Bug Bytes #6 -25k Facebook CSRF, how to get IDOR, a raise and more!

BY INTIGRITI · FEBRUARY 19, 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.*

Sign up for the newsletter here.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 08 of February to 15 of February.

Our favorite 5 hacking items

1. Tool of the week

> "Dnsgrep & Tutorial"

This is a great new tool for quickly searching large DNS datasets like those from the Rapid7 Project Sonar. It's like *grep* except it can search dozens of gigabytes of data really fast.
You can either install it and use it locally, or use the online version. But the author said he will likely take down the online service in the future.

2. Writeup of the week

> "CSRF on Facebook"

This is what a $25,000 bug on Facebook looks like!
The URL *https://www.facebook.com/comet/dialog_DONOTUSE/?url=XXXX* triggers a POST request to whatever relative path is specified in XXXX. The problem is that it also adds a CSRF token automatically to the request body, which makes it vulnerable to CSRF.
Basically, leveraging this vulnerable URL allows executing any other POST request while bypassing CSRF protections. The writeup details many different ways to exploit this: how to delete other user accounts, post on someone else's timeline, delete profile pictures and most importantly perform account takeovers.
This is a great example of a well written detailed writeup, which includes business impacts and technical details. The bounty is well deserved!

3. Video of the week

> "Web Security 101 – Insecure Direct Object Reference – You are who you say you are, right?"

PwnFunction is an excellent Youtube channel for anyone interested in Web app hacking. The style reminds me of a mix between Hacker101 and LiveOverflow.

This particular video explains how IDOR works, the link with forced browsing and HTTP parameter pollution, what to do when you find an IDOR but cannot exploit it, how to bypass checks, etc.
Also, I love the humor… "Most of you might add a single or double quote at the end (of a URL like *website.com/…?user_id=12*) because it's just an OCD thing at this point"

4. Non technical item of the week

> "Salary Negotiation Tips from White Men in Tech: Part 1"

This is a must read article for any woman in this industry.
I don't understand why, but we generally have a tendency to ask for lower salaries than men. I noticed this from my own experience in two different countries (in Europe and Africa), and also from interviewing people. Men with a lot less qualifications than the women we finally hired were asking for much higher salaries.
When I was interviewed for my last job as a consultant, I was able to get a really good salary only thanks to my husband. He coached me on what to ask for, how to negotiate, the minimal salary that I would accept, etc. And the minimum he told me was sky high in my mind and I was very uncomfortable asking for that. But guess what… I got it and deserved it considering the job that I had to do!
So if you are looking for a job or for a raise, and you have trouble asking for what you're really worth, the tangible advice in this article could help a lot.

5. Tutorial of the week

> "[Sqli] Extracting data without knowing columns names & Similar technique"

This is a great tutorial on how to exploit an SQL injection without knowing column names.
You might need this if you can't get column names because a WAF blocks calls to information_schema, and bruteforcing the names doesn't work.
The trick is to use *select 1,2,3,4,5,6 union select * from users;* instead of *select * from users;*.

Other amazing things we stumbled upon this week

Videos

- HackerOne Hacker Interviews: @Hogarth45
- Python SSTI: Attack Flask framework using Jinja2 template engine
- OWASP DevSlop E22: HaveIBeenPwned?
- DevSlop: Mentoring

Podcasts

- Security In Five Ep. 428: Do Not Participate In DNA Testing To See Your Heritage, How To Delete Your Data

- Security In Five Ep. 429: Are Contactless Banking Cards A Greater Security Risk
- 7MS #349: Interview with Ameesh Divatia of Baffle
- CyberSpeak Podcast: Closing the Cyber Skills Gap
- Securiosity: Marcus Carey's 'Tribe of Hackers'
- Security Now 701: Adiantum
- Smashing Security 115: Love, Nests, and is 2FA destroying the world?
- TrustedSec Podcast E. 3.9 – Turn off the Internet, The Containers are Leaking, and Why are my genitals in the Enquirer
- Sophos podcast Ep. 019 – Android holes, iOS screengrabbing and USB poo [PODCAST]

Webinars & Webcasts

- Practical Serverless Security with DVFaaS: Register before Feb 26, 2019 11:00 AM in Eastern Time (US and Canada)
- BHIS Webcast: Blockchain and You! InfoSec Edition
- Webinar: Using MITRE ATT&CK(TM) for Coverage and Effectiveness Assessments

Conferences

- Hacking NodeJS applications for fun and profit & Slides
- Disobey 2019
- BlueHat IL 2019 & Schedule
  - No Code No Crime: UPnP as an Off-the-Shelf Attacker's Toolkit

Slides only

- Security Issues in Modern JavaScript
- Practical White Hat Training #6: Post Exploitation
- DNS rebinding in 2k18: Ancient artifact or a new era?
- Offensive WMI

Tutorials

Medium to advanced

- Unveiling Amazon S3 bucket names

- How to Bypass Virtually Every News Paywall
- PostgreSQL for red teams
- Pwning WPA/WPA2 Networks With Bettercap and the PMKID Client-Less Attack
- Evil Twin Attack: The Definitive Guide
- Day 44: Linux Capabilities Privilege Escalation via OpenSSL with SELinux Enabled and Enforced
- Find The CEO's Email — in a cloud world
- Make It Rain with MikroTik
- Getting PowerShell Empire Past Windows Defender
- Suck it, Windows Defender.

Beginners corner

- How to bypass Instagram SSL Pinning on Android (v78)
- Burp Suite Visual Aids
- Docker Image Security in 5 Minutes or Less
- Extracting SSL Ports From Nessus Exports
- Day 45: tcpdump, a digital predator capable of giving low-level hackers god-like powers
- Remote Code Execution with Groovy console in Jenkins & Jenkins Groovy Console cmd runner
- Bug Bounty Diaries – Week III – CSRF
- Day 43: Reverse Shell with OpenSSL
- RogueOne: Creating a Rogue Wi-Fi Access Point using a Raspberry Pi

Writeups

Challenge writeups

- Hacking With Frida — FridaLab #1
- RFI to RCE Challenge By Zixem (Writeup)

Pentest writeups

- X Forwarded for SQL injection
- Exploiting XSS via Markdown
- A short tale of Session Fixation
- OSGi Console – Gateway to (s)hell

- A tale of a widespread wide CSRF vulnerability

Responsible disclosure writeups

- How I Found Stored XSS in Thousands of Sites under Typepad
- Oracle MAF store bypass, a how-to
- Achieving remote code execution on a Chinese IP camera
- Unauthenticated Blind SSRF in Oracle EBS
- Don't Give Me a Brake – Xiaomi Scooter Hack Enables Dangerous Accelerations and Stops for Unsuspecting Riders
- Privilege Escalation in Ubuntu Linux (dirty_sock exploit)

Bug bounty writeups

- IDOR on Facebook ($15,000)
- Information disclosure on private program ($241.93)
- Subdomain takeover via HubSpot still possible
- Rate limiting bypass on private program
- Privacy violation on Twitter ($1,120)
- Authentication bypass on Dovecot ($1,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Aurebesh.js: Translate JavaScript to other writing systems
- Gorsair: A penetration testing tool for discovering and remotely accessing the exposed Docker APIs of vulnerable Docker containers
- Hasherbasher: SQL injection via bruteforced MD5 hash reflection of random strings
- Dnsdmpstr: Unofficial API & Client for dnsdumpster.com and hackertarget.com. Wrapper around only their free IP tools. Quick & lazy enumeration in one command

More tools, if you have time

- Vhost-finder: Virtual host finder made in PHP
- Uptux: Privilege escalation checks for Linux systemd
- Chashell & Introduction: Reverse Shell over DNS

- CookieMonster: C# tool for extracting cookie and credential data from browsers (currently only Google Chrome)
- SecureCodeBox: A docker based environment for continuous security scans. Out of the box upport for Nmap, Nikto, SSLyze, SQLMap, Arachni, WPScan & Amass (also compatible with Burp Suite)
- Freevulnsearch: Free and open NMAP NSE script to query vulnerabilities via the cve-search.org API
- Pubsploit.py: Quick and dirty script to search for public exploits based on a CVE
- Get-NetNTLM: Powershell module to get the NetNTLMv2 hash of the current user. "RCE as a low priv user and no credentials? Use Get-NetNTLM to get a crackable NetNTLMv2 hash"
- Napper-for-tpm: TPM vulnerability checking tool for CVE-2018-6622. This tool will be published at Black Hat Asia 2019

Misc. pentest & bug bounty resources

- Cloud-metadata-services: List of metadata service endpoints for different cloud providers for your pentesting needs
- IoTsecurity101: Telegram channel
- Database Hardening Best Practices: Might be useful to IT security auditors
- NetSec Focus: A community for Cybersecurity / IT professionals

Challenges

- LUN.game
- CTF where you have to find the targets online using @shodanhq or similar tools
- RIPS Technologies source code analysis challenge (answers in the Tweet's comments)

Articles

- HTTP Strict Transport Security: Five common mistakes and how to fix them
- Notes from Overthewire Bandit
- Lets talk about email spoofing and prevention (Alt: "That's not how SPF works...."): Learn about SPF, DKIM & DMARC
- I scanned the whole country of Austria and this is what I've found: IP cameras, printers, industrial controls to name a few
- Why any encryption backdoor would be a threat to online security
- Thunderson's Journey To The OSCP
- Under Cover of Darkness: Advice on physical penetration testing

- What is the best fuzzer (automated software testing tool) to find 0-days? Why? Quora Answer

News

Breaches & Vulnerabilities

- 620 million records from 16 websites listed for sale on the Dark Web: Another reminder to use 2FA & a password manager
- Email provider VFEmail's US servers wiped: "@VFEmail is effectively gone. It will likely not return"
- Hackers Find New Ways to Use .EXE File Against macOS to Launch Malware that Bypass Protection & Steal Data: Bypassing Mac security to deliver payloads via .exe files
- Downgrade Attack on TLS 1.3 and Vulnerabilities in Major TLS Libraries: Someone already pwned TLS 1.3!
- Chinese facial recognition database exposes 2.5m people
- Major Container Security Flaw Threatens Cascading Attacks: "A fundamental component of container technologies like Docker, cri-o, containerd and Kubernetes contains an important vulnerability that could cause cascading attacks"

Malicious apps/sites

- Facebook Login Phishing Campaign
- First Android Clipboard Hijacking Crypto Malware Found on Google Play Store
- Your Lenovo Watch X Is Watching You & Sharing What It Learns

Other news

- Use an 8-char Windows NTLM password? Don't. Every single one can be cracked in under 2.5hrs: If you use 8 characters passwords anywhere, change them ASAP!
- Which countries have the worst (and best) cybersecurity?
- Microsoft Advises Users to Stop Using Internet Explorer Browser: Microsofy recommends to stop using Internet Explorer, it's a compatibility solution
- Trusted Types help prevent Cross-Site Scripting: New experimental API by Google to prevent DOM XSS
- Penetration testing of corporate information systems: statistics and findings, 2019: "Attempts to breach the network perimeter and obtain access to LAN resources were successful in 92 percent of external pentests"
- New Offensive USB Cable Allows Remote Attacks over WiFi
- Apple fighting pirate app developers, will insist on 2FA for coders

- China's cybersecurity law update lets state agencies 'pen-test' local companies

Non technical

- The Ultimate Guide To Memorable Tech Talks & Key takeways
- When you can't do awesome things, because of crushing bureaucracy
- Researcher Spotlight: Ambassador Alyssa Herrera
- Q&A with Winter Hack4Levels Winner: Mohamed

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 01/25/2019 to 02/01/2019.

Curated by Pentester Land & Sponsored by Intigriti

Sign up for the newsletter here.