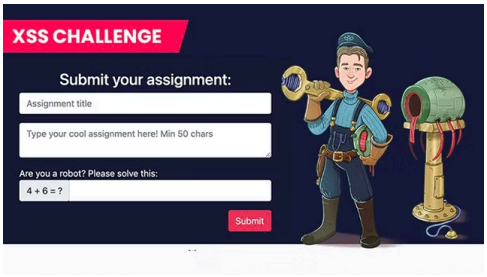
Bug Bytes #110 – Scope based recon, Finding more IDORs & How to hack Sharepoint

BY ANNA HAMMOND · FEBRUARY 17, 2021 · LAST UPDATED ON MARCH 6, 2025

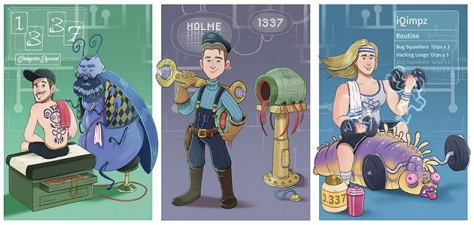
Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the week from February 8 to February 15.

Intigriti News



New XSS challenge, curated by @holme_sec



Congratulations @StanFaas, @holme_sec and @qimpz for your new hacker portraits!

New “Bounty bag” item in our swag store

Google’s Open Source Vulnerabilities, A US town’s water supply hack & Windows/Chrome security concerns

Our favorite 5 hacking items

1. Article of the week

Scope Based Recon Methodology: Exploring Tactics for Smart Recon

You might’ve already seen Harsh Bothra (@harshbothra)’s past talks on this same topic. This is a nice complement that includes a recon methodology with three options based on the program’s scope (small, medium and large), links to tools and a summary mindmap.

2. Writeup of the week

OAuth Misconfiguration Leads to Full Account takeover

This is an interesting finding by Yasser Mohammed (@boomneroli). It starts with OAuth CSRF that doesn’t work despite a missing CSRF token, debugging it with postMessage-logger, and ends up being a cool bug chain involving OAuth CSRF, postMessage and Clickjacking leading to account takeover.

For other cool writeups, also keep an eye on @Samm0uda who started sharing some of his 50 bugs found in Facebook.

3. Tutorials of the week

Finding More IDORs – Tips And Tricks
The Lone Sharepoint

Who doesn’t like IDOR? The first tutorial goes over several IDOR techniques to check on ID parameters and API calls.

The second article is a nice collection of Sharepoint attacks that might come in handy during a pentest?

4. Tool of the week

Confused

Short after the new dependency confusion writeup was published, @joohoi shared this tool that automates checking for it. It is in Go and currently supports three package managers (pypi, npm and composer).

5. Resource of the week

Language Agnostic Security Code Review

This article provides a language-independent methodology for security code review. Of course, the more knowledge you have of a programming language, the better code review you can do but this is a good start. It's a basic methodology to build upon with experience.

Other amazing things we stumbled upon this week

Videos

- Bounty Thursdays #25 – Will AI really destroy the cyber security industry? find out now!
- Android App Security Basics (Static Analysis – Part 1)
- How to get into Infosec?
- Q&A session with Katie Paxton! & Q&A session with ZSEANO!
- Exploring the Human Element: Interview with Dave Kennedy
- [Live Stream] CodeQL Code Scanning Language Tutorial #CodeReview #CodeQL

Podcasts

- C.O.M.B. – Florida Water Supply Hack Update, Major Patch Tuesday, Android SHAREit Vulnerability
- DAY[0] Episode 64 – ICS Fails, iOS and Windows Kernel Bugs, and a Package Disguised

Webinars & Webcasts

- Exploiting Android Messengers with WebRTC | Natalie Silvanovich

Slides

- @orange_8361's presentation slides

Tutorials

- The CVE That Will Never Die!
- A ffuf Primer

- Pentesting Non-Proxy Aware Mobile Applications Without Root/Jailbreak
- DNS exfiltration of data: step-by-step simple guide
- Group Policy For Script Kiddies
- Reverse Engineering Keys from Firmware. A how-to

Writeups

Challenge writeups

- JWT Key Confusion Attack: Part2

Responsible(ish) disclosure writeups

- GPGME Used Confusion, It's Super Effective ! #API #VMWare
- Exploiting CVE-2021-25770: A Server-side Template Injection In Youtrack
- Swarm of Palo Alto PAN-OS vulnerabilities #RCE #Web
- CVE-2020-35700: Exploiting a Second-Order SQL Injection in LibreNMS < 21.1.0 #Web
- CVE-2021-22652: Advantech iView Missing Authentication RCE (FIXED) #RCE #Web

Bug bounty writeups

- Self-XSS to rXSS via Uploaded File Name
- Hacking Chess.com and Accessing 50 Million Customer Records (Chess.com)
- Access files uploaded by employees to internal CDNs / Regenerate URL signature of user uploaded content. (Facebook, $12,500)
- The "P" in Telegram stands for Privacy
- Takeover an account that doesn't have a Shopify ID and more (Shopify, $23,550)
- External SSRF and Local File Read via video upload due to vulnerable FFmpeg HLS processing (TikTok, $2,727)
- Remote hacker can download all the files of master branch in public projects where everything is members only. (GitLab, $1,500)
- Regular expression denial of service in ActiveRecord's PostgreSQL Money type

See more writeups on The list of bug bounty writeups.

Tools

- dooked: DNS and Target HTTP History Local Storage and Search

- RepeaterClips: Burp extension that sends a compressed Base64 encoding of any request to your clipboard for easily sharing it
- BurpParamFlagger: Burp extension that adds a passive scan check to flag parameters whose name or value may indicate a possible insertion point for SSRF or LFI
- Reconmap: Open-source pentesting management and reporting platform

Tips & Tweets

- Alternative to @terjanq's unlimited iframe DOM-clobbering without the need of name="X"
- So you've decided to give dependency confusion a try...
- Avoid Google ReCAPTCHA detecting Burp proxy and raising the challenge difficulty
- @LooseSecurity's XSS WAF bypass example
- Different ways to handle CSRF tokens in Burp that must be different for each request

Misc. pentest & bug bounty resources

- OSV: Google's new database for open source vulnerabilities
- xajkep/wordlists
- regex.rip: Check if a regex is vulnerabel to ReDoS

Challenges

- Damn Vulnerable GraphQL Application
- Intigriti Community XSS Challenge: @holme_sec

Articles

- Electron APIs Misuse: An Attacker's First Choice
- Docker image history modification – why you can't trust `docker history`
- Hacking a SlackBot (That I Made)

Bug bounty & Pentest news

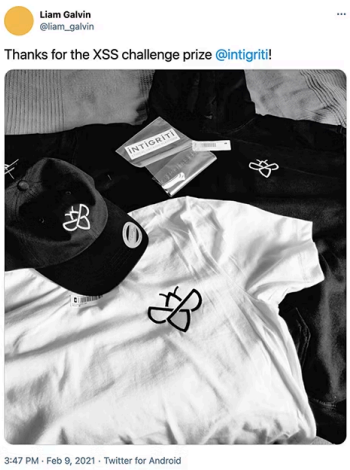
- NahamCon2021 (March 14)
- Frida 14.2 Released ∞
- Burp Professional / Community 2021.2.1 updates:
  - Two update channels introduced (Stable & Early Adopter)

- Burp Scanner now natively reports vulnerable JS libraries
- It's easier to read and edit hex content

Non technical

- Hacker Spotlight: Interview With Notnaffy

Community pick of the week



Well-done on the XSS challenge, @liam_galvin!

Do you want swag too? Then make sure to check out our current XSS challenge! And tag us on social media if you want to share any cool swag, bug bounty wins and joys.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com