

The Art of Bug Bounty Reporting: Mastering Effective Communication and Persuasion



Rafael Silva · Follow
3 min read · May 7



1



TL;DR: Dive into the world of bug bounty reporting and learn how to create comprehensive, persuasive bug reports that effectively communicate your findings to program owners and security teams, increasing the chances of getting your submissions accepted and rewarded.

• • •

Introduction

A critical yet often overlooked aspect of bug bounty hunting is the art of reporting. An excellent bug hunter not only finds vulnerabilities but also effectively communicates their findings to program owners and security teams. In this blog post, we will explore how to create comprehensive and persuasive bug reports that showcase your expertise, boost your credibility, and increase your chances of getting your submissions accepted and rewarded.

Section 1: The Anatomy of a Great Bug Report

An effective bug report should contain the following elements:

1.1 Title

A clear, concise, and descriptive title that summarizes the issue and immediately captures the attention of the reader.

1.2 Summary

A brief overview of the vulnerability, its potential impact, and why it's relevant to the target application.

1.3 Technical Details

A detailed explanation of the vulnerability, including:

- Vulnerability type
- Affected component(s)
- Preconditions and requirements for exploitation
- Step-by-step reproduction guide
- Proof-of-concept (PoC) code or screenshots, if applicable

1.4 Impact Assessment

A thorough analysis of the potential consequences of the vulnerability, including:

- Data exposure or exfiltration
- Unauthorized access or privilege escalation
- System or application compromise
- Denial of service

1.5 Remediation Recommendations

Proposed mitigation strategies or fixes to address the vulnerability, demonstrating your understanding of the target application's architecture and security controls.

1.6 References

Relevant external resources, such as CVE identifiers, OWASP guidelines, or industry best practices, to support your findings and recommendations.

Section 2: Tips for Effective Bug Bounty Reporting

2.1 Be Clear and Concise

Ensure your bug report is easy to understand and avoids unnecessary jargon or technical terms. Use simple language, clear formatting, and well-structured sentences to make your report accessible to a broad audience.

2.2 Be Thorough and Detailed

Provide all the necessary information to reproduce and validate the vulnerability. Include step-by-step instructions, PoC code, and any additional information that demonstrates the issue's legitimacy and impact.

2.3 Be Professional and Respectful

Maintain a professional tone and be respectful when addressing the security team or program owners. Avoid using aggressive or confrontational language, as this can harm your credibility and the chances of your submission being accepted.

2.4 Revise and Proofread

Before submitting your bug report, revise and proofread it carefully. A well-written report with proper grammar, spelling, and punctuation demonstrates your professionalism and attention to detail.

Section 3: Additional Resources for Learning Bug Bounty Reporting

To learn more about effective bug bounty reporting and improve your writing skills, consider exploring the following resources:

3.1 HackerOne's Guide to Effective Vulnerability Disclosure:

<https://www.hackerone.com/sites/default/files/2018-01/Guide%20to%20Effective%20Vulnerability%20Disclosure.pdf>

3.2 Bugcrowd's Vulnerability Rating Taxonomy:

<https://www.bugcrowd.com/resource/vulnerability-rating-taxonomy/>

3.3 The Web Application Hacker's Handbook: <https://www.wiley.com/en-us/The+Web+Application+Hacker%27s+Handbook%3A+Finding+and+Exploiting+Security+Flaws%2C+2nd+Edition-p-9781118026472>

Conclusion

Mastering the art of bug bounty reporting is crucial for success in the bug bounty hunting field. By creating clear, concise, and persuasive reports, you'll not only showcase your expertise but also improve your credibility and reputation within the community. Investing time and effort in refining your reporting skills will ultimately increase your chances of getting your submissions accepted and rewarded, making you a more effective and sought-after bug bounty hunter. Keep honing your communication skills, and happy hunting!

<https://buymeacoffee.com/lopseg>

Bug Bounty

Bug Bounty Tips

Bug Bounty Writeup

Cybersecurity Report

👏 1

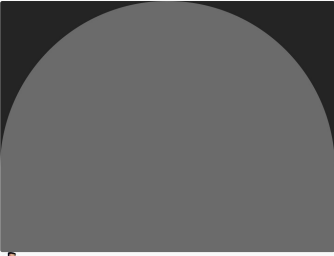


Written by Rafael
Silva

194 Followers

Follow

More from Rafael Silva



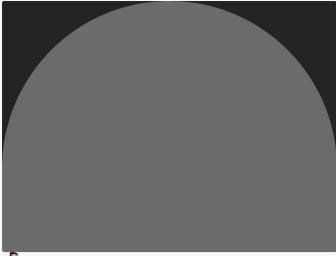
 Rafael Silva

Discover Hidden Domains with DomainSleuth

TL;DR: DomainSleuth is a simple yet powerful Python tool that leverages Server Name...

3 min read · May 7

 10 



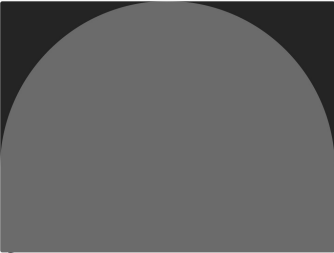
 Rafael Silva

Bug Bounty Writeup: Stored XSS Vulnerability WAF Bypass

Introduction

2 min read · Apr 30

 76 



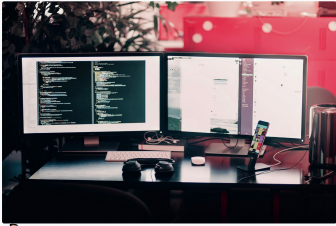
 Rafael Silva

Cross-Site Scripting (DOM) on Login Page

A few years ago, I discovered a Cross-site Scripting (DOM) vulnerability on the...

1 min read · Apr 6

 6 



 Rafael Silva

Digging Deeper: Unearthing Business Logic Vulnerabilities in...

Farzad Unsplash

4 min read · May 20

 52 



See all from Rafael Silva

Recommended from Medium



 Khod4li


P1 XSS?

Hello to all you curious hackers. It's been two weeks since I discovered this vulnerability,...

6 min read · Oct 7

 113 



 Karthikeyan Nagaraj

Best Ways to Find XSS in Web App Penetration Testing

Uncovering Cross-Site Scripting Vulnerabilities for Robust Security

3 min read · 5 days ago

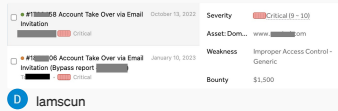
 15 



Lists



Medium Publications
Accepting Story Submissions



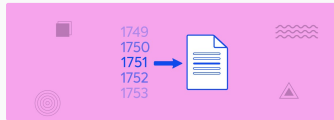
How do I change HTMLi from Low to Critical? Is your mailbox safe?

In this post, I'm just sharing how I increased the impact of regular HTMLi bugs from Low t...

6 min read · Oct 6



176



Radian ID

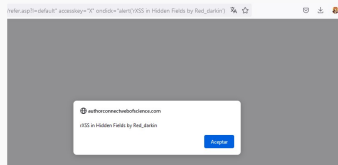
IDOR and Mass Assignment attacks leads to Full Account...

Hi everyone, I hope you are doing well. It's been a while since I last published an article...

4 min read · Sep 30



60



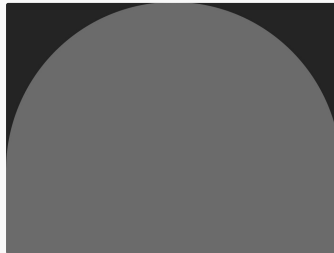
Red Darkin

Reflected Cross-Site Scripting in Hidden Input Fields

2 min read · Oct 7



111



Rafael Silva



Kickstart Your Bug Bounty Hunting Journey

A methodology for study and practice

3 min read · May 12



5



2



See more recommendations