Bug Bytes #144 – Bug hunting on the modern Web, Token spraying & Discourse RCE

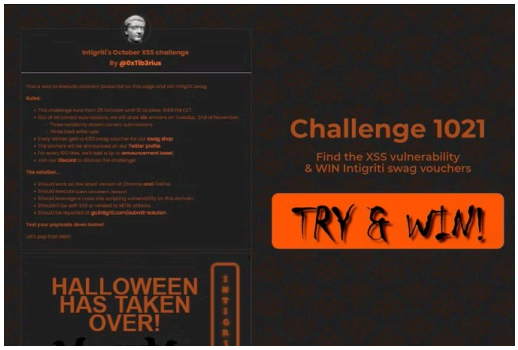
BY ANNA HAMMOND · OCTOBER 27, 2021 · LAST UPDATED ON MARCH 6, 2025

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 October 18 to 25.

Intigriti news



Intigriti's October XSS challenge By @0xTib3rius

Our favorite 5 hacking items

1. Tool of the week

DataExtractor

DataExtractor is a Burp extension by @gwendallecoguic that adds passive scans to extract data from source code.
There are already other tools to do the same thing, but this one is particularly interesting because it is easily customizable. It allows you to ignore extensions and to use regexp to ignore files, extract data or exclude results.

2. Writeups of the week

Discourse SNS webhook RCE (Discourse)

This is a great writeup by @joernchen. He exploited Discourse's AWS notification webhook handler to obtain OS command injection. It wasn't that simple of course! SNS messages must be signed by Amazon. Bypassing the payload's signature involved chaining weaknesses in AWS SNS and in Ruby's x509 parsing, and a lot of staring at the code.

3. Challenge of the week

Design Flaw in Security Product – ALLES! CTF 2021, @LiveOverflow's video, & @gregxsunday's walkthrough

@liveoverflow released this fun Web app challenge that he created for the ALLES! CTF 2021. I don't want to spoil what the vulnerability is, so let's just say that it involves WAF bypass and blind exploitation.

4. Resource of the week

Nuclei token-spray templates, Token Spray – Introduction to self-contained template & A Snapshot of CAST in Action: Automating API Token Testing

Have you ever found an exposed API token without knowing for which service it is intended? This happens often to the Bishop Fox CAST team. So, they created Nuclei templates to quickly check the validity of an API token against all possible services.
Interestingly, these new templates are "self-contained". This new type of Nuclei template "does not require any external information to run, such as target or input URLs."

5. Video of the week

Katie Explains: Modern Web Development (GIVEAWAY)

This is an amazing introduction to the modern Web for bug hunters. If you want to know what today's websites are made of, this is the most beginner friendly video that you'll find.
@InsiderPhD explains microservices, the OOP paradigm, the MVC model, frameworks, middleware, controllers, inheritance, etc, and what all this means in terms of bugs that you should look for.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- S1E1: What is Bug Bounty Hunting & "The Suck Factor", S1E2: Tools – Hacking with "The Firefox", S1E3: Tools – Connect Burp Suite to Firefox and the Advanced Proxy, S1E4: Tools – Notepad++, IP Vanish, Python 3, and Google & S1E5: Payload Basics & Intro to SQL Injection (Login Bypass)
- $2,500 Leaking parts of private Hackerone reports – timeless cross-site leaks
- INDIAN HACKER with Mind BLOWING Achievements HACKING At It's Best...
- Career and Community building with Bug Bounties | NahamCon Panel

Podcasts

- A Slack Attack and a MySQL Scientific Notation Bug [Bug Bounty podcast]

Webinars

- Android Exploits 101 Workshop & Slides
- Landing a Job: Resumes and the Application Process

Conferences

- FuzzCon Europe 2021 – WebSecurity Edition
- ROOTCON 15
- Objective by the Sea, v4.0
- 2021 Layer 8 Conference

Tutorials

Medium to advanced

- Exploiting Request forgery on Mobile Applications.
- Finding Gadgets Like It's 2015: Part 1
- From Default Printer Credentials to Domain Admin
- Servers are overrated – Bypassing corporate proxies (ab)using serverless for fun and profit.
- Lateral Movement – WebClient

Beginners corner

- Attacking Access Control Models In Modern Web Applications
- The Ultimate Guide to Android SSL Pinning Bypass
- Attacks & Defenses: Dumping LSASS With No Mimikatz
- A Primer for Testing the Security of GraphQL APIs
- 8 Different Ways to Bypass SSL Pinning in iOS application

Writeups

Challenge writeups

- Privilege Escalation with MySQL User Defined Functions

- How To Search For CSRF!, How To Circumvent CSRF Protection! & Stored XSS Simplified!
- CSRF – Lab #8 CSRF with broken Referer validation

Pentest writeups

- Shells And SOAP: Websphere Deserialization To RCE & Nuclei template

Responsible(ish) disclosure writeups

- PHP-FPM Local Root Vulnerability #Web
- Moodle – Stored XSS and blind SSRF possible via feedback answer text #Web
- Support Board 3.3.4 Arbitrary File Deletion to Remote Code Execution #Web #CodeReview
- Multiple vulnerabilities in Nagios XI < 5.8.6 #Web #CodeReview
- SuDump: Exploiting suid binaries through the kernel #Linux #LPE

0-day & N-day vulnerabilities

- 50 Shades of SolarWinds Orion Deserialization (Part 1: CVE-2021–35215) & PoC
- GitLab CE CVE-2021-22205 in the wild & Exploit

Bug bounty writeups

- A Scientific Notation Bug in MySQL left AWS WAF Clients Vulnerable to SQL Injection (Amazon)
- CVE-2021-2471 MySQL JDBC XXE (Oracle)
- All Your (d)Base Are Belong To Us, Part 2: Code Execution in Microsoft Office (CVE-2021-38646) (Microsoft)
- Google Chrome Vulnerability Worth for $6K: Use After Free (CVE-2021-30573) (Google, $6,000)
- Deleting all DMs on RedditGifts.com (Reddit, $5,000)
- How I was able to revoke your Instagram 2FA (Facebook, $5,000)
- Hash-Collision Denial-of-Service Vulnerability in Markdown Parser (Reddit, $500)
- IDOR to pay less for coin purchases on oauth.reddit.com (Reddit, $500)

See more writeups on The list of bug bounty writeups.

Tools

- Go Whois: WHOIS library, CLI tool and server with restful APIs to query whois information for domains and IPs
- Fugu14 – Untethered iOS 14 Jailbreak

- ZipExec: A unique technique to execute binaries from a password protected zip for EDR bypass
- Phishious: An open-source Secure Email Gateway (SEG) evaluation toolkit designed for red-teamers

Tips & Tweets

- Turbo Intruder's 'wordlists.observedWords'
- TIL HTTP Digest Authentication was removed in v2020.7
- Payload for XXE in Java apps
- Oneliner to find hidden params in javascript files
- Emails are exposed by default in Slack workplaces
- Kerberos basics & (ab)use of Certificates within Active Directory (i.e. AD CS and PKINIT)

Misc. pentest & bug bounty resources

- New Web Security Academy topic: Advanced request smuggling
- How to Hack Like a Ghost – Breaching the Cloud (starting at $20.99 on Amazon)
- Stored XSS flyer
- OffensiveVBA
- Internal Security Assessment: Field Guide (Updated) (starting at $8.99)

Challenges

- Intigriti's October XSS challenge By @0xTib3rius
- xss-challenge.ysamm.com
- OVIA (Oversecured Vulnerable iOS App)
- Escape the Container – BugHuntr.io

Articles

- Abusing Registries For Exfil And Droppers
- Misusing BeyondTrust Remote Support Leads To Data Exposure
- Using Kerberos for Authentication Relay Attacks & Windows Exploitation Tricks: Relaying DCOM Authentication
- Shadow Attacks ... the smallest attack vector ever
- The 2021 TLS Telemetry Report

Bug bounty & Pentest news

- Not just deprecated, but deleted: Google finally strips File Transfer Protocol code from Chrome browser
- Android Rust Introduction
- UAParser.js npm Package Supply Chain Attack: Impact and Response
- Tool updates
  - Nuclei v2.5.3 (Breaking changes)
  - r2c Semgrep: Taint mode is now in beta
  - CTFNote v2
  - Introducing Shodan Trends