Bug Bytes #118 – Kiterunner, Server-side XSS & Abusing payment systems for free money

BY ANNA HAMMOND · APRIL 14, 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 April 5 to 12.

Intigriti News

Get to know iQimpz, one of Intigriti's top hackers

Our favorite 5 hacking items

1. Article of the week

Contextual Content Discovery: You've forgotten about the API endpoints & Kiterunner

This is about Kiterunner, a groundbreaking content discovery tool that Assetnote released at BSides Canberra 2021. Its premise is that existing tools are mostly based on file/folder bruteforcing with

wordlists. They miss routes in modern apps and APIs that expect specific HTTP methods, headers or parameters.

Kiterunner solves these limitations by performing context-aware bruteforce, based on Swagger files collected from different datasources and by scanning the Internet.

Note that in addition to the tool itself, the article presenting the whole research is a gem. It also links to the Swagger dataset used and slides.

2. Writeups of the week

What if you could deposit money into your Betting account for free? Oh wait where has this 25k came from...
Unexpected Journey #7 – GravCMS Unauthenticated Arbitrary YAML Write/Update leads to Code Execution (CVE-2021-21425)

@mikey96_bh shares interesting research on abusing payment systems of UK online gambling companies. Leveraging logic bugs and bruteforce, it was possible to deposit money ($25k!) for free on his betting account.

The second writeup is a detailed account of a remote code execution @mdisec found in GravCMS. It is an excellent read and a good example of RCE found with PHP code review.

3. Video of the week

XSS to LFI to RCE – Search for LFI everywhere!

Did you know that XSS can be server-side and lead to RCE? That's what this video by @PinkDraconian is all about. It's short but so well-explained!

4. Tool of the week

Autowasp

Autowasp is a Burp suite extension for Web penetration testers. It creates a tab where you can load the OWASP Web Security Testing Guide (WSTG) checklist or your own custom checklist.

Since pentesters often have to follow this type of checklist, the extension streamlines the process. It allows you to keep track of your progress, add comments, note requests related to each check (via a "Logger tab"), etc. All in all, a pretty handy extension!

5. Conferences of the week

NahamCon2021
Exploiting Misconfigured JIRA Instances for $$ with Harsh Bothra & Slides

All NahamCon2021 talks are now public. If you're into bug bounty, recon or Web app security, make sure to check them out! Also for slides and villages talks that were previously released, take a look at Bug Bytes 114.

Another interesting talk by @harshbothra_ is about exploiting misconfigured Jira instances. If you're new to the topic, this is a nice introduction to Jira hacking.

Other amazing things we stumbled upon this week

Videos

- Running Out Of Hacking Video Ideas
- Explaining the exploit to $31,337 Google Cloud blind SSRF
- JSON Web Tokens (JWT)
- Crack passwords with these techniques
- Interview With An XSS Hero: Brutelogic
- SQL Injection – Lab #6 SQL injection UNION attack, retrieving multiple values in a single column

Podcasts

- DAY[0] Episode 72 – Pwn2own, Linux Kernel Exploits, and Malicious Mail
- PwnIt And OwnIt – Port 10080 Blocked, FLoC Rollout, PHP GIT Hack Revisited, CISCO Router Problems
- Darknet Diaries Ep 90: Jenny

Webinars & Webcasts

- How to Perform Effective Web Application Security Assessments

Conferences

- Hacking is NOT a Crime HackerCON
- Exploiting XPC in AntiVirus Software

Slides & Workshop material

- FTP2RCE

Tutorials

Medium to advanced

- Writing Network Templates with Nuclei & Writing nuclei templates for WordPress CVEs

- Red Team Tooling: Writing Custom Shellcode
- Do You Really Know About LSA Protection (RunAsPPL)?

Beginners corner

- Azure Storage Security: Attacking & Auditing & Az-Blob-Attacker
- Exploiting weak configurations in Amazon Cognito
- Digging Deep Into Dom XSS
- Exploit cross-site request forgery (CSRF) – Lab & Exploit a misconfigured CORS – Lab
- Encrypted Reverse Shell for Pentester

Writeups

Challenge writeups

- Bypassing a Super-Secure MFA
- I earned over 4000 euro's following this simple methodology

Responsible(ish) disclosure writeups

- CVE-2021-25646: Getting Code Execution On Apache Druid #Web
- From 0 to RCE: Cockpit CMS #Web
- Royal Flush: Privilege Escalation Vulnerability in Azure Functions #Cloud
- [BugHunt] Authenticated RCE found in HorizontCMS — Part 1 (Malicious Plugins) & Part 2 (PHP Filetype Bypass) #Web
- Time for an upgrade #Network #MiTM

Bug bounty writeups

- Path traversal in Ruby's Tempfile and mktmpdir on Windows (Ruby, $500)
- Stored XSS on the DuckDuckGo search results page (DuckDuckGo)
- CVE-2020-27069 & Other APVI writeups
- Unauthenticated Account Takeover Through Forget Password
- XSS at https://www.glassdoor.com/Salary/* via filter.jobTitleExact (Glassdoor, $900)
- Intro to Open-source Bug Bounty (Mailtrain)

See more writeups on The list of bug bounty writeups.

Tools

- PD Actions & Intro : Continuous recon and vulnerability assessment using Github Actions
- burpsuite-copy-as-xmlhttprequest: Burp extension that allows you to copy multiple requests as Javascript's XmlHttpRequest, which simplifies PoC development when exploiting XSS
- Kubesploit & Intro : A cross-platform post-exploitation HTTP/2 Command & Control server and agent written in Golang, focused on containerized environments
- goop: Yet another tool to dump a git repository from a website
- GodSpeed: Fast and intuitive manager for multiple reverse shells
- protoscan: Prototype Pollution Scanner in Golang, based on @TomNomNom's NahamCon2021 talk
- Bloodhound for Linux & Intro: Ingest openldap data into bloodhound

Tips & Tweets

- Escalating Spring and FreeMarker Template Injection to RCE
- CloudFlare XSS bypass using `?.`
- A nice way to grab deeplinks on iOS
- Using glow to search repos like PayloadsAllTheThings & HackTricks
- Escaping out of a double-quoted string when `a"` is reflected as `a\"`
- BBRF allows you to run advanced jq queries on your data, like list urls that you haven't scanned yet
- Lessons learned from using k8s clusters for bug bounty recon

Misc. pentest & bug bounty resources

- The Extended AWS Security Ramp-Up Guide
- @TJ_Null's new list of VM's from @offsectraining Proving Grounds Practice Environment
- HashingZine & SOPZine
- Windows privilege escalation cheat sheet
- Ultimate List of Nmap NSE Scripts (Interactive Spreadsheet)

Challenges

- Full Stack Web Attack – RCE Challenge
- Cybears CTF

- 10kchallenge

Articles

- Rootless Sniffing
- XSS filter bypass: using DOM APIs to generate characters that aren't allowed
- A closer look at the security of React Native biometric libraries
- Detecting Exposed Cobalt Strike DNS Redirectors
- HTML Maldoc Remote Macro Injection
- Man in the Terminal & cliProxy

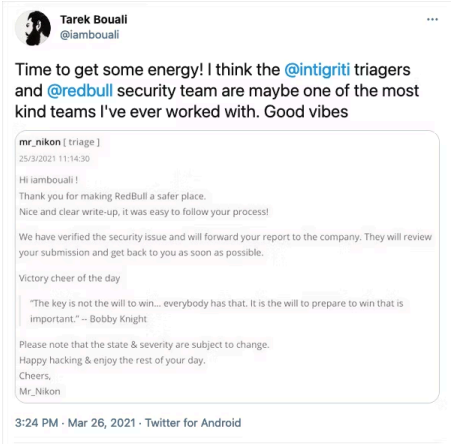
Bug bounty & Pentest news

- Pwn2Own 2021: Zero-click Zoom exploit among winners as payout record smashed
- BugBountyHunter.com Updates
- dnssecuritytxt
- Update on git.php.net incident
- A security researcher has dropped a Chrome and Edge zero-day on Twitter
- PlaidCTF 2021: Plaid+ (April 16)

Non technical

- Beginners Bug Bounty – what bug classes should you start with?
- Get to know iQimpz, one of Intigriti's top hackers
- How To Succeed In Bug Bounties As A Pentester
- The Power of Being a Misfit: Speaking with Fredrik Alexandersson STÖK
- Bug bounty burnout and your mental health

Community pick of the week



Thank you for the compliment @iambouali, you are too kind!

Do you also have bug bounty wins, swag and joys to share with other Bug Bytes readers? Tag us on social media, we love to hear from you!