Bug Bytes #130 – DOM Invader, The extended BApp store & Will Google kill XSS?

BY ANNA HAMMOND · JULY 7, 2021 · 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 June 28 to July 5.

Our favorite 5 hacking items

1. News of the week

Trusted Types – mid 2021 report
alert() is dead, long live print()

Google is waging war against XSS with Trusted Types and soon disabling alert for cross-domain iframes in Chrome. If you're wondering whether XSS (especially DOM XSS) and alert() are dead, these resources will provide some insightful answers.

2. Tool of the week

Introducing DOM Invader: DOM XSS just got a whole lot easier to find

DOM Invader is a new Burp tool implemented as an extension to the embedded browser. Until Trusted Types are adopted everywhere, DOM XSS is still an issue and this extension will make it much easier to test for it.

3. Writeups of the week

Taking over Uber accounts through voicemail
Kaspersky Password Manager: All your passwords are belong to us
Fail2exploit: a security audit of Fail2ban

@assetnote disclosed a creative Uber account takeover. Basically when signing into the app, they force the OTP to be sent to voicemail which can be hacked in different ways to retrieve the OTP. Even though the report was closed as informative, it is a cool finding and informative writeup.

The second writeup is about Kaspersky Password Manager using a weak password generator. Jean-Baptiste Bédrune found several issues in it, mostly that its PRNG used the current time as a single source of entropy. This meant all passwords could be bruteforced in seconds!

The third writeup isn't about a successful hack, rather about pentesting an open source project and not finding anything. Despite the lack of vulnerabilities, it is an insightful dive into fail2ban's security, and how to approach such a pentest.
@kevin_backhouse shows his methodology from identifying the attack surface to auditing the code and testing for different vulnerabilities.

4. Video of the week

Live Recon on Rockstar Games With @zseano

In this Live Recon session, @zseano shares with @NahamSec his bug hunting workflow and many tips including how he uses Burp.
If you are into Web application security testing, this is a goldmine of information. It's like watching over a bug hunter's shoulder to see how they do their magic.

5. Resource of the week

The extended BApp store & Intro

The BApp Store is great for finding Burp extensions but it lacks some features like a search functionality or knowing when an extension's original repo has updates not yet merged into the BApp Store.
To solve these issues, @BurpSuiteGuide came up with this brilliant site. It allows you to quickly search extensions (including the open source ones that are not yet on the BApp Store), supports tags, and tells you which extensions are deprecated or have updates.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Hacker Heroes #3 – @TomNomNom (Interview)
- Fuzzer Crash Root Cause Analysis With ASAN (AddressSanitizer)
- 20yrs Old Girl Found Bugs In Facebook && Google | Bug Bounty Hunter
- Staying Up-To-Date In CYBERSECURITY!

Podcasts

- The Kaseya Saga – Microsoft PrintNightmare, WD's MyCloud OS3 Troubles, SpinRite in a BMW

Webinars

- Attacking And Defending The Microsoft Cloud (Office 365 & Azure AD)
- Maniacal Keyboards

Conferences

- BSides Amman 2021 2nd Edition – Talks Day
- Wild West Way West RENO!

Tutorials

Medium to advanced

- Using tmux for automating interactive reverse shells
- PimpMyBurp #5 – Intruder: Use the tool to its full advantage
- BITS Persistence For Script Kiddies
- Navigating the impact of Wi-Fi FragAttacks: users, developers and asset owners

Beginners corner

- Hacker tools: Gobuster – the all-in-one tool for you
- JSON Web Token attacks and vulnerabilities
- Exploiting Dependency Confusion
- Docker for Pentesters And Bug Bounty.

Writeups

Challenge writeups

- A (not so) Gentle Intro to Active Directory: Øx [0xF09F8EA3] Challenge
- SQL Injection – Lab #14 Blind SQL injection with time delays and information retrieval

Pentest writeups

- Operation Eagle Eye
- IoT/ICS Armageddon: hacking devices like there's no tomorrow (part 1)
- Protonmail penetration testing report by Securitum

Responsible(ish) disclosure writeups

- Exploiting Less.js To Achieve RCE #Web
- CVE-2021-35368 – CRS Request Body Bypass #Web
- Multiple vulnerabilities in Cisco Identity Services Engine (XSS to RCE as root) & Video PoC #Web

- Microsoft finds new NETGEAR firmware vulnerabilities that could lead to identity theft and full system compromise #Router
- An EPYC escape: Case-study of a KVM breakout #KVM #Virtualization
- Shared License or Crack? Access to 1000+ servers #Web #Binary

0-days

- PrintNightmare / CVE-2021-34527 (originally considered as CVE-2021-1675):
  - What happened
  - Microsoft advisory
  - New attack vectors found by @cube0x0 and @gentilkiwi
  - Exploitability flowchart
  - Metasploit module
  - @byt3bl33d3r's Python scanner

Bug bounty writeups

- Finding DOM Polyglot XSS in PayPal the Easy Way (Paypal)
- How We Are Able To Hack Any Company By Sending Message – $20,000 Bounty [CVE-2021–34506] (Microsoft, $20,000)
- How I found my first Chrome bug (CVE-2021–21210) (Google)

See more writeups on The list of bug bounty writeups.

Tools

- Fleex: Go tool that allows you to create multiple VPS on cloud providers (Linode & DigitalOcean) and use them to distribute your workload
- hashit: Small bash script for encoding piped input to then pass on
- Gotator: A Go tool to generate DNS wordlists through permutations
- storenth/lazyrecon
- Trello_dorker: Google dorker via Serpapi to find exposed Trello boards

Tips & Tweets

- Intercepting localhost traffic on Firefox
- rack_session RCE
- Script to create a MacOS App from Burp Jar file for Macbook M1 users

- XSS via QR code
- A quick hack to modify your font/fontsize settings of Turbo Intruder
- How to run sqlmap with random delays
- Docker image to route all Burp traffic through a VPN via a local proxy
- Build target-based custom wordlists using Turbo Intruder's "observedWords"

Misc. pentest & bug bounty resources

- FFUF Me
- @0xAwali's methodologies for testing Sign Up, ATO: Reset Password & OAuth: Sign Up and Log In
- Android Security Notes
- Offensive Software Exploitation (OSE) Course
- Exploitation Mitigations

Challenges

- TyphoonCon 2021 CTF (July 12-15)
- Hack The Box Business CTF 2021 (for companies only, registration closes on July 16)
- Grammarly $50K CTF (ongoing)
- redpwnCTF 2021 (July 9-12)

Articles

- Towards Systematic Black-Box Testing for Exploitable Race Conditions in Web Apps
- x8, Arjun, Param Miner comparison
- Hunting for Windows "Features" with Frida: DLL Sideloading & Windows Feature Hunter (WFH)
- How a Docker footgun led to a vandal deleting NewsBlur's MongoDB database (TL;DR: Docker edits iptables rules to bypass the firewall, in this case exposing MongoDB to the world)
- Detecting SSH Honeypots with non-persistent filesystems.

Bug bounty & Pentest news

- REvil ransomware attackers demand $70m following Kaseya VSA supply chain attack & 'Apex predators': Why the Kaseya ransomware attack has experts worried
- Introducing the new OWASP Amass Information Sharing Feature (and contest)

- PortSwigger: Women in tech university scholarship scheme
- Upcoming events
  - July Lightning Conference: Beyond the Bounty (featuring Ben Sadeghipour) (July 13)
- Tool updates
  - TLS 1.3 support added to Nmap NSE scripts
  - Hakrawler v2 (complete code rewrite)
  - Measuring Security Risks in Open Source Software: Scorecards Launches V2
  - SpiderFoot 10x speed improvement

Non technical

- Meet the hacker: Tom Hudson
- My Experience For 2 Years In Bug Bounty Hunting

Community pick of the week

That's how you do it! Congratulations @bug_dutch, we're happy for you too

If you too have bug bounty wins, swag and joys to share with other Bug Bytes readers, tag us on social media. We love hearing from you!