Bug Bytes #19 – The Real Impact of Open Redirect, Advanced CORS Exploitation Techniques & Common API Pitfalls

BY INTIGRITI · MAY 21, 2019 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as **PentesterLand.** Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 10 to 17 of May.

Our favorite 5 hacking items

1. Article of the week

> "The real impact of an Open Redirect"

Open redirects are often considered low impact bugs by bug bounty programs (including Google). As such, they are not rewarded unless they can be used to exploit other vulnerabilities like XSS or OAuth token disclosure. So you want to increase their impact by chaining them with other bugs.
Also, if you're a pentester not a bug bounty hunter, the same logic applies. If you want to convince clients which bugs are the most damaging and must absolutely be fixed, you need to tell them why by providing detailed attack scenarios.
This article can help. It shows how to combine open redirect with Referrer check bypass, XSS-Auditor bypass, SSRF & OAuth token theft.

2. Writeup of the week

> "Think Outside the Scope: Advanced CORS Exploitation Techniques **($1,500)**"

This an excellent writeup of two CORS misconfigurations and how to exploit them in great detail (with code, PoCs, specifics of each browser, other good references...).
Highly recommended if you want to see practical examples of real-life CORS vulnerabilities.

3. Conference of the week

> "Common API security pitfalls"

This is an awesome presentation on API security. If you're into this, make sure to watch the video to better understand the slides. I didn't realize there was a video embedded in the page at first...
The bugs described include the lack of rate-limiting, IDOR, session flaws, mishandling client-side session data, JWT weaknesses, CSRF, CORS misconfigurations and more. Juicy stuff!

4. Non technical item of the week

> "Key lessons from an ethical hacker"

I found this article really interesting because it is a walkthrough of the pentest of a power station. Personally, I find physical pentests & red teaming fascinating specifically because I lack experience in this area (having done mostly "regular" pentests).
This walkthrough touches on many things including why not phishing is not always the best approach, a concrete example of recon (different from recon done for Web app testing), how to convince boards of the importance of security, etc.
It's probably nothing new if you're already doing these kinds of tests, but it's a nice high-level view for anyone who's striving to become a pentester.

5. Tutorial of the week

> "SameSite cookies in practice"

Have you heard of Samesite cookies recently and wondered what they are? If yes, this is a great introduction to this relatively new cookie attribute.
It's a protection against CSRF and it seems very effective. I think we will see less and less CSRF bugs in bug bounty.
So check out this tutorial if you're into Web app security.

6. Intigriti News

6.1 5K Followers XSS Challenge

Time to celebrate! We reached the 5k twitter followers! As a celebration, we made a new XSS challenge. Are you able to solve it?

> "NEW CHALLENGE: We're giving away a Burp Pro license, swag & invites to celebrate 5k followers! Claim your prize: https://t.co/KYQHSOpGvn #BugBounty #CTF #HackWithIntigriti pic.twitter.com/h2jDTM3qos
> — Intigriti (@intigriti) May 21, 2019"

Other amazing things we stumbled upon this week

Videos

- Content-Security-Policy: An Introduction
  - https://twitter.com/abhaybhargav/status/1127996679431393280?s=20
- The Origin of Script Kiddie – Hacker Etymology
  - https://twitter.com/LiveOverflow/status/1127734310340055042?s=20
- Active Directory Exploitation – LLMNR/NBT-NS Poisoning

- Zero to Hero: Week 9 – NTLM Relay, Token Impersonation, Pass the Hash, PsExec, and more

Podcasts

- Security Now 714 – Android 'Q'
- Risky Business #541 — NSO Group makes global headlines. What next?
- Darknet Diaries Ep 38: Dark Caracal
- 7MS #363: Interview with Ryan Manship and Dave Dobrotka – Part 2
- Hack Naked News #218 – WhatsApp, Linux Kernel, & Marcin Szary
- Paul's Security Weekly #604 – Singapore, Cisco, and Israeli Spyware

Conferences

- Common API security pitfalls
- Le Tour Du Hack 2019: Red Teaming On A Shoestring – James Hickie
- WebHacking Training 2019 – INFILTRATE 2019

Slides only

- Gimme a bit!" – Exploring Attacks in the "Post-XSS" World
- Dork to bounty – And other bug bounty stories...
- Top 11 Security Mistakes in Active Directory and How to Avoid Them

Tutorials

Medium to advanced

- Weaponising Staged Cross-Site Scripting (XSS) Payloads
- XSS without parentheses and semi-colons
- SameSite cookies in practice
- Exploiting Remote File Inclusion (RFI) in PHP application and bypassing remote URL inclusion restriction
- JWT: Signature-vs-MAC attacks
- Owning O365 Through Better Brute-Forcing
- Mounting VHD file on Kali Linux through remote share

- Adventures in WhatsApp DB—extracting messages from backups (with code examples) & alternatives
- Dynamic Microsoft Office 365 AMSI In Memory Bypass Using VBA
- Weaponizing AMSI bypass with PowerShell

Beginners corner

- 6 Methods to bypass CSRF protection on a web application
- Attack Surface: Concept, Types, Tools and Attack Surface Reduction Strategies
- Four nmap NSE scripts for penetration testing.
- Scanning TLS Server Configurations with Burp Suite & TLS-Attacker-BurpExtension: Burp extension for evaluating TLS configurations (like http://testssl.sh), based on TLS-Attacker
- Github OSINT
- Analyzing and Preventing Sub-domain Takeovers: Real Risks? Causes?
- Debugging iOS apps with Zaproxy

Writeups

Responsible disclosure writeups

- "Web scraping considered dangerous": Exploiting the telnet service in scrapy < 1.5.2
- How to brick all Samsung phones
- CVE-2018-7841: Schneider Electric U.Motion Builder Remote Code Execution 0-day
- Arbitrary file read vulnerability in Hackerrank
- Joplin ElectronJS based Client: from XSS to RCE
- CVE 2018-16858 Write up – or the joy of macros
- A Questionable Journey From XSS to RCE

Bug bounty writeups

- DoS on GitLab ($3,000)
- Xs-search on Twitter & Video PoC ($1,470)
- Privacy violation on Twitter ($560)
- Race condition on HackerOne ($500)
- Authorization flaw on Shopify ($500)
- XSS via parameter pollution on private program

- Open redirect on private program
- Logic flaw on Facebook ($500)
- XSS on private program
- Stored XSS on Google

See more writeups on The list of bug bounty writeups.

Tools

- Match and Replace: Script used to automatically generate JSON option file to BurpSuite. Useful for SSRF testing
- Pyscripter_utils.py : Burp Python Scripter scripts & Why use it's not redundant with Match and Replace rules
- DS_Store_crawler_parser: A parser + crawler for .DS_Store files exposed publically
- Grepips.py: Little Python script to dump IP addresses from a file
- jwt_tool: The JSON Web Token Toolkit, A toolkit for testing, tweaking and cracking JSON Web Tokens
- Gitmail: Quickly grab a GitHub users email from commits, even when their email privacy is enabled
- Crosslinked: LinkedIn enumeration tool to extract valid employee names from an organization through search engine scraping. Names can be formatted in a defined naming convention for further security testing
- Trigmap: A wrapper for Nmap to automate the pentest
- ExtAnalysis: Browser Extension Analysis Framework
- SCWF: CTF tool for identifying, brute forcing and decoding encryption schemes in an automated way
- LES: Linux privilege escalation auditing tool
- EITR: Automates the deployment and provisioning of a remote host to be used for pentesting labs and CTF games, such as HackTheBox and VulnHub
- PeekABoo: Enables Remote Desktop on targets using PowerShell. Useful for internal penetration testing
- Muraena: An almost-transparent reverse proxy aimed at automating phishing and post-phishing activities

Misc. pentest & bug bounty resources

- XSS Without parentheses ()
- Fascinating & Frightening Shodan Search Queries (AKA: The Internet of Sh*t)

- Bugreader by @JubaBaghdad
- Writeups.io by @TDesarmo
- Personal Information Retrieval Mindmap
- The Hacker's Hardware Toolkit
- Internal Security Assessment: Field Guide: $7.99 e-book by Paul Seekamp (@nullenc0de)
- OSINT: How to find information on anyone

Challenges

- Pwn.now.sh: Page vulnerable to many common web attack vectors for practice
- Announcing Facebook CTF 2019
- Mossad Cyber Challenge 2019

Articles

- Content-Type and Status Code Leakage
- The real impact of an Open Redirect
- Latest Bypassing Techniques Beat SOAP/XML API Protection
- Seven Surprising Bash Variables
- Android Application Diffing: Analysis of Modded Version
- Beginner Tips to Own Boxes at HackTheBox !
- Find hidden friends and communities for any Facebook user
- The Risk of Authenticated Vulnerability Scans
- Metasploit Development Diaries: Q1 2019
- WannaCry, Two Years On: Current Threat Landscape, Forgotten Lessons, and Hope for the Future

News

Bug bounty / Pentest news

- ITSecurityguard's Bug Bus spreadsheet
- https://twitter.com/mubix/status/1128387385220378625?s=20
- Faster smarter JavaScript debugging in Firefox DevTools
- European Security Blogger Awards 2019 Nominations

- Better Bug Bounties
- @nnwakelam joined the bug bounty millionaires club
- Oh, btw, what I didn't mention is that in the new @msfminute episodes there will be a hidden $100 Hak5 store gift code. First come first serve just sayin...

Vulnerabilities

- A Cisco Router Bug Has Massive Global Implications
- Information disclosure vulnerability impacts 25,000 Linksys routers
- Cloud providers and OS vendors scramble to decapitate ZombieLoad vulnerability
- Microsoft warns of major WannaCry-like Windows security exploit, releases XP patches

Breaches & Attacks

- Keyloggers Injected in Web Trust Seal Supply Chain Attack
- WhatsApp voice calls used to inject Israeli spyware on phones & The NSO WhatsApp Vulnerability – This is How It Happened

Other news

- Dutch NCSC updates TLS guidance for orgs
- SHA-1 collision attacks are now actually practical and a looming danger
- Break up Facebook, cofounder says: it's an un-American monopoly

Non technical

- Key lessons from an ethical hacker
- How to Deal With Information Overload
- My Journey to Now by @daeken
- Organising-awesome-meetups: Do you want to start a meetup group but you don't know exactly where to start? You're in the right place!
- Speaker style bingo: 10 presentation anti-patterns

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 05/03/2019 to 05/10/2019.

Subscribe to the newsletter here!

Disclaimer:
The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti. ***Curated by Pentester Land & Sponsored by Intigriti***