means least, I am immensely thankful to my family, colleagues, and friends for their unwavering support, endless patience, and unwavering understanding throughout this challenging journey.

It is important to emphasize that this journal would not have come to fruition without the collective efforts of these exceptional individuals and entities. I sincerely hope that my work will make a valuable contribution to the broader understanding of bug bounty programs in the field of cybersecurity.

3. Abstract

Bug bounty programs have become an integral part of modern cybersecurity, with numerous organizations inviting ethical hackers to identify vulnerabilities within their digital ecosystems. This bug bounty journal provides a comprehensive account of my experiences, challenges, and insights gained throughout my monthly journey as a bug bounty hunter.

From this you will learn about Top reported vulnerabilities and an idea on bug bounty programs. This journal comprises a compilation of reports, each detailing the journey of each bug bounty discovering responsibly disclosing vulnerabilities in a variety of digital assets and showcases the utilization of tools and techniques at the disposal of an undergraduate enthusiast, shedding light on the critical role these resources play in identifying and verifying vulnerabilities.

In addition to the technical aspects, the journal explores my personal growth and development as they navigate the complexities of bug bounty programs. It emphasizes the importance of ethical considerations and the principles of responsible disclosure in the pursuit of security enhancement.

The narrative unfolds through a series of experiences, each report providing valuable lessons learned, challenges overcome, and successes achieved. It illustrates my relentless commitment to improving security while contributing to the bug bounty community's collective knowledge base. The journal also reflects on the impact of bug bounty programs on the undergraduate's academic and career aspirations. I think it serves as an inspirational resource for students interested in cybersecurity, demonstrating the growth and knowledge that can be gained from participating in bug bounty programs.

4. OWASP Vulnerabilities.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

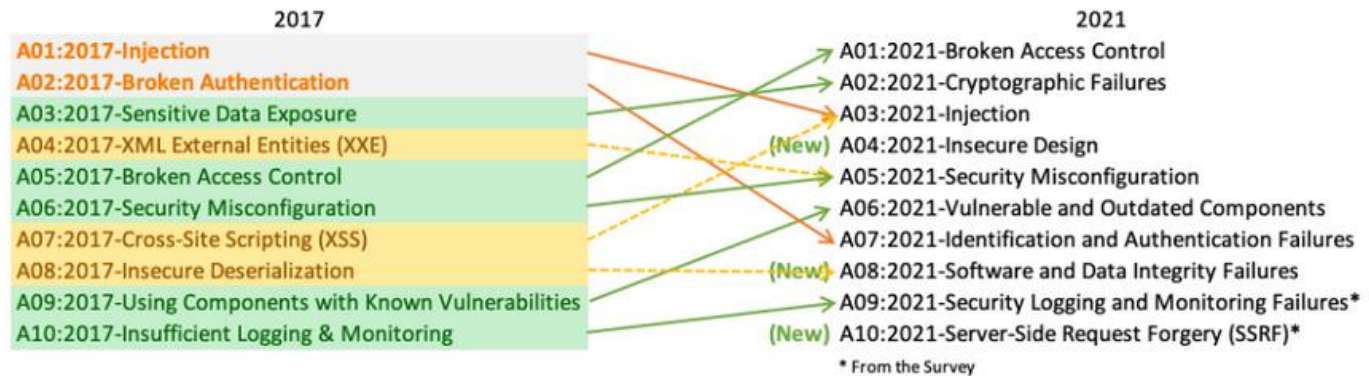


Figure 1 Top 10 Web Application Security Risks [1]

4.1. Broken access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

4.2. Cryptographic Failures

Cryptographic failures refer to weaknesses or vulnerabilities in the encryption and decryption processes, often leading to unauthorized access or data breaches due to improperly implemented encryption protocols.

4.3. Injection

Injection attacks occur when malicious code or data is inserted into an application, typically through user input, to exploit vulnerabilities and gain unauthorized access or manipulate data. Common types include SQL injection and Cross-Site Scripting (XSS).

4.4. Insecure Design

Insecure design indicates a fundamental flaw in the architecture or design of a system or application, making it susceptible to security breaches. This can include poor access control, improper data handling, and other design-related issues.

4.5.Security Misconfigure

Security misconfigurations involve improper or inadequate configuration settings within an application or system, leaving it open to security threats. Examples include overly permissive permissions, open ports, and default passwords.

4.6.Vulnerable and Outdated Components

This relates to using outdated or insecure third-party libraries, frameworks, or software components within an application. These components may have known vulnerabilities that attackers can exploit.

4.7.Identification and Authentication Failures

Identification and authentication failures occur when there are weaknesses in the processes of verifying and validating users, leading to unauthorized access. This can involve weak passwords, lack of multi-factor authentication, or other flaws in identity management.

4.8.Software and Data integrity Failures

Software and data integrity failures refer to situations where unauthorized changes or tampering of software or data occur, leading to data corruption or unauthorized modifications, potentially compromising system integrity.

4.9.Security logging and monitoring failures

Security logging and monitoring failures involve insufficient or ineffective logging and monitoring practices, making it challenging to detect and respond to security incidents in a timely manner.

4.10. Server-side request forgery SSRF

SSRF is a type of vulnerability that allows an attacker to manipulate a server into making unintended requests to internal resources or external services, potentially exposing sensitive information or launching attacks from the server's perspective.

Each of these issues can pose significant security risks and should be addressed proactively to protect systems and data from potential threats and vulnerabilities.

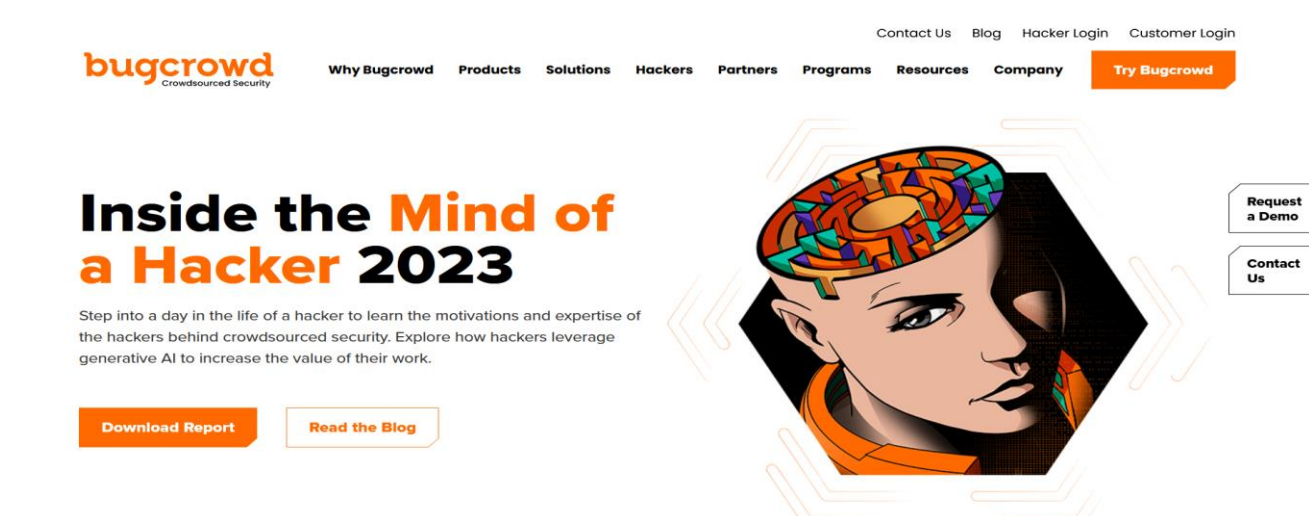
5. Bug Bounty Programs

A bug bounty program is a deal offered by many websites, organizations, and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

These are some platforms that provide the companies the bug bounty programs and hackers to participate.

5.1. Bugcrowd

Bugcrowd's platform-powered Managed Bug Bounty brings the right security researchers (the Crowd) into your workflows at the right time to find hidden flaws in your attack surface.



5.2.Hackerone

HackerOne is a company specializing in cybersecurity, specifically attack resistance management, which blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to find and close gaps in the digital attack surface.

The screenshot shows the HackerOne website with a dark theme. The main headline reads "One Platform. Preemptive security. Delivered." followed by the sub-headline "Outmatch cybercriminals with a legion of ethical hackers who work for you to continuously protect your attack surface." Below this are two buttons: "Explore the Platform" and "Request a Demo". The top navigation bar includes links for "PLATFORM", "SOLUTIONS", "PARTNERS", "COMPANY", "HACKERS", and "RESOURCES". A "Login" button and a "Contacted by a hacker?" button are also visible. On the right side, there is a dashboard preview showing a "Top Weaknesses" pie chart, a table of weaknesses, and a "Weakness trends" line chart. The table lists weaknesses like "Information Disclosure" (31), "Improper Access Control - Generic" (18), and "Insecure Direct Object Reference (IDOR)" (11). The line chart shows trends for Q1, Q2, Q3, and Q4.

5.3.Microsoft BB program

The screenshot shows the Microsoft Bug Bounty Program page. The header includes the Microsoft logo and navigation links for "MSRC", "Report an issue", "Customer guidance", "Engage", "Who we are", "Blogs", "Acknowledgments", "All Microsoft", and "Sign in". The main heading is "Microsoft Bug Bounty Program". Below this, there is a paragraph explaining Microsoft's commitment to security research and a link to "Click here to submit a security vulnerability". At the bottom, it mentions that the programs are subject to legal terms and conditions outlined "here" and the "Safe Harbor" policy.

Microsoft strongly believes close partnerships with the global security researcher community make customers more secure. Security researchers play an integral role in the ecosystem by discovering vulnerabilities missed in the software development process and sharing them under Coordinated Vulnerability Disclosure (CVD). Each year we partner together to better protect billions of customers worldwide.

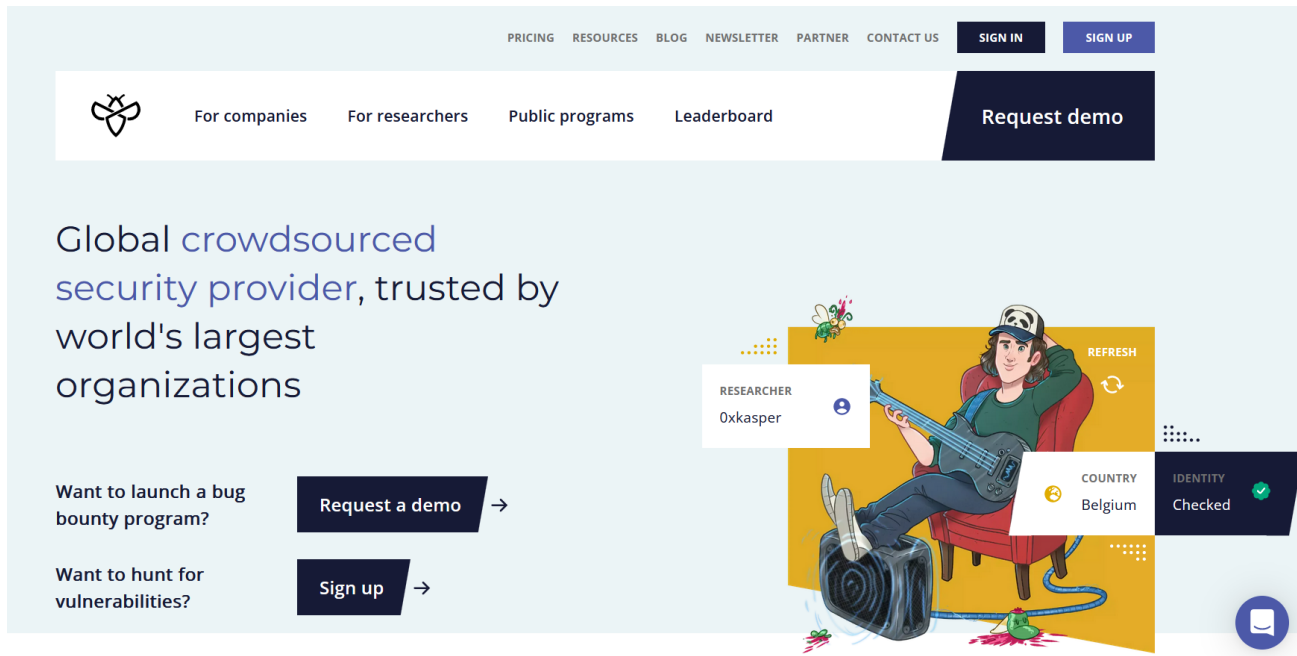
If you are a security researcher that has found a vulnerability in a Microsoft product, service, or device we want to hear from you. If your vulnerability report affects a product or service that is within scope of one of our bounty programs below, you may receive a bounty award according to the program descriptions. Even if it is not covered under an existing bounty program, we will publicly acknowledge your contributions when we fix the vulnerability. All vulnerability submissions are counted in our [Researcher Recognition Program](#) and [Researcher Leaderboard](#), even if they do not qualify for bounty award.

[Click here to submit a security vulnerability](#)

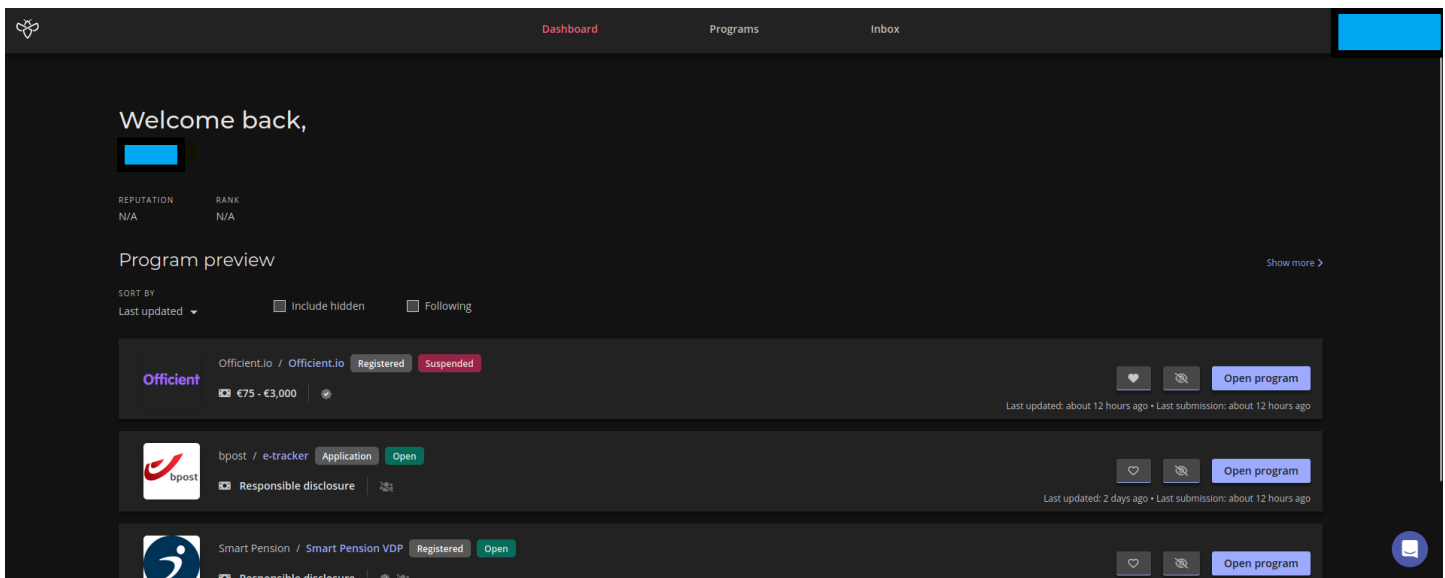
The Microsoft Bug Bounty Programs are subject to the legal terms and conditions outlined [here](#), and our bounty [Safe Harbor](#) policy.

5.4.Intigriti.com

I used this website for the whole experience.



This is the Dashboard



Most of the Bug bounty programs have rules of engagements like below.

Rules of engagement

@intigriti.me

Required

User agent

Not applicable

Automated tooling

max. 2 requests/sec

Request header

Not applicable

By participating in this program, you agree to:

- Respect the **Community Code of Conduct**
- Respect the **Terms and Conditions**
- Respect the scope of the program
- Not discuss or disclose vulnerability information without prior written consent (Including PoC's on YouTube and Vimeo)
- Please do *not* use automatic scanners -be creative and do it yourself! We cannot accept any submissions found by using automatic scanners. Scanners also won't improve your skills, and can cause a high server load (we'd like to put our time in thanking researchers rather than blocking their IP's 😊)

Safe harbour for researchers is applied

Show safe harbour ▾

View changes

They have Given us an email alias to use.

Using your intigriti.me e-mail address

Every researcher that signs up for the platform gets an intigriti.me e-mail alias. All e-mails sent to <yourusername>@intigriti.me will be forwarded to the e-mail address you signed up with. If a program requires the use of intigriti.me, it means that you will need to use your personal e-mail alias to sign up. You can read more about intigriti.me e-mail aliases [here](#).

And user agent and a header if needed to apply.

Add custom user agent:

1. Go to Proxy – Options tab
2. Scroll down to “Match and Replace”
3. Click on “Add”
4. Set rule to:

```
Type: Request Header  
Match: ^User-Agent.*$  
Replace: User-Agent: <Agent as defined in bug bounty brief>  
Comment: <a comment of your choice - not needed>
```

Make sure to tick the “Regex match” box

5. Search for your rule in the list and click on “Enabled”

Add custom header:

1. Go to Proxy – Options tab
2. Scroll down to “Match and Replace”
3. Click on “Add”
4. Set rule to:

```
Type: Request Header  
Match: (leave empty)  
Replace: <New header as defined in bug bounty brief>  
Comment: <a comment of your choice - not needed>
```

5. Search for your rule in the list and click on “Enabled”

6. Methodology and tools

6.1.Reconnaissance:

Reconnaissance also known as ‘Information Gathering’ and ‘Foot printing’, is the first step and action that hackers do when approaching a target to search for weaknesses and use the advantage of vulnerabilities found in Exploiting the target system. Recon is a process of Gathering as much information as possible about the target, for identifying various techniques to intrude into the target system.

6.2.Scanning:

In bug bounty programs, scanning refers to the process of systematically scanning target systems or applications for known vulnerabilities or misconfigurations. Security researchers use automated scanning tools to identify potential weaknesses, such as open ports, exposed services, or common vulnerabilities like SQL injection, which can help them discover low-hanging fruit.

6.3.Exploitation:

Exploitation is the phase where security researchers attempt to leverage the vulnerabilities, they've discovered to gain unauthorized access or control over a target system or application. This may involve crafting and executing attacks to demonstrate the impact of the vulnerabilities, potentially leading to privilege escalation, data breaches, or system compromise.

6.4. Traffic interception and manipulation:

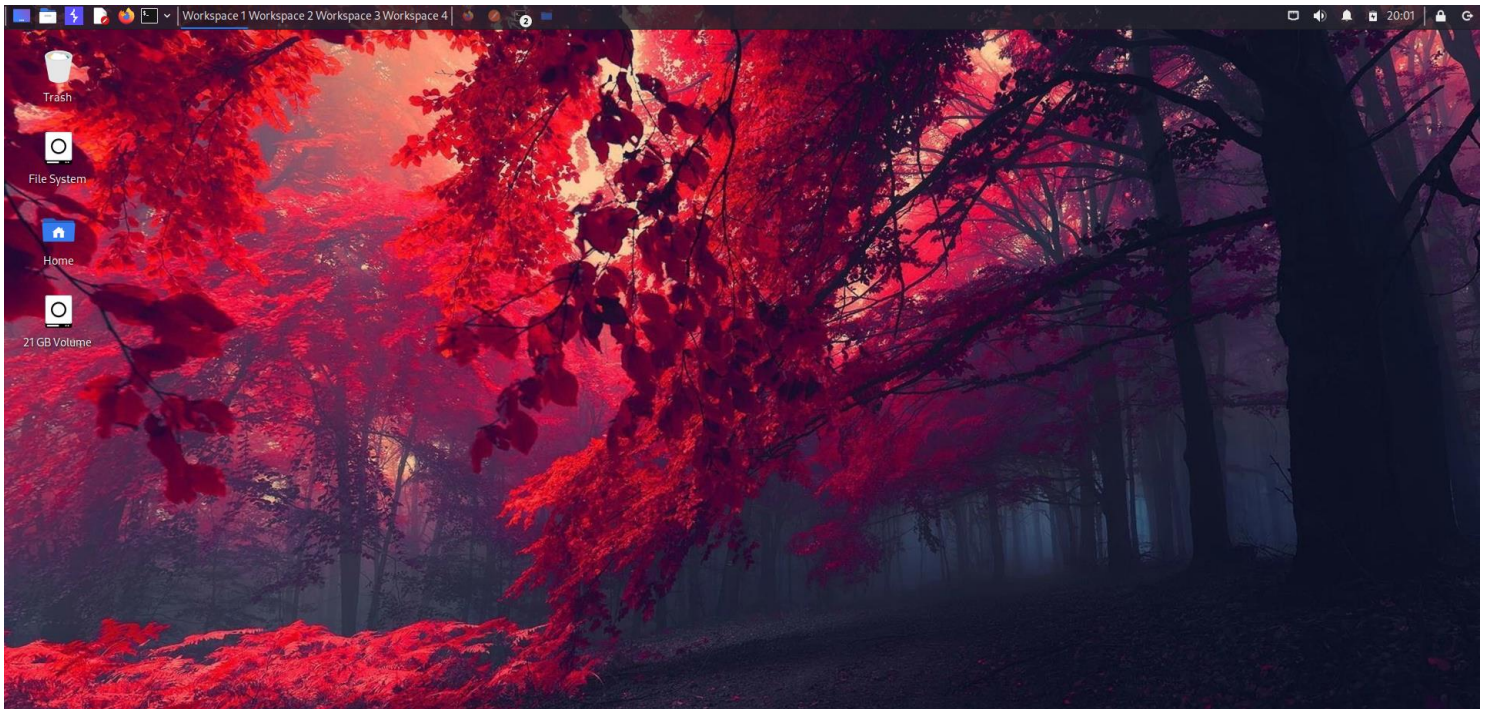
This technique involves intercepting and manipulating network traffic between the user and the target system to uncover vulnerabilities, such as Man-in-the-Middle (MitM) attacks. By eavesdropping on communications, attackers can potentially steal sensitive information, alter data in transit, or inject malicious content into user sessions.

6.5.Automation:

Automation plays a crucial role in bug bounty programs, as it enables security researchers to scale their efforts efficiently. Researchers often create custom scripts, use specialized tools like Burp Suite extensions, or leverage frameworks like Metasploit to automate repetitive tasks, streamline the discovery and exploitation of vulnerabilities, and increase their productivity in finding and reporting security issues. These automated processes help uncover vulnerabilities faster and enhance the effectiveness of bug hunting efforts.

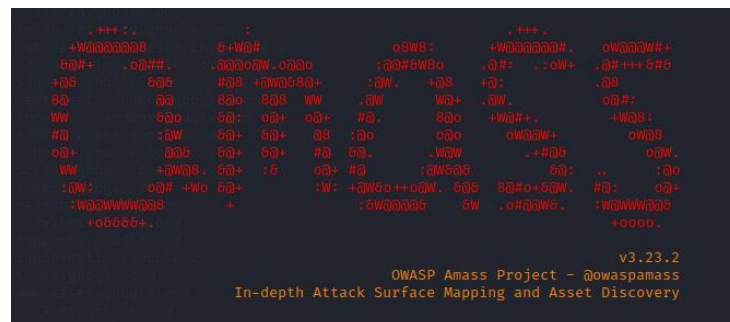
6.6.Kali-Linux

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.



6.7.Amass

This package contains a tool to help information security professionals perform network mapping of attack surfaces and perform external asset discovery using open-source information gathering and active reconnaissance techniques.



6.8.Sublist3r

Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting.



6.9.Knock.py

Knock is a tool written in Python and is designed to enumerate subdomains in a target domain through a wordlist.

```
knockpy
usage: knockpy [-h] [-v] [--no-local] [--no-remote] [--no-scan] [--no-http] [--no-http-code CODE [CODE ...]]
               [--no-ip NO_IP [NO_IP ...]] [--dns DNS] [--user-agent USERAGENT] [--plugin-test] [-w WORDLIST]
               [-o FOLDER] [-t SEC] [-th NUM] [--silent [{False,json,json-pretty,csv}]]
               [domain]

* SCAN
full scan:      knockpy domain.com
quick scan:     knockpy domain.com --no-local
faster scan:    knockpy domain.com --no-local --no-http
ignore code:    knockpy domain.com --no-http-code 404 500 530
silent mode:    knockpy domain.com --silent

* SUBDOMAINS
show recon:     knockpy domain.com --no-local --no-scan

* REPORT
show report:    knockpy --report knockpy_report/domain.com_yyyy_mm_dd_hh_mm_ss.json
plot report:    knockpy --plot knockpy_report/domain.com_yyyy_mm_dd_hh_mm_ss.json
csv report:     knockpy --csv knockpy_report/domain.com_yyyy_mm_dd_hh_mm_ss.json
```


6.10. Dmitry

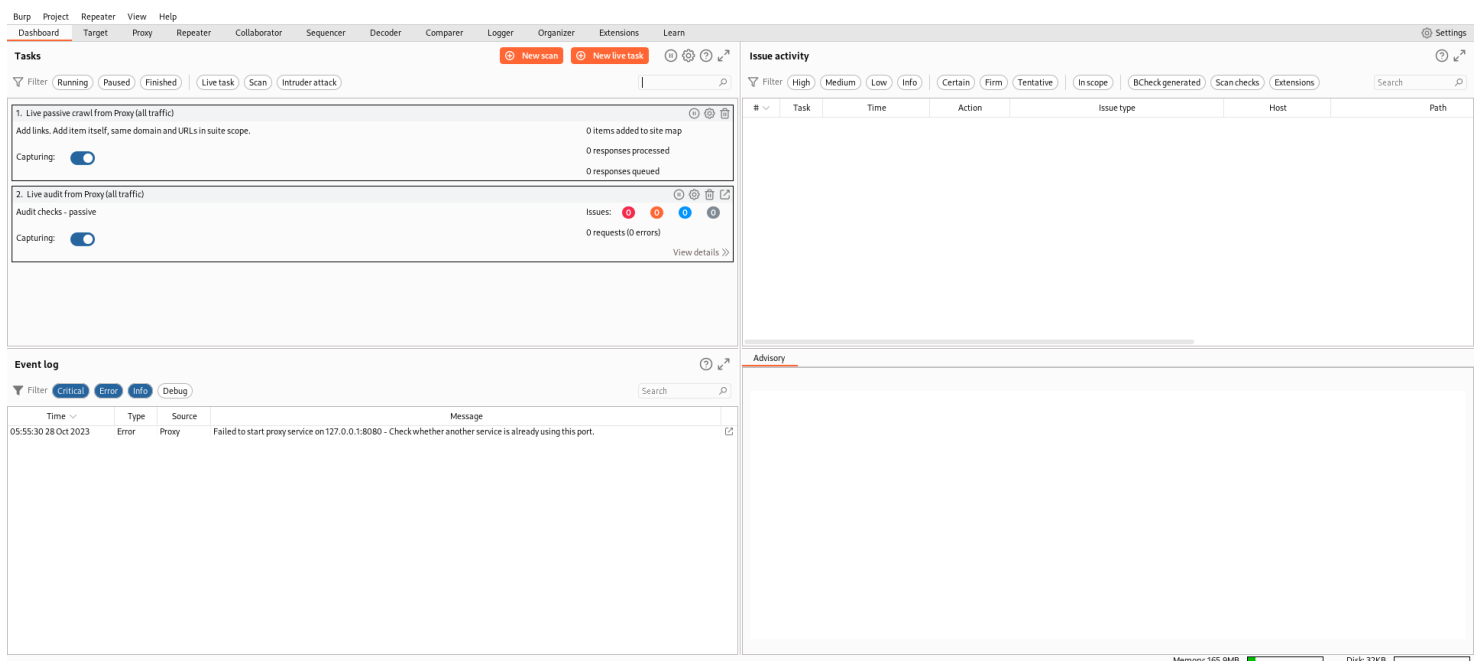
DMitry is a UNIX/(GNU)Linux command line application written in C. DMitry can find possible subdomains, email addresses, uptime information, perform tcp port scan, whois lookups, and more.

```
$ dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
-o      Save output to %host.txt or to file specified by -o file
-i      Perform a whois lookup on the IP address of a host
-w      Perform a whois lookup on the domain name of a host
-n      Retrieve Netcraft.com information on a host
-s      Perform a search for possible subdomains
-e      Perform a search for possible email addresses
-p      Perform a TCP port scan on a host
* -f    Perform a TCP port scan on a host showing output reporting filtered ports
* -b    Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

6.11. Burp suite

Burp Suite Professional is the web security tester's toolkit of choice. Use it to automate repetitive testing tasks - then dig deeper with its expert-designed manual and semi-automated security testing tools. Burp Suite Professional can help you to test for OWASP Top 10 vulnerabilities - as well as the very latest hacking techniques.



6.12. Nikto

Nikto is a pluggable web server and CGI scanner written in Perl, using rfp's LibWhisker to perform fast security or informational checks.

```
$ nikto
- Nikto v2.5.0

+ ERROR: No host (-host) specified

Options:
  -ask+          Whether to ask about submitting updates
                  yes   Ask about each (default)
                  no    Don't ask, don't send
                  auto   Don't ask, just send
  -check6+       Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -Cgidirs+      Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+       Use this config file
  -Display+      Turn on/off display outputs:
                  1     Show redirects
                  2     Show cookies received
                  3     Show all 200/OK responses
                  4     Show URLs which require authentication
                  D     Debug output
                  E     Display all HTTP errors
                  P     Print progress to STDOUT
                  S     Scrub output of IPs and hostnames
                  V     Verbose output
```

6.13. Nmap

Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

```
$ nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
```

6.14. Recon-ng

Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open-source web-based reconnaissance can be conducted quickly and thoroughly.

[illegible]

6.15. RapidScan

RapidScan is a free and open-source tool available on GitHub which is based upon Open Source Intelligence (OSINT), the easiest and useful tool for reconnaissance. The RapidScan interface is very similar to Metasploit 1 and Metasploit 2, which provides a command-line interface that you can run on Kali Linux.

```
(user@user)-[~/Documents/Programs/rapidscan-master]
$ python rapidscan.py

  _____
 /  _  _  \  /  _  \  /  _  \
(  (  (  )  (  (  )  (  (  )
 \  _  _  \  /  _  \  /  _  \
  _____

(The Multi-Tool Web Vulnerability Scanner)

Check out our new software, NetBot for simulating DDoS attacks - https://github.com/skavngr/netbot

Information:
./rapidscan.py example.com: Scans the domain example.com.
./rapidscan.py example.com --skip dmitry --skip theHarvester: Skip the 'dmitry' and 'theHarvester' tests.
./rapidscan.py example.com --nospinner: Disable the idle loader/spinner.
./rapidscan.py --update : Updates the scanner to the latest version.
./rapidscan.py --help : Displays this help context.

Interactive:
Ctrl+C: Skips current test.
Ctrl+Z: Quits RapidScan.

Legends:
[●]: Scan process may take longer times (not predictable).
[●]: Scan process may take less than 10 minutes.
[●]: Scan process may take less than a minute or two.

Vulnerability Information:
critical : Requires immediate attention as it may lead to compromise or service unavailability.
high : May not lead to an immediate compromise, but there are considerable chances for probability.
medium : Attacker may correlate multiple vulnerabilities of this type to launch a sophisticated attack.
low : Not a serious issue, but it is recommended to tend to the finding.
info : Not classified as a vulnerability, simply an useful informational alert to be considered.
```


6.16. Wapiti

Wapiti allows you to audit the security of your web applications. It performs “black-box” scans, i.e. it does not study the source code of the application but will scan the web pages of the deployed web applications, looking for scripts and forms where it can inject data. Once it gets this list, Wapiti acts like a fuzzer, injecting payloads to see if a script is vulnerable.

```
Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] You are lucky! Full moon tonight.
usage: wapiti [-h] [-u URL] [--scope {page,folder,domain,url,punk}] [-m MODULES_LIST]
              [--skip-crawl] [--resume-crawl] [--flush-attacks] [--flush-session]
              [--max-files-per-dir MAX] [--max-scan-time SECONDS] [--max-attack-time SECONDS]
              [--external-endpoint EXTERNAL_ENDPOINT_URL] [--internal-endpoint INTERNAL_ENDPOINT_URL]
wapiti: error: one of the arguments -u/--url --list-modules --update is required
```

6.17. Exploit-DB

The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.



☐ Verified
 ☐ Has App

Filters

Reset All

Show

15

Search:

Date	D	A	V	Title	Type	Platform	Author
2023-10-09				Splunk 9.0.5 - admin account take over	WebApps	Multiple	Redway Security
2023-10-09				OpenPLC WebServer 3 - Denial of Service	DoS	Multiple	Kai Feng
2023-10-09				Shuttle-Booking-Software v1.0 - Multiple-SQLi	WebApps	PHP	nu11secu1ty
2023-10-09				Limo Booking Software v1.0 - CORS	WebApps	PHP	nu11secu1ty
2023-10-09				Webedition CMS v2.9.8.8 - Blind SSRF	WebApps	PHP	Mirabbas Ağalarov
2023-10-09				Atcom 2.7.x.x - Authenticated Command Injection	Remote	Hardware	Mohammed Adel
2023-10-09				BoidCMS v2.0.0 - authenticated file upload vulnerability	WebApps	PHP	1337kid
2023-10-09				Cacti 1.2.24 - Authenticated command injection when using SNMP options	WebApps	PHP	Antonio Francesco Sardella

6.18. Metasploit

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

```

** Metasploit Framework Initial Setup Complete **

Metasploit tip: Use help <command> to learn more about any command


      / \
     ((   ))
    (( _ ,,_ _ ))
     (_ ) 0 0 (_ )
        |  |
       o_o | M S F
          | | | | | |
         ||| ww|||
         ||| |||

                                     *

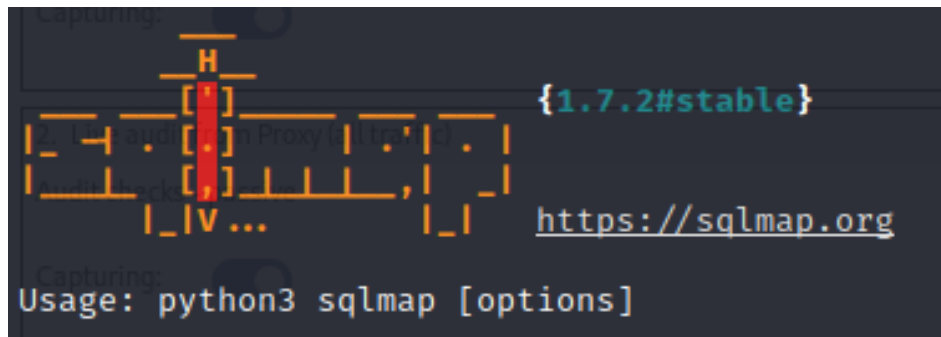
= [ metasploit v6.3.41-dev- ]
+ -- --=[ 2370 exploits - 1229 auxiliary - 414 post ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
msf6 > 
```

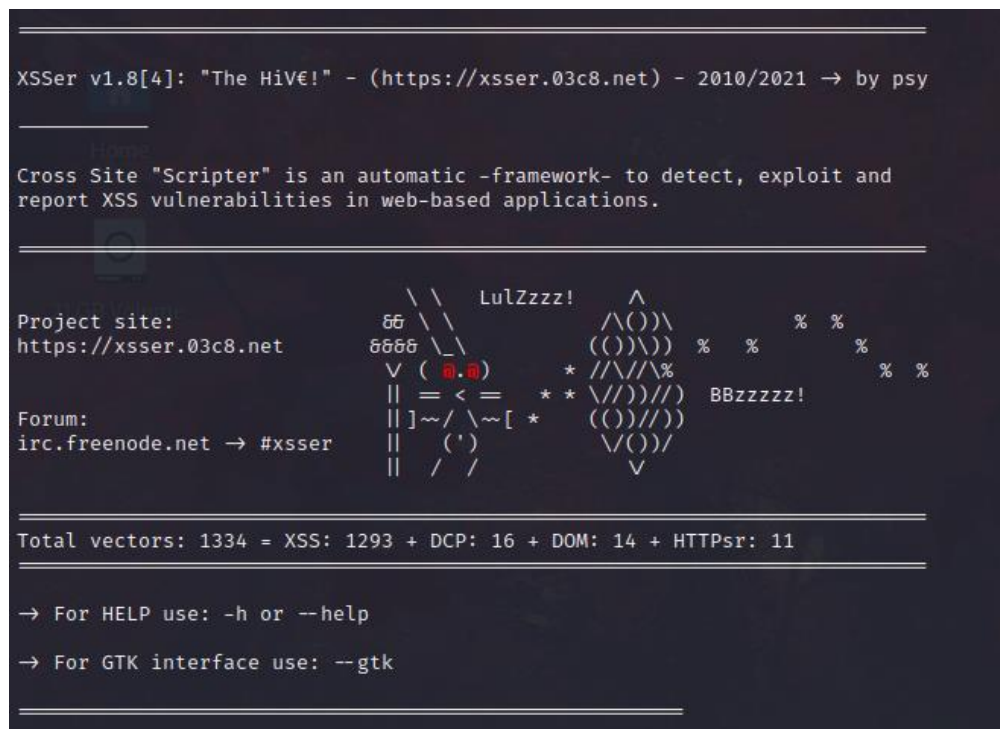
6.19. SQL Map

SQL map is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester, and a broad range of switches including database fingerprinting, over data fetching from the database, accessing the underlying file system, and executing commands on the operating system via out-of-band connections.



6.20. XSSer.

Cross Site "Scripter" (aka XSSer) is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based applications.



7. Report Journal

7.1.First Step

<ul style="list-style-type: none">• I journaled my process of the bug bounty	Date : 2023/10/9
Summary of the day's activities <ul style="list-style-type: none">• Researching about bug bounty programs, software, and methodologies.• Register for the bug bounty programs.• Getting the basic idea of the programs.	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• Not enough skill sets for do a bug bounty.	
Challenges faced and how they were overcome. <ul style="list-style-type: none">• Lack of knowledge in the field – Try to understand and learn.	
New tools, techniques, or concepts learned. <ul style="list-style-type: none">• Learned about already installed kali Linux tools	

	01 - Information Gathering
	02 - Vulnerability Analysis
	03 - Web Application Analysis
	04 - Database Assessment
	05 - Password Attacks
	06 - Wireless Attacks
	07 - Reverse Engineering
	08 - Exploitation Tools
	09 - Sniffing & Spoofing
	10 - Post Exploitation
	11 - Forensics
	12 - Reporting Tools
	13 - Social Engineering Tools

- Most of them are explained above methodologies and tools section.
- Found some new tools like rapidscan.

Reflections and takeaways

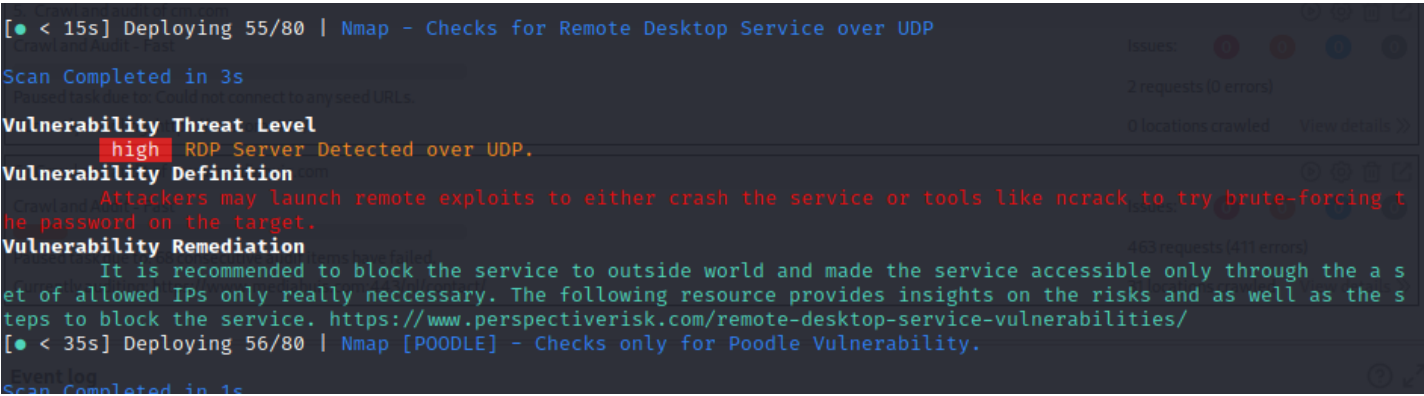
Starting of the bug bounty process.

References

Owsap.org [1]

<https://www.kali.org/>

7.2.Reports 1

Bug bounty Details: CM.com – Web testing – login.cm.com	Date: 2023/10/10
Summary of the day's activities <ul style="list-style-type: none">• Staring the bug bounty by reading and researching about web testing• Journaling• Finding some tools for gathering information.	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• XSS Protection is not present.• Subdomains discovered with Dmitry.• Found subdomains with fierce.• Secure Client initialized renegotiation is acquired.• SNMP Service Detected• RDP server Detected over UDP 	

Challenges faced and how they were overcome.

- Finding tools to do – used alternativeto.com to find alternatives to the existing one.
- Install some tools – view some YouTube tutorials.
- Some tools do not work on the target URL – use alternatives.
- Troubleshooting the tools – Reinstall the tool or Searched Website

New tools, techniques, or concepts learned.

- Dmitry

```
(user@user)-[~]ediahuis.com
$ sudo dmitry login.cm.com
[sudo] password for user:
DeePMagic Information Gathering Tool
"There be some deep magic going on"
Currently auditing: https://www.mediahuis.com/en/43/nl/contact/







HostIP:104.16.121.74
HostName:login.cm.com

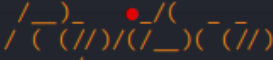
Event log
Gathered Inet-whois information for 104.16.121.74

Filter  Search  Watch  Info  Debug

inetnum: 103.253.144.0 - 104.37.31.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
```

- Rapid scan

Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec



(The Multi-Tool Web Vulnerability Scanner)

Check out our new software, **NetBot** for simulating DDoS attacks - <https://github.com/skavngr/netbot>

Reflections and takeaways

- Got more experience with the bug bounty.
- Learned about some tools.

References

<https://www.kali.org/tools/dmitry/>

<https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers-Cheat-Sheet.html>

7.3.Reports 2

Bug bounty Details:	Date: 2023/10/18																																																
Officient.io – Web testing – product.analytics.officient.io																																																	
Summary of the day's activities <ul style="list-style-type: none">Started to search for vulnerabilities.JournalingFamiliarize with some tools that are being used.																																																	
Vulnerabilities discovered or explored. <p>Found these but they are informational severity level.</p> <ul style="list-style-type: none">Browser cross- site scripting filter disabled.Cross-origin resource sharingCross-origin resource sharing: arbitrary trusted certificatecross-site scripting filter disabled.Cacheable HTTPS responsecross-site scripting filter disabled. <p>Founded by Burp suite</p> <table><thead><tr><th>Action</th><th>Issue type</th><th>Host</th><th>Path</th><th>Insertion point</th><th>Severity</th></tr></thead><tbody><tr><td>Issue found</td><td>🔍 Browser cross-site scripting filter disabled</td><td>https://product-analytics....</td><td>/favicon.ico</td><td></td><td>Information</td></tr><tr><td>Issue found</td><td>🔍 Cross-origin resource sharing</td><td>https://product-analytics....</td><td>/</td><td></td><td>Information</td></tr><tr><td>Issue found</td><td>🔍 Cross-origin resource sharing: arbitrary origin trusted</td><td>https://product-analytics....</td><td>/</td><td></td><td>Information</td></tr><tr><td>Issue found</td><td>🔍 TLS certificate</td><td>https://product-analytics....</td><td>/</td><td></td><td>Information</td></tr><tr><td>Issue found</td><td>🔍 Browser cross-site scripting filter disabled</td><td>https://product-analytics....</td><td>/robots.txt</td><td></td><td>Information</td></tr><tr><td>Issue found</td><td>🔍 Cacheable HTTPS response</td><td>https://product-analytics....</td><td>/</td><td></td><td>Information</td></tr><tr><td>Issue found</td><td>🔍 Browser cross-site scripting filter disabled</td><td>https://product-analytics....</td><td>/</td><td></td><td>Information</td></tr></tbody></table>		Action	Issue type	Host	Path	Insertion point	Severity	Issue found	🔍 Browser cross-site scripting filter disabled	https://product-analytics....	/favicon.ico		Information	Issue found	🔍 Cross-origin resource sharing	https://product-analytics....	/		Information	Issue found	🔍 Cross-origin resource sharing: arbitrary origin trusted	https://product-analytics....	/		Information	Issue found	🔍 TLS certificate	https://product-analytics....	/		Information	Issue found	🔍 Browser cross-site scripting filter disabled	https://product-analytics....	/robots.txt		Information	Issue found	🔍 Cacheable HTTPS response	https://product-analytics....	/		Information	Issue found	🔍 Browser cross-site scripting filter disabled	https://product-analytics....	/		Information
Action	Issue type	Host	Path	Insertion point	Severity																																												
Issue found	🔍 Browser cross-site scripting filter disabled	https://product-analytics....	/favicon.ico		Information																																												
Issue found	🔍 Cross-origin resource sharing	https://product-analytics....	/		Information																																												
Issue found	🔍 Cross-origin resource sharing: arbitrary origin trusted	https://product-analytics....	/		Information																																												
Issue found	🔍 TLS certificate	https://product-analytics....	/		Information																																												
Issue found	🔍 Browser cross-site scripting filter disabled	https://product-analytics....	/robots.txt		Information																																												
Issue found	🔍 Cacheable HTTPS response	https://product-analytics....	/		Information																																												
Issue found	🔍 Browser cross-site scripting filter disabled	https://product-analytics....	/		Information																																												
Challenges faced and how they were overcome. <ul style="list-style-type: none">Finding new tools, and techniques																																																	
New tools, techniques, or concepts learned. <ul style="list-style-type: none">Burp suite professional																																																	
Reflections and takeaways <ul style="list-style-type: none">Most of the bugs are out of scope or they are not that severe.																																																	
References https://github.com/mmgordon82/BurpSuiteInstaller																																																	

7.4.Reports 3

Bug bounty Details: Ada Health – Web testing – care-navigation-fe.int.eu.enterprise.ada.com	Date: 2023/10/19
Summary of the day's activities <ul style="list-style-type: none">• Research about the target• Gather information.• Vulnerability scanning• Exploitation the target• Documenting the Founding• Continuous learning	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• SNMP Service Detected: An SNMP service has been identified, which could potentially pose a security risk due to its exposure and could lead to unauthorized access or information disclosure.• X-XSS Protection is not Present: The absence of XSS protection in a web application or website means that it may be vulnerable to cross-site scripting attacks, potentially allowing attackers to inject malicious scripts into web pages.• Found Subdomains with Amass: Subdomains have been discovered using the Amass tool, which may indicate a potential attack surface expansion or information exposure risk.• RDP Server Detected over UDP: The presence of an RDP server running over the UDP protocol can pose security risks and may result in vulnerabilities in remote desktop access. <div><p>Vulnerability Threat Level High RDP Server Detected over UDP.</p><p>Vulnerability Definition Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password on the target.</p><p>Vulnerability Remediation It is recommended to block the service to outside world and made the service accessible only through the a set of allowed IPs only really necessary. The following resource provides insights on the risks and as well as the st to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/</p></div>	
Challenges faced and how they were overcome. <ul style="list-style-type: none">• It can be challenging to gather complete information about the target, including its technology stack and architecture. - Overcoming thorough online research and using specialized tools for reconnaissance, such as WHOIS, helped in obtaining a detailed overview of the target.• Documenting the discovered vulnerabilities in a clear and comprehensive manner is crucial but can be a time-consuming task. – Overcoming detailed documentation templates were used, ensuring that each vulnerability was well-documented, including steps to reproduce, potential impact, and mitigation recommendations.	

New tools, techniques, or concepts learned. <ul style="list-style-type: none">• Learned about RDP server operating over UDP.
Reflections and takeaways <ul style="list-style-type: none">• Detecting vulnerabilities like the absence of XSS protection and misconfigured RDP servers highlighted the need for organizations to prioritize security in their applications and systems.
References https://purerds.org/remote-desktop-protocol/udp-support-over-rdp/ https://winaero.com/microsoft-has-confirmed-the-bug-with-udp-in-rdp-on-windows-11-22h2/

7.5.Reports 4

Bug bounty Details: Ubisoft – Web Testing - www.Ubisoft.com	Date: 2023/10/23
Summary of the day's activities <ul style="list-style-type: none">• Started the bug bounty by gathering information about the web testing.• Vulnerability scanning• Exploitation the target• Documenting the Founding• Continuous learning	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• Web Cache Poisoning: A vulnerability that can lead to the contamination of cached web content, allowing attackers to serve malicious content to users.• X-XSS Protection is not Present: The absence of an XSS protection header in a web application, potentially making it susceptible to cross-site scripting attacks.• Subdomains Discovered with Dmitry: Discovery of subdomains using the Dmitry tool, potentially expanding the attack surface, and exposing sensitive information.• Secure Client Initiated Renegotiation Supported: The presence of secure client-initiated renegotiation in a communication protocol, which can have security implications.• Some Vulnerable Headers Exposed: Certain headers are exposed, which could potentially be exploited or provide information for further attacks.• WHOIS Information Publicly Available: Publicly accessible WHOIS information, potentially exposing sensitive domain registration details.	

! Web cache poisoning	https://www.ubisoft.com	/en-us/game/valiant-hearts	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/game/assassins-creed/discovery-tour	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/parks-experiences/escape-gam...	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/parks-experiences	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/werewolves-within-mo...	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/splinter-cell-series	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/rabbids-invasion-missi...	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/captain-laserhawk	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/assassins-creed-movie	Medium
! Backup file	https://www.ubisoft.com	/en-us/	Information
! Backup file	https://www.ubisoft.com	/en-us/careers/search.aspx/	Information
! Web cache poisoning	https://www.ubisoft.com	/en-us/	Medium
! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/books-music	Medium
! Email addresses disclosed	https://www.ubisoft.com	/en-us/studio/laforge	Information
! Email addresses disclosed	https://www.ubisoft.com	/en-us/game/assassins-creed/discovery-tour	Information
! Email addresses disclosed	https://www.ubisoft.com	/en-us/entertainment/film-tv	Information
! Email addresses disclosed	https://www.ubisoft.com	/en-us/entertainment/education-events/play-to-learn	Information
! Cross-domain script include	https://www.ubisoft.com	/en-us/company/careers/search	Information
! Cross-domain script include	https://www.ubisoft.com	/en-us/company/careers	Information
! Cacheable HTTPS response	https://www.ubisoft.com	/en-us	Information
! Frameable response (potential Clickjacking)	https://www.ubisoft.com	/en-us	Information
! Strict transport security not enforced	https://www.ubisoft.com	/	Low
! TLS certificate	https://www.ubisoft.com	/	Information
! Robots.txt file	https://www.ubisoft.com	/robots.txt	Information

Challenges faced and how they were overcome.

- Documenting the discovered vulnerabilities in a clear and comprehensive manner is crucial but can be a time-consuming task. – Overcoming detailed documentation templates were used, ensuring that each vulnerability was well-documented, including steps to reproduce, potential impact, and mitigation recommendations.

New tools, techniques, or concepts learned.

- Web Cache Poisoning
- Holistic Approach

Reflections and takeaways

• Holistic Approach:

- A holistic approach to bug bounty hunting involves not only identifying vulnerabilities but also understanding the potential impact and implications of each finding.

• Security Best Practices:

- The day's activities underscore the importance of implementing security best practices, such as proper header configurations and secure subdomain management.

• Data Privacy:

- The exposure of publicly available WHOIS information highlights the importance of data privacy and the need to protect sensitive domain registration details.

References

<https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cyber%20risk%20measurement%20and%20the%20holistic%20cybersecurity%20approach/Cyber-risk-measurement-and-the-holistic-cybersecurity-approach-vf.pdf>

7.6.Reports 5

Bug bounty Details: Axel Springer SE – Web testing - www.travelbook.de	Date: 2023/10/24
Summary of the day's activities: <ul style="list-style-type: none">• Perform the bug bounty.• Research about the target• Gather information.• Vulnerability scanning• Exploitation the target• Documenting the Founding• Continuous learning	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• Some Vulnerability Headers Exposed:<ul style="list-style-type: none">◦ The exposure of vulnerable headers indicates potential security weaknesses within the HTTP response headers. These headers might be misconfigured or contain security-related issues.◦• Does Not Have an IPv6 Address:<ul style="list-style-type: none">◦ The absence of an IPv6 address may limit the website's compatibility with the next-generation Internet Protocol, IPv6, which is becoming increasingly important for network infrastructure.◦• Secure Client-Initiated Renegotiation Supported:<ul style="list-style-type: none">◦ The support for Secure Client-Initiated Renegotiation may introduce security risks if not configured correctly. This can potentially facilitate man-in-the-middle attacks.◦• X-XSS Protection is Not Present:<ul style="list-style-type: none">◦ The absence of the "X-XSS-Protection" header suggests a vulnerability to cross-site scripting (XSS) attacks. Malicious scripts could be injected into web pages, compromising user security and data.◦• Freak Vulnerability<ul style="list-style-type: none">◦ The "FREAK" vulnerability, which stands for "Factoring attack on RSA-EXPORT Keys," is a security flaw that primarily affects the security of encrypted communications on the internet. It was discovered in 2015.◦ FREAK enabled a man-in-the-middle (MITM) attacker to intercept and potentially decrypt supposedly secure communications between a client (e.g., a web browser) and a server. This could expose sensitive information, such as login credentials, credit card numbers, and more.◦	

```
Vulnerability Threat Level
[high] FREAK Vulnerability Detected.
Vulnerability Definition
With this vulnerability the attacker will be able to perform a MITM attack and thus compromising the confidentiality factor.
Vulnerability Remediation
Upgrading OpenSSL to latest version will mitigate this issue. Versions prior to 1.1.0 is prone to this vulnerability. More information can be found in this resource.
vulnerability-cve-2016-2183/
```

- **Subdomain Discovery with Dmitry and Fierce:**
 - Subdomains were discovered using the tools Dmitry and Fierce, potentially expanding the attack surface

Challenges faced and how they were overcome.

- Finding about Freak Vulnerability

New tools, techniques, or concepts learned.

- None.

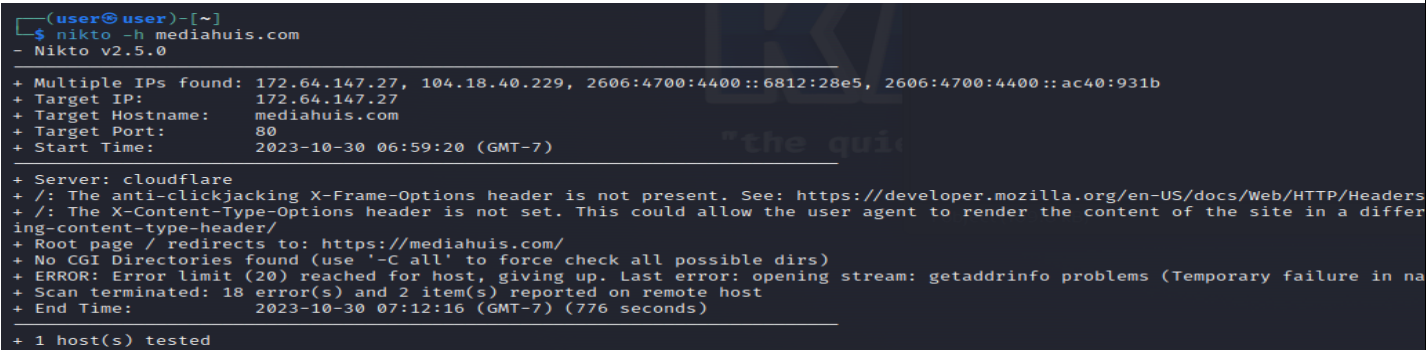
Reflections and takeaways

- FREAK serves as a reminder of the long-lasting security consequences of historical decisions. It underscores the importance of regularly reviewing and updating security protocols and the need to phase out legacy encryption mechanisms.

References

<https://resources.infosecinstitute.com/topics/vulnerabilities/the-freak-vulnerability-from-discovery-to-mitigation/>
<https://www.techtarget.com/searchsecurity/tip/Understanding-and-mitigating-a-FREAK-vulnerability-attack>

7.7.Reports 6

Bug bounty Details: Mediauhis.com – Web Testing – www.mediahuis.com	Date: 2023/10/25
Summary of the day's activities <ul style="list-style-type: none">• Research about the target• Gather information.• Vulnerability scanning• Exploitation the target• Documenting the Founding• Continuous learning	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• Some Vulnerable Headers Exposed: Certain headers are exposed, which could potentially be exploited or provide information for further attacks.• Found Subdomains with Fierce: Subdomains have been discovered using the Fierce tool, potentially expanding the attack surface, and exposing sensitive information.• Secure Client Initiated Renegotiation Supported: The presence of secure client-initiated renegotiation in a communication protocol, which can have security implications.• X-XSS Protection is not Present: The absence of an XSS protection header in a web application, potentially making it susceptible to cross-site scripting attacks. 	
Challenges faced and how they were overcome. <ul style="list-style-type: none">• Understanding the implications and potential security risks associated with secure client-initiated renegotiation in a communication protocol can be complex.• Overcoming: In-depth research and analysis were performed to grasp the implications and potential mitigations for this feature.	

New tools, techniques, or concepts learned.

None.

Reflections and takeaways

- **Comprehensive Analysis:**
 - The day's activities emphasized the need for a comprehensive analysis of potential vulnerabilities, including headers, subdomains, and web application security features.
- **Security Awareness:**
 - The identification of vulnerabilities like the absence of an XSS protection header highlights the critical importance of ensuring robust security measures in web applications.

Responsible Reporting:

- Reporting vulnerabilities responsibly and providing clear documentation is essential to assist organizations in addressing security issues promptly and effectively.

References

Bug bounty Details: Smart pension SDP – Web testing – id.sandbox.autoentrolment.co.uk/user/sign-in	Date: 2023/10/26
Summary of the day's activities <ul style="list-style-type: none"> • Research about the target • Gather information. • Vulnerability scanning • Exploitation the target • Documenting the Founding • Continuous learning 	
Vulnerabilities discovered or explored. <ul style="list-style-type: none"> • Found Subdomains with Fierce and Amass: <ul style="list-style-type: none"> ◦ Subdomains were discovered using the tools Fierce and Amass, which could potentially widen the attack surface, exposing additional points of vulnerability and unauthorized access. ◦ • XSS Protection is Not Present, and Filter Disabled: <ul style="list-style-type: none"> ◦ The absence of XSS protection headers and filters indicates a vulnerability to cross-site scripting (XSS) attacks, where attackers can inject malicious scripts into web pages to compromise user data and security. ◦ • Secure Client-Initiated Renegotiation Supported: <ul style="list-style-type: none"> ◦ The support for Secure Client-Initiated Renegotiation may introduce security risks if not configured correctly, potentially facilitating man-in-the-middle attacks. ◦ • SNMP Service Detected: <ul style="list-style-type: none"> ◦ The presence of the Simple Network Management Protocol (SNMP) service may expose sensitive information and configuration details, potentially posing a security risk if not adequately secure. ◦ • Open Directories Found with DirB: <ul style="list-style-type: none"> ◦ The discovery of open directories using DirB reveals potentially sensitive or unprotected files and resources that can be accessed by unauthorized individuals, raising security concerns. ◦ • RDP Server Detected Over UDP: <ul style="list-style-type: none"> ◦ Detecting an RDP (Remote Desktop Protocol) server operating over UDP (User Datagram Protocol) may present security concerns, as it might expose the server to various security risks if not properly configured. 	

Challenges faced and how they were overcome.

Open Directory Discovery:

- Identifying open directories can result in a vast amount of data; prioritizing and analyzing them effectively can be time-consuming.
- Overcoming: A methodical approach was applied to categorize and assess open directories based on their sensitivity and potential security implications.

Secure Client-Initiated Renegotiation:

- Evaluating the implications of Secure Client-Initiated Renegotiation can be complex, as it requires a deep understanding of the specific protocol and its security settings.
- Overcoming: In-depth research and analysis were conducted to grasp the implications and potential mitigations for this feature.

New tools, techniques, or concepts learned.

- **Secure Client-Initiated Renegotiation:**
- Understanding the presence of Secure Client-Initiated Renegotiation in communication protocols broadened the awareness of security features and their implications.
- **SNMP Service Analysis:**
- Learning to assess SNMP service configuration and potential vulnerabilities deepened knowledge about network security and management protocols.
- **Open Directory Assessment:**
- The systematic evaluation of open directories provided insights into the importance of securing sensitive files and resources.

Reflections and takeaways

- Bug bounty hunters must remain committed to continuous learning to keep up with evolving security threats, vulnerabilities, and potential attack vectors.
- Prioritizing vulnerabilities and security findings based on their potential impact is essential for efficient mitigation and risk management.
- **Holistic Security Analysis:**
- The day's activities emphasized the importance of comprehensive security assessments, covering web security, network security, and protocol security.

References

7.9.Report 8

Bug bounty Details: Social Deal – Web Testing – www.socialdeal.nl	Date: 2023/10/27
Summary of the day's activities <ul style="list-style-type: none">• Research about the target• Gather information.• Vulnerability scanning• Exploitation the target• Documenting the Founding• Continuous learning	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• Anti-Clickjacking X-Frame Options Not Present:<ul style="list-style-type: none">◦ The absence of the "X-Frame-Options" header leaves the website potentially vulnerable to clickjacking attacks, where attackers can frame the website within malicious contexts.◦• X-Content-Type-Options Header Not Present:<ul style="list-style-type: none">◦ The missing "X-Content-Type-Options" header can expose the website to content type sniffing attacks, allowing browsers to interpret responses in unintended ways.◦• X-XSS Protection Not Present:<ul style="list-style-type: none">◦ The lack of "X-XSS-Protection" header indicates a vulnerability to cross-site scripting (XSS) attacks, where malicious scripts can be injected into web pages.◦• Secure Client-Initiated Renegotiation Supported:<ul style="list-style-type: none">◦ The support for Secure Client-Initiated Renegotiation may introduce security risks if not configured correctly, potentially facilitating man-in-the-middle attacks.◦• Some Vulnerable Headers Exposed:<ul style="list-style-type: none">◦ Vulnerable headers are exposed, suggesting that certain HTTP headers may be misconfigured or insecure.◦• No web application firewall detected.	
<div>Vulnerability Threat Level Medium No Web Application Firewall Detected Vulnerability Definition Without a Web Application Firewall, An attacker may try to inject various attack patterns either manually or using automated scanners. An automated scanner may send hordes of attack vectors and patterns to validate an attack, if the app does not have the application to get blocked (Denial of Service) Vulnerability Remediation Web Application Firewalls offer great protection against common web attacks like XSS, SQLi, etc. They also provide an additional line of defense to your security infrastructure. This resource contains information on web application firewalls that could suit your application. https://www.gartner.com/reviews/market/web-application-firewall</div>	

Challenges faced and how they were overcome.

- Identifying the absence of the "X-Frame-Options" header and its potential clickjacking risks is a crucial security concern.
- Overcoming: In-depth research and analysis were conducted to understand the impact and potential exploitation of the vulnerability. Solutions and recommendations for mitigation were explored.
- Evaluating the security risks associated with Secure Client-Initiated Renegotiation in a communication protocol can be intricate.
- Overcoming: Detailed research and analysis were performed to understand the implications and potential mitigations for this feature.

New tools, techniques, or concepts learned.

- Click jacking Defense

Reflections and takeaways

- **Web Security Best Practices:**
 - The day's activities reinforced the significance of implementing web security best practices, including the use of HTTP security headers and secure configurations.
- **Risk Mitigation:**
 - Prioritizing security measures to mitigate potential risks and vulnerabilities, especially in the absence of specific security controls like a WAF, is crucial for overall web application security.

References

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

7.10. Report 9

Bug bounty Details: Toyota Motor Europe – Web testing -www.toyota.fe	Date : 2023/10/28
Summary of the day's activities <ul style="list-style-type: none">• Research about the target• Gather information.• Vulnerability scanning• Exploitation the target• Documenting the Founding• Continuous learning	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• No DNS/HTTP-Based Load Balancers Found:<ul style="list-style-type: none">◦ The absence of DNS or HTTP-based load balancers indicates that the website may not have a mechanism to distribute incoming traffic across multiple servers for redundancy and load balancing.◦ This could impact on the website's availability during traffic spikes or server failures.◦• Found Subdomains with Fierce and Amass:<ul style="list-style-type: none">◦ Subdomains were discovered using the tools Fierce and Amass, potentially revealing additional attack surfaces or potential points of vulnerability.◦ The presence of unmonitored or unsecured subdomains can pose security risks, including unauthorized access.◦• X-XSS Protection is not Present:<ul style="list-style-type: none">◦ The absence of the "X-XSS-Protection" HTTP response header suggests a lack of protection against cross-site scripting (XSS) attacks.◦ This vulnerability can expose users to XSS attacks, where malicious scripts can be injected into web pages, potentially compromising user data and security.	
<div>Vulnerability Threat Level medium X-XSS Protection is not Present Vulnerability Definition As the target is lacking this header, older browsers will be prone to Reflected XSS attacks. Vulnerability Remediation Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.</div>	
Challenges faced and how they were overcome. <ul style="list-style-type: none">• Identifying: the lack of DNS or HTTP-based load balancers and understanding its potential impact on website availability can be complex.	

- Overcoming: Detailed research was conducted to assess the website's architecture and the potential implications of not having load balancers. Recommendations for redundancy and load balancing were explored.

New tools, techniques, or concepts learned.

- **Load Balancer Impact:**

- Understanding the potential impact of load balancers on website availability deepened knowledge about infrastructure and redundancy measures.

Reflections and takeaways

- **Website Redundancy and Availability:**

- The day's activities highlighted the importance of website redundancy and load balancing measures to ensure availability and performance during traffic spikes or server failures.

References

<https://www.nginx.com/resources/glossary/load-balancing/>

7.11. Report 10

Bug bounty Details: Intigriti - Web Testing – www.intigriti.com	Date: 2023/10/29
Summary of the day's activities <ul style="list-style-type: none">• Research about the target• Gather information.• Vulnerability scanning• Exploitation the target• Documenting the Finding• Continuous learning	
Vulnerabilities discovered or explored. <ul style="list-style-type: none">• Anti Clickjack X-Frame Options Header:<ul style="list-style-type: none">○ This vulnerability arises from the absence of the "X-Frame-Options" header. It is a security feature that prevents clickjacking attacks by denying a web page from being displayed in iframe.○ Without this header, attackers could potentially frame your website in a malicious context and trick users into taking unintended actions.○• Uncommon Header 'Refresher':<ul style="list-style-type: none">○ The presence of an unusual HTTP header named 'refresher' with the value '0; URL = https://intigriti.com' suggests an atypical server configuration.○• Secure Client-Initiated Renegotiation:<ul style="list-style-type: none">○ Secure Client-Initiated Renegotiation is a security concern related to SSL/TLS renegotiation. It allows a client to request a renegotiation of the security parameters during an ongoing SSL/TLS session.○ This feature, when supported, can introduce vulnerabilities if not configured correctly. Attackers could potentially abuse this to launch man-in-the-middle attacks.○• No DNS/HTTP-based Load Balancers:<ul style="list-style-type: none">○ The absence of DNS or HTTP-based load balancers means that the website might not have a mechanism to distribute incoming traffic across multiple servers for redundancy and load balancing.○ This could affect the website's availability and scalability, making it vulnerable to traffic spikes or server failures.○	

- **Publicly Available WHOIS Information:**

- Publicly available WHOIS information exposes domain registration details, such as the registrant's name, contact information, and domain creation/update dates.
- This information can be leveraged for social engineering, spam, or other malicious activities.
-

- **Lack of IPV6 Address:**

- The absence of an IPV6 address means the website may not be compatible with the next-generation Internet Protocol, IPV6.
- As IPV6 adoption increases, not having an IPV6 address could limit the website's reach and functionality.

Challenges faced and how they were overcome.

- Identifying: an unusual HTTP header like 'refresher' can be perplexing as it deviates from common HTTP headers.
- Overcoming: Detailed research was performed to understand the purpose and implications of this atypical header, ensuring it didn't introduce security risks.

New tools, techniques, or concepts learned.

- **WHOIS Information Awareness:**

- Understanding the potential risks associated with publicly available WHOIS information reinforced knowledge about domain privacy and security measures.

Reflections and takeaways

The day's activities emphasized the importance of implementing web security best practices, including the use of security headers, secure SSL/TLS configurations, load balancing, and domain privacy.

References

7.12. End

Finalize the report	Date: 2023/10/30 2023/10/31
Summary of the day's activities <ul style="list-style-type: none">• Finalize all reports.• Checked all the reports one by one.• Fill out the left-out information.	
Challenges faced and how they were overcome. <ul style="list-style-type: none">• Finalizing the reports and completing the old incomplete reports• Finding the references that I had not saved.	
Reflections and takeaways <ul style="list-style-type: none">• Completion of the bug bounty process	

8. Summary

This bug bounty journal provides a comprehensive overview of a bug bounty hunter's journey over the course of a month, offering valuable insights into the world of ethical hacking and cybersecurity. It highlights the critical role of bug bounty programs in identifying and responsibly disclosing vulnerabilities in digital ecosystems. The journal covers a wide range of reported vulnerabilities, including broken access control, cryptographic failures, injection attacks, insecure design, security misconfigurations, vulnerable and outdated components, and more. Each report details the challenges faced and the lessons learned during the bug bounty journey, emphasizing the importance of responsible disclosure and ethical considerations.

In addition to the technical aspects, the journal delves into the bug bounty hunter's personal growth and development throughout the journey, illustrating their unwavering commitment to improving digital security and contributing to the broader cybersecurity community's knowledge base. The methodology and tools used in the bug bounty journey are also explored, with a focus on reconnaissance, scanning, exploitation, traffic interception, and automation. These techniques are essential for efficiently identifying and reporting vulnerabilities, ultimately enhancing digital security in our ever-evolving digital landscape. This journal serves as an inspirational resource for students and enthusiasts interested in cybersecurity, offering a glimpse into the bug bounty experience and the knowledge gained from participating in such programs.

9. References

[1] OWSAP.