Bug Bytes #30 – Chaining Cache Poisoning To Stored XSS, How To Bypass Cloudflare's WAF & Ghostwriter by SpecterOps

BY INTIGRITI · AUGUST 6, 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 26 of July to 02 of August.

Our favorite 5 hacking items

1. Tool of the week

> "Ghostwriter, Introduction – Part 1 & Part 2"

Ghostwriter is a new project management & reporting engine by SpecterOps. It is open source and free and has a lot of interesting features:

- Client management: for tracking your pentest clients & the information like points of contact, project history, notes...
- Project management: for information like the type of project (pentest, vulnerability assessment, etc), start & end dates, the team assigned to the project...
- Infrastructure management: for tracking and monitoring the domain names & servers you use for the project (like C2 servers)
- Reporting engine: to generate reports in different formats (JSON, docx, xlsx & pptx) with support for template keywords
- Automation: running tasks in the background, released C2 domains at the end of a project & Slack notifications

These are just some functionalities. Ghostwriter is an excellent tool for pentest teams and red teams.

2. Writeup of the week

> "Chaining Cache Poisoning To Stored XSS"

I'm always interested in writeups about bugs chained together for a higher impact. This one is a good example of reflected XSS and Cache poisoning combined, which means that the XSS becomes stored.

(Credits to nahoragg for the writeup).
The writeup itself brings many lessons such as:

- Drupal has many known misconfigurations. So a CMS being used doesn't mean there are no bugs!
- Drupal's internal caching system is enabled by default
- To find out if caching is enabled, look for the x-drupal-cache response header
- To find input that gets reflected in the response, try the X-Original-URL and X-Rewrite-URL headers, or parameter bruteforcing

3. Challenge of the week

> "Leaky Repo"

This is @dijininja's latest Web challenge. It's a Github repo that has many sensitive information disclosures.
At first sight, it looks empty (except for the README file and a solutions file). So this is an interesting challenge for beginners who want to learn about information leaks, where to look for interesting information in Github repositories (beyond the visible files), how to use tools like Gitrob & truffleHog, etc.

4. Article of the week

> "Finding the Balance Between Speed & Accuracy During an Internet-wide Port Scanning"

Most port scanning tutorials for bug hunters recommends using Masscan to get a list of open ports, then re-scanning these same ports with Nmap to get their exact version.
The problem with this method is that Masscan can miss many open ports. Nmap is more accurate but so much slower when the testing range is large.
So what's the solution? This is the question that @CaptMeelo tried to answer by doing some benchmarking.
His conclusion: Run 2 or 3 concurrent Masscan jobs with all 65535 ports split into 4-5 ranges. Then run Nmap on the open ports found to get their version.

5. Tutorial of the week

> "Bypassing Cloudflare WAF with the origin server IP address"

Websites behind a WAF are protected against DDoS and many Web vulnerabilities (XSS, SQLi, CSRF...). If you can entirely bypass a WAF and speak directly to your target's servers, you will be able to go faster and test for more vulnerabilities. WAF bypass provides an edge to Web app pentesters and bug hunters.
This article by @gwendallecoguic is an excellent introduction to this topic. It provides several techniques for detecting the real IP address of a server, as well as tools for automation and resources to go further.

Other amazing things we stumbled upon this week

Videos

- Burp Suite Webinar for h1-702
- Live Bug Bounty Recon Session on Yahoo (Part 2 – 7/21/2019)
- We talking bugs
- postMessage: exchange data between different domains
- Popping a Shell with SMB Relay and Empire
- Teaching my Wife Computer Networking

Podcasts

- Coalcast Episode 6 – Esteban Rodriguez (N00py)
- The Secure Developer Ep. #35, Secure Coding in C/C++ with Robert C. Seacord of NCC Group
- Hackable? 30 – The Mr. Robot Spectacular
- Security Now 725 – Urgent/11
- Risky Business #550 — CapitalOne owned, Hutchins sentenced, VxWorks horror-show and more!
- Smashing Security – 139: Capital One hacked, iMessage flaws, and anonymity my ass!
- Hack Naked News #229
- Paul's Security Weekly #613 – Security News & #614
- Sophos Podcast S2 Ep2: EvilGnome, leaky browser add-ons and BlueKeep – Naked Security Podcast

Webinars & Webcasts

- Angular and the OWASP Top 10
- Weaponizing Active Directory
- Threat Modelling with Avi Douglan

Slides only

- Introduction to Application Security
- DBI-Assisted Android Application Reverse Engineering & Scripts, demo videos and apps

Tutorials

Medium to advanced

- Cryptographic Attacks: A Guide for the Perplexed
- If CORS is just a header, why don't attackers just ignore it?
- How to break out of restricted shells with tcpdump
- Gaining SYSTEM in any Windows box
- How do I download files in a Remote Desktop Session over SSH
- Credential theft without admin or touching LSASS with Kekeo by abusing CredSSP / TSPKG (RDP SSO)
- Exploiting H2 Database with native libraries and JNI

Beginners corner

- Bloodhound 2.1 – A Tool for Many Tradecrafts
- Server Side Template Injection
- How I harvested Facebook credentials via free wifi?
- Eternal Blue DoublePulsar Exploit

Writeups

Challenge writeups

- Bypassing PHP disable_functions with Chankro

Pentest writeups

- Android Pen-testing/Hunting 101
- More Thick Client Fun!
- Bypass File Upload Restrictions: CVE-2019–13976

Responsible disclosure writeups

- LinkedIn jobs, we have a problem #Web
- WARNING: Pre-Auth Takeover of OXID eShops #Web
- How I Bypassed HotStar OTP Verification. #Web
- Resource Consumption DOS on Edgemax v1.10.6 #DoS
- Samsung NVR WebViewer Remote DoS Vulnerability — CVE-2019-12223 #DoS

- How I was able to access complete storage of any ES-FileExplorer end-user #Mobile #Android
- Opera Android Address Bar Spoofing: CVE-2019–12278 #Mobile #Android
- I Always Feel Like Somebody's W a t c h i n g Listening to Me & TL;DR #IoT
- R7-2019-18: Multiple Hickory Smart Lock Vulnerabilities #IoT

Bug bounty writeups

- Information disclosure on HackerOne ($500)
- Browser extension flaw ($3,000)
- Information disclosure on TTS Bug Bounty ($750)
- Information disclosure
- RCE via Mustache Templates
- IDOR on Paypam ($10,500)
- Solr Injection on Zomato ($700)
- IDOR via email

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- XSS Payload generator and dropper & Introduction: XSS payload generator with obfuscation, filter bypass & polyglots
- PhanTap (Phantom Tap): An 'invisible' network tap aimed at red teams
- Extended XSS Searcher and Finder: A better version of @damian*89*s xssfinder tool – scans for different types of xss on a list of urls
- Extended ssrf search: Smart ssrf scanner using different methods like parameter brute forcing in post and get... Replaces @damian*89*s simple-oob-scanner
- Extended baserequest importer: Helps @damian*89* with some workflows when working with Burp, e.g. extract relevant params, scan them via intruder, watch passively!

More tools, if you have time

- Cloudcheck: Checks using a test string if a Cloudflare DNS bypass is possible using CloudFail
- Goop: Proof of concept for bypassing Google search rate limiting CAPTCHA (remember, scraping Google search results is illegal!)

- Pyrobots: a tool that reads “robots.txt” file and append each path to the domain/subdomain you entered
- Atomic-Caldera: Plugin for @MITREattack’s Caldera framework. It makes it easier to convert @redcanaryco’s Atomic Red Team tests to be used with Caldera
- LURE: User Recon Automation for GoPhish
- Wordlistctl: Fetch, install and search wordlist archives from websites and torrent peers
- Ipdiscover
- Gowhois: whois command implemented by golang with awesome whois servers list
- Inveigh: Windows PowerShell ADIDNS/LLMNR/mDNS/NBNS spoofer/man-in-the-middle tool

Misc. pentest & bug bounty resources

- Data from my Sunday streams: All the recon data from @nahamsec’s Sunday streams
- Payloads to try to discover blind SQLi when no error is returned.
- F5 BIG-IP Security Cheatsheet
- Collection of References on Why Password Policies Need to Change
- References on modern password policies
- APIsecurity.io Issue 42: HTTP Security Headers
- Awesome Damn Vulnerable Applications
- OSCP Cheatsheet
- Go-SCP: Go programming language secure coding practices guide
- The OpenID Connect Handbook
- IppsecTribute V1.1: Website that allows you to search ippsec videos by keywords

Challenges

- Disobey 2020 Puzzle: “Solve the Disobey puzzle and you may get access to a special discounted hacker ticket”

Articles

- Lessons in auditing cryptocurrency wallets, systems, and infrastructures
- S3 Bucket Namesquatting – Abusing predictable S3 bucket names
- POC or STOP THE CALC POPPING VIDEOS

- Chatbot Security Framework: Everything you need to know about Chatbot security
- Why Hackers Abuse Active Directory & Essential Active Directory Security Defenses
- The Art of Man-in-the-Middle Attack
- Analyzing iOS Stalkerware Applications
- Hijacking browser TLS traffic through Client Domain Hooking: The author got a bounty from Google!
- Vehicle Telematics Security; getting it right

News

Bug bounty & Pentest news

- PowerShell Empire Framework Is No Longer Maintained & Alternatives
- BlueKeep Exploits May Be Coming: Our Observations and Recommendations
- Introducing Pingback Payloads: "a new, non-interactive payload type that provides users with confirmation of remote execution on a target—and absolutely nothing else"
- "Passive income" opportunity for security researchers: submit your fuzzers to the Chrome Fuzzer Program and receive rewards for vulnerabilities found (with an extra $1K bonus for each vuln).
- BlueKeep exploit by @zerosum0x0 submitted to Metasploit
- NIST Releases Draft Security Feature Recommendations for IoT Devices
- GreyNoise Visualizer: New visualizer that supports IP queries, CIDR queries, ASN queries, free text search over organizations, tag queries, JA3 fingerprint queries, etc. You can filter by interesting entries. Also check out the Walkthrough video, Query reference & Query examples.

Reports

- How has DMARC adoption evolved since 2018? It's...complicated.
- Cyber Attack Trends: 2019 Mid-year Report
- Bugcrowd Releases Priority One Report: Payouts and Vulnerabilities Double Year over Year

Vulnerabilities

- 'Urgent/11' flaws affect 200 million devices – from routers to elevators
- DHS Warning: Small Aircraft are Ripe for Hacking
- Researchers Hack Surveillance Systems to Show Fake Video Feed
- Visa card vulnerability can bypass contactless limits

- New Dragonblood vulnerabilities found in WiFi WPA3 standard
- Google researchers disclose vulnerabilities for 'interactionless' iOS attacks – The six bugs, if sold on the exploit market, would have brought in well over $5 million

Breaches & Attacks

- The Capital One breach is more complicated than it looks, An SSRF, privileged AWS keys and the Capital One breach & The Technical Side of the Capital One AWS Security Breach
- Equifax data breach settlement: Regulators fire the first 'warning shot' of many
- Hackers target Telegram accounts through voicemail backdoor
- Russia targeted all 50 states in 2016 election, Senate report says
- Unsecured Database Exposes Security Risks in Honda's Network
- An exposed password let a hacker access internal Comodo files

Other news

- Apple Suspends Siri Program After Privacy Backlash
- Data is safer in the cloud than in the bank: NAB: "The public cloud is more secure than the security a bank can put around its proprietary data centres"
- Cisco to pay $8.6 million for selling vulnerable software to US government
- Google Chrome Hides WWW and HTTPS:// in the Address Bar Again
- Five Eyes nations demand access to encrypted messaging

Non technical

- Know Your Assets: Talking with Jonathan Cran from Intrigue
- Journey Towards The Life as a Bug Hunter
- Journey Of My First Bug Bounty.
- Your Reporting Matters: How to Improve Pen Test Reporting
- Best Practices For Business Travellers
- Practical Prepping for Hacker Summer Camp
- Managers, You're More Intimidating Than You Think
- Top 10 Cybersecurity Legends You Should Know About

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 07/26/2019 to 08/02/2019.

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