Bug Bytes #26 – File upload to SQLi, Google's CTF & Data Breach 101

BY INTIGRITI · JULY 9, 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 28 of June to 05 of July.

Intigriti news

We partnered up with PwnFunction to create a writeup video on Google's 2019 CTF.
We'll be releasing more content soon, so make sure to subscribe to our channel!

> **"Very excited to announce that we've partnered up with @PwnFunction to create snackable video content for security researchers!**
> **Check out our first video on how to solve @Google's CTF here**
> **#HackWithIntigritihttps://t.co/JO3ONBQZl7**
>
> **— Intigriti (@intigriti) July 8, 2019"**

Our favorite 5 hacking items

1. Webinar of the week

> "Intro to Cloud for Pentesters and Bug hunters | Security and Research Company (SECARMY)"

This is an excellent introduction to cloud security for pentesters and bug hunters. If you've ever felt intimidated by AWS testing, this is a perfect opportunity to tackle this topic.
You'll learn about cloud computing, the difference between IaaS, PaaS and SaaS, common misconfigurations of four components of AWS (including AWS S3 and IAM) with examples and links to writeups.

2. Writeup of the week

> "File upload blind SQL injection"

I've never thought that the file name specified during a file upload could be saved to a database, and so potentially vulnerable to SQL injection!
It seems like an unusual entry point for this kind of attacks. So it's good to know and add to one's list of locations to fuzz for SQL injection.

3. Conference of the week

> "Pass the SALT 2019 videos & all slides, especially:
> – Hacking Jenkins & Slides
> – Time-efficient assessment of open-source projects for Red Teamers & Slides
> – Better curl ! & Slides
> – Dexcalibur – automate your android app reverse & Slides
> – Mini-Internet using LXC (MI-LXC): A first step towards a free CyberRange ? & Slides
> – JWAT... Attacking JSON Web Tokens & Slides
> – KILL MD5 – Demystifying hash collisions & Slides"

When I first saw the name of this conference, I thought it was only about passwords, hashes and crypto (because of the word "SALT").
But it's actually very eclectic with talks on interesting offensive security topics like: reversing Android apps, why MD5 is so weak, JSON Web tokens, Curl, red teaming & open source, Jenkins security, etc.
And with brilliant speakers like Orange Tsai and Louis Nyffenegger, I'm sure quality is there too.

4. Tool of the week

> "Asset Discover & Introduction"

Asset Discover is a Burp Suite extension that passively collects asset-related information. While you're browsing the target app, it parses responses and extracts the following assets: domains, subdomains, IP addresses, S3 buckets, DigitalOcean space URLs and Azure Blob URLs.
Having this kind of information passively gathered and easily accessible is interesting. It's worth testing.

5. Article of the week

> "Data Breaches are on the Rise — Is it too hard to p r e v e n t control data breaches?"

Being obsessed with offensive security, defense is not my forte. But it's interesting to consider both to be able to understand the other side (developers, clients, bug bounty programs...) and, if necessary, advise them on how to remedy bugs or up their security.
This article provides multiple practices that can help avoid breaches, with links to resources (tools, checklists, people to follow, articles, etc).
It's good to know for both hackers and defenders.

Other amazing things we stumbled upon this week

Videos

- GraphQL: The Documentary (Official Release)
- Let's Learn Rust by d0nutptr
- Don't use assert in PHP
- Teaching My Wife to Hack...Maybe (Part 2)
- Hacking with intruder

Podcasts

- Security Now 721 – Exposed Cloud Databases
- Risky Business #546 — The fifth domain sees some action
- How to Get Buy-In When Your C-Suite Doesn't Speak Security
- Hackable? 28 – Up Your Game
- Chats On The Road To Hacker Summer Camp 2019 | DEF CON 27 | A Conversation With Jeff Moss
- Episode 530 – Why You Should Not Pay The Ransom From Ransomware
- Security In Five – Episode 528 – Things To Thnk About Before Using A Password Manager
- Hack Naked News #225 – Yubico, Attunity, & Trump Crackdown
- Business Security Weekly #134 – Mastercard, Gen Z, & Leadership

Webinars & Webcasts

- OWASP WIA + InfoSecGirls knowledge exchange webinars: August 2018, October 2018, December 2018, January 2019, February 2019, March 2019, April 2019,

Conferences

- An Attackers View of Serverless and GraphQL Apps
- Captain Marvelous JavaScript – A look at the versality of JavaScript and how hackers use it
- BSidesPGH Black 2019, especially:
  - How to Frustrate a Penetration Tester
  - How to Get Started in Cybersecurity

Slides only

- From pen testing to bug bounty -Tips and tricks to get you started
- Hack in Paris 2019 slides
- Hash collision exploitation with files (Workshop)
- Google – Seeing Inside the Encrypted Envelope

Tutorials

Medium to advanced

- How do I automate the enviroment setup for android pentesting using simple bash scripts

- Testing SAML Endpoints for XML Signature Wrapping Vulnerabilities
- Eternalrelayx.py—Non-Admin NTLM Relaying & ETERNALBLUE Exploitation
- Linux for Pentester: cp Privilege Escalation
- Bypassing Email Security Controls (P1: URL Scanning)
- Some ways to dump LSASS.exe
- Ninja Turtles in your network: LAN Turtle 3G. A how-to for red teaming
- Use Microsoft.com Domains to Bypass Firewalls & Execute Payloads
- ASREQRoast – From MITM to hash

Beginners corner

- Amass — Automated Attack Surface Mapping
- Using Shodan Better Way!
- Exploiting the xmlrpc.php on all WordPress versions
- Redirects: 301, 302, 307 | How-To 301 guide
- Fall in love with Regex
- XPath Injection
- SQL Injection
- Kali Linux in the DigitalOcean Cloud
- Guide to SSH Lockdown

Writeups

Challenge writeups

- Pwning OWASP Juice Shop (Free e-book) & Online version
- Bugbounty Tips – Zseano Live Mentoring Series – XSS
- HIP 2019 LiveHackingEvent Yogosha / Truc 1 & 2
- CloudGoat 2 Walkthrough – Part One, Part Two, Part Three, Part Four & Part Five
- CloudGoatChallenges – RCE Web App

Pentest writeups

- Discovering and Exploiting API Attack Surface Using Client-Side Javascript

- Red Team Techniques: Gaining access on an external engagement through spear-phishing
- Mimikatz and hashcat in practice
- How I Hacked Into Your Corporate Network Using Your Own Antivirus Agent
- How we hacked our colleague's smart home
- Black Team War Stories: Which company are you a contractor with?

Responsible(ish) disclosure writeups

- Lerhan: Bypassing IDOR protection with URL shorteners
- Magento 2.3.1: Unauthenticated Stored XSS to RCE
- AWS IAM Managed Policy Review
- Firefox Local Files Theft – not patched yet
- How I Hacked the Microsoft Outlook Android App and Found CVE-2019-1105
- Snyk research team discovers severe prototype pollution security vulnerabilities affecting all versions of lodash
- An Analysis of Arlo
- Slok API
- Centreon v19.04 Remote Code Execution (CVE-2019-13024)
- Mimecast Threat Center discovered a weakness in the Microsoft Excel tool that allows embedding malicious payloads remotely.

Bug bounty writeups

- SSTI ($1,200)
- Information disclosure
- Improper access control on GitLab & TL;DR ($7,000)
- SSRF blacklist bypass on OX App Suite ($850)
- Another SSRF blacklist bypass on OX App Suite ($500)
- Privilege escalation on Shopify ($500)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Cazador & Introduction
- FridaLoader: A quick and dirty app to download & launch Frida x86 on Genymotion. Useful during Android engagements when you don't want to download & run the @fridadotre Server on the device every time
- iframeBusterXSS: Tool for identifying iFrameBuster files (which often contain easy XSS)
- Glorified Grep & Introduction

More tools, if you have time

- CollabOzark: A simple tool which helps the researchers track SSRF, RCE, Blind XSS, XXE, External Resource Access payloads triggers
- Slothy: Open source information gathering tool from publicly available sites against a target domain
- CRLF-Injection-Scanner: Command line tool for testing CRLF injection on list of domains
- KNOXSS Community Edition
- Recon: Easy Fast recon script
- Hershell: Multiplatform reverse shell generator

Misc. pentest & bug bounty resources

- Bug Bounty Methodology (TTP- Tactics,Techniques and Procedures) V 2.0
- PENTESTING-BIBLE
- Useful Commands by @LearnerPentest
- Richelieu: List of the most common French passwords
- Top 12 Cyber Security APIs
- Top 10 Browser Extensions for Hackers & OSINT Researchers
- SRT AMA – I am Robin/Digininja, a professional penetration tester working in industry. Ask me anything!
- Security/Server Side TLS & TL;DR: Changes in Mozilla's TLS server configuration guide for the first time in 2.5 years
- Ipless-scan.py & Introduction: Perform a port scan without having an IP configured on your network interface
- Active Directory Recon Cheat-sheet
- OSCP Exam Report Template in Markdown
- How DNS works

Challenges

- New GraphQL challenges on Hacker101 CTF: BugDB v1, v2 & V3
- Give some space to this XSS Filter.
- FastFoodHackings – Is our new profile updater secure?

Articles

- The Bug Bounty Bucket List
- Finding vulnerabilities in Source Code
- Pentest Skills To Land a Job in 2019
- Using the 'screen' utility to run recon tools while you are asleep!
- DKIM: What is it and should you configure it?
- The null choice. A social engineering example in the wild
- RDP Security Explained
- (Ab)using Cloudflare Argo Tunnel for fun and profit
- How to not be a script kiddie:Stop the Metasploit Over-reliance! Part 1
- Notes on the OSI Model
- Exploiting UPnP, literally childsplay.
- OSCP

News

Bug bounty news

- Follow @nahamsec on Instagram for weekly tips
- FastFoodHackings: zseano's live hands on live mentoring session
- New HackerOne feature: downloading a Burp Suite config file to automatically configure scope for a program
- 5798! This is the impressive number of bugs discovered by @todayisnew while bug hunting
- $50,000 award won by @seanmeals. Congrats!!
- $2, that's the bounty @evanricafort got for a critical IDOR!

Vulnerabilities

- 17-Year-Old Weakness in Firefox Let HTML File Steal Other Files From Device
- Microsoft Teams Can Be Used to Download and Run Malicious Packages
- OpenID Foundation says 'Sign In with Apple' is not secure enough

Breaches & Attacks

- Mac Malware Pushed via Google Search Results, Masquerades as Flash Installer
- Inside the West's failed fight against China's 'Cloud Hopper' hackers
- 7 Eleven launch mobile payment app: a day after launching it attackers stole half a million USD from customers, as the app had no security around password reset
- First malware to abuse DNS over HTTPS poses challenge for defenders
- OpenPGP experts targeted by long-feared 'poisoning' attack

Malicious apps/sites

- Popular Android Zombie game phish users to steal Gmail credentials

Other news

- Mozilla revamps SSL Configuration Generator tool
- A Plan to Stop Breaches With Dead Simple Database Encryption
- Control-Alt-Delete? Swiss gov't puts the brakes on e-voting
- Firefox extension to protect users from reverse tabnabbing
- China Is Forcing Tourists to Install Text-Stealing Malware at its Border
- YouTube's 'instructional hacking' ban threatens computer security teachers – YouTube now says takedown of a 'white hat' hacking channel was a mistake
- YouTube BANNING Hacking Videos – Hot Take (video)

Non technical

- When Passion Leads to Burnout
- No "yes." Either "HELL YEAH!" or "no."
- How To Land A Job In Infosec
- 10 Presentation Ideas That Will Radically Improve Your Presentation Skills

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 06/28/2019 to 07/05/2019.

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*