Bug Bytes #39 – HTTP Desync Attacks 2.0, Google Sponsors Vulnerability Disclosure & 7 New Tools

BY INTIGRITI · OCTOBER 8, 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.

This issue covers the week from 27 of September to 04 of October.

Our favorite 5 hacking items

This time, exceptionally, we're featuring way more items than usual... Why limit ourselves to 5 if both quantity and quality are there?
The following links are all really worth checking out if you are into Web application security.

1. Articles of the week

> "– HTTP Desync Attacks: what happened next
> – Karim Rahal: Security Features of Firefox
> – The Top 8 Burp Suite Extensions That I Use to Hack Web Sites
> – 5 Subdomain Takeover ProTips"

These articles are, in order, about:

- New research by @albinowax on HTTP Request Smuggling
- 3 Firefox security features explained by @KarimPwnz, with good tips on how to use the "Multi-Account Containers" extension for hacking
- A list of 8 Burp extension worth using, with everything you need to know about them in one page (what they do, installation & usage tips)
- 5 tips by subdomain takeover master @0xpatrik

2. Writeup of the week

> "Google Paid Me to Talk About a Security Issue!"

Google sponsored @LiveOverflow for making this video. It is a writeup of a bug found by @wtm_offensi on Google's Cloudshell.
Basically, Git cloning a repo with Cloudshell lead to RCE. But this is not a simple bug and I am not going to try to sum it up in a few words like I usually do. This finding is probably the result of hundreds of hours of work.
This is why I find it so inspiring. The level of persistence and work involved to understand both the technologies behind Cloudshell and its inner workings is amazing.
It is also interesting to hear about @wtm_offensi's thought process: How he chose the target to focus on

based on criticality, how he keeps asking himself questions to really understand the app (almost like an investigation), how he doesn't look for a technical vulnerability but for an outcome (RCE), and for any conditions that could lead to that outcome...

3. Tools of the week

> "– Varanid.io
> – Cyber.dic & Introduction
> – Mobexler & Introduction
> – Swamp
> – Syborg
> – Fav-up
> – Dnsgen, Introduction"

- **Varanid.io** is an all-in-one tool that makes it really easy to monitor a lot of thing for pentest/bug bounty purposes. This includes DNS records, SSL certificates, file changes (e.g. changes to JavaScript files), response headers, status codes, page title, up/down time and more. I've never seen all these features on one site, with such ease of use!

- **Cyber.dic** is a spellcheck dictionary to add support of 1700+ technical terms to Microsoft Word & LibreOffice Writer. Finally, I can write "pentest" without it being highlighted as a mistake...

- **Mobexler** is a customised virtual machine, based on Elementary OS, designed to help in penetration testing of Android & iOS apps. I like the idea of having all (or most) of the tools you need for mobile testing already installed on a VM. It's like the Kali of mobile testing.

- **Swamp** is an OSINT tool for discovering associated sites through Google Analytics Tracking IDs. It's not a novel idea but being able to automate this is helpful for recon.

- **Syborg** is a recursive DNS Domain Enumerator with dead-end avoidance system. It is inspired from a discussion between @tomnomnom and nahamsec on the drawbacks of current subdomain enumeration tools.

- **Fav-up** is so creative! It helps you find a server's origin IP behind Cloudflare by looking up its favicon on Shodan.

- **Dnsgen** is like altdns on steroïds. It generates a combination of domain names from provided input. This is useful for finding new subdomains and account takeovers. And apparently, it generates way more combinations than altdns.

4. Non technical item of the week

> "My baby steps towards Bug Bounty Hunting — an arduous yet exciting journey"

@sharathsanketh recounts how he went from knowing nothing in Web hacking to his first bounty.
He doesn't give any technical advice, but I think his story and advice are so relatable and useful for beginners. He did two things I find noteworthy: He forced himself to focus on learning, not bug hunting without knowing the basics. And he didn't start with the most recommended books on bug bounty. He started with less known introductory books on how technology and the Web work, because that's what he needed to understand before going deeper.
This is a great mindset to adopt: "You need to know where you stand and reverse engineer in order to even know what you have to learn".

5. Tips of the week

> "– What are some endpoints that make you excited when it pops up while performing a directory brute force?
> – Any way to import a big url list into burpsuite?"

It's always fun to get a peak at what other hackers are using as tools and wordlists. The first link is basically a crowdsourced list of interesting endpoints to add to your directory bruteforce wordlist. The second one is about several ways for importing a list of URLs to Burp: using Burp API, BurpFeed, Burp-Importer...

Other amazing things we stumbled upon this week

Videos

- 09/15/2019 – Live Bug Bounty Recon Session on Yahoo (creating a wordlist) w/ @TheCyberMentor
- Google Paid Me to Talk About a Security Issue!
- Web App Testing: Ep 5: SQL Injections and Live Bug Bounty Hunting
- A Hacker's Toolkit – Hak5 Elite Kit, Pentest Dropboxes, Wireless Gear, and More
- HackerOne Hacker Interviews: Jon (mayonaise)), Calle (@zetatwo), Michael (mgianarakis) & Jack (wkcaj)

Podcasts

- Security Now 734 – The Joy of Sync
- Risky Business #558 — Trump targets Crowdstrike, Apple jailbreakers rejoice
- Darknet Diaries EP 48: Operation Socialist
- Absolute AppSec Ep. #72 – Consulting Horror Stories
- 7MS #383: Tales of Internal Network Pentest Pwnage – Part 10
- Hack Naked News #236
- Paul's Security Weekly #622
- Second Order Chaos Presents Jack Rhysider: For fans of Darknet Diaries

Webinars & Webcasts

- Dominating the Active Directory

Conferences

- RomHack 2019

- 44con 2019
- Black Hat USA 2019

Slides only

- The State of Credential Stuffing and the Future of Account Takeovers
- Security Vulnerabilities Decomposition: Another way to look at Vulnerabilities
- Def Con 27 Cloud Village

Tutorials

Medium to advanced

- Polyglot Files: a Hacker's best friend
- SAML All the Things! A Deep Dive into SAML SSO
- Search Tip: Finding Historic WhoIs Data
- Identifying & Exploiting Leaked Azure Storage Keys
- Diving into unserialize(): Magic Methods
- Building and Attacking an Active Directory lab with PowerShell
- Getting Started With AppLocker
- Phishing Users using Evilginx and Bypassing 2FA
- Cracking 256-bit RSA Keys – Surprisingly Simple!
- Persistence – Registry Run Keys
- Understanding and Defending Against Access Token Theft: Finding Alternatives to winlogon.exe

Beginners corner

- Lesson #1: Understand Docker from a security perspective
- How to Use Chrome to Debug JavaScript – Stop Console.Logging! NOW
- Exposed Kubernetes API, Elastic Search, Exposed Docker API & Google Cloud Storage
- Web Application Pentest Lab setup Using Docker
- Offensive Netcat/Ncat: From Port Scanning To Bind Shell IP Whitelisting
- Bind vs Reverse vs Encrypted Shells — What Should You Use?
- Deep Dive Into Nmap Scan Techniques
- Covenant Install & Example usage with PowerShell Launcher

- Penetration testing: TOR, VPN or proxy

Writeups

Pentest writeups

- SQL injection to RCE

Responsible(ish) disclosure writeups

- Butor Portal Arbitrary File Download Vulnerability (CVE-2019-13343) #Web #Pathtraversal
- Remote Code Execution in Firefox beyond memory corruptions #Web #Browser #RCE
- CompleteFTP Server Local Privilege Escalation CVE-2019-16116 #PrivilegeEscalation #Windows
- URL Bar Spoofing Flaw in Safari for iOS 12.3 and iOS 13 Beta | CVE-2019–8727 #Browser
- KSWEB for Android Remote Code Execution #Android #RCE
- Buying Internal Domain Access Again #Network

Bug bounty writeups

- Reflected XSS with a twist
- IDOR
- RCE ($1,000)
- Authentication bypass
- Parameter tampering ($900)
- Information disclosure on HackerOne ($500)
- Denial of Service on GitLab ($1,000)
- Password reset flaw on U.S. Dept Of Defense
- Authorization flaw on GitLab ($750)

See more writeups on The list of bug bounty writeups.

Tools

- Bucket-decloaker: A simple tool to decloak/expose the bucket name behind a domain
- Gitpillage.py: Gitpillage.sh rewritten in Python by @gwendallecoguic
- PortswiggerXSS: Go tool that gathers payloads from PortSwigger's XSS Cheatsheet & creates a usable wordlist
- PHP 7.0-7.3 disable_functions bypass: Tool for bypassing disable_functions

Misc. pentest & bug bounty resources

- CMS Detector: What CMS a Website is Using and the Best Tools to Find Out
- D4rkXSS: A list of useful payloads & Bypasses for Web Application Security & Bug Bounty/CTF
- Windows Notes / Cheatsheet & Linux Notes / Cheatsheet
- Google Guide
- Zero to OSCP: Concise Edition

Challenges

- Can you find the XSS vulnerability?: Win a Burp Pro license & private invites on Intigriti
- 24/7 CTF
- Hacking Playground Apps: New Android & iOS vulnerable apps by the OWASP Mobile Security Testing Guide

Articles & Papers

- Same-Site Cookies By Default
- Access Control and the PHP Header Function #CodeReview
- So You Want to Learn [Red] Teaming?
- Hiding from cats: Abusing /usr/bin/cat to hide commands in shell script
- Do You Know If Your DNS Server Can Be Used For DDoS Attacks?
- IEEE Access: Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach #CarHacking
- Smoke and Mirrors | Red Teaming with Physical Penetration Testing and Social Engineering

News

Bug bounty & Pentest news

- SecAppDev 2020 Scholarships
- The new official Twitter account for the @PortSwigger research team
- I Got Banned from Twitch for Hacking + Pentesterlab.com Giveaway! (video)

Reports

- Hacking 2020 voting systems is a 'piece of cake'
- Of All State-Backed Hackers, the Chinese Hit Most Industries

Vulnerabilities

- New iOS exploit checkm8 allows permanent compromise of iPhones & Developer of Checkm8 explains why iDevice jailbreak exploit is a game changer
- WhatsApp vulnerability could compromise Android smartphones
- New SIM card attack disclosed, similar to Simjacker
- Another UXSS bug found in Safari WebKit
- Researchers discover 'severe weaknesses' in PDF encryption standard

Breaches & Attacks

- Actively Exploited Android Zero-Day Impacts Google, Samsung Devices
- Why This New Cybergang is Heralding a New Age For BEC
- Comodo stung by vBulletin forum exploit

Malicious apps/sites

Other news

- Cloudflare, Google Chrome, and Firefox add HTTP/3 support
- O.MG! Evil Lightning cable about to hit mass distribution
- Even the tech expert from 'Mr. Robot' can't figure out this iPhone hack

Non technical

- The Best Password Managers to Secure Your Digital Life
- How to Become a Slack Ninja
- What Einstein's Most Famous Equation Says About Maximizing Your Productivity

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 09/27/2019 to 10/04/2019.

Curated by Pentester Land & Sponsored by IntigritiDisclaimer:The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.