Bug Bytes #51 – ArneSwinnen's secrets, Hunting in the Dark & OSINT movie picks

BY INTIGRITI · DECEMBER 31, 2019 · LAST UPDATED ON JULY 30, 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 20 to 27 of December.

Our favorite 5 hacking items

1. Video of the week

> "-@Arneswinnen Talks About Full Time Bug Hunting, Burp Suite Plugins, and Recon"

I haven't had the time to watch this whole video, but it is in my top work priorities given who the interviewee is.
@Arneswinnen literally made it rain bounties at Intigriti's 1337UP1119 live hacking event. The bugs he found were out of this world. So, it is awesome to get to know more about him, his thought process, how he manages bug bounty full-time while still having a life, etc.

2. Writeup of the week

> "– Microsoft Edge (Chromium) – EoP via XSS to Potential RCE
> – Hunting in the Dark – Blind XXE"

The first writeup might make you want to get into browser hacking. $40,000 for XSS on Microsoft Edge!
The Second writeup is about a blind XXE, how it was found and used for port scanning and identifying files existing on the target.
This serves as a great example of OOB attack, perfect for reading after this week's tutorial

3. Article of the week

> "A Phonetic Approach to Calculate Linguistic Information in Text"

This is really cool research by @s0md3v. He created an algorithm that detects valid linguistic data in a given text based on linguistics. In other words, it can differentiate between random and meaningful text.

From his benchmark, it is fast and more accurate that algorithms based on Shannon Entropy. But there is no need to understand the math to appreciate that the idea is very interesting for Web security testing. One useful application is finding API tokens scattered in strings, as shown in this demo.

4. Tutorial of the week

> "Out-of-band Attacks"

This is an good introduction to out of band attacks. It includes examples of blind XSS, blind SQL injection, blind command injection, SSTI, and also how to exfiltrate data using DNS.
It's worth reading if you want to learn about the OOB technique.

5. Non technical item of the week

> "OSINT Movie Time for the Holidays"

This is the first time I see a list about OSINT movies. It's a nice change from classic hacker movies.
I've also heard good things on "Don't f**k with cats" and Bellingcat's documentary. So, movies added to watchlist!

Other amazing things we stumbled upon this week

Videos

- "How to Get Started with Bug Bounty" – Resource Lists & Advice
- Advanced PHP Deserialization – Phar Files
- Hacking My Instagram Account
- Mastering Shodan Search Engine Filters – OSINT [5]

Podcasts

- Security Now 746 – A Decade of Hacks
- Darknet Diaries EP 54: NotPetya
- 7MS #393: Interview with Peter Kim
- 7MS #392: LAPS Reloaded
- The Privacy, Security, & OSINT Show 150-Password Managers Revisited
- Hacker Culture Roundtable
- Paul's Security Weekly #631 – Blue Team Tactics and Techniques & The State of Penetration Testing

Webinars & Webcasts

- Don't Patch – Transformative Security Programs go Beyond the Vulnerability (Free registration required)

- VyAPI with Riddhi
- Let's Talk About ELK Baby, Let's Talk about You and AD

Conferences

- Analysing vulnerabilities in Smart Contract – By Shrutirupa Banerjiee, During CyberFrat Pune Meet
- BlackAlps 2019, especially:
  - Google Bug Hunters – Eduardo Vela Nava
  - How To Find And Prevent Entire Classes Of Security Vulnerabilities – Sam Lanning
  - Blockchain Vulnerabilities And Exploitation In Practice – Nils Amiet

Tutorials

Medium to advanced

- Using Mozilla Rhino to Run JavaScript in Java: Useful if you want to create a @Burp_Suite extension that runs JavaScript
- Jailbreaking – Checkra1n Configuration
- How Unix Works: Become a Better Software Engineer
- 2FA Bypass Techniques — Only Checklists
- How to Pivot Into Target Network with SSH
- No Shells Required – a Walkthrough on Using Impacket and Kerberos to Delegate Your Way to DA
- DNS Beacon through DNSMasq Redirectors

Beginners corner

- Make Your Own Google Chrome Extension to Show WWW Again
- NetHunter Rootless — Official Kali NetHunter for non rooted phones
- Mail Security – SPF – WTF
- Guide To Using Reverse Image Search For Investigations
- Hacking Git Directories
- Source Code Analysis Race Conditions #CodeReview
- Automating BURP to find IDORs
- Would you notice if you are hacked this way?

- Email to Twitter account
- hackndo tutorials translated to English: BloodHound, Get credentials from remote lsass dumps & Pass the Hash
- DNS Admin Privesc in Active Directory (AD)(Windows)
- Crack WPA & WPA2 Wi-Fi Passwords with Pyrit

Writeups

Challenge writeups

- Write-up LEHACK19

Pentest writeups

- Pwning an outdated Kibana with not so sad vulnerabilities

Responsible(ish) disclosure writeups

- Cross-Site Scripting on a big bank's Payment Gateway
- WordPress DoS: Rediscovering an Unpatched 0-Day #Web
- CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') #Web
- Hackin' around the Christmas tree #IoT #Android
- Reversing Android firmware to get secret codes #Android
- CVE-2019-17556: Unsafe deserialization in Apache Olingo #Web #CodeReview
- NGINX error_page request smuggling #Web
- Firefox IOS QR Code Reader XSS (CVE-2019-17003) #IoS

Bug bounty writeups

- Effortlessly finding Cross Site Script Inclusion (XSSI) & JSONP for bug bounty
- From broken link to subfolder takeover on Bukalapak
- SOP Bypass via browser-cache ($1,500)
- How we hacked one of the worlds largest Cryptocurrency Website
- Airbnb : Steal Earning of Airbnb hosts by Adding Bank Account/Payment Method (IDOR) ($3,000)
- Bugbounty | A Dom Xss ($500)
- reCAPTCHA Exploits

- Disclosing privately shared gaming clips of any user on Facebook ($2,000)
- CRLF injection on Twitter ($2,940)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- KeyFinder: A tool that let you find keys while surfing the web
- Sr2t: Parse and convert Nessus, Nmap (and more tools) to XLSX, CSV
- Token-Hunter & Introduction: Gather OSINT from GitLab groups and group members. Inspect GitLab assets like snippets, issues, and comments/discussions for sensitive information like GitLab Personal Access Tokens, AWS Auth Tokens, Google API Keys, and much more.
- Ipconverter: Simple functions to add into .bashrc to convert Ip address into binary, hexadecimal, decimal, octal formats and viceversa
- Asscan: Automated Subnet Scanner

More tools, if you have time

- Burp Suite – Secret Finder: Burp Suite extension to discover apikeys/accesstokens and sensitive data from HTTP response
- Git-vuln-finder: Finding potential software vulnerabilities from git commit messages
- Aron: A GO script for finding hidden GET & POST parameters
- Buster: An advanced tool for email reconnaissance
- S3tk: A security toolkit for Amazon S3
- huskyCI: Performing security tests inside your CI
- Harpoon: A collection post-exploitation scripts for determining if that shell you just got is in a container, what kind, and ways to escape
- Mad-metasploit
- RProcDump: Remote process dumping automation. Use it to dump Windows credentials remotely and extract clear text with Mimikatz offline
- ACLight: A script for advanced discovery of Privileged Accounts – includes Shadow Admins

Misc. pentest & bug bounty resources

- The top 10 best pentesting tools and extensions in Burp Suite
- Automotive Cyber Security: An Introduction: Free online course, starts 20 January 2020

- Career Mastery™ Kickstart 2020: Free virtual summit that offers career tips and strategies. January 6 – 23
- Google Dorks
- JWT-Exploitation: Ruby script for automating JWT token generation for None Algorithm & RS256 to HS256, might come handy in CTFs & testing application/ APIs
- APIsecurity.io Issue 63: Microsoft and Google dropping Basic Auth, Thinkrace exposing 47mln+ devices
- Roadmap for Application Security
- Facebook Matrix: Formulas for Searching Facebook
- Top 5 Private Search Engines

Challenges

- 15 minute Web CTF by @GrahamBleaney

Articles

- Crossing The Borders : The illegal trade of HTTP requests
- Opening Up the Samsung Q60 series smart TV: For anyone interested in Smart TV hacking but not knowing where to start
- Building Android Spyware / Xombie APK
- Using WebRTC ICE Servers for Port Scanning in Chrome, Online demo, turnscan.js source & JSFiddle
- Mass Surveillance, is an (un)Complicated Business
- War Never Changes: Attacks Against WPA3's Enhanced Open — Part 2: Understanding OWE & Part 1: How We Got Here

News

Bug bounty & Pentest news

- The Empire (3.0) Strikes Back
- These are the kind of reports, which are very discouraging.
- CeWLer can now be built independently of CO2

Reports

- Living off the land: Attackers leverage legitimate tools for malicious ends

- The Rising Tide of E-commerce Fraud: Methods, Patterns, and Defensive Measures
- 2019 Global Security Attitude Survey

Vulnerabilities

- Google Chrome impacted by new Magellan 2.0 vulnerabilities
- Twitter Fixes Bug that Enabled Takeover of Android App Accounts
- A Twitter app bug was used to match 17 million phone numbers to user accounts

Breaches & Attacks

- Operation Wocao : Shining a light on one of China's hidden hacking groups & – Chinese Hackers Bypassing Two-Factor Authentication
- Canadian banks targeted in a massive phishing campaign
- Frankfurt shuts down IT network following Emotet infection
- Wyze Exposes User Data via Unsecured ElasticSearch Cluster
- Report: 267 million Facebook users IDs and phone numbers exposed online
- Twitter shuts down Saudi state-backed information operations

Other news

- Smartphone location data can be used to identify and track anyone
- Congress passes anti-robocall bill
- How Close Did Russia Really Come to Hacking the 2016 Election? & TL;DR
- Cisco Self-Signed Certificate Expiration on Jan. 1, 2020: What You Need to Know
- Serious Security: The decade-ending "Y2K bug" that wasn't
- No, Spotify, you shouldn't have sent mysterious USB drives to journalists
- The Hacker Who Took Down a Country
- 2020 Pentest Predictions: Platforms, Sprints, and Analytics
- Most useful gadgets of 2019
- Swig Security Review 2019: Part I & Part II
- The Cybersecurity Stories We Were Jealous of in 2019
- 30 years of ransomware: How one bizarre attack laid the foundations for the malware taking over the world

Non technical

- 7 types of virus – a short glossary of contemporary cyberbadness
- Defend Against SIM Swapping
- CTF Design Guidelines
- 4 Steps to Communicate Anything Clearly, According to a Scientist Who Teaches Quantum Physics to Kids
- Comparing Offensive Security Tooling and Gun Control
- Should there be restrictions on the release of hacking tools?
- Misconceptions Regarding "Offensive Security Tools"
- Ransomware: Towards an Economic Equilibrium

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 12/20/2019 to 12/27/2019.

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.

Curated by Pentester Land & Sponsored by Intigriti