Bug Bytes #23 – 20K IDOR Trick, Bug Bounty Vloggers everywhere & Persistent Burp Collaborator

BY INTIGRITI · JUNE 18, 2019 · LAST UPDATED ON JULY 31, 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.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 07 to 14 of June.

intigriti news

- The European Commission launched a public bug bounty program for DSS (Digital Signature Services)
- @MattiBijnens shows how he and his team earned €20.000 at an intigriti live hacking event with an IDOR trick:

> "MUST-READ: learn how @MattiBijnens and his team earned a whopping €20K with one IDOR trick at an @intigriti live hacking event! #HackWithIntigriti #BugBounty #WriteUphttps://t.co/lZ0CZgejs9
> — Intigriti (@intigriti) June 14, 2019"

Our favorite 5 hacking items

1. Conference of the week

> "BSides London 2019, especially:
> – Understanding Stress, Anxiety And Depression And How To Cope"

Stress, anxiety and depression are three health risks that we should all be aware of and have strategies to avoid. This talk is a perfect reminder of their distinctions, why they affect us and what to do to avoid them or to get better.
This is very helpful especially for us, hackers, who can spend days in front of our computers, forgetting to exercise, sleep or eat properly.

2. Writeup of the week

> "How spending our Saturday hacking earned us 20k ($20,000)"

This is the writeup of an unsual kind of IDOR found during a live hacking event.
Arne Swinnen, Matti Bijnens & Jeroen Beckers were able to bypass several defense mechanisms including

encrypted parameters. The thought process is very detailed and so interesting that I can't summarize it in a few lines. Check out the article, it's worth it!

3. Video of the week

> "Live mentoring with zseano"

To be honest, last week was so crazy busy that I haven't had the time to watch this video yet. But it is on the top of my list!
Apart from the technical details, getting advice from one of the top bug hunters is perfect for getting you into the right hacking mindset.
Live mentoring is an awesome opportunity especially if you're just starting out.

4. Tool of the week

> "BurpJSLinkFinder"

BurpJSLinkFinder is a Burp Suite plugin that passively detects JS files and scans them for endpoint links. If you are planning to do some JavaScript code analysis/ bug hunting on Web apps, you really want to try it.
It is very helpful because until now you had to export JS files then run a tool like LinkFinder on them to find new endpoints. Such a time saver!

5. Tutorial of the week

> "Achieving Persistent Access to Burp Collaborator Sessions"

If you have played with Burp Collaborator before, you know that Collaborator sessions are closed as soon as you close Burp. That's not very practical if you need to shut down your laptop and resume tests later. This tutorial shows a way around this. Basically, you launch Wireshark and sniff out communications between Burp and the Collaborator server. You should see a secret key pertaining to your Collaborator session. This is what will allow you to query the Collaborator server at any time even after closing Burp. This solution is not perfect but it is a workaround until Portswigger releases a new feature to save Collaborator sessions.

Other amazing things we stumbled upon this week

Videos

- 10 Minute Tip: OSINT and Web Analytics Codes and Tags
- Scoping out your project

Podcasts

- Security Now 718 – Update Exim Now!

- Risky Business #545 — US Government loses control of customs mugshot database
- Application Security Podcast – Caroline Wong — Self-care and self-aware for security people
- Security In Five – Episode 512 – Google Is Making It Easy For You To Dump Chrome
- Darknet Diaries – Ep 40: No Parking
- Business Security Weekly #131 – Leadership Articles
- Secure Digital Life #114 – Mock Interview, Q&A
- Hack Naked News #222
- Purple Squad Security – Episode 57 – Tinker After Dark – Tinker Tales by the Fire

Webinars & Webcasts

- InfoSec Girls + OWASP WIA knowledge exchange webinar – 08 June 2019
- OWASP DevSlop Show: Catching Secrets in the Cloud with Pawel Rzepa!
- OWASP DevSlop Show: Security Code Review 101 with Paul Ionescu!
- Hacking without Domain Admin

Conferences

- ShowMeCon 2019 Videos
- Micah Hoffman – Getting the Good Stuff: Understanding the Web to Achieve Your OSINT Goals

Slides only

- There's no place like 169.254.169.254 – Ab(using) cloud metadata URLS
- The Unsearchables – Finding Things That Google Doesn't
- The Right Way To Do Wrong-2019.pptx

Tutorials

Medium to advanced

- Intro to CakePHP for Bug Hunters
- Bypassing SSRF Protection
- Bypass XSS filters using JavaScript global variables
- Exploiting POST-Based CSRF

- Analyzing Multiple APKs At Once
- Anatomy of a Linux DNS Lookup – Part I
- Attacking Weakly-Configured EAP-TLS Wireless Infrastructures
- Privilege Escalation: Hijacking Python Library
- Linux Privilege Escalation exploiting Sudo Rights—Part I
- Exploiting ViewState Deserialization using Blacklist3r and YSoSerial.Net
- Analyzing ARP to Discover & Exploit Stale Network Address Configurations
- AMSI Bypass
- Bypassing CrowdStrike in an enterprise production network [in 3 different ways]
- Brute Forcing Accounts that have logged onto an AD joined computer

Beginners corner

- Regular Expressions | A Complete Beginners Tutorial
- From SSRF To AWS Credentials Disclosure
- HTTP screenshots with Nmap, Chrome, and Selenium
- HTTP response splitting exploitations and mitigations
- Web Services & API Pentesting-Part 2
- Google sites misconfiguration
- How to hack WordPress website via xmlrpc.php?
- Exploit PoC: Linux command execution on Vim/Neovim vulnerability (CVE-2019–12735)
- LDAP SWISS ARMY KNIFE – A directory server for LDAP client analysis and exploitation
- Linux for Pentester: Wget Privilege Escalation , ZIP Privilege Escalation & Find Privilege Escalation
- Rapidly Creating Fake Users in your Lab AD using Youzer

Writeups

Challenge writeups

- Solving ESET's Pentest Challenges

Pentest writeups

- From SQLi to ROOT

Responsible disclosure writeups

- Critical Vulnerability Discovered in Evernote's Chrome Extension
- MyBB <= 1.8.20: From Stored XSS to RCE
- XSS on Samy.pl (Samy Kamkar)
- Security Advisory: Critical Vulnerabilities in NTLM Allow Remote Code Execution and Cloud Resources Compromise
- The Return of the WIZard: RCE in Exim (CVE-2019-10149)
- Alert Logic Researchers Find Another Critical Vulnerability in WordPress WP Live Chat – CVE-2019-12498

Bug bounty writeups

- Information disclosure on GitLab & additional info ($3,500)
- Authorization flaw on Shopify ($2,000)
- XML Entity Expansion (Billion Laughs Attack) on Central Security Project
- IDOR
- Reflected XSS
- Authorization flaw / Race condition
- Denial of Service on Facebook ($1,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Malcolm: A powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files) and Zeek logs
- BKScan: BlueKeep scanner supporting NLA (Network Level Authentication)
- BurpTabEssentials: This changes the style of Burp Suite's Repeater tabs to help the testers
- Blue: A web-panel designed to make reconnaissance faster and easier accessible
- Deeplack: Deeplack is a python script designed for comparing images (screenshots) using DeepAI to detect changes on websites & push notifications to Slack
- Yaazhini: Free Android APK & API Vulnerability Scanner

More tools, if you have time

- Python .DS_Store parser: A library for parsing .DS_Store files and extracting file names
- href-urls.sh: Bash script that takes a text file containing URLs & creates an HTML file containing clickable links (of these same URLs)
- Cloud_metadata_extractor: Cloud metadata extraction tools and scripts
- Rustbuster: DirBuster for Rust
- burp-subdomains: Burp Suite extension to easily export sub domains
    - https://twitter.com/Regala_/status/1138421549919363072?s=20
- WayRobots: Tool to find stored robots.txt files from the past
- Kali Customize Script: Script for Kali that adds a bunch of tools and customizes it to be much better
- TOR Router: A tool that allows you to make TOR your default gateway & send all internet connections under TOR (as transparent proxy) for increased privacy/anonymity without extra unnecessary code
- s3-ransomware-bucket-check.py: Python script for checking Amazon S3 bucket configurations & detecting buckets vulnerable to ransomware
- Using Nmap to extract Windows host and domain information via RDP
- Eavesarp: Analyze ARP requests to identify hosts that are communicating with one another
- FB-search: Free OSINT tool / Interface to the new Facebook search engine

Misc. pentest & bug bounty resources

- Can I takeover XYZ (Steps)
- The arsenal, armory & library by Maderas (@hackermaderas)
- XSS cheat sheet
- Security tool list from 2 years on Twitter
- OSCP Approved Tools
- Pre-computed Hash Table, v. 1.0
- Recipe for Root – Your Cookbook for Privilege Escalation
- Rainbow Crackalack: Make Rainbow Tables Great Again

Challenges

- Meltdown Explained
- Authentication lab – User Agent based challenge

Articles

- An odd quirk with XSS through JavaScript URI
- Complete Web Application Firewall Guide
- Detecting Cross-Site Scripting Vulnerabilities
- WhatsApp Buffer Overflow Vulnerability: Under the Scope
- A look at CVE-2019-10149, RCE in Exim
- Exploiting CVE-2019-1040 – Combining relay vulnerabilities for RCE and Domain Admin
- SPA source code recovery by un-Webpacking source maps
- Want to take over the Java ecosystem? All you need is a MITM!
- Modern Red Team Infrastructure

News

Bug bounty / Pentest news

- The HackerOne Top 10 Most Impactful and Rewarded Vulnerability Types
- The Web Security Academy labs are now covered by Portswigger's bug bounty program
- OWASP Top 10 of security risks for APIs – Draft available for review

Reports

- Data Insights on the BlueKeep Vulnerability
- 2019 State of the Internet / Security: Web Attacks and Gaming Abuse
- SQL Injection Attacks: So Old, but Still So Relevant. Here's Why (Charts)

Vulnerabilities

- Warning: Google Researcher Drops Windows 10 Zero-Day Security Bomb
- Medical infusion pumps vulnerable to remote attacks
- New Pervasive Worm Exploiting Linux Exim Server Vulnerability
- RAMBleed Attack Can Steal Sensitive Data From Computer Memory

Breaches & Attacks

- The GoldBrute botnet is trying to crack open 1.5 million RDP servers

- A Year Later, U.S. Government Websites Are Still Redirecting to Hardcore Porn: Open redirect exploited in the wild
- Cybercrooks using text-based images in phishing emails to bypass spam filters
- That push notification on your phone might be a phishing attempt
- Google Calendar Attacks Target Unwitting Mobile Users
- Microsoft Warns of Email Attacks Executing Code Using an Old Bug

Malicious apps/sites

Other news

- Troy Hunt Looks to Sell Have I Been Pwned
- GitHub platform improvements are helping orgs keep their dependencies in check
- To Trust Apple Sign-In, You Need to Trust Apple
- Facebook Quietly Changes Search Tool Used by Investigators, Abused By Companies

Non technical

- No, yeah... yeah no...
- When Bug-Bounty becomes cheap/free Pentest(s)

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 05/31/2019 to 06/07/2019.

Subscribe to the newsletter here!

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*