Bug Bytes #56 – Pwning A Pwned Citrix, Upgrading Your Recon with Discord & Tip of the week by @jobertabma

BY INTIGRITI · FEBRUARY 5, 2020 · 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 24 to 31 of January.

Our favorite 5 hacking items

1. Tip of the week

> "Hacker tip: when you're looking for IDORs in a model that references another model, try storing IDs that don't exists yet. I've seen a number of times now that, because the model can't be found, the system will save the ID. Because authorization checks often only happen on write, you can come back after the ID was created. Because the model references a model that isn't yours, you may be able to bypass authorization, often leading to information disclosure."

Awesome IDOR technique by @jobertabma! The idea is to replace an ID with one that does not exist yet (e.g. ID+1). Wait for ID+1 to exist and see if you can access its information.

Now to revisit old programs to test for potentially missed IDORs/info disclosures...

2. Writeup of the week

> "Pwning A Pwned Citrix"

This is an excellent writeup on Shitrix (CVE-2019-19781). It shows how to exploit the vulnerability "manually" when public exploits are not working. In this case, the NOTROBIN malware had infected the target and made changes to prevent other exploitation attempts.

Knowing how to bypass it can be helpful for penetration tests.

3. Podcast of the week

> "The Bug Bounty Podcast Episode #2 ft. 0xacb"

Yay! My favorite bug bounty podcast is back, with @0xacb this time. No spoilers, let's just say that it is worth listening to if you're into bug bounty and want to know how to reach "cosmic brain level 10".

4. Articles of the week

> "– Samesite by Default and What It Means for Bug Bounty Hunters
> – Bug Business #1: Inside Logic Flaws with EdOverflow"

The first article is awesome work but will break a few hearts! It explains the impact of Samesite cookies beyond CSRF. Many other client-side bugs are affected including Clickjacking, XSSI, XSLeaks, Cross-Site WebSocket Hijacking...

The second article in an awesome interview with @EdOverflow. Among other things, he shares insight on finding logic flaws and discovering "goldmines" (untapped areas of research).

5. Tutorial of the week

> "Upgrading Your Recon with Discord"

This is a great tutorial on leveraging Discord WebHooks for automated recon. This feature makes it easy to send notifications to Discord from Bash scripts.

A subdomains monitoring example is also given. It has never been so easy!

Other amazing things we stumbled upon this week

Videos

- Finding Your First Bug: Cross-Site Request Forgery (CSRF)
- HackTheBox – AI: A cool out of band SQL Injection using "Speech To Text"
- @STÖK Talks About Team Disturbance, Getting Started With Bug Bounties, and Live Hacking Events!
- TOOL TIME: Stream #4
- Server Message Block (SMB) Protocol
- How to Start a Career in Cyber Security with The Cyber Mentor
- Bypass Windows Authentication With Kon-Boot
- Spring Boot Actuator – security point of view
- Recon-ng V5 – Web Interface

Podcasts

- Security Now 751 – SHAmbles
- Risky Business #570 — FTI report lands like a lead balloon

- CoalCast #11 – TinkerSec
- How the Innocent Lives Foundation Uses OSINT to Uncover Online Predators
- 7MS #398: Securing Your Network with Raspberry Pi Sensors
- Insane In The Mainframe w/ Big Endian Smalls
- Security Weekly News #8 – Coronavirus, Ragnarok Ransomware, Ned In The Basement, Cisco
- Application Security Weekly #93 – Pwn2Own In Miami, Cloud Vuln., Deconstructing Web Cache Deception Attacks

Webinars & Webcasts

- Secure by Default? Scoring the Big 3 Cloud Providers
- Are You Properly Using JWTs?

Conferences

- LASCON 2019

Slides only

- Owning the cloud through SSRF and PDF generators – Public v2
- An Opinionated Guide to Scaling Your Company's Security & Twitter thread
- NullHyd Jan Meetup Talk on Chaining bugs and Writing single click Exploits
- Windows / Linux Local Privilege Escalation Workshop

Tutorials

Medium to advanced

- KubeCon NA 2019 Tutorial Guide
- Attacking Azure, Azure AD, and Introducing PowerZure & PowerZure
- SHA1 is Dead, Long Live SHA1
- GoPhish & Evilginx2 Auto-Deployment w/ Phish Composer
- MSBuild without MSBuild
- Windows Defender Bypassing For Meterpreter

Beginners corner

- HTTP Request Smuggling. A how-to

- Mail Technologies(DKIM & DMARC) – Part 2
- Pokémon GO OSINT Techniques: Part II
- (Ab)using Kerberos from Linux
- Hacking in 5 minutes with Remote Procedure Call and Active Directory enumeration
- Windows Persistence using Application Shimming
- Multiple Ways to Persistence on Windows 10 with Metasploit

Writeups

Challenge writeups

- More Intigriti XSS – Just Shy of Success

Pentest writeups

- Extracting Source Code from Pre-Compiled ASP.Net applications
- A Not-So-Blind RCE with SQL Injection

Responsible(ish) disclosure writeups

- Remote Cloud Execution – Critical Vulnerabilities in Azure Cloud Infrastructure (Part I) & Part II #Web #Cloud
- Zoom-Zoom: We Are Watching You #Web
- xmlrpc-common deserialization vulnerability (CVE-2019-17570) #Web
- CVE-2020-1925: Requests to arbitrary URLs in Apache Olingo #Web #CodeReview
- Validating the SolarWinds N-central "Dumpster Diver" Vulnerability #DesktopApp
- Picking apart an IOT Camera (Bloomsky) #Web #IoT
- Code injection in Workflows leading to SharePoint RCE (CVE-2020-0646) #RCE #Web
- LPE and RCE in OpenSMTPD (CVE-2020-7247) #RCE #SMTP
- High Severity CSRF to RCE Vulnerability Patched in Code Snippets Plugin #Web

Bug bounty writeups

- Race Condition allows to redeem multiple times gift cards which leads to free "money" on Reverb.com ($1,500)
- WordPress unzip file path traversal ($800)
- Account take over of 'light' starbuckscardb2b users on Starbucks

- WAF bypass via double encoded non standard ASCII chars permitted a reflected XSS on response page not found pages on Starbucks
- Escalating reflected XSS with HTTP Smuggling
- Improper Input Validation | Add Custom Text and URLs In SMS send by Snapchat | Bug Bounty POC ($1,000)
- XSS on Facebook's acquisition Oculus CDN Server
- 2FA Bypass via Logical Rate Limiting Bypass ($500)
- OK Google: bypass the authentication!

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Go-pillage-registries & Introduction: Pentester-focused Docker registry tool to enumerate and pull images
- Collaborator++ & Introduction
- Shodomain: Shodan subdomain finder
- Flamingo & Introduction: Go tool for capturing credentials sprayed across the network by various IT and security products

More tools, if you have time

- Wordlistgen: Quickly generate context-specific wordlists for content discovery from lists of URLs or paths
- Burp-teams: A Burp extension to enable teams of people to share repeater tabs and data
- XSS tag_event analyzer & : Python script for detecting valid tags/events on XSS exploitation
- GoLinkFinder: A fast and minimal JS endpoint extractor
- Dom-red: Python script to check a list of domains against open redirect vulnerability
- Chain Reactor & Introduction: Open source framework for composing executables that simulate adversary behaviors and techniques on Linux endpoints
- StickyReader & Introduction: Powershell script to read Sticky Notes from compromised Windows 10 hosts
- Socialscan: Check email address and username availability on online platforms with 100% accuracy
- Prettyloot: Convert the loot directory of ntlmrelayx into an enum4linux like output
- Red_Team: Some scripts useful for red team activities

- TikTokOSINT: Python script that dumps public data of any user
- Content Security Policy Evaluator
- MoveKit, StayKit & Introduction: Cobalt Strike lateral movement & persistence kits

Misc. pentest & bug bounty resources

- Alternatives to Extract Tables and Columns from MySQL and MariaDB
- Top 15 OSINT Web Browser Extensions
- Awesome Unicode
- Kompar & Choosing the right static code analyzers based on hard data
- Infosec Skills Matrix
- Priv2Admin: Exploitation paths allowing you to (mis)use the Windows Privileges to elevate your rights within the OS
- Awesome Google VRP Writeups

Articles

- Identifying the Modern Attack Surface: Part 1
- SVG animate XSS vector
- Exploiting email address parsing with AWS SES
- Internet Explorer mhtml: – Why you should always store user file uploads on another domain
- Have you configured Nessus to betray you?
- Upgrading my Hotel Internet
- Wide open banking: PSD2 and us
- How to decrypt WhatsApp end-to-end media files, whats-enc.py & WhatsApp Media Decrypt

News

Bug bounty & Pentest news

- Dallas County attorney agrees to drop charges against men contracted by judicial branch to test courthouse security
- No more reset password token leaks via referrer
- Burp Suite Pro / Community 2020.1 released, with major enhancements to HTTP message editor and more

- HTTP Request Smuggler now supports overriding the request method!
- What's new in Ffuf 1.0
- Kali Linux 2020.1 Release: Non-Root users by default now
- @hakluke AMA
- Microsoft launches Xbox bug bounty program with rewards of up to $20,000
- Google Vulnerability Reward Program: 2019 Year in Review
- In the line of fire: Will California's AB5 labor law cause havoc for cybersecurity consultants?

Reports

- State of Cybersecurity at Top 100 Global Airports
- The State of Vulnerabilities in 2019 by Imperva
- 2019 Website Threat Research Report
- 2019 saw more cryptocurrency hacks than any other year

Vulnerabilities

- Dismissed PHP flaw shown to pose code execution risk
- CacheOut vulnerability hype comes under fire
- LoRaWAN networks are spreading but security researchers say beware
- Serious Security – How 'special case' code blew a hole in OpenSMTPD
- Patching the Citrix ADC Bug Doesn't Mean You Weren't Hacked
- 200K WordPress Sites Exposed to Takeover Attacks by Plugin Bug

Breaches & Attacks

- Wawa's massive card breach: 30 million customers' details for sale online
- UN hacked via unpatched SharePoint server
- Breach at Indian airline SpiceJet affects 1.2 million passengers
- Five Years Later, Ashley Madison Data Breach Fuels New Extortion Scam
- TrickBot Uses a New Windows 10 UAC Bypass to Launch Quietly
- Ragnarok Ransomware Targets Citrix ADC, Disables Windows Defender
- Iranian hackers target US government workers in new campaign

Other news

- Avast Shuts Down Jumpshot After Getting Caught Selling User's Data
- Government Report Reveals Its Favorite Way to Hack iPhones, Without Backdoors
- Coronavirus claims new victim: 'DEF CON cancelled' joke cancelled after DEF CON China actually cancelled
- Ring Android App Sent Sensitive User Data to 3rd Party Trackers
- Sodinokibi Ransomware Group Sponsors Hacking Contest
- First MageCart Hackers Caught, Infected Hundreds of Web Stores
- Facebook knows a lot about your online habits – here's how to stop it
- Google now charges the government for user data requests, report says
- Sonos Makes It Clear: You No Longer Own The Things You Buy

Non technical

- How to Hack Your Employees With a Phishing Simulation Campaign
- 5 things to avoid in bug bounty
- Making Mr. Robot: Jeff Moss on the push for authenticity in award-winning hacker show
- What's the difference? Information Assurance vs Information Security vs Cyber Security
- Volunteer in the Security Community to Benefit Your Career
- Being a noob
- Breaking Cybersecurity Myths

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 01/24/2020 to 01/31/2020.

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