Bug Bytes #45 – DEFCON 27 Recap, JWT Playbook, Leaky repo & new XSS challenge

BY INTIGRITI · NOVEMBER 19, 2019 · LAST UPDATED ON JULY 30, 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.

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

Intigriti news

We launched another XSS challenge! You can win a Burp Suite Pro license if you solve it before Monday. Check it out:

> **"We're celebrating 10K followers with a challenge!**
> **Find the XSS flaw and WIN a @burp_suite license!**
> **Challenge: https://t.co/dYnctSfAAq**
> **More info: https://t.co/CllyXhC7oL pic.twitter.com/lRfN0wndkl**
>
> **— Intigriti (@intigriti) November 18, 2019"**

Our favorite 5 hacking items

1. Conference of the week

> "DEF CON 27"

Finally, DEF CON 27 videos are released! There is no introduction needed, right?
I'm watching this first: "Owning The Clout Through Server Side Request Forgery" by @NahamSec & @daeken. What about you?

2. Resource of the week

> "JWT Attack Playbook (for methodical pentesting)"

This is a wiki for the [jwt_tool](https://github.com/ticarpi/jwt_tool) toolkit for testing JSON Web Tokens. I was surprised to see how detailed it is.
It explains everything from recognizing and reading JWTs, an attack methodology, how to test for known exploits, fuzzing, stealing JWTs by exploiting other vulnerabilities, and more. An excellent resource to get into hacking JWTs!

3. Challenge of the week

> "Leaky repo"

This Github repository has many vulnerabilities. It is intended to be used as a target for benchmarking tools like github-dorks or truffleHog.
Personally, I also plan on using it as a challenge to practice finding secrets on Github.

4. Non technical item of the week

> "Tips for an Information Security Analyst/Pentester career – Ep. 78 – Nothing is impossible"

This is @mattiacampagnan's story on how he found a pentesting job. Basically, he created a blog and wrote dozens of articles related to penetration testing. This gave him some exposure. A company contacted him for an interview, he got a remote part-time position, did the work for 3 months, and finally it became a full-time position.
I loved reading this story because it is another reminder that there is no secret way to success. Do your work and find a way to differentiate yourself. Simple, but a lot of people do not want to hear that...
I personally can attest to the same thing: Maintaining a blog and being consistent opens up so many possibilities and professional options. If you are struggling to find work, you should really consider starting a blog, video course or Youtube channel. Anything that you put out there that shows technical abilities and professionalism will help you find employers or customers.

5. Tutorials of the week

> "– Fasten your Recon process using Shell Scripting
> – Different Approaches For Reconnaissance — Bug Bounty's"

These are two nice tutorials that go a bit further that most typical recon articles.
Apart from classic subdomain enumeration, they show how to programmatically fetch URLs with their status code & page title, and search results for keywords. This will certainly aid process data collected from large scope bug bounty programs (or pentest targets).

Other amazing things we stumbled upon this week

Videos

- Live Bug Bounty Recon Session on Verizon Media's Yahoo.com with @0xteknogeek
- Bounty Thursdays – Live from HackerOne's H1213 with (STÖK, Nahamsec, TomNomNom, BugbountyHQ)
- I did a live QA about hacking and bug bounties!
- RECON with random internet ip addresses & BUG Bounty (Playing around RECON/METASPLOIT/SSH)
- Whitebox pentesting and exploit development
- SQL and XSS Vulnerability Code Review [25] #CodeReview
- 10 Minute Tip: Using Web Developer Tools with Instagram and Pinterest for OSINT

- Password Spraying – Kerberos, LDAP, SMB – Mitre T1110
- Red Team Operations with Cobalt Strike (2019): Free course on course on Adversary Simulations and Red Team Operations using Cobalt Strike 4.0
- Linux Essentials For Hackers
- Complete bug bounty tutorial of 2019 – common web attacks for beginners
- Breaking Stigmas: Teaching Porn Stars Ethical Hackin

Podcasts

- InfoSec Career Podcast – Episode 4: Interview with Ed Skoudis
- Security Now 740 – Credential Delegation
- Darknet Diaries EP 51: The Indo-Pak Conflict
- Risky Business #562 — Two former Twitter staff charged over Saudi spying

Webinars & Webcasts

- SANS Dark Web Solutions Forum – Illuminating the Dark Web: Harvesting and Using OSINT Data from Dark Web Resources (Free registration required)
- Successful Infosec Consulting: Lessons from Three Decades in The Field (Free registration required)
- Getting into Security
- Pen-testing with Phillip Wylie

Conferences

- BSidesCT 2019 Videos

Slides only

- How I use weapons!
- Conclusions from Tracking Server Attacks at Scale
- DEF CON 26 Workshop – Attacking & Auditing Docker Containers Using Open Source
- Why Johnny Still Can't Pentest: A Comparative Analysis of Open-source Web Application Vulnerability Scanners
- How I met your browser
- A Post-Exploitation tale (in real life)

Tutorials

Medium to advanced

- Exploiting SQL Server Global Temporary Table Race Conditions
- Rainy Day Windows Command Research Results
- Hacking Python Applications
- RdpThief: Extracting Clear-text Credentials from Remote Desktop Clients & RdpThief
- Persistence – Accessibility Features
- From arbitrary file overwrite to SYSTEM

Beginners corner

- All You Need to Know to Search like a Pro on Instagram
- Banner Grabbing: Top Tools and Techniques Explained
- Creating a pocket pentest platform with P4wnP1: Part 1
- Configuring Frida with BurpSuite and Genymotion to bypass Android SSL Pinning
- Extracting Kerberos Credentials from PCAP

Writeups

Responsible(ish) disclosure writeups

- Story Behind Spoyl Data Leak !!! #Web
- Sendy is Insecure: How Not to Implement reCAPTCHA #Web
- Microsoft Edge – Local File Disclosure and EoP #Web #Browser
- Exhibitor UI command injection vulnerability #RCE #Web
- CVE-2019-1405 and CVE-2019-1322 – Elevation to SYSTEM via the UPnP Device Host Service and the Update Orchestrator Service #PrivilegeEscalation #Windows
- Ghost Potato #Windows #NTLM

Bug bounty writeups

- Blind SSRF due to Sentry Misconfiguration ($300)
- Broken API authorization ($440)
- Caching & CORS issue on Chromium
- SSRF Using DNS Rebinding

- DoS via Commit Hash Collisions on GitHub ($5,000)
- CSS injection on Slack ($500)
- Massive XS-Search over multiple Google products
- XXE on Starbucks ($4,000)
- OS command injection on Starbucks ($4,000)
- Information disclosure on HackerOne ($1,000)
- LFI via MySQL on Infogram
- SSRF in Python (IBB) ($500)
- XSS on WordPress ($350)

See more writeups on The list of bug bounty writeups.

Tools

- CSVPretty: Pretty print csv files
- Gplaycli: Google Play Downloader via Command line
- Projectdiscovery.io & Reconnaissance – The way it should be: Automated asset recon and monitoring solution
- Automated-Scanner: Trying to make automated recon for bug bounties
- Rsdl: Subdomain Scan With Ping Method
- HostInjector: Multithreaded Host Header Redirection Scanner
- Diggy: Extract endpoints from apk files
- Monitorizer: The ultimate subdomain monitorization framework
- Nmap-diff.sh & Network monitoring with nmap
- tfsec:Static analysis powered security scanner for your terraform code
- Recon tools: Bash script to automate running subdomain enumeration, screenshots and directory enumeration tools
- SCShell: Fileless lateral movement tool that relies on ChangeServiceConfigA to run command
- Hackbar Java Version

Misc. pentest & bug bounty resources

- WP-XSS-Admin-Funcs: JavaScript functions intended to be used as an XSS payload against a WordPress admin account

- Notes for @thecybermentor's Beginner Network Pentesting Course
- Helm Security Audit Report by Cure53
- Tale of the dubious crypto
- New on Web Security Academy: Cross-origin resource sharing (CORS)

Challenges

- GitHub Security Lab 'Capture The Flag' challenges
- otp_vulnerable_app
- Great little intro challenge for those that want to get into geolocation osint
- Can you spot the vulnerability? (RIPS PHP challenge)
- CSP bypass challenge: csp.xss.stackchk.fail
- Intigriti XSS challenge

Articles

- Modern Wireless Tradecraft Pt III — Management Frame Access Control Lists (MFACLs) & Pt II — MANA and Known Beacon Attacks
- When Kirbi walks the Bifrost & Bifrost
- Hunting for LoLBins

News

Bug bounty & Pentest news

- Sounds like AWS fixed @albinowax's HTTP request smuggling issues in ALBs on Monday
- @ChloeMessdaghi and @Alyssa*Herrera* have started a bug bounty team that has over 100 women members from all levels. Interested in bug bounty and want to hack with some amazing people? DM @WomenHackerz to join!
- If you need a primer on the Coalfire Pentester situation, read this.
- GitHub's latest security announcements are quite impressive. Deploying Semmle's CodeQL, streamlined disclosure, CVE requests, exposed token scans (+ automated revocation), and more.
- Supporting the Source: Why HackerOne is Upgrading its Free Tools for Open Source
- Great news: AutoChrome is back to a working state, thanks to Marmelatze's work

Reports

- IoT security: Bug bounties a vital last line of defense, academic study suggests
- Healthcare security report: Organizations face 'uphill battle' against cybercriminals

Vulnerabilities

- Just-Released Checkra1n iPhone Jailbreak Stirs Security Concerns
- Popular Android phones can be tricked into snooping on their owners
- [CVE-2019-11931: A stack-based buffer overflow could be triggered in WhatsApp by sending a specially crafted MP4 file to a WhatsApp user]
- Multiple XS-Leak issues fixed in Google products
- Microsoft fixes IE zero-day in November Patch Tuesday

Breaches & Attacks

- Spam campaign uses 'double-loaded' ZIP to smuggle malware onto Windows devices
- Iranian hacking group built its own VPN network
- Breach affecting 1 million was caught only after hacker maxed out target's storage
- The Ukrainian Power Grid Was Hacked Again

Other news

- National Cyber League: Ethical hacking competition enters fall season with a bang
- Government Must Have Reasonable Suspicion of Digital Contraband Before Searching Electronic Devices at the U.S. Border
- This Bank Had the Worst Password Policy We've Ever Seen
- DNS over HTTPS: What, Why, & Who Cares
- Apple vs Corellium

Non technical

- Getting your 1st Information Security (InfoSec) job
- YyesWeHack Prophile ON Zseano
- We are Michael Coates and Rich Mason. We have served as Chief Information Security Officers at Twitter and Honeywell. Ask us anything about becoming a CISO.

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 11/08/2019 to 11/15/2019.

*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***