Bug Bytes #5 -Lazy Hackers, Stök's blind XXE and Inception

BY INTIGRITI · FEBRUARY 12, 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. You can 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 01 to 08 of February.

Our favorite 5 hacking items

1. Conference of the week

> "A $7.500 BUG Bounty Bug explained, step by step. (BLIND XXE OOB over DNS)"

Another great video by @stokfredrik! It's a writeup for a blind XXE OOB over DNS using a PDF file upload. Classic file upload payloads & attacks didn't work, so the last thing that @stokfredrik tried was sneaking XML entities through PDF files. He was able to trigger a DNS request from the target server (using Burp Collaborator). He then escalated the attack over multiple stages until he got a full blind XXE.
This is pretty advanced stuff but every stage is detailed and well explained, including tools and references.

2. Writeup of the week

> "Reverse RDP Attack: Code Execution on RDP Clients"

Check Point researchers tested different RDP clients: rdesktop, FreeRDP and Mstsc.exe (Microsoft's RDP client). They found 25 security vulnerabilities.
This made the news on generic infosec sites because two of the clients tested are vulnerable to reverse RDP attacks. The bugs detected allow malicious RDP servers to get remote code execution on these clients...

3. Slides of the week

> "It's the Little Things II: Exploiting Vulnerabilities Through Proper Reconnaissance – Slides for Exploiting Vulnerabilities Through Proper Reconnaissance (ShellCon 2018) & Its the little things (Anycon 2018)"

This is a nice addition to existing public recon methodologies. It touches a little bit of everything: asset discovery, OSINT, content discovery, and more. It's worth reading and merging with your own current methodology.
Also, I'm not sure these are the right talks accompanying the slides, but they should at least give you some context around them:

- Exploiting Vulnerabilities Through Proper Reconnaissance (ShellCon 2018)

- Its the little things (Anycon 2018)

4. Tool of the week

> "Inception"

Imagine you want to test a list of targets from your previous bugbounty notes for one specific test, a new endpoint, an XSS payload, a search for a hidden file/directory (like .git)... What would you use?
Tools like Burp Intruder allow sending multiple requests to the same target. Inception does the opposite: test the same thing on a list of targets.
It's inspired from Snallygaster but includes more tests, is fast (because written in Go), and is highly customizable (new tests can be easily added without writing code).

5. Article of the week

> "The Lazy Hacker"

The author of this blog post, a professional pentester, shares some tidbits on his pentesting methodology and custom tools.
What's most intriguing/interesting is his framework "recron" which is an "automated continuous recon framework". He didn't release it but his explanations might give you new ideas for improving your own automated bug hunting tools.
Also, he shared his tool Scanomaly, a web application fuzzer scanner, which is part of that framework.

Other amazing things we stumbled upon this week

Videos

- Remote Code Execution on Electron Applications
- HackerOne Hacker Interviews – @cdl
- PHP: Bypass filters using less-than sign

> **"Bypass filters using < (less-than sign). A string consisting of two "less-than" signs when passed to the file_get_contents function gets replaced with an asterisk – only on Windows"**

Podcasts

- Hackable 24 – The Weakest Link
- Darknet Diaries Ep 31: Hacker Giraffe
- Absolute AppSec Ep. #45 – Sean Poris
- Security Now 700: 700 and Counting!
- Securiosity:What's going on with Derbycon?
- Sophos podcast Ep. 018 – Home invasions, snoopy apps and Android versus iOS [PODCAST]

- Hack Naked News #206 – RDP Servers, Mimikatz, & LibreOffice
- Getting Into Infosec: Nipun Gupta – From Security Consultant to Security Innovator

Webinars & Webcasts

- Top 10 Writing Mistakes in Cybersecurity and How You Can Avoid Them: February 22nd, 2019 at 1:00 PM EST
- Webinar: From Dev to InfoSec: #MyInfoSecStory on Feb 21, 2019: February 21, 2019 at 1:00 PM US Eastern

Conferences

- BSides Tampa 2019, especially:
  - Personal security while on travel with additional pro-tips from seasoned travelers
  - Hacking IoT devices by chaining application security vulnerabilities
  - Securing Shadow IT
  - Election Hacking Getting Ready for the Russian Onslaught in 2020
  - The Sound of Evil
  - Serverless Security Top 10

Slides only

- OWASP SF – Reviewing Modern JavaScript Applications
- Hacking NodeJS applications for fun and profit
- Trends, challenge, and shifts in software vulnerability mitigation (BlueHat IL 2019)

Tutorials

Medium to advanced

- How I created a backdoor in a system exploiting CSV functionality of an Application by performing Formula Injection...!!
- SSRF Protocol Smuggling in Plaintext Credential Handlers : LDAP: SSRF Protocol Smuggling in LDAP authentication, quite common with enterprise and multi-tenancy products
- Bypassing NAC: A handy How-to Guide & bypass/nac_bypass
- Vulnerability Analysis of Windows Contact File
- BACNet javascript Injection -Persistent XSS in BACNet devices CVE-2019–7408

Beginners corner

- Day 35: XSS Payloads, getting past alert(1)

- Burp Extension Python Tutorial – Encode/Decode/Hash
- Interlace: A Productivity Tool For Pentesters and Bug Hunters – Automate and Multithread Your
- Jenkins Pentest Lab Setup
- Multiple Ways to Exploiting Windows PC using PowerShell Empire
- A guide to ethical hacking — Understanding Nmap
- Day 40: Privilege Escalation (Linux) by Modifying Shadow File for the Easy Win
- Day 36: Hack your own NMAP with a BASH one-liner

Writeups

Challenge writeups

- HackIM Nullcon CTF 2019 – Proton
- Spying Challenge 2018: Write-up from a CTF with OSINT, social engineering, physical intrusion & hacking

Pentest & Responsible disclosure writeups

- Exploiting SSRF in AWS Elastic Beanstalk #Web
- Hacking To Deface Into Indian News Media Outlet- ANI News Agency #Web
- Vulnerabilities in Tightrope Media Systems Carousel <=7.0.4.104 (and likely newer) #Web
- OpenMRS – Insecure Object Deserialization #Web #API
- Your Smart Scale is Leaking More than Your Weight: Privacy Issues in IoT #IoT #Mobile
- Multiple Vulnerabilities Found in Mobile Device Management Software #Mobile
- Oracle MAF store bypass, a how-to #Mobile
- Dissecting into Gree+ Android Application #Mobile
- Reverse engineering of a mobile game, part 2: they updated, we dumped memory #Mobile
- Hacking an Aftermarket Remote Start System (Part 1) #Carhacking
- Libreoffice (CVE-2018-16858) – Remote Code Execution via Macro/Event execution #App

Bug bounty writeups

- Information disclosure on HackerOne ($20,000) & I told you so
- Information disclosure on HackerOne ($500)
- XSS & Open redirect on Twitter ($1,120)
- Privacy violation on Twitter ($1,120)
- Violation of Secure Design Principles on Ratelimited

- Cache deception on Medium ($100)
- LFI, RCE on Private program
- Directory listing, SQL injection, Authentication bypass on Private program
- Mass-assignment on Private program

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Armory & Introduction: A tool meant to take in a lot of external and discovery data from a lot of tools, add it to a database and correlate all of related information
- Subjs: A tool to get javascript files from a list of URLS or subdomains
- GitHub HistoryBrowse the history of any file from GitHub with style

More tools, if you have time

- Burp HMAC Header Extension & How-to
- Whatruns.py: Python Script to Fetch the technologies of given domain using whatruns API
- Nmap-censys: NSE script which leverages the Censys IPv4 API for passive data collection
- IPOsint: Discover IP Address of the target from a great resource without register or any API key
- Goscan: Interactive Network Scanner
- Golookup: A simple tool written in GoLang, which looks for CNAME(s) ,A and AAAA Records , TXT Records , NameServer(s) / MX Record of any domain
- 420 & Introduction: Automated XSS Vulnerability Finder
- Leaks_parser: Parser for data dumps Collection #1 / Collection #2-5
- tmpnix: An alternative to static binaries for post-exploitation
- PowerPriv & Introduction: A Powershell implementation of PrivExchange designed to run under the current user's context
- DnsCache: Reference example for how to call the Windows API to enumerate cached DNS records in the Windows resolver
- Bashfuscator: A modular and extendable Bash obfuscation framework written in Python 3, intended to help both red team and blue team

Misc. pentest & bug bounty resources

- AWS Hacking: Offensive guide to securing AWS infrastructures
- HackerOne-Lessons: Transcribed video lessons of HackerOne to pdf's

- Effective SSH usage for Pentesters Workshop
- The Burp Methodology
- APIsecurity.io Issue 17: 83 percent of web traffic is API, and why query parameters are bad for secrets
- Infosec-jobs.com
- Acunetix Web Application Vulnerability Report 2019
- Check Point Research Report: Under the Hood of Cyber Crime
- Information Security
- Hacker Tools & Lectures
- Intranet Penetration Tips (Original in Chinese)

Challenges

- Getpwning.com / Mini-CTF

Articles

- Google CTF (2018): Beginners Quest – Introduction
- Bug Hunting Methodology (part-1)
- Pentesting Azure — The Report
- Yet another plea against using public WiFi
- Day 33: XSS, JSON/JS Injection
- A guide to HTTP security headers for better web browser security
- The Difference Between Threats, Threat Actors, Vulnerabilities, and Risks
- No DA? No Problem! How Attackers Can Access Sensitive Data without Escalated Privileges
- Third-Party Library Depdencies
- PHPMyAdmin 3.5.X-3.5.8 Reflected XSS: What could have been, but really wasn't
- Your drivers may have an open Web server exposing you to attacks

News

Bug bounty news

- Public hacker test on Swiss Post's e-voting system: Between Feb. 25th and Mar. 24th 2019. Register on https://www.onlinevote-pit.ch/
- 2019 Researcher Incentive Programs (Bugcrowd)

- Bugcrowd 2018 MVP Researcher Wrap Up
- Introducing My Programs (HackerOne)](https://www.hackerone.com/blog/Introducing-My-Programs
- H1-415 Hacking Mentee sign up
- It's 2019. Should billion-dollar corps do better than offer swag for vulns?: A t-shirt for RCEs on Sony & Sony Pictures
- Researcher Assaulted By A Vendor After Disclosing A Vulnerability
- BountyCon: Invitation-only security conference by Google & Facebook, in Singapore on March 30-31, 2019. Airfare & accommodations covered for some selected students

Breaches & Vulnerabilities

- Phishing Attacks Against Facebook / Google via Google Translate
- Critical Android Bug that Allows Attackers to Compromise your Android Device Using PNG Image
- Unlimited crypotocurrency? Zcash fixes counterfeiting flaw
- Major Security Breach Found in Hospital and Supermarket Refrigeration Systems
- Half of IoT devices let down by vulnerable apps
- SpeakUp: A New Undetected Backdoor Linux Trojan
- KeySteal could allow someone to steal your Apple Keychain passwords: 18-year-old German researcher found a critical iOS 0-day but refuses to share details with Apple in protest of their invite-only/iOS-only bounties
- Apple will pay the teenager who discovered the Group FaceTime bug
- LibreOffice patches RCE flaw – Apache OpenOffice doesn't

Other

- Google open sources cloud-based fuzzing tool
- Google's New Tool Alerts When You Use Compromised Credentials On Any Site
- Android Security Monthly Recap #1 | January 2019

Non technical

- The Definition of a Purple Team
- Red team, blue team and rockstar culture in infosec (interesting comments too)
- The 1/3, 10/30, 100/300 Better Every Day Formula
- Meet our hackers – Intruderx
- Researcher Spotlight: Ambassador Dinesh V.

- How Dr. Jessica Barker Brought Positivity Into Cybersecurity

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