

Sri Lanka Institute of Information Technology



WEB SECURITY (IE2062)

BUG BOUNTY Journal

Thilakarathna S.T.D- IT22578914

**B.Sc. (Hons) in Information Technology Specializing in cyber
security**

Contents

Abstract	3
Introduction.....	4
Day 01	5
Day 02	6
Day 03	8
Day 04.....	10
Day 05	12
Day 06.....	14
Day 07	16
Day 08	18
Day 09	20
Day 10.....	22
Conclusion	24
References	25

Abstract

Businesses can crowdsource security testing to identify and address vulnerabilities through bug bounty programs. While crowdsourced security testing is a relatively new concept, its roots may be traced back to penetration testing initiatives. Within the information security industry, bug bounty programs have started to gain traction throughout the last five years.

As bug bounty programs continue to proliferate, evaluations of both the platforms they operate on and the programs themselves are imperative. The creation, maintenance, and sustainability of bug bounty programs were examined in this study. A select few bug bounty platforms oversee the majority of bug bounty initiatives. These systems might be difficult to set up initially and keep up, but they provide many security advantages to any firm willing to use them. The results of this study finally showed that a bug reward oversight committee was required, and that there should be more public vulnerability reports. Most often, hackers taking part in bug bounty schemes are hired to find vulnerabilities. Since 2013, programs advertised on bug bounty sites like HackerOne have been responsible for the discovery of tens of thousands of vulnerabilities. As of July 2019, these platforms feature over 200 publicly listed programs. We provide the findings of an empirical research that was conducted utilizing data from two bug bounty platforms in order to comprehend the expenses and advantages of bug bounty programs for both individuals and organizations. We examine the costs and advantages of running bug bounty programs as well as the incentives offered to hackers who contribute to the discovery of vulnerabilities. The average expense of running a bug bounty program for a year is now less than the cost of hiring 2 additional software engineers.

Introduction

This journal includes ten Bug Bounty reports that were made in relation to common vulnerabilities in online applications that should be fixed as soon as possible for a certain organization. We were given guidance and information on how to address online application-based vulnerabilities that we found through scanning and investigation as second-year, second-semester undergraduate cybersecurity students.

As a cybersecurity student, this assignment has given me a great opportunity to learn how to apply my knowledge and abilities into practical reality by identifying real-world security holes in web sites and understanding the morals of ethical hackers.

Broken Access Control, Cryptography Failures, Injections, Vulnerable and Outdated Components, Insecure Design, Security Misconfiguration, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, and Server-Side Request Forgery are the OWASP Top 10.

We are told to make advantage of the many tools available for vulnerability scanning, exploitation, reconnaissance (obtaining information about targets), etc.



Day 01

Date: 28/04/2024

Summary of the day's activities;

- Went through the assignment and did a research on what is meant by OWASP TOP 10 vulnerabilities.

Vulnerabilities discovered or explored:

- none

Challenges faced and how they were overcome

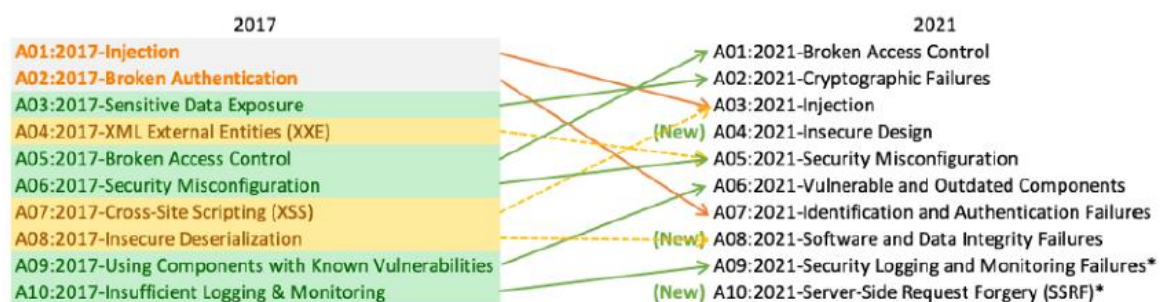
- Not having knowledge on what to do and how to do the given assignment was the biggest challenge

New tools, techniques or concepts learned

- I learned that OWASP is a non-profit organization that conducts researches to find about the dangerous threats to help organizations to improve web application security whereas the top 10 OWASP vulnerabilities are as follows:

Reflections and takeaways:

- Awareness of common threats for an organization



Day 02

Date: 30/04/2024

Summary of the day's activities;

- I was able to find more vulnerabilities using new tools and techniques and created few more reports for the vulnerabilities found.

Vulnerabilities discovered or explored:

- Absence of Anti-CSRF Tokens
- CSP Header not set

Edit Alert

Absence of Anti-CSRF Tokens

URL: <https://indrive.com/en/driver/>

Risk: Medium

Confidence: Low

Parameter:

Attack:

Evidence: `<form class="f1rgtnau">`

CWE ID: 352

WASC ID: 9

Challenges faced and how they were overcome


- After examining the vulnerabilities, they were discovered, and it was difficult to determine how they arise and what harm they do to the web application. Websites, YouTube videos, and lectures were some of the resources I used to learn about these risks.

New tools, techniques or concepts learned

- I used several scanning tools for information gathering and for vulnerability scanning.
- I used knockpy, Amass, DNSDumpster, DNSrecon, WHOIS, Whatweb, Wafw00f, Nikto, Sub404 for subdomain, vulnerability and other information gathering and PWNWSS and SQLMAP for exploiting those vulnerabilities.

Reflections and takeaways:

- I was able to learn things related to different tools, and new tools through researches and learned how to use them for information gathering, vulnerability scanning, and exploitation. This experience inspired me to actively engage with the bug bounty program and enhance my knowledge further with the skills.



inDrive
inDrive is a global mobility and urban services platform with over 150 million downloads in more than 700 cities across 47 countries.
<https://indrive.com/> · @indrive

[Submit report](#)

Bug Bounty Program
Launched in Feb 2023
[Collaboration enabled](#)

Reports resolved
95

Assets in scope
28

Average bounty
\$150-\$300

[Give feedback](#)

[Bookmarked](#) [Subscribe](#)

[Overview](#) [Scope](#) [Hacktivity](#) [Thanks](#) [Updates \(3\)](#) [Collaborators](#)

Rewards

Last updated on July 17, 2023. [View changes](#)

Low	Medium	High	Critical
Avg. bounty \$106 29.89% submissions	Avg. bounty \$487 47.70% submissions	Avg. bounty \$820 13.79% submissions	Avg. bounty \$1,311 8.62% submissions
\$50	\$150	\$750-\$1,500	\$2,000-\$8,000

The list of vulnerabilities that can be rewarded and their severity are listed in the table at the end of the rules.

Response Efficiency

4 hours
Average time to first response

4 hours
Average time to triage

6 days, 20 hours
Average time from triage to bounty

Day 03

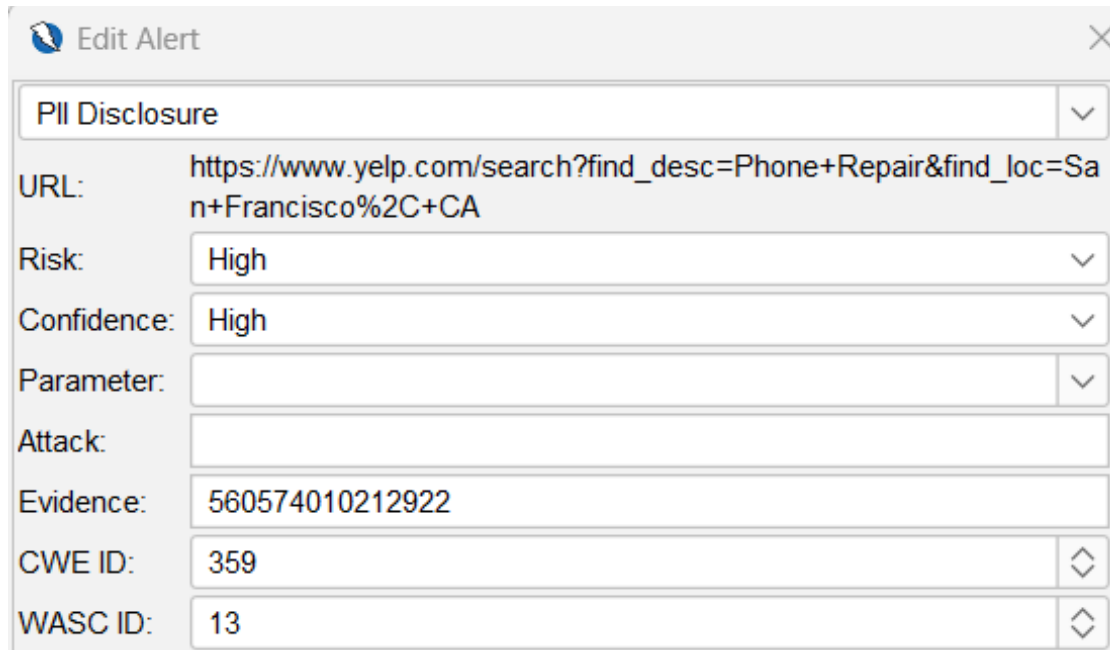
Date: 01/05/2024

Summary of the day's activities;

- I was able to find vulnerabilities and started to create reports and did a research on the found vulnerabilities.

Vulnerabilities discovered or explored:

- PII Disclosure



Edit Alert	
	PII Disclosure
URL:	https://www.yelp.com/search?find_desc=Phone+Repair&find_loc=San+Francisco%2C+CA
Risk:	High
Confidence:	High
Parameter:	
Attack:	
Evidence:	560574010212922
CWE ID:	359
WASC ID:	13

Challenges faced and how they were overcome


- These vulnerabilities were learnt after researching the vulnerabilities and it was a challenge to identify how these vulnerabilities occur, what are the negative impacts of these vulnerabilities towards the web application. I studied about these vulnerabilities through websites, YouTube videos and also referred lectures as well.
-

New tools, techniques or concepts learned

- I used several scanning tools for information gathering and for vulnerability scanning.
- I used Assetfinder, google dorking, DNSdumpster, DNSrecon, WHOIS, Nikto, Nmap, SQLMAP for subdomain, vulnerability and other information gathering and SQLMAP for exploiting those vulnerabilities.

Reflections and takeaways:

- Through research, I was able to learn about various tools and acquired new skills in using them for information gathering, vulnerability scanning, and exploitation.
- The experience motivated me to actively participate in the bug bounty programme and expand my knowledge and skill set.



Yelp
Connecting people to great local businesses in communities around the world.
<https://www.yelp.com>

Reports resolved
381

Assets in scope
9

Average bounty
\$300-\$500

[Submit report](#)
[Give feedback](#)

Bug Bounty Program
Launched in Sep 2016

Includes retesting ⓘ

Collaboration enabled ⓘ

[★ Bookmarked](#) [🔔 Subscribe](#)

[Overview](#) [Scope](#) [Hacktivity](#) [Thanks](#) [Updates \(1\)](#) [Collaborators](#)

Rewards

Last updated on September 21, 2022. [View changes](#)

Low	Medium	High	Critical
Avg. bounty \$381 40.87% submissions	Avg. bounty \$688 36.52% submissions	Avg. bounty \$992 18.26% submissions	Avg. bounty \$2,517 4.35% submissions
\$500-\$1,250	\$1,500-\$4,000	\$4,500-\$6,000	\$7,000-\$10,000

Response Efficiency

1 day, 21 hours
Average time to first response

5 days, 19 hours
Average time from triage to bounty

5 days, 19 hours

Day 04

Date: 02/05/2024

Summary of the day's activities;

- I was able to find more vulnerabilities and researched, explored about those vulnerabilities and created reports on them.

Vulnerabilities discovered or explored:

- Hash Disclosure – Mac OSX salted SHA-1
- PII Disclosure
- Missing Anti-clickjacking Header

[illegible]

Challenges faced and how they were overcome


- Referencing and researching about the vulnerabilities found were challenging and after conducting study, these vulnerabilities were discovered, and it was difficult to determine how they arise and what harm they may do to the online application.

New tools, techniques or concepts learned

- I used Syblist3r, Amass, Netcraft, DNSrecon, Whatweb, Wafw00f, Nmap, Nikto, for subdomain, vulnerability and other information gathering and PwnXSS, SQLMAP for exploiting those vulnerabilities.

Reflections and takeaways:

- I got the chance to obtain essential insights into the complexities of discovering and reporting vulnerabilities in software systems through this practical experience. Taking part in bug bounty programs gave me real-world experience and a greater comprehension of cybersecurity, enabling to make significant contributions to the defense of digital infrastructures.



Netlify
Netlify is the fastest way to combine your favorite tools and APIs to build the fastest sites, stores, and apps for the web.
<https://www.netlify.com> · @Netlify

Reports resolved
149

Assets in scope
14

Average bounty
\$200-\$250

Give feedback

Submit report

Bug Bounty Program
Launched in Nov 2020
Managed by HackerOne
Includes retesting

★ Bookmarked

🔔 Subscribe

Overview Scope Hacktivity Thanks Updates (8)

Rewards

Last updated on March 10, 2023. [View changes](#)

Low	Medium	High	Critical
Avg. bounty \$151 39.62% submissions	Avg. bounty \$364 33.96% submissions	Avg. bounty \$1,228 18.24% submissions	Avg. bounty \$2,312 8.18% submissions
\$200	\$500	\$2,500	\$6,000

Our rewards are based on severity per CVSS (the Common Vulnerability Scoring Standard). Please note these are general guidelines, and that reward decisions are up to the discretion of Netlify.

Response Efficiency

2 days, 16 hours
Average time to first response

1 week, 4 days
Average time from triage to bounty

1 week, 4 days
Average time from submission to bounty

Day 05

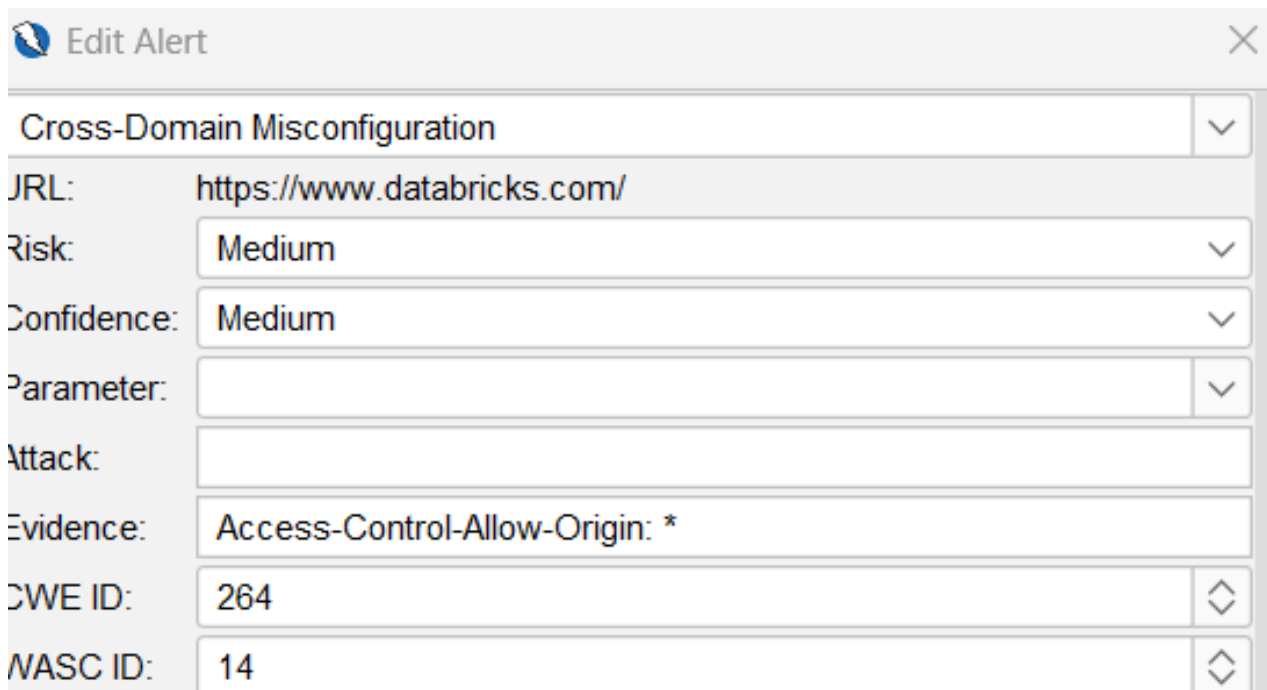
Date: 04/05/2024

Summary of the day's activities;

- I was able to find more vulnerabilities and this findings were a new experience for me and I kept working on them using new tools and techniques.

Vulnerabilities discovered or explored:

- Cross-Domain Misconfiguration



Edit Alert		×
Cross-Domain Misconfiguration		
JURL:	https://www.databricks.com/	
Risk:	Medium	
Confidence:	Medium	
Parameter:		
Attack:		
Evidence:	Access-Control-Allow-Origin: *	
CWE ID:	264	◇
NASC ID:	14	◇

Challenges faced and how they were overcome

- Referencing and researching about the vulnerabilities found were challenging and after conducting study, these vulnerabilities were discovered, and it was difficult to determine how they arise and what harm they may do to the online application.

New tools, techniques or concepts learned

- I used Knockpy, Google Dorking, DNS Dumpster, DNSrecom, Nslookup for subdomain, vulnerability and other information gathering and BurpSuite, SQLMAP for exploiting those vulnerabilities.

Reflections and takeaways:

- Finding bugs strengthened my knowledge and advanced my skills. I feel interested as my abilities have improved and practical learning have taught me more through the hands-on experience.



Databricks

Databricks combines the best of data warehouses and data lakes to offer an open and unified platform for data and AI.

<https://databricks.com/>

Reports resolved
272

Assets in scope
17

Average bounty
\$200

Submit report

Give feedback

Bug Bounty Program
Launched in Feb 2022

Managed by HackerOne

Includes retesting

Collaboration enabled

Bookmarked Subscribe

Overview Scope Hacktivity Thanks Updates (2) Collaborators

Rewards

Last updated on April 8, 2024. [View changes](#)

Asset	Low	Medium	High	Critical
	Avg. bounty \$112 28.03% submissions	Avg. bounty \$211 56.06% submissions	Avg. bounty \$727 11.62% submissions	Avg. bounty \$1,129 4.29% submissions
All other assets	\$100	\$200	\$650	\$1,000
https://dbc-9a3f8ed...	\$100	\$400	\$3,000	\$10,000
https://community.c...	\$100	\$400	\$3,000	\$10,000

Response Efficiency

1 day, 18 hours

Average time to first response

3 days

Average time to triage

1 week, 5 days

Average time from triage to bounty

2 weeks, 1 day

Day 06

Date: 05/05/2024

Summary of the day's activities;

- I became more technically proficient but also develop the innovative and vigilant mentality that was necessary to protect websites and applications in the face of constantly changing threats.

Vulnerabilities discovered or explored:

- Absence of Anti-CSRF Tokens
- Content-Security-Policy Header not set

Challenges faced and how they were overcome


- This bug bounty programs helped to overcome obstacles like the technical complexities of codes, juggling time constraints and academic obligations, handling the possibility that reported vulnerabilities will not be accepted, and also protecting legal ramifications of cybersecurity testing.

New tools, techniques or concepts learned

- I used Assetfinder, Amass, DNS Dumpster, DNSrecom, Wappalyzer, Whatweb, Wafw00f, Nmap, Nikto for subdomain, vulnerability and other information gathering and PWNXSS for exploiting those vulnerabilities.

Reflections and takeaways:

- Programs that provide bug bounties act as a spark for lifelong learning by the motivation it gives me to keep up with the latest developments in cybersecurity technology and dangers.



Bumble
Bumble - Date, Meet, Network Better
<https://bumble.com/> · [@bumble](#)

Reports resolved
297

Assets in scope
31

Average bounty
\$260-\$284

Submit report

Give feedback

Bug Bounty Program
Launched in Jun 2017

Managed by HackerOne

Includes retesting

Collaboration enabled

Bookmarked

Subscribe

Overview Scope Hacktivity Thanks Updates (0) Collaborators

Rewards

Last updated on April 17, 2024. [View changes](#)

Asset	Low Avg. bounty \$228 44.66% submissions	Medium Avg. bounty \$362 32.04% submissions	High Avg. bounty \$816 16.50% submissions	Critical Avg. bounty \$1,090 6.80% submissions
com.official.rnapp	—	\$50-\$100	\$200-\$400	\$500-\$750
chatdate.app	\$10-\$50	\$50-\$100	\$100-\$250	\$500-\$750
com.bumble.app	\$50-\$200	\$250-\$600	\$1,000-\$2,000	\$2,000-\$3,000

Response Efficiency

23 hours
Average time to first response

1 week, 4 days
Average time from triage to bounty

1 week, 4 days
Average time from submission to bounty

2 weeks, 1 hour

Day 07

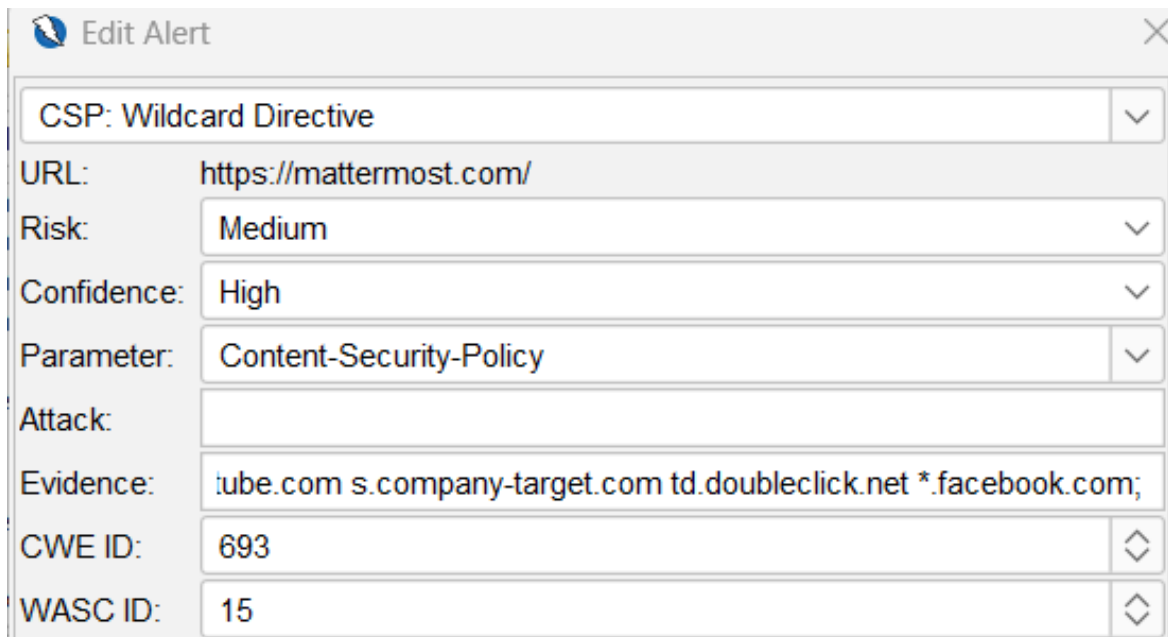
Date: 06/05/2024

Summary of the day's activities;

- Technologically, I improved, but I also developed the creative and alert mindset needed to safeguard websites and applications against ever-evolving dangers

Vulnerabilities discovered or explored:

- PII Disclosure
- Cross-Domain Misconfiguration
- CSP: Wildcard Directive



Edit Alert		✕
CSP: Wildcard Directive		
URL:	https://mattermost.com/	
Risk:	Medium	
Confidence:	High	
Parameter:	Content-Security-Policy	
Attack:		
Evidence:	tube.com s.company-target.com td.doubleclick.net *.facebook.com;	
CWE ID:	693	◇
WASC ID:	15	◇

Challenges faced and how they were overcome


- The bug bounty programmes assisted in overcoming challenges such as the intricate technical codes, managing time restrictions and academic commitments, addressing the risk that vulnerabilities revealed may not be approved, and safeguarding the legal implications of cybersecurity testing.

New tools, techniques or concepts learned

- I used Sublist3r, Google Dorking, DNSdumpster, DNSrecon, Wafw00f, Netcraft, Nmap, Nikto, Dirsearch, Uniscan, for subdomain, vulnerability and other information gathering and OWASP ZAP for exploiting those vulnerabilities.

Reflections and takeaways:

- The practical experience I gained offered priceless insights into the complexities involved in locating and disclosing software system vulnerabilities.



Mattermost
Open-source collaboration, self-managed or SaaS
<https://mattermost.com> · [@Mattermost](#)

Reports resolved
230

Assets in scope
9

Average bounty
\$150-\$300

[Submit report](#)

Gold standard

Give feedback

Bug Bounty Program
Launched in Mar 2021

Managed by HackerOne

Includes retesting

Bookmark

Subscribe

Overview Scope Hacktivity Thanks Updates (4) Safe Harbor

Rewards

Last updated on March 1, 2024. [View changes](#)

Low	Medium	High	Critical
Avg. bounty \$165 52.02% submissions	Avg. bounty \$302 37.22% submissions	Avg. bounty \$716 9.42% submissions	Avg. bounty \$1,550 1.35% submissions
\$150	\$300	\$750	\$2,000

First-time submissions by researchers are also eligible for swag rewards.

Response Efficiency

1 day, 3 hours
Average time to first response

3 days, 1 hour
Average time to triage

2 days, 17 hours
Average time from triage to bounty

Day 08

Date: 08/05/2024

Summary of the day's activities;

- Today's bug bounty experience was also interesting and technically challenging, but I feel I have improved in so many ways for the past few days since I have started working on this bug bounty program.

Vulnerabilities discovered or explored:

- HTTP Strict Transport Security (HSTS) Errors and Warnings
- Insecure HTTP Usage
- Missing X-Frame-Options Header

1. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM  1

NetSparker detected errors during parsing of Strict-Transport-Security header.

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Vulnerabilities

1.1. <https://www.zomato.com/>

Challenges faced and how they were overcome


- The bug bounty programmes helped overcome obstacles including complex technical codes, balancing deadlines and studies, mitigating the possibility that vulnerabilities found may not be accepted, and protecting the legal ramifications of cybersecurity testing.

New tools, techniques or concepts learned

- I used Sublist3r, Google Dorking, DNSdumpster, DNSrecon, WHOIS, Wafw00f, Nmap, Nikto, NetSparker for subdomain, vulnerability and other information gathering and, SQLMAP for exploiting those vulnerabilities.

Reflections and takeaways:

- As I made my way through the challenges of finding vulnerabilities and responsibly disclosing them, I soon come to understand the depth of expertise needed in cybersecurity.
- Every defect found becomes a benchmark, highlighting how crucial perseverance and close attention to detail are.



Zomato

The fastest way to search for great places to eat at and order from around you.
Serving 24 countries worldwide.

<https://www.zomato.com> · @Zomato

Submit report

Bug Bounty Program
Launched in Feb 2016
[Includes retesting](#)

Reports resolved
1027

Assets in scope
17

Average bounty
\$200-\$250

Give feedback

Bookmark

Subscribe

Overview

Scope

Hacktivity

Thanks

Updates (20)

This program requires two-factor authentication enabled to participate in.

Rewards

Last updated on April 1, 2024. [View changes](#)

Asset	Low	Medium	High	Critical
	Avg. bounty \$135 31.50% submissions	Avg. bounty \$312 39.63% submissions	Avg. bounty \$615 19.03% submissions	Avg. bounty \$1,612 9.84% submissions
All Blinkit assets (in s...	\$100-\$200	\$200-\$500	\$500-\$1,000	\$1,000-\$2,000

Response Efficiency

1 hour
Average time to first response

1 hour
Average time to triage

...

Average time from triage to bounty

...

Day 09

Date: 09/05/2024

Summary of the day's activities;

- The bug bounty experience I had today was interesting and technically difficult, but I feel like I've come a long way in the few days since I started working on this program.

Vulnerabilities discovered or explored:

- HTTP Strict Transport Security (HSTS) Errors and Warnings
- Weak Ciphers Enabled
- Cookie not marked as HttpOnly

2. Weak Ciphers Enabled

MEDIUM



1

CONFIRMED



1

Vulnerability Description

Weak ciphers are activated during secure communication (SSL), according to Netsparker's detection.

To safeguard secure communication with your visitors, you should only permit robust ciphers on your web server.

Challenges faced and how they were overcome


- The bug bounty programs assisted in overcoming challenges such as the correct studying, researching and learning of vulnerabilities, and providing a comprehensive report about the reported vulnerabilities.

New tools, techniques or concepts learned

- I used Sublist3r, Google Dorking, DNSdumpster, DNSrecon, WHOIS, Wafw00f, Nmap, NsLookUp, Sub404, NetSparker for subdomain, vulnerability and other information gathering and, PWNXSS, SQLMAP for exploiting those vulnerabilities.

Reflections and takeaways:

- When I think back on my bug bounty experiences, I get the feeling of confidence and with abilities I got in from all the experience.
- As a beginner, I discovered the importance of Cybersecurity to the present world because these can lead society to a more secured environment from malicious activities.



Chime

We're a financial technology company building products that help our members manage money easily. It's your money. It's your life. Chime in.

<https://www.chime.com/> · [@chime](#)

Submit report

Bug Bounty Program
Launched in Feb 2021

Managed by HackerOne

Includes retesting ⓘ

Collaboration enabled ⓘ

★ Bookmarked 🔔 Subscribe

Reports resolved

84

Assets in scope

24

Average bounty

\$100

Give feedback

[Overview](#)
[Scope](#)
[Hacktivity](#)
[Thanks](#)
[Updates \(3\)](#)
[Collaborators](#)

Rewards

Last updated on November 3, 2023 · [View changes](#)

Low	Medium	High	Critical
<p>Avg. bounty \$114</p> <p>64.86% submissions</p>	<p>Avg. bounty \$432</p> <p>20.27% submissions</p>	<p>Avg. bounty \$1,775</p> <p>5.41% submissions</p>	<p>Avg. bounty \$7,329</p> <p>9.46% submissions</p>
\$100	\$500	\$5,000	\$10,000–\$20,000

Our rewards are based on severity per CVSS (the Common Vulnerability Scoring Standard). Please note these are general guidelines, and reward decisions are up to the discretion of Chime Financial, Inc.

Response Efficiency

1 day, 18 hours
Average time to first response

1 week, 2 days
Average time to triage

3 weeks, 21 hours
Average time from triage to bounty

Day 10

Date: 10/05/2024

Summary of the day's activities;

- As for today I have gained some kind of experience, knowledge, skills and improved my abilities and I feel interested and motivated to engage in bug bounty programs and I was able to find vulnerabilities and have a thorough understanding of them in detail.

Vulnerabilities discovered or explored:

- HTTP Strict Transport Security (HSTS) Errors and Warnings
- Insecure HTTP Usage
- Weak Ciphers Enabled
- Missing X-Frame-Options Header

4. Missing X-Frame-Options Header

LOW  1

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Challenges faced and how they were overcome

- Taking part in bug bounty programmes helped me overcome a number of obstacles on my path to becoming an expert in cybersecurity. Navigating the complex terrain of vulnerabilities as a novice required a rigorous attitude to learning, researching, and studying.

New tools, techniques or concepts learned

- I used Sublist3r, Google Dorking, Nmap, Nikto, for subdomain, vulnerability and other information gathering and, SQLMAP for exploiting those vulnerabilities.

Reflections and takeaways:

- When I think back on my bug bounty experiences, the information and abilities I've picked up along the road give me a sense of confidence and success. Every obstacle I've overcome, from overcoming difficult vulnerabilities to grasping the nuances of responsible disclosure, has helped me develop as a cybersecurity enthusiast.


Tesla
Accelerating the world's transition to sustainable energy

\$100 – \$100,000 per vulnerability

Partial safe harbor

Submit report

Do you like this program?



Program details

Announcements 2

CrowdStream

Hall of Fame

Post

Share 204

Overview

Tesla values the work done by security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify, reproduce, and respond to legitimate reported vulnerabilities. We encourage the community to participate in our responsible reporting process. We will coordinate and communicate with researchers through the bug bounty process.

For vehicle or energy products

While we use Bugcrowd as a platform for rewarding all issues, please report vehicle and product related issues directly to vulnerabilityreporting@tesla.com, using our GPG key to encrypt reports containing sensitive information.

Third-party bugs

Vulnerabilities rewarded

772

Validation within

1 day

75% of submissions are accepted or rejected within 1 day

Average payout

\$701.85

within the last 3 months

23 | Page

Conclusion

In conclusion, I would say that beginning this bug bounty journey has been an incredible experience filled with invaluable lessons and insights. Thanks to the challenges faced, the vulnerabilities discovered, and the collaborative efforts with other security enthusiasts, I now have a greater understanding of web application security and the importance of continual vigilance in safeguarding digital assets.

Not only was each issue that was reported a source of pride, but it also demonstrated the critical role bug bounty programmes play in strengthening the security posture of companies worldwide. The experience has brought to light how crucial it is to continuously learn, adapt, and persevere in the dynamic sector of cybersecurity.

When I reflect on the incidents documented in this diary, I'm reminded of the community's resilience, generosity, and collective commitment to improving safety in the digital realm. All of my experiences—from the highs of filing successful bug reports to the lows of frustrating dead ends—have contributed to my growth as a security researcher and member of this vibrant community.

I'm eager to continue refining my skills, experimenting with new technologies, and supporting the ongoing efforts to strengthen online defences in the future. The fact that every bug is discovered, vulnerability is patched, and lesson learned serves as a continual reminder of the enormous impact that each individual can have on building a more secure future for the digital ecosystem.

References

1. OWASP 10P 10: *OWASP Top 10:2021*. (n.d.). <https://owasp.org/Top10/>
2. BugCrowd: *#1 Crowdsourced Cybersecurity Platform* / Bugcrowd. (2024, April 26). Bugcrowd. <https://www.bugcrowd.com/>
3. HackerOne: *HackerOne* / *#1 Trusted Security Platform and Hacker Program*. (n.d.). <https://www.hackerone.com/>
4. DNS Enumeration Tools: *Mastering DNS Enumeration Techniques in Linux* / Infosec. (n.d.). <https://www.infosecinstitute.com/resources/penetration-testing/dns-enumeration-techniques-in-linux/>