Bug Bytes #108 – Browser to automate XSS, Finding bug bounty collaborators & Ending the SameSite confusion

BY ANNA HAMMOND · FEBRUARY 3, 2021 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the week from January 25 to of February 1st.

Intigriti News

Baron Samedit bug, Zhang Guo deception, SAP attacks & DDoS via RDP

Our favorite 5 hacking items

1. Resource of the week

findhunters

findhunters is a platform by @sametsahinnet for findings hunters that want to collaborate. You can announce that you're looking for collaborators, which payout split you want, the type of testing, vulnerability or target you're interested in, etc. It's a great idea as it may help you reach people you wouldn't have otherwise known.

2. Writeup of the week

Applying Offensive Reverse Engineering to Facebook Gameroom (Facebook)

@spaceraccoonsec has a talent for explaining complex vulnerabilities and findings. With this writeup, we learn about an insecure deserialization bug he discovered on Facebook Gameroom (a Windows-native client) during Bountycon.

3. Videos of the week

Burp Suite BApp Management for Pentesters and Bug Bounty Hunters
Commonly Misunderstood Bugs: DDoS & DOS
Bug Bounty Fundamentals: Scope

If you want to level up your bug hunting game, @codingo_'s Youtube channel is a really good place to start. These three new videos are short but packed with information on how to test for Denial of Service vulnerabilities in bug bounties, how to approach scope, and how to manage Burp extensions and configuration.

4. Article of the week

The great SameSite confusion

@jub0bs lifts the veil on a common misconception about the SameSite cookie attribute. It's an excellent read that helps understand the difference between a site and an origin, and why conflating the two can lead to vulnerabilities.

5. Tool of the week

XSSTRON

XSSTRON is an Electron JS Browser that passively detects XSS while you are browsing. It can find reflected, stored and DOM XSS with support of POST requests. I haven't tested it yet, but it is from @RenwaX23 who (judging from their Twitter feed and challenges) know a thing or two about XSS.

Other amazing things we stumbled upon this week

Videos

- Bounty Thursdays #24 – TOP 10 web penetration testing techniques of 2020???
- Blind Cross Site Scripting (XSS) Overview – Bug Bounty Hunting & Web App Pentesting
- Get Your Bug Report Triaged Faster!
- Demystifying Reverse Proxy Misconfigurations
- Attacking Sites Using CSRF – Security Simplified
- Patch sudo NOW! CVE-2021-3156
- Android Pentesting – Android Architecture + Static Analysis with apktool + gf + jadx – Pt. 01

Podcasts

- NAT Slipstreaming 2.0 – SUDO Was Pseudo Secure, BigNox Supply-Chain Attack, iMessage in a Sandbox

- DAY[0] Episode 62 – OSED, North Korean hackers, NAT Slipstream 2.0, and PGP (in)security
- Darknet Diaries Ep 84: Jet-setters

Webinars & Webcasts

- Evading Detection A Beginner's Guide to Obfuscation

Conferences

- Wild West Hackin' Fest – December 2020 Roundup

Slides & Workshop material

- XSLeaks in redirect flows

Tutorials

Medium to advanced

- GRPC Made Easy – Project Crobat
- Don't stop at alert(1): Demonstrate impact with low severity bugs
- Keeping your GitHub Actions and workflows secure: Untrusted input

Beginners corner

- Bypassing the Protections — MFA Bypass Techniques for the Win
- Testing Compiled Applications
- Android Penetration Testing: Frida

Writeups

Challenge writeups

- Intigriti January XSS challenge winners & writeups & @TomNomNom's solutions in video
- Solving ISA's 2021 Web Challenges

Pentest writeups

- XSS Via XML Value Processing
- Snooping on proprietary protocols with Frida
- From N-day exploit to Kerberos EoP in Linux environments

Responsible(ish) disclosure writeups

- Vue.js devtools Universal XSS (Chrome extension) #Web
- Bad Neighbor on FreeBSD: IPv6 Router Advertisement Vulnerabilities in rtsold (CVE-2020-25577) #IPv6
- NAT Slipstreaming v2.0: New Attack Variant Can Expose All Internal Network Devices to The Internet #Network
- Exploiting the Nespresso smart cards for fun and profit coffee #SmartCard
- YouPHPTube <= 10.0 and 7.8 multiple vulnerabilities #Web #CodeReview

Bug bounty writeups

- Launching Internal & Non-Exported Deeplinks On Facebook (Facebook, $4,000)
- Analysing Crash Messages To Achieve Blind Root Command Injection
- Remote Code Execution – LimeSurvey (CVE-2018-7556)
- How We Escaped Docker in Azure Functions (Microsoft)
- Get paid by smuggling, the legal way
- Applying Offensive Reverse Engineering to Facebook Gameroom (Facebook)
- nextcloud-snap CircleCI project has vulnerable configuration which can lead to exposing secrets & Shaking secrets out of CircleCI builds – insecure configuration and the threat of malicious pull requests
- Weird functionality leads to Account Takeover (Millions of Users affected) ($4,000)
- Unpatched Google Bug | Youtube (Race condition) (Google)

See more writeups on The list of bug bounty writeups.

Tools

- Bludger & Intro: GitHub Actions Automation Framework for the command line
- frogy-subdomain-enumeration: Subdomain enumeration tool in Bash (with recursion over N level of subdomains)
- NtHiM (Now, the Host is Mine!): Fast sub-domain takeover detection in Rust, based on can-i-take-over-xyz data
- Name-that-hash: Hash identification tool

Tips & Tweets

- Underscores in subdomains

- @ajxchapman's race condition in Docker engine
- Poc RCE Opentsdb (CVE-2020-35476)

Misc. pentest & bug bounty resources

- BugBountyHunting Search Engine
- A bug bounty hunting journey (Ebook at $9.99)
- Pentest Playbook
- Conda (Youtube channel)

Articles

- Intercept SSM Agent Communications
- A Special Attack Surface of the Android System (1): Evil Dialog Box
- Injecting Rogue Dns Records Using DHCP
- Introducing FComm – C2 Lateral Movement
- Silencing Microsoft Defender for Endpoint using firewall rules

Bug bounty & Pentest news

- How to turn your cybersecurity hobby into a career – An Introduction to Bugbounties: March 15
- CactusCon: February 5-6
- ShaktiCon
- 1st Ever ZAPCon – Call For Papers
- Announcing Pwn2own Vancouver 2021

Non technical

- Machine learning offers fresh approach to tackling SQL injection vulnerabilities
- Hacker Spotlight: Interview With Pnig0s
- No, Java Is Not A Secure Programming Language
- How to enable dark mode in Burp Suite

Community pick of the week

See how badass @DattanaMayank looks! Congratulations for the cool bug(s) behind these RedBull crates!

We'd love to hear from you too about your bug bounty wins, swag and joys. Tag us on social media if you want to share them with other Bug Bytes readers.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com