Bug Bytes #32 – XSS in Google.org, Burp Teams & Paged out!

BY INTIGRITI · AUGUST 20, 2019 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-32-markdown-madness-pwning-child-companies-why-people-hate-you

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 09 to 16 of August.

Our favorite 5 hacking items

1. Slides of the week

> Bounty hunters: how do you organize your notes on targets, especially when switching targets back and forth and doing it for a long time?

This is a cool Twitter thread. Fisher (@Regala_) prompted the question about how other bug hunters organize their notes, and many hunters responded.
Tools mentioned include a private Github repo, simple notes and folders, SwiftnessX, OneNote, a whiteboard for logic flaws, Google Docs, XMind, etc.
It's nice to get a peak at what others are using!

2. Writeup of the week

> Clickjacking DOM XSS on Google.org

This is a good read to learn about you can go from self-XSS to a valid XSS by leveraging clickjacking.
The technique is nice to know in case you're stuck with self-XSS and want to increase its impact.
@ThomasOrlita does an awesome job explaining all technical details as well as how he was able to find this on Google: he focused on Google Crisis Map, an old project that doesn't seem to be used much anymore.

3. Tutorial of the week

> Improve Your Reconnaissance Performance By Using GNU Parallel

This is a concise tutorial about GNU Parallel. You might already know about it. But if you don't and want to speed up your Bash scripts, this is the quickest way to learn about it and start using it today.
Parallel is interesting because it bring multi-threading to Bash. So if you want to iterate any tests on network protocols or targets (for recon, network pentesting...), Parallel allows you to go faster than if you use a while or for loop.

4. Tool of the week

> BurpSuite-Team-Extension

This new Burp extension is a must if you're planning on collaboration with another Web app tester.
It allow you to share live/historical proxy requests, scope and reapeater/intruder payloads with each other in real time!
This is so useful for both bug bounty / pentest collaboration, and for education and mentorship.
You might also want to check out the other tools previously shared by the same author, Tanner Barnes (@*StaticFlow*).

5. Resource of the week

> Paged out!

Paged out! is a new free zine that features short articles on a variety of topics. It reminds me a bit of PoC||GTFO and Phrack.
This first issue has articles on no less than 12 categories: Algorithmics, Assembly, Electronics, File formats, OS internals, Phreaking, Programming, Radio, Retro (retro games), Reverse engineering, Sec/Hack (Web app security, reverse shells, Windows exploitation...) & SysAdmin.
I love that there is something for everyone. Personally, my focus is on pages 17, 52 and 62 because I'm more interested in Web app security.
If you would like to submit an article, the next submission deadline is October 20th.

Other amazing things we stumbled upon this week

Videos

- Owning the Clout through SSRF & PDF Generators – Defcon 27 – (SSRF on ads.snapchat.com)
- Live chat with @nahamsec, @stokfredrik, 5w0rdFish & @daeken
- Live chat with @nahamsec, @stokfredrik, @fransrosen & @avlidienbrunn
- Live chat with @nahamsec & @stokfredrik
- Web App Testing: Episode 1 – Enumeration

Podcasts

- Security Now 727 – BlackHat & DefCon
- Risky Business #551 — Post Vegas edition, more news than we can handle
- 7MS #376: Tales of SQL Injection Pwnage (starting at 14 min 05s)
- Security In Five Episode 557 – Apple Steps Up Their Bug Bountry Program To $1 Million
- 7MS #377: DIY Pentest Dropbox Tips
- PSW #616 – Blue Team To Red Team, Offensive Security – Tony Punturiero
- PSW #616 – Security News

Webinars & Webcasts

- Black Hat, DEF CON, and BSides 2019: Highlights and Emerging Industry Trends

Conferences

- BSides Las Vegas 2019 (live streams)
- Demystifying Frida & Slides
- Hacker Days: Raining shells in AWS by chaining vulnerabilities & Slides
- Security in open source projects & Slides

Slides only

- DEF CON 27 Media Server
- Abusing MSSQL Part II

Tutorials

Medium to advanced

- Uploading web.config for Fun and Profit 2
- Intercepting traffic from Android Flutter applications
- BloodHound Tips and Tricks
- Offensive Lateral Movement
- Making it Rain shells in Kubernetes
- Using CloudFront to Relay Cobalt Strike Traffic
- Linux for Pentester: scp Privilege Escalation
- Linux for Pentester: pip Privilege Escalation

Beginners corner

- DNS – Setting the Record Straight
- Interactive SSRF tutorial that reconstructs the recent Capital One data breach
- AWS NS Takeover – From 101 to Detection and Exploitation!
- JSON and Common Web Encodings Demystified
- Clickjacking Attacks: What They Are and How to Prevent Them
- Configuring A Droplet For Recon

- Regex For Noobs (like me!) – An Illustrated Guide
- ARP Cache Poisoning using Scapy

Writeups

Challenge writeups

- Recon Village CTF @ Defcon 27

Pentest writeups

- LLMNR Poisoning and WPAD Spoofing

Responsible(ish) disclosure writeups

- Recognizing basic security flaws in local password managers #PasswordManager
- Zero to Root in 60 seconds #OS #PrivilegeEscalation
- Unauthenticated option changes in WordPress Simple 301 Redirects Addon Bulk Uploader plugin #Web #CodeReview
- Why you shouldn't do client-sided checks; EE's gifting system #Web
- How Not To Do Cross-Site Request Forgery Protection – The Netgear Nighthawk M1 # Web
- Subdomain takeover – Chapter two: Azure Services #Web
- The Year of Linux on the Desktop (CVE-2019-14744) #OS #RCE

Bug bounty writeups

- OS command injection on Twitter ($20,160)
- Authentication flaw on Grammarly ($2,500)
- Authentication flaw on Shopify (Android) ($500)
- Open redirect on OX App Suite ($900)
- Information disclosure via Github on Twitter ($1,540)
- Subdomain takeover on Starbucks ($2,000)
- Information disclosure via Travis Logs on Tron Foundation ($100)
- Stored XSS & Account takeover on Medium ($1,000)
- Stored XSS & Account takeover
- Privilege escalation using Webhooks

Tools

If you don't have time

- Httprebind: Automatic tool for DNS rebinding-based SSRF attacks
- PyFunnels & Introduction: Data Normalization for InfoSec Workflows
- IPRotate_Burp_Extension & Introduction: Burp extension that changes your source IP address using the AWS API Gateway, to bypass IP based blocking

More tools, if you have time

- rapid7_OSINT
- NSBrute: Python script that automatically takes over domains vulnerable to NS subdomain takeover
- GraphQL Raider
- WAES: Web Auto Enum & Scanner
- Rhodiola & Introduction: Generating Personalized Wordlists with NLP For Password Guessing Attacks
- Nray: A free, distributed & platform independent port scanner
- PBDataRecon: Pastebin Analysis and Storage Tool
- Lure & Introduction: User Recon Automation for GoPhish

Misc. pentest & bug bounty resources

- SVG SSRF Cheatsheet
- BugBountyTemplate: A simple Cherry Tree template that can be used to organize bug bounties
- Top 25 Reddits – SubReddits Communities [Information Security]

Challenges

- Secure Coding Dojo – Security Code Review 101

Articles

- From email to phone number, a new OSINT approach & email2phonenumber: A OSINT tool to obtain a target's phone number just by having his email address
- Attacking Sites Using CSRF
- AttackSurfaceMapper – Automate and Simplify the OSINT Process
- RCE in Jira(CVE-2019–11581)

News

Bug bounty & Pentest news

- Nmap Defcon Release! 80+ improvements include new NSE scripts/libs, new Npcap, etc.
- Backslash Powered Scanner can now detect proxy subfolder escapes using @orange_8361's path normalization research from last year – just enable 'experimental folder attacks'
- Feds plan to use SecureDrop as a vulnerability reporting portal
- Santiago Lopez (@santi_lopezz99) got 179 bounties and 282 reports in one night... Whaaat?!
- Azure Security Lab: a new space for Azure research and collaboration

Reports

- Huge Survey of Firmware Finds No Security Gains in 15 Years
- New Research: Lessons from Password Checkup in action
- APT41: A Dual Espionage and Cyber Crime Operation

Vulnerabilities

- Clickjacking Evolves to Hook Millions of Top-Site Visitors
- British Airways sending vulnerable check-in links
- Hacked devices can be turned into acoustic weapons
- Vulnerability in Microsoft CTF protocol goes back to Windows XP
- HTTP/2 pinged by DDoS vulnerabilities
- August 2019 Microsoft Remote Desktop Services (RDP) Patches: What You Need to Know (Dejablue)

Breaches & Attacks

- More than a million people have their biometric data exposed in massive security breach
- Digital camera ransomware threat may extend to other vendors

Other news

- How a 'NULL' License Plate Landed One Hacker in Ticket Hell
- Mozilla joins Google in making Extended Validation a browser footnote
- Facebook got humans to listen in on some Messenger voice chats
- What a security researcher learned from monitoring traffic at Defcon
- Confidential company documents exposed in public sandboxes

- Hacker gets a whopping 14 years in prison for running Scan4You service
- These Legit-Looking iPhone Lightning Cables Will Hijack Your Computer

Non technical

- The Difference Between Data, Information, and Intelligence
- Hacker Jeopardy, Wrong Answers Only Edition
- DNS Root Servers: What Are They and Are There Really Only 13?

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 08/09/2019 to 08/16/2019.

Curated by Pentester Land & Sponsored by IntigritiCurated 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.