Bug Bytes #36 – Hacking a University, XSS to RCE & Bypassing LinkedIn Rate Limits

BY INTIGRITI · SEPTEMBER 17, 2019 · LAST UPDATED ON JULY 30, 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.

This issue covers the week from 06 to 13 of September.

Our favorite 5 hacking items

1. Video of the week

> "Hacking Gotham University"

Watch @uraniumhacker hack a fake university for 2 hours. The vulnerable subdomains (and ports) don't seem to be up anymore, but it's an excellent walkthrough on hacking Web apps and APIs. @uraniumhacker explains his methodology, what to look for at each step, how to exploit bugs like SSRF on Jira, IDOR, RCE, how to take notes with screenshots and proofs during the whole pentest process, etc.

2. Writeup of the week

> "Exploiting File Uploads Pt. 2 – A Tale of a $3k worth RCE **($3,000)**"

This is a great walkthrough of a blind XSS found in a file upload functionality. It is really well-written and encompasses many interesting takeaways:

- The file upload functionality had only client-side validation. It was possible to upload files with arbitrary extensions by modifying the upload request in Burp.
- The server returned a 500 error, but it was misguiding since the file was listed as uploaded anyway.
- @HackerOn2Wheels uploaded an HTML file that included a blind XSS payload (using XSS Hunter). Since the payload fired, it meant that he could have uploaded an EXE file and obtained a reverse shell! So the blind XSS was proof of potential RCE.
- Explaining this bug's impact was instrumental in convincing triage to fix the bug and getting a good bounty. Risk isn't always so obvious!

3. Article of the week

> "Bypassing LinkedIn Search Limit by Playing With API"

Adam Leos found a bug in LinkedIn that allows for getting more search results than what is normally allowed for a free account. Basically, the API returns more information than what is visible to the user and you can query it directly to bypass any limits.
LinkedIn hasn't fixed this, so the technique and extension Adam provides could be very helpful for OSINT and recon.

4. Resource of the week

> "OWASP API Security Top 10"

OWASP released the API Security Top 10 Release Candidate. The final version will not be available before September 26, but everyone is welcome to share any feedback or even disagreement before the official version is released. Also, pentesters might want to start adapting their report templates or checklists.
The two documents you want to read are the Top 10 PDF and the presentation slides.
Among the 10 categories, some are common with the OWASP Top 10 2017. Others are specific to APIs like Mass Assignments, Improper Assets Management and Lack of Resources & Rate Limiting.

5. Tutorial of the week

> "Stealing JWTs in localStorage via XSS"

This is a short introduction to JSON Web Tokens (JWT), how they compare to cookies, and how you can exploit an XSS to steal them.
This is basic stuff but it could be helpful for beginner pentesters/bug hunters who are short on time and want to quickly learn a practical way for increasing XSS impact.

Other amazing things we stumbled upon this week

Videos

- 09/01/2019 – Live Bug Bounty Recon Session on Yahoo (Amass, crts.sh, dirsearch) w/ @TheDawgyg
- HackerOne Hacker Interviews: Alex (ajxchapman)
- TomNomNom Repeatedly Fails at Writing JavaScript
- My Entrepreneurial Journey – Episode 5: The Subtle Art of F*cking Up
- Nine hours of hacking and $375,000 in bounties (HackerOne H1-4420 – Uber)
- Burp for Beginners: A practical intro to help you find your first bug
- Null Ahmedabad August 2019 meetup – Metasploit in nutshell by Swar Shah

Podcasts

- Webcast 20190908 – #20 with @s0md3v
- Security Now 731 – DeepFakes
- Risky Business #555 — Bluekeep Metasploit module released, Paige Thompson pleads not guilty and more
- HNN #233
- ASW #75 – Bugs, Breaches, & More
- How They Got Hacked Episode Twenty 25

- Strangest Phishing Lures of 2019: From Divorce Papers to Real Estate Decoys

Webinars & Webcasts

- Owning Your PC Through An Innocuous USB

Conferences

- BSidesMCR 2019
- From Villains to Heroes: The Hacking Evolution [HackerOne]

Slides only

- Out of Sight, But Within Reach: Utilizing The Hidden Treasures in Web Apps
- Radare2 and Frida in the OWASP Mobile Security Testing Guide
- DerbyCon 9 slides, especially:
  - Red Team Methodology – A Naked Look
  - Assumed Breach: A Better Model for Pen Testing

Tutorials

Medium to advanced

- Serverless Blind XSS hunter with Cloudflare Workers
- Run PowerShell without Powershell.exe — Best tools & techniques
- Maintaining Azure Persistence via Automation Accounts
- DNS Spoofing on Kubernetes Clusters
- Microsoft Exchange series: NTLM Relay, Mailbox Post Compromise, Code Execution & ACL

Writeups

Pentest writeups

- PreAuth RCE on Palo Alto GlobalProtect Part II (CVE-2019-1579)
- SnakeYaml Deserilization exploited
- Hacking Mandated Apps

Responsible(ish) disclosure writeups

- Web tracking via HTTP cache cross-site leaks
- OpenEMR 5.0.1(6) – RCE and XSS

Bug bounty writeups

- Information disclosure on Uber ($6,500)
- Information disclosure on HackerOne ($500)
- DOM XSS on Shopify ($500)
- Reflected XSS on Shopify ($1,750)
- IDOR & Account takeover on Uber ($6,500)
- Information disclosure
- Stored XSS & SQL injection
- Authentication bypass & IDOR on Verizon Media
- An Accidental SSRF Honeypot in Google Calendar

See more writeups on The list of bug bounty writeups.

Tools

- shhgit: Find secrets & sensitive files across GitHub code & Gists committed in near real time by listening to the GitHub Events API
- PyScripter-er: A framework built on top of Burp's Python Scripter extension
- Jsearch: A Python script that greps info from javascript files (like AWS endpoints, api URLs...)
- Kicks3: S3 bucket finder from html,js and bucket misconfiguration testing tool
- XSS-flare: XSS hunter on cloudflare serverless workers
- Enumeration-Script: Bash Enumeration Script
- Social Mapper: A Social Media Mapping Tool that correlates profiles via facial recognition
- fileGPS: A tool that help you to guess how your shell was renamed after the server-side script of the file uploader saved it
- SharpSniper: Find specific users in active directory via their username and logon IP address
- Sepriv: Tool to manage user & process privileges
- BOtB: A container analysis and exploitation tool for pentesters and engineers

Misc. pentest & bug bounty resources

- OSCP & Bug bounty notes
- A practical guide for Red Teams and Offensive Security
- MITM cheatsheet

- Information security resources for laypeople

Challenges

- 44CON CTF 2019
- XSS challenge by @SecurityMB
- Wordy challenge (VM)

Articles

- Using Burp Suite's Cookie Jar for Java Web Tokens
- JWT Exfiltration Optimization & Blind MySQLi
- Securing React Native Apps
- A Brief Comparison of Reverse Image Searching Platforms
- Pass-The-Hash with RDP in 2019
- Quiet in the Windows: Dropping Network Connections & Invoke-DropNet
- MacOS Red Teaming 208: macOS ATT&CK Techniques
- Kubernetes Pod Escape Using Log Mounts

News

Bug bounty & Pentest news

- The end is nigh: Browser-makers ditch support for aging TLS 1.0, 1.1 protocols
- CSRF is (really) dead...or is it?
- Microsoft is finally taking a stance against NTLM relaying to LDAP, by enforcing LDAP signing and channel binding by default starting January 2020
- Meet three Indian ethical hackers who made over $40,000 each in 2018 from bug bounties
- Intigriti Hackademy

Reports

- IoT security concerns raised as researchers detect massive increase in malicious traffic
- Threats to macOS users
- Flashlight Apps on Google Play Request Up to 77 Permissions

Vulnerabilities

- iPhone iOS 13 Lockscreen Bypass Flaw Exposes Contacts: “The issue got closed in mid-August, Apple had promised me a gift in rewarding for the reports, but finally I didn’t get anything, only a thank you”
- Serious vulnerabilities in popular Netgear router can crash your device
- Google To Fix Malicious Invites Issue For 1 Billion Calendar Users
- WordPress XSS Bug Allows Drive-By Code Execution
- E-voting intrusion test: Swiss Post bug bounty moderator tallies submissions
- Telnet Backdoor Opens More Than 1M IoT Radios to Hijack

Breaches & Attacks

- Intel: SSH-stealing NetCAT bug not really a problem
- 1B Mobile Users Vulnerable to Ongoing ‘SimJacker’ Surveillance Attack
- Instagram Confirms Security Issue Exposed User Accounts And Phone Numbers—Exclusive
- Leaky database full of fake Groupon emails turns out to belong to crooks
- “The Russians are advanced, the Chinese are persistent, and the Israeli’s are the actual threat.”

Malicious apps/sites

Other news

- From pen-test to penitentiary: Infosec duo cuffed after physically breaking into courthouse during IT security assessment
- Shortcomings in approval process for Extended Validation certificates exposed
- North Korean Hackers Behind WannaCry and Sony Hack Sanctioned by USA
- Google Unveils DNS-over-HTTPS (DoH) Plan, Mozilla’s Faces Criticism
- The year-long rash of supply chain attacks against open source is getting worse

Non technical

- When corporate communications look like a phish
- Never feel overwhelmed at work again: how to use the M.I.T. technique
- 190 universities just launched 600 free online courses. Here’s the full list.

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 09/06/2019 to 09/13/2019.

Curated by Pentester Land & Sponsored by Intigriti

Disclaimer:
The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com