Bug Bytes #47 – SecTalks, My First RCE, Smuggler.py and interview with @0xacb

BY INTIGRITI · DECEMBER 5, 2019 · LAST UPDATED ON MARCH 6, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.

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 22 to 29 of November.

Our favorite 5 hacking items

1. Conference of the week

> "SecTalks Live 2019 – The Changing Landscape of Web Tooling \| Questions? !questions & @xyantix's notes"

This is recap by @codingo_ of the latest changes in open source Web security tooling. Categories discussed are scaling, directory brute forcing, XSS subdomain discovery, API keys and build logs, and cloud based services.

With the year ending, it is nice to stop and reflect on the state of our tools. Better ones with more features and attack techniques are released all the time. Following the trends is necessary to avoid using outdated tools.

2. Writeup of the week

> "My first RCE: a tale of good ideas and good friends"

Alternative title: How to go from beginner to RCE using basic automation.

If you feel that critical bugs and automation elude you, this is the writeup for you! It is very well written and present a step-by-step guide that you could follow for finding different types of bugs.

3. Tools of the week

> "– Smuggler.py
> – Corsy
> – Jaeles & Documentation"

The common theme for these tools is automation.

Smuggler.py is for testing a list of URLs for HTTP request smuggling.

Corsy is a CORS misconfiguration scanner (with currently 10+ checks).

Jaeles is a framework in Go for building your own Web Application Scanner. I have not tested it yet, but it looks powerful and easy to use. You can add signatures for new tests and integrate it with Burp.

4. Non technical item of the week

> "Joplin"

I've been on a quest for the perfect note-taking app for years. Some of the criteria I'm looking for are: Web Clipper, supports multiples OSes including Linux, mobile apps available, automatic synchronization and backups ideally with self-hosted server, markdown, and possibility to encrypt notes.

Evernote was good especially for its Web Clipper and mobile apps, but it does not have a Linux version.

Laverna was impractical and lacked basic features like searching inside notes.

SwiftnessX can be very useful for creating pentest templates, checklists and payload lists. But it does not have markdown and I found it not suitable for being used as a full knowledge base app.

QOwnNotes was a good candidate that I used for months. But it had an annoying bug (cursor moving by itsef while I was writing notes).

So, when Alexandre Dulaunoy tweeted about Joplin, I instantly installed it. It has all the features I'm looking for, even a Web Clipper and mobile apps! I also like that you can change the layout (whether to display markdown text, rendered markdown, or both).

Only time will tell, but this looks like the perfect note-taking app for me!

5. Webinar of the week

> "Accelerate Your Career By Building FIVE Critical Professional Skills"

Ted Demopoulos offers great advice in this webinar, for both people who want to become entrepreneurs or move up the corporate ladder.

You probably have already heard some of these things. But it is good to hear the reminder and detailed tips from someone who has 20+ years of experience as an independent consultant.

Other amazing things we stumbled upon this week

Videos

- @0xacb talks about getting RCE on Shopify and Valve, CTF, reverse engineering and bug bounties!
- ZAP in Ten
- Bug Bounty Tips: Amass Recon Tool
- Finding Your First Bug: Choosing Your Target

- Whoami: My Bug Bounty Story
- Recon-ng V5
- Live Recon Stream #2 (by @jhaddix)
- Burp Suite Pro Walkthrough
- Zero-day vulnerability in Bash – Suidbash Google CTF Finals 2019 (pwn)
- Presentation and Social Media tips with SheHacksPurple
- Sunday Cyber Show with Magda Chelly – Episode2

Podcasts

- Security Now 742 – Pushing "DoH"
- Risky Business #564 — PRC suffers leak, alleged defection
- Darknet Diaries EP 52: Magecart
- Application Security Weekly #86
- Paul's Security Weekly #628 – Coalfire Incident & DerbyCon Communities
- Paul's Security Weekly #628 – The Marvel Universe
- HAck Naked News #243

Webinars & Webcasts

- How to perform API testing – LIVE!
- Awareness Con 2019 – Adel, IA

Conferences

- BSides CT 2019

Slides only

- Adversarial Emulation – WWHF
- Building your Car Hacking Labs & Car Hacking Community from Scratch
- How to Train Your Red Team (for Cloud Native) & related resources

Tutorials

Medium to advanced

- [55] – 27.11.2019 – Attacking JWT consumers with Burp and JWT4B
- The power of variant analysis (Semmle QL) CVE-2019-15937 and CVE-2019-15938
- How to start penetration testing with a Windows VM
- Attacking FreeIPA — Part I Authentication
- Linux for Pentester: Perl Privilege Escalation
- Using and Abusing Aliases with PowerShell
- macOS Red Team: Spoofing Privileged Helpers (and Others) to Gain Root

Beginners corner

- Hacking WebSocket
- Flan Scan – The New Vulnerability Scanner from Cloudflare
- Google Exposed Firebase Database & Firebase
- Exposed Log and Configuration Files
- Multiple Methods to Bypass Restricted Shell
- Gab OSINT Techniques & Github repo
- Get Root with Metasploit's Local Exploit Suggester

Writeups

Challenge writeups

- EGCTF 2019 — Secure Document Portal
- Intigriti 10k followers XSS challenge,

Pentest writeups

- Demonstrating Impact of Penetration Testing to Board (BIG Guys!) | Importance of POST EXPLOITATION
- Argument injection and getting past shellwords.escape

Responsible(ish) disclosure writeups

- Report: We Tested 5 Popular Web Hosting Companies & All Were Easily Hacked #Web
- The De-anonymization of the Technion Confessions Admin #Web
- Getting Malicious Office Documents to Fire Without Protected View #Phishing
- Weak encryption cipher and hardcoded cryptographic keys in Fortinet products #Crypto

- Xiaomi Mi6 WiFi Captive Portal Remote Code Execution (Pwn2Own 2018) #Wifi #Android
- Xiaomi Mi6 Browser Remote Code Execution (Pwn2Own 2018) #RCE #Android

Bug bounty writeups

- Padding oracle / Account takeover
- Privilege escalation on GitLab ($12,000)
- Reflected XSS on Facebook ($5,000)
- DOM XSS on Razer ($250)
- CORS misconfiguration, Open redirect, Reflected XSS & Session management flaw ($1,500)
- OAuth flaw on Discord

Tools

If you don't have time

- Peasant: LinkedIn reconnaissance tool
- Asnip: ASN target organization IP range attack surface mapping for reconnaissance, fast and lightweight

More tools, if you have time

- Tplmap: Server-Side Template Injection and Code Injection Detection and Exploitation Tool
- DockerPwn.py: Python automation of Docker.sock abuse
- Heimdall: Tool to distribute scanning and recon activities across multiple parallel cloud services
- Mongot: Easily connect to open MongoDB and dump data
- Nessus Map: Parse .nessus file(s) and shows output in interactive UI
- rotaTOR: Bash script to change TOR ip – timer based
- Andor: Blind SQL Injection Tool in Go
- T1tl3: A simple python script which can check HTTP status of branch of URLs/Subdomains and grab URLs/Subdomain title
- Actarus: A custom tool for bug bounty in Symfony
- Cypheroth: Automated, extensible toolset that runs cypher queries against Bloodhound's Neo4j backend and saves output to spreadsheets

Misc. pentest & bug bounty resources

- Bug Bounty Playbook ($24.99)
- Awesome Android Application Security
- API wordlist by @NahamSec
- Top 10 vulnerable websites for penetration testing and ethical hacking training
- SQL Injection Payload List, RFI/LFI Payload List & XML External Entity (XXE) Injection Payload List
- Kali Linux Tutorials
- Genesis: A framework to generate unique test cases that are mapped to the MITRE ATT&CK framework
- APIsecurity.io Issue 59: Vulnerabilities in Fortinet, Truecaller, Nykaa Fashion, SMA M2 smartwatch
- Awesome CyberSecurity
- personal-osint

Challenges

- Java Security Calendar 2019 #CodeReview
- [Advent of Cyber] Get Started With Cyber Security In 25 Days

Articles

- Cached and Confused:Web Cache Deception in the Wild
- The Pen Testing Tools We're Thankful for This Season
- #ProTips: Silence the noise with Andrew Morris
- What's Changed in Recon-ng 5.x
- Code Review 101
- Tenable Nessus tips and tricks
- The Short History of Unauthenticated Site Options Update Vulnerabilities

News

Bug bounty & Pentest news

- 2019 CWE Top 25 Most Dangerous Software Errors
- I'm going to start picking some random people out of the @Bugcrowd discord each Friday (Australia time) to do some 1:1 training with

- DHS Mandates Federal Agencies to Run Vulnerability Disclosure Policy
- Kali Linux 2019.4 Release: Undercover mode to impersonate Windows 10, PowerShell, NetHunter Kex...

Reports

- Exploit kits are slowly migrating toward fileless attacks
- Almost 60% Of Malicious Ads Come from Three Ad Providers

Vulnerabilities

- Internal Kaspersky API still exposed to websites, alleges researcher
- Cheap kids smartwatch exposes the location of 5,000+ children
- Fortinet took 18 months to strip software of flawed crypto cipher and keys
- Exploit code published for two dangerous Apache Solr remote code execution flaws
- Lights That Warn Planes of Obstacles Were Exposed to Open Internet
- Dozens of VNC Vulnerabilities Found in Linux, Windows Solutions

Breaches & Attacks

- Hotel front desks are now a hotbed for hackers
- Two third-party SDKs allowed secret harvesting of Twitter and Facebook user data
- A hacking group is hijacking Docker systems with exposed API endpoints

Other news

- Cloudflare releases 'Flan Scan' tool to the masses... infosec backlash ensues
- This App Will Tell You if Your iPhone Gets Hacked
- HPE tells users to patch SSDs to prevent failure after 32,768 hours of operation
- Apple-Corellium lawsuit raises concerns among security research community
- From July to September 2019 Google sent more than 12,000 warnings to users in 149 countries that were targeted by government-backed attackers. 90% were credential stealing phishing mails.
- The RIPE NCC has run out of IPv4 Addresses
- Web trackers using CNAME Cloaking to bypass browsers' ad blockers

Non technical

- How to Become a Web Pentester

- A decade of hacking: The most notable cyber-security events of the 2010s
- Christmas socialising, Goodwill to all, and keep your devices safe
- The Best Christmas Presents for Hackers in 2019
- Hacker Holiday Gift Guide (HHGG) 2019

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 11/22/2019 to 11/29/2019.

*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***