Bug Bytes #91 – The shortest domain, Weird Facebook authentication bypass & GitHub Actions secrets

BY ANNA HAMMOND · OCTOBER 7, 2020 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the week from 25 of September to 04 of October.

Intigriti News

Red Bull rewards friendly hackers at the Intigriti platform in their own unique way

Intigriti Q3 2020 leaderboard

Our favorite 5 hacking items

1. Video of the week

What's the shortest domain? & Unicode Mapping on Domain names

In this video, @filedescriptor tackles the question of short domains. He goes over why they are interesting, how to buy short domains that do not cost thousands of dollars, and how you can use IDN and Unicode tricks to bypass SSRF/URL validation checks.

2. Writeups of the week

Story of a weird vulnerability I found on Facebook (Facebook)
Forcing Firefox to Execute XSS Payloads during 302 Redirects
The Powerful HTTP Request Smuggling (_) ($17,050)

Here are three things these writeups taught me:

- 403 permission denied errors can be bypassed just by sending multiple simultaneous requests. This is how @amineaboud obtained authentication bypass and sensitive information disclosure on Facebook!
- If you find an XSS but cannot execute it because the payload is reflected in the HTTP response Location header, it's not useless. @QKaiser shows how browsers can be forced to not follow a 302 redirect, and execute the XSS payload!
- Always try to escalate impact. @ricardo_iramar found HTTP request smuggling and escalated its impact from "Universal Redirect" worth $2,000 to full compromise of the target's MDM and a $17,050 bounty.

3. Tool of the week

Rusolver

Rusolver is a lightweight DNS resolver in Rust by Eduard Tolosa (@edu4rdshl), the creator of Findomain. By default, it can resolve 1226 hosts in average per second. So, speed is obviously a strength but it would be interesting to test its accuracy compared to other tools such as massdns.

4. Article of the week

Stealing secrets from GitHub Actions & Intentionally vulnerable repo

This is excellent new research on Github Actions by Rojan Rijal (@uraniumhacker). He looked at Github action workflows and found out that some misconfigured implementations can be exploited to exfiltrate secret tokens. Since this is caused by a misconfiuguration and not a flaw inherent to Github, it is worth knowing and testing for on bug bounty and pentest targets.

5. Tutorial of the week

Setting The 'referer' Header Using Javascript

This tutorial presents a technique for manipulating the Referer header from JavaScript. I was under the impression that it wasn't possible, so it is interesting to read about it. Setting the Referer from JavaScript is useful for bypassing Referer checks and, in rare cases, even exploiting XSS.

Other amazing things we stumbled upon this week

Videos

- How To Play Htb Without A Vpn Or Kali Linux (Pwn Box)
- bsidesahmedabad AMA with Ahmad Ashraff aka Yappare
- Bug Bounty: Creating Target Specific Word lists for SSRF
- Server Side Request Forgery (SSRF) All-In-One

Podcasts

- Darknet Diaries EP 75: COMPROMISED COMMS
- The InfoSec & OSINT Show 27 – Joona Hoikkala and Advanced FFuF Scanning
- Security Now – ZeroLogon++ – Amazon Flying Security Cam, ZeroLogon on GitHub, Ransomware Roundup
- SWN #69 – Microsoft Outage, Joker Trojan, & Alien Android Trojan

Webinars & Webcasts

- Android Hacking Proving Ground (requires free registration)

Conferences

- Ekoparty 2020 & Ekoparty Trainings 2020
- HACON 20′ Virtual Conference, Day 2
- #RomHack2020 & Slides

Tutorials

Medium to advanced

- Artifactory Hacking guide
- AWS IAM explained for Red and Blue teams
- Design Considerations for Secure GraphQL APIs
- Building a hipster-aware pi home server
- Attacks On Gcm With Repeated Nonces

Beginners corner

- Intro To Web App Security Testing: Logging
- Using Log Analysis with Command Line Tools to Explore Linux Log
- How to Spot Vulnerabilities of Custom SAML Implementations Before They Happen
- When there is no Google Earth or Street View, what can you do?
- Attacking and Defending WPA Enterprise Networks & Whitepaper

Writeups

Challenge writeups

- SpidersecNinja XSS Challenges Walkthrough
- Failed DOM Clobbering Research – All The Little Things 1/2 (web) Google CTF 2020
- r2-pay: anti-debug, anti-root & anti-frida (part 1) & whitebox (part 2)

Pentest writeups

- Combining Hadoop and MCollective for total network compromise
- Exploiting fine-grained AWS IAM permissions for total cloud compromise: a real world example (part 1/2) & part 2/2
- Attacking Smart Card Based Active Directory Networks

Responsible(ish) disclosure writeups

- Hacking Grindr Accounts with Copy and Paste #Web
- Discovering new vulnerabilities in Cisco AnyConnect Secure Mobility Client for Windows #Windows #VPN
- Exploiting Other Remote Protocols In Ibm Websphere #Web
- The Anatomy Of A Bug Door: Dissecting Two D-link Router Authentication Bypasses #HNAP #Web
- Zentao Pro 8.8.2 RCE #Web #CodeReview

Bug bounty writeups

- Write Up – Google Bug Bounty: XSS To Cloud Shell Instance Takeover (Rce As Root) – $5,000 USD (Google, $5,000)
- Arbitrary code execution on Facebook for Android through download feature (Facebook, $10,000)
- Advisory: security issues in AWS KMS and AWS Encryption SDKs (Amazon)

- Ability to bypass email verification for OAuth grants results in accounts takeovers on 3rd parties (GitLab, $3,000)
- [cs.money] Open Redirect Leads to Account Takeover (CS Money, $750)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- chru: Fetch URLs, do segmentation then append endpoints for each path/route
- Grinder Framework: Python framework to automatically discover and enumerate hosts from different back-end systems (Shodan, Censys)
- MFASweep & Exploiting MFA Inconsistencies on Microsoft Services: A tool for checking if MFA is enabled on multiple Microsoft Services
- HTTP Toolkit: Open-source tool for debugging, testing and building with HTTP(S) on Windows, Linux & Mac

More tools, if you have time

- feroxbuster: Forced browsing tool in Rust, similar to ffuf with a few notable differences
- XSScope & Intro: Advanced XSS payload generator to use for increasing impact
- RmiTaste: Allows security professionals to detect, enumerate, interact and attack RMI services by calling remote methods with gadgets from ysoserial
- Gitdorker & Intro: A Python program to scrape secrets from GitHub through usage of a large repository of dorks
- Nuggets: Burp Suite Extension to easily create Wordlists based off URI, URI Parameters and Single Words (Minus the Domain)
- FHC: Fast HTTP Checker in Rust
- Massprint: A Rust tool to do basic fingerprinting across a large number of hosts
- CertAlert: Online service that will alert you to a TLS/SSL Certificate that is due to expire
- HackBrowserData: Decrypt passwords/cookies/history/bookmarks from the browser
- GHunt: OSINT tool to extract information from any Google Account using an email
- Salesforce Policy Deviation Checker
- Sharp Wifi Password Grabber: C# toolto retrieve clear-text Wi-Fi passwords saved in a workstation
- SMB AutoRelay: Bash script that automates the SMB/NTLM Relay technique for pentesting and red teaming exercises in active directory environments

Misc. pentest & bug bounty resources

- New Web Security Academy topic: HTTP Host header attacks
- Top 20 bug bounty YouTube channels to follow in 2020!
- siLLyDaddy.me AMAs
- Reverse Shell Generator
- Client-Side Prototype Pollution and useful Script Gadgets
- Bug Bounty Tips #7
- My Modern interpretation of The Web Application Hackers Handbook
- Simon Willison's TIL (e.g. Escaping strings in Bash using !:q)
- Web Skills: A visual overview of useful skills to learn as a web developer

Articles

- NGINX may be protecting your applications from traversal attacks without you even knowing
- #ProTips: Understanding a Leaky Internet with Gregory Boddin
- Phishing with Worms – The Greatest Password Theft I've Ever Seen
- Tinkering with TikTok Timestamps
- Talk about automated static code audit tools
- Phishing Your Password Manager
- Dear X, your staff passwords, numbers & confidential data is on Google – a report on searching and ethics
- Exploitability Analysis: Smash the Ref Bug Class
- The Fresh Smell of ransomed coffee

Bug bounty & Pentest news

- Nmap 7.90 Released! First release since August 2019
- Turbo Intruder now has IPv6 support
- Burp Professional / Community 2020.9.2
- Google Announcing the Fuzzilli Research Grant Program
- Bugcrowd's October Challenge Month!
- September 2020 Monthly Vulnerability Roundup

- Microsoft Exchange 2010 End of Support and Overall Patching Study

Non technical

- Burp Suite tips from power user and “hackfluencer” Stök
- Hacker Spotlight: Interview With Ajxchapman
- Hacker Spotlight: Interview With Albinowax
- Pentester Spotlight: Özgür Alp
- Cyber Pearl Harbor Is Happening Right Now — It’s Ransomware
- Secure Messaging Apps Comparison
- Everyday Threat Modeling
- Information Asymmetry and the 1950s Nuclear Bounty

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 09/25/2020 to 10/04/2020.