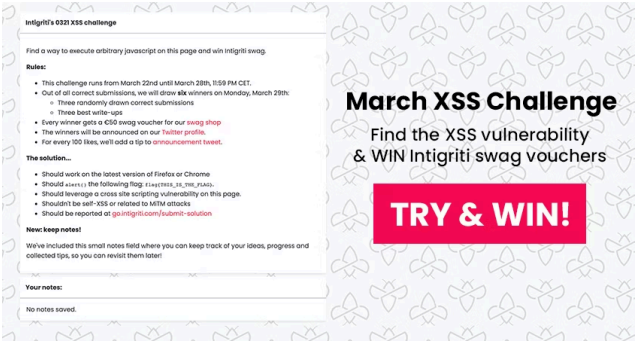
Bug Bytes #115 – Hacking Facebook & Google's networks, H2C smuggling revisited & Networking fundamentals

BY ANNA HAMMOND · MARCH 24, 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 March 15 to 22.

Intigriti News



Intigriti's 0321 XSS challenge

Our favorite 5 hacking items

1. Writeups of the week

H2C Smuggling in the Wild & h2cSmuggler
How I hacked Facebook: Part Two (Facebook, $54,800)

@seanyeoh published amazing research on H2C smuggling. He built on Jake Miller's research on this vulnerability and exploited it in cloud providers that were initially considered not vulnerable.

The second writeup is about a cool bug chain that allowed @alaa0x2 to access a Facebook employee's account and to compromise Facebook's internal network. It involves SSRF, account takeover and cookie manipulation.

2. Article of the week

How we found and fixed a rare race condition in our session handling

GitHub released details about an interesting bug they fixed. It's a race condition in their session handling that caused users logged into github.com to randomly be authenticated as other users.

3. Videos of the week

Hacking into Google's Network for $133,337
Networking Fundamentals & Slides

Two videos of very different flavors: The first one is @LiveOverflow interviewing @epereiralopez about winning the 2020 Google Cloud Platform VRP Prize and the RCE that made it possible. So inspirational!

The second video is an excellent primer on networking fundamentals by @TomNomNom.

4. Tutorials of the week

Burp Suite – solving E-mail and SMS TAN multi-factor authentication with Hackvertor custom tags
Attack Surface Analysis – Part 2 – Custom Protocol Handlers

If you're not familiar with the Hackvector Burp extension, the first tutorial shows cool examples of its usage and capabilities (e.g. how it helps automate MFA authentication).

In the second tutorial, @CryptoGangsta dives deep into the attack surface of custom protocol handlers. It's an excellent read, packed with information for hackers interested in destop apps.

5. Resource of the week

Ways to alert(document.domain)

@TomNomNom shared this list of ~40 ways to execute alert(document.domain). It's old and somehow I'm just finding out about it, but it's still very relevant for bypassing WAFs and regexes.

Other amazing things we stumbled upon this week

Videos

- Hunting for bugs in GraphQL APIs (Demo) & Live GraphQL Q&A Session
- How to escape docker container?
- SQL Injection – Lab #3 SQLi UNION attack determining the number of columns returned by the query
- ZAP Deep Dive: Report Generation
- WE GOT BREACHED! – An attack and defense scenario using custom Malware and Defender For Endpoints!
- Watch Hackers Demonstrate a Ransomware Attack (ft. Kilian from SecurityFWD)
- LiveQL Episode 2 – The Rhino in the room
- SecuriTEA & Crumpets – Episode 3 – PwnFunction

Podcasts

- DAY[0] Episode 69 – Fast Fuzzing, Malicious Pull Requests, and Rust in my kernel?!

- What the FLoC? – Automatic Fix for Exchange Server Flaw, Firefox 87 Features, MyBB Patch

Webinars & Webcasts

- Introduction to Wireless Penetration Testing

Conferences

- PancakesCon

Tutorials

- Make Burp Community feel a little more like Burp Professional
- authorized_keys File Format
- The most common on premises vulnerabilities & misconfigurations
- Deserialization vulnerability
- Anatomy of the Session Management Tests & Session Management All-In-One
- Android reverse engineering for beginners – Dexcalibur
- Paving The Way To DA – Complete Post (Pt 1,2 & 3)

Writeups

Challenge writeups

- CTFSecurinets Quals 2021 Writeup

Pentest writeups

- From TikiWiki to Domain Admin – Journey to pwning a company

Responsible(ish) disclosure writeups

- F5 Discloses Eight Vulnerabilities—Including Four Critical Ones—in BIG-IP Systems & wvu-r7's assessment of CVE-2021-22986 #Web
- DuckDuckGo Privacy Essentials vulnerabilities: Insecure communication and Universal XSS #Web
- Hack the Stack with LocalStack: Code Vulnerabilities Explained #Web
- [CVE-2021-28379] Abusing file uploads to get an SSH backdoor #Web
- All my Intune users could become Local Administrators and it's a Feature? #Cloud #LPE
- MyBB Remote Code Execution Chain #Web
- Exploiting remote DoS vulnerability in my not-so-smart TV #IoT

Bug bounty writeups

- Abusing Data Protection Laws For D0xing & Account Takeovers
- Stealing arbitrary GitHub Actions secrets (GitHub, $25,000)
- TikTok for Android 1-Click RCE (TikTok)
- How to Harpon Big Blue! (IBM)
- An Interesting Account Takeover!!
- Dangling DNS: Worksites.net
- CVE-2021-27076: A Replay-style Deserialization Attack Against Sharepoint
- How I made it to Google HOF? (Gogole, $1,000)

See more writeups on The list of bug bounty writeups.

Tools

- normal.py: Find unicode codepoints to use in normalisation and transformation attacks
- UnChain: A tool to find redirection chains in multiple URLs
- gitlab-unauth-parser & Intro: Parses unauthenticated Gitlab APIs for users, repos, groups and secrets
- xeuledoc: Fetch information about a public Google document
- Spectroscope: Chrome extension that helps search for endpoints potentially vulnerable to Spectre
- nList: An nmap script to produce target lists for use with various tools

Tips & Tweets

- Found a private SSH key and want to know whose it is?
- Hiding a ZIP archive or MP3 files in PNG images
- File upload encoded hash trick
- Get a very good subdomain list without any tool using GitHub DNS block listing
- How to execute a script on ssh login prior to your shell or command, even if you disable TTY allocation!
- Query Shodan like it's a SQL database using a Steampipe integration

Misc. pentest & bug bounty resources

- HolyTips: Middlewares
- 0dayfans.com

- Financial-grade API (FAPI) 1.0 final Specifications

Challenges

- Intigriti's 0321 XSS challenge
- ctf.thepa.in
- Trusted Types bypass challenge

Articles

- GitLab: How we found and fixed a rare race condition in our session handling
- Browser powered scanning in Burp Suite
- Bypass Strict Input Validation With Remove Prefix and Suffix Patterns & Challenge
- Another approach to portable Javascript Spectre exploitation
- Side channels in web browsers
- Subdomain Takeover in AWS: making a PoC

Bug bounty & Pentest news

- Google: Announcing the winners of the 2020 GCP VRP Prize
- @bbuerhaus's launching $ziot coin, "an experimental hacker themed social coin that is backed by NFT minted bug bounty vulnerability reports"
- What's new in Ffuf 1.3.0
- Is Responder part of your pentest/red team workflow? It needs your support to continue existing!
- Infosec Income Questionnaire v2
- OWASP Top Ten 2021 survey
- HackerCon (March 27)

Non technical

- Establishing asset ownership in vulnerability reporting
- Hacker Rates 12 Hacking Scenes In Movies And TV | How Real Is It? (video)
- How To Make Remote Work Not Suck: The Bishop Fox WFH Guide

Community pick of the week

Well done, @sunilyedla2! Continue keeping calm and hacking, it suits you

Want to share your bug bounty wins, swag and joys with other Bug Bytes readers? Tag us on social media, we'd love to hear from you too!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com