Bug Bytes #126 – XSS in AWS, exotic Python RCE vectors, zseano's methodology

BY ANNA HAMMOND · JUNE 9, 2021 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-126-xss-in-aws-exotic-python-rce-vectors-zseanos-methodology

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 May 31 to June 7.

Intigriti News

The Ethical Hacker Insights Report 2021 webinar

Our favorite 5 hacking items

1. Conference of the week

Unexpected Execution: Wild Ways Code Execution can Occur in Python & Repo

In this talk, Graham Bleaney and Ibrahim Mohamed show several functions that enable Remote Code Execution in Python other that the standard eval and exec libraries. This is so insightful for anyone interested in RCE, SSTI or Deserialization vulnerabilities in Python apps.

2. Writeup of the week

XSS in the AWS Console (Amazon)

@Frichette_n found two XSS vulnerabilities in AWS Console. Like he says, the writeup has everything from XSS to CSP bypass, Client-Side template injection and memes. A great read and cool findings!

3. Resources of the week

zseano's methodology & Other BugBountyHunter.com news
NotKeyHacks

@zseano's methodology is freeee! It's a 71 pages ebook where he details his own methodology for bug hunting, including tools and all the questions he asks himself at each step that allow him to find vulnerabilities that most people miss.

@dee__see's NotKeyHacks is such a great idea! It's the opposite of KeyHacks, so a collection of tokens that look sensitive but are not. Next time you intent to report hardcoded tokens or API keys, make sure to check if they appear in this repo.

4. Tools of the week

XSS Hunter Express

page-fetch & What is a Prototype Pollution vulnerability and how does page-fetch help?

If you want a self-hosted version of XSS Hunter to test for Blind XSS, this is it! @IAmMandatory re-wrote the tool to make it easy to install and maintain thanks to Docker and Let's Encrypt certificates.

page-fetch is @TomNomNom's latest open source tool that helps test for client-side bugs like Prototype pollution. It comes with a detailed tutorial on this vulnerability class, how it works and how page-fetch helps detect it.

5. Tutorial of the week

ASP.NET Cryptography for Pentesters & Cheatsheet

This tutorial by @paulmmueller covers the practical exploitation of ASP.NET cryptography, with a cheatsheet for pentesters. This could be an invaluable resource when you're testing an ASP.NET app for the first time.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Learn with @trouble1_raunak: Cloud Pentesting – Azure (Illicit Consent Grant Attack) !!
- Hacker Culture Meritocracy?
- This Website Has No Code or Does It?

Podcasts

- SecuriTEA & Crumpets – Episode 8 – Andy Li – Segment
- Extrinsic Password Managers – Great CyberSecurity Awakening of 2021, NAT vs IPv6, Tavis Ormandy

Webinars

- WWHF | Abusing Microsoft Office for Post-Exploitation – Kyle Avery – 1 Hour

Conferences

- Black Hat Europe 2020
- SSTIC 2021

Tutorials

Medium to advanced

- Writing security templates for Apache Airflow
- Retrieving AWS security credentials from the AWS console
- Why your exploit completed, but no session was created? Try these fixes..
- Public Remote File Share in The Cloud
- Object Injection to SQL Injection

Beginners corner

- How to properly install Nuclei
- Hacker tools: Amass – hunting for subdomains
- Getting Started with Android Application Security
- Thick Client Penetration Testing Approach

- An Introduction to Manual Active Directory Querying with Dsquery and Ldapsearch

Writeups

Challenge writeups

- Intigriti's 0521 XSS challenge (by @GrumpinouT) winners & @GrumpinouT's solution

Pentest writeups

- PHPObjectInjection: LFI to RCE
- Passbolt security audit 2021 #PentestReport

Responsible(ish) disclosure writeups

- Joomla Password Reset Vulnerability And A Stored XSS For Full Compromise #Web
- XSS to Account Takeover — Gambling Sites #Web #DOMXSS
- Pwning a Backend with a Backdoor #Web
- The 0xDABB of Doom: CVE-2021-25641 #RCE #Dubbo
- CVE-2021-3198 and CVE-2021-3540: MobileIron Shell Escape Privilege Escalation Vulnerabilities #Web
- XSS to Account takeover in payu.in #Web
- WE.LOCK: Unlocking Smart Locks with Web Vulnerabilities #SmartLocks #IoT

N-day vulnerabilities

- POC Exploit from a CVE: Apache Airflow 1.10.10. RCE
- Vcenter Server CVE-2021-21985 RCE PAYLOAD, Nmap NSE script & Learning JNDI Injection From CVE-2021-21985
- Akamai EAA Impersonation Vulnerability – A Deep Dive #SAML
- WordPress PHPMailer vulnerability analysis
- SolarWinds Orion Deserialization to RCE vulnerability analysis (CVE-2021–31474)

Bug bounty writeups

- XSS in the AWS Console (Amazon)
- Exploiting Open Redirect – Whitelist Bypass Using Salesforce Environment
- Shopify Multipass Misconfiguration
- Executing CSRF With Phone Validation
- Android: Exploring vulnerabilities in WebResourceResponse

- Pop-Ups in a good-world ($2,000)
- Server Side Request Forgery – A Forged Document ($500)
- Header modification results in disclosure of Slack infra metadata to unauthorized parties (Slack, $500)
- Blind XSS on Google Nest (Google)

See more writeups on The list of bug bounty writeups.

Tools

- PrOfESSOS & Security Analysis in an OpenID Connect Lab Environment: An open source implementation for fully automated Evaluation-as-a-Service for SSO
- Spyse API wrapper for Go: The official wrapper for Spyse API, written in Golang, aimed to help developers build their integrations with Spyse
- Pinaak: A bash script that automatically finds vulnerable paramters and runs some commonly used tools to find various vulnerabilities
- Request Logger: @adamtlangley's dockerized application for logging HTTP and DNS requests

Tips & Tweets

- Simplifying the development of your own one-shot extensions
- How to create a custom audit profile in Burp to only scan for passive issues from extensions
- How to easily search through Hackerone reports? #shorts
- 20 Burp Suite tips from the Burp user community
- Invalid UTF sequences in Burp

Misc. pentest & bug bounty resources

- NoSql Injection Cheatsheet
- The 10 Most Popular Bug Bounty Courses and Training Programs for Beginners
- Open Source Insights (deps.dev)
- Android Application Penetration Testing Mindmap & 2FA Bypass Techniques MindMap

Challenges

- Metarget: Framework providing automatic constructions of vulnerable infrastructures
- hpAndro Vulnerable Android Application Challenges

Articles

- CloudFare and Abusing HTTP Cache
- Baking Mojolicious Cookies
- UI Security – Thinking Outside the Viewport
- Your Microsoft Teams chats aren't as private as you think..

Bug bounty & Pentest news

- Hack Hard. Have Fun. Increase Security
- Supreme Court Overturns Overbroad Interpretation of CFAA, Protecting Security Researchers and Everyday Users
- GitHub changes policy to welcome security researchers
- Do you have a Burp extension or recon project idea? @Regala 's offering bounty based sponsorship
- Upcoming events:
  - GitLab: Join us on for an AMA with @vakzz (June 16)
  - THCon 2021 (June 11)
- Tools updates:
  - Interactsh web client now supports self-hosted instances
  - Gau: concurrency added with new `-t` flag
  - Kali Linux 2021.2 Release (Kaboxer, Kali-Tweaks, Bleeding-Edge & Privileged Ports)
  - New Hashcat feature: autodetect hash-mode
  - pwncat: several fundamental framework updates including adding Windows support

Non technical

- Think outside the box with Devansh Batham
- Hacker Spotlight: hunt4p1zza & pmnh & Bug Bounty Update: Introducing our Most Valuable Hackers!
- Accessibility in Security
- Password Managers.

Community pick of the week

Awesome! It looks good, @sumgr0, and is very well deserved!

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!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com