Bug Bytes #164 – New Collaborator domain, BITB attack & XSS to RCE on an almost static site

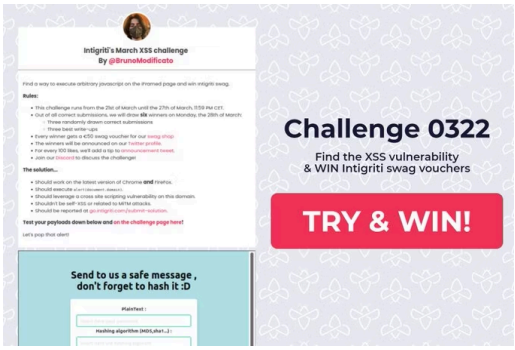
BY ANNA HAMMOND · MARCH 23, 2022 · LAST UPDATED ON MARCH 6, 2025

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.

CLICK HERE TO SUBSCRIBE

This issue covers the week from March 14 to 21.

Intigriti news



Intigriti's March XSS challenge By @BrunoModificato

Our favorite 5 hacking items

1. Tip of the week

Using privacy.com to generate cards with $0 spending limit

Tell the truth, have you ever been charged after signing for a trial then forgetting to cancel the subscription?
It happened to me more times than I'd like to admit, but it won't anymore thanks to @hacker_ fantastic tip: Using privacy.com's free tiers, it is possible to create virtual cards with a $0 spending limit and never get charged for anything.

2. Writeups of the week

From XSS to RCE (dompdf 0day)
CVE-2022-0337 System environment variables leak on Google Chrome, Microsoft Edge and Opera

(Google, Microsoft & Opera, $10,000)

@positive_sec penetration testers discovered an XSS on a mostly static site. They share how this low impact finding led to RCE because of a functionality to export pages as PDF. A creative tale involving HTML injection in a HTML-to-PDF converter and injecting PHP disguised as a font.

The second writeup is about a system environment variables leak in the Chromium engine, found by @pulik_io and impacting Google Chrome, Microsoft Edge, and Opera.

3. Tutorial of the week

Basic security for humans in 4 Fridays

This reminds me of a cousin who has trouble remembering all her passwords but refuses to use a paid password manager or anything complex to set up.
This tutorial is the perfect solution to share with her and anyone in our lives who needs a simple solution to manage passwords, MFA and secure their devices using only reputable free software.
Thanks to securibee for sharing this link on your newsletter where I discovered it!

4. Article of the week

Browser In The Browser (BITB) Attack & Repo

@MrDox demonstrates a simple but terrifyingly effective phishing technique: Using HTML/CSS to create a fake "Login with Google/Microsoft/Apple/etc" popup window. It is just appears like a popup with the right URL, but is actually just an image inside the attacker's site.
Note that this is not new, similar attacks have been known as "picture-in-picture attack".

5. Video of the week

Q: PENTEST VS BUGBOUNTY? (Bounty Thursday's – ON AIR)

I know I've already mentioned this show before, but it just brings me so much joy.
The production is top notch, the bug bounty news part is always informative, and the new Q&A / chat part brings the show to a whole new level.
I am sure y'all already know about it, so this is essentially a shoutout to @stokfredrik for sharing such quality and joyful content for hackers.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Career Conversations with seclilc – Offensive Cybersecurity!
- Alissa Knight Talks About API Hacking, Car Hacking, Creating Content for Hackers and More!
- $100k Hacking any website in Safari with uXSS – a 0-day chain

- iOS + Frida Tutorial, Part I, iOS + Frida Tutorial, Part II & iOS + Frida Tutorial, Part III
- Missing HTTP Security Headers – Bug Bounty Tips
- All About DLL Hijacking – My Favorite Persistence Method
- Heap Exploitation on Linux 101: The House of Force Technique

Podcasts / Audio

- Bug Bounty Community Chats #4

Webinars

- The NET Assembly and You! – Matthew Toussain
- Introduction to Automotive Security from an attackers point of view | Payatu

Conferences

- 1337UP LIVE 2022 (playlist)
- BlueHat IL 2022

Tutorials

Medium to advanced

- Google Cloud Storage Explorer: Enumerating Google Cloud's Bucket Access Permissions
- Lucky 13 and other padding oracle attacks on CBC ciphers
- Unconstrained Delegation

Beginners corner

- 6 Privacy Pitfalls for Developers to Avoid
- Getting Started with iOS Penetration Testing (Part 1) & Part 2
- Create an Azure Vulnerable Lab

Writeups

Challenge writeups

- HackTheBox – Stacked & Blog post
- CORS – Lab #1 CORS vulnerability with basic origin reflection
- Intigriti 1337UP CTF (pwn challenges):

- Leaking Values with printf (Format String Vuln) – Search Engine
- Buffer Overflow with Shellcode Injection – Easy Register
- Overwriting RBP with an Off-by-One Buffer Overflow – Cake
- Bypassing Stack Canaries and NX/DEP (Ret2Lib-C) – Bird

Pentest writeups

- Bypass Crowd Strike Falcon to Dump Windows Hashes

Responsible(ish) disclosure writeups

- Prototype Pollution in plist v3.0.4 and simple-plist (CVE-2022-22912) #Web #CodeReview
- How I Discovered Thousands of Open Databases on AWS #Web #Cloud
- How We Discovered Vulnerabilities in CI/CD Pipelines of Popular Open-Source Projects #CI/CD
- Infinite loop in BN_mod_sqrt() reachable when parsing OpenSSL certificates (CVE-2022-0778), PoC by @Drago1729
- CVE-2022-27226: CSRF to RCE in iRZ Mobile Routers through 2022-03-16 #Router #Web
- cr8escape: New Vulnerability in CRI-O Container Engine Discovered by CrowdStrike (CVE-2022-0811)

Known vulnerabilities

- New Linux Vulnerability CVE-2022-0492 Affecting Cgroups: Can Containers Escape? & PoC

Bug bounty writeups

- Securing Developer Tools: Git Integrations (Microsoft, JetBrains, GitHub)
- Git honours embedded bare repos, and exploitation via core.fsmonitor in a directory's .git/config affects IDEs, shell prompts and Git pillagers
- How I Tracked You Around The Globe (Google)
- CVE-2022-22616: Simple way to bypass GateKeeper, hidden for years (Apple)
- Arbitrary file read via the bulk imports UploadsPipeline (GitLab, $29,000)

See more writeups on The list of bug bounty writeups.

Tools

- Smap: Replica of nmap that uses shodan's free API for scanning
- frequest & How I was able to find 50+ Cross-site scripting (XSS) Security Vulnerabilities on Bugcrowd Public Program?: Quickly test multiple URLs for XSS and SQL injection

- DomainAlerting: Get notifications when a new domain name is registered and contains your keywords
- redirex: Go tool that generates bypasses for open redirects
- mksub: Make subdomains using a wordlist
- CrackHound & Intro: Introduce plain text passwords into BloodHound
- AWS Scaled Command Bash Script – Run AWS commands for many profiles

Tips & Tweets

- Oneliner to find subdomain takeovers using BBRF, nuclei and Axiom
- The problem @pry0cc solved with "tew"
- LFI WAF bypass: `.%00./file.php`
- How @xnwup finds secrets in GitHub repos
- Can you spot the vulnerability on the code block below?
- @Jhaddix's testing environment, #BugBountyDiary & The next innovations in recon frameworks

Misc. pentest & bug bounty resources

- Top10 CI/CD Security Risks
- Arya & Intro: The New Tailor-made EICAR Using YARA
- Internal Network Attack Flow
- Cloud Labs AD: Provisioning scripts for an Active Directory lab environment on Azure
- Last Week in Security (LWiS) – 2022-03-21

Articles

- AWS RDS does not force clients to connect using a secure transport layer
- Retrieving your browsing history through a CAPTCHA
- Abusing Arbitrary File Deletes To Escalate Privilege And Other Great Tricks
- Bypassing UAC in the most Complex Way Possible!

Challenges

- Intigriti's March XSS challenge By @BrunoModificato (March 21 – 27)
- Winja CTF – Berlin 2022 (April 9)

- wifichallengelab.com
- CI/CDon't

Bug bounty & Pentest news

- Cybersecurity
  - Researcher uses Dirty Pipe exploit to fully root a Pixel 6 Pro and Samsung S22
  - Okta 'identifying and contacting' customers potentially affected by Lapsus$ breach
  - NPM maintainer targets Russian users with data-wiping 'protestware'
  - Apple Safari empowers developers to mitigate web flaws with WebKit CSP enhancements
- Upcoming events
  - Trace Labs Global OSINT Search Party CTF 2022.03 (March 26)
  - OSINT Summit 2022 (April 7)
- Tool updates
  - tls.bufferover.run cloud data is now refreshing hourly
  - Burp Professional / Community 2022.3 (Collaborator now uses `oastify.com` instead of `burpcollaborator.net`) & New "Fastest" crawl strategy
  - Nuclei v2.6.5 & Interactsh v1.0.2
  - ScoutSuite 5.11.0

Non technical

- Unraveling Assets from Android Apps at Scale
- @NahamSec AMA