Bug Bytes #148 – Google SSRF filmed, A 1 N/A bug to $15k & Tuning raced conditions

BY ANNA HAMMOND · NOVEMBER 24, 2021 · LAST UPDATED ON MARCH 6, 2025

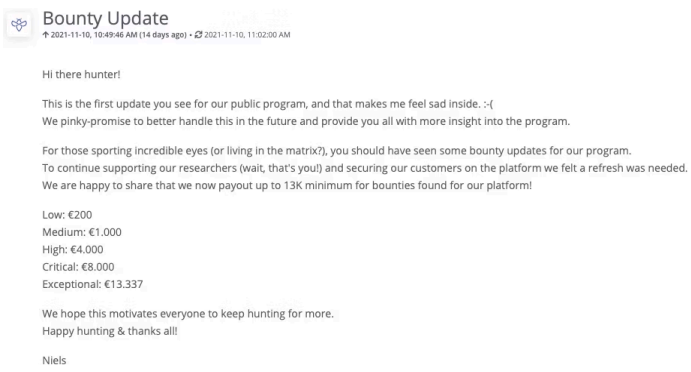
Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

CLICK HERE TO SUBSCRIBE

This issue covers the week from November 15 to 22.

Intigriti news

Why join Intigriti? Here's 16 reasons why you'll love working here


Bounty Update

2021-11-10, 10:49:46 AM (14 days ago) • 2021-11-10, 11:02:00 AM

Hi there hunter!

This is the first update you see for our public program, and that makes me feel sad inside. :-(
We pinky-promise to better handle this in the future and provide you all with more insight into the program.

For those sporting incredible eyes (or living in the matrix?), you should have seen some bounty updates for our program.
To continue supporting our researchers (wait, that's you!) and securing our customers on the platform we felt a refresh was needed.
We are happy to share that we now payout up to 13K minimum for bounties found for our platform!

Low: €200
Medium: €1.000
High: €4.000
Critical: €8.000
Exceptional: €13.337

We hope this motivates everyone to keep hunting for more.
Happy hunting & thanks all!

Niels

Increase in the Intigriti program's bounty table

Our favorite 5 hacking items

1. Video of the week

Reacting to myself finding an SSRF vulnerability in Google Cloud & Blog post (Google, $10,401.1)

@xdavidhu discovered an SSRF on Google Cloud and filmed the entire process from the bug's discovery, to exploiting it for RCE, creating the PoC, reporting it, then bypassing the fix.
If you've ever dreamed of peeking over the shoulder of a bug hunter *while* they are finding a critical bug (not just doing recon or practicing in a lab), this is a truly rare opportunity.

2. Writeups of the week

Finding Zero-Day Vulnerabilities in the Supply Chain
How I accidentally hacked many companies using N/A vulnerability in Atlassian Cloud (Atlassian, $15,000)

The first writeup is about CSTI, bypassing signed requests (with a JavaScript breakpoint), and exploiting an SSRF with the SMB scheme to steal NTLM hashes. The techniques are not new but @0xLupin does an amazing job of explaining these critical pentest findings, and showing how to escalate the bugs' impact as much as possible.

The second writeup by @Krevetk0Valeriy is about issues in the Atlassian Cloud's registration flow. This is an interesting read if you like authentication bugs, or an example of digging deep into strange behaviors so that an N/A turns into a $15k finding.

3. Resource of the week

FirstBloodv2 disclosed reports

BugBountyHunter disclosed writeups submitted by members during their last *Hackevent*, FirstBlood v2. If you can't get enough of bug bounty writeups, this is a nice collection to explore whether you are interested in server-side, client-side or logic vulnerabilities.

4. Tools of the week

ChronoRace
h2rs

ChronoRace is a Python tool for fine-tuning race condition attacks. @itscachemoney used it to execute carefully timed race condition attacks that circumvent application business logic, such as this email confirmation bypass on Shopify.

If HTTP request smuggling is more your thing, you might be interested in h2rs. This Python tool by @ricardo_iramar can detect request smuggling via HTTP/2 downgrades.

5. Conference of the week

Swiss Cyber Storm 2021 & Slides, especially:

- Impact of Frameworks on Security of JavaScript applications By Ksenia Peguero
- mXSS in 2021 – One long solved problem? By Mario Heiderich
- Bug Bounty Switzerland: Tales and Vulnerabilities from our Bug Bounty Adventures
- Patterns and anti-patterns in software development By Philippe de Ryck

- State of the art credential stuffing By Jarrod Overson

I haven't heard of Swiss Cyber Storm before, but wish I did. These talks are excellent and particularly relevant to Web app testers. Make sure to give them a watch for the state-of-the art of mutation XSS, JavaScript apps security or interesting bug bounty tales.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Server-Side Request Forgery (SSRF) | Complete Guide
- Find endpoints in the blink of an eye! GoSpider – Hacker Tools
- S1REN: OSCP Prep Advice
- Testing Your Assumptions with Red Teaming (feat. @mangopdf)

Podcasts

- Radio Hack Ep7: Ransomwares – John Hammond

Webinars

- Analyzing source code for vulnerabilities: A how-to workshop

Conferences

- Using binary search algorithms for blind SQL injection by Juan Pablo Quiñe Paz
- Ekoparty 2021: Main Track & Bug Bounty Space, especially:
  - How to do Code Review by Shubs
- INTENT (Security Research Summit) Talks On Demand

Conference slides, material & whitepapers

- XSinator.com: From a Formal Model to the Automatic Evaluation of Cross-Site Leaks in Web Browsers & XSinator.com (XS-Leak browser test suite)
- DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale, DoubleX tool repo & Tutorial
- Out of Sight, Out of Mind: Detecting Orphaned Web Pages at Internet-Scale

- Ceterum censeo: Visited esse delendam & Research has come a long way, but gaps remain – security researcher Artur Janc on the state of XS-Leaks

Tutorials

- Backdooring Rust crates for fun and profit
- An introduction to secure code review on Go applications
- A simple Data Exfiltration! (Blind XXE via Excel file upload)

Writeups

Challenge writeups

- Client side template injection (CSTI) – November XSS Challenge Writeup & Winners and more writeups
- HackTheBox – BountyHunter
- How to turn an XXE into an SSRF exploit!

Pentest writeups

- Pentest tale – Dumping cleartext credentials from antivirus #Windows #PostExploitation
- Finding a 0 Day Race Condition #ThickClient

Responsible(ish) disclosure writeups

- All Roads Lead To OpenVPN: Pwning Industrial Remote Access Clients #VPN #Web
- PoC of CVE-2021-42321, Exchange Post-Auth RCE & Some notes about Microsoft Exchange Deserialization RCE (CVE-2021–42321) #Web
- CVE-2021-43557: Apache APISIX: Path traversal in request_uri variable #Kubernetes
- CVE-2021-41277: Metabase LFI & Nuclei template #Web
- Diving into Open-source LMS Codebases #Web #CodeReview

Bug bounty writeups

- CVE-2021-42306 CredManifest: App Registration Certificates Stored in Azure Active Directory (Microsoft)
- Impact of an Insecure Deep Link
- Write Up – Apple N/A: PII Information, Full Contact List, Main Phone No. And Main Icloud Email Extracted; Bug Patched: Arbitrary Local File Read Via Zip File And Symlinks On Ios Files App.
- The tale of CVE-2021–34479 (VSCode XSS) (Microsoft)

- A common defect in java system-Memory DoS (include CVE-2021-2344, CVE-2021-2371, CVE-2021-2376, CVE-2021-2378) (Oracle)

See more writeups on The list of bug bounty writeups.

Tools

- TProxer: A Burp Suite extension made to automate the process of finding reverse proxy path based SSRF
- hakfindinternaldomains: Go tool that takes a list of subdomains, resolves them and tells you which ones are internal
- Jira-Lens: Fast and customizable vulnerability scanner For JIRA written in Python

Tips & Tweets

- Strict CSP is now defined in the CSP spec
- You don't need to use a proxy/vpn when blocked by a WAF...
- Apache mod_proxy SSRF PoC added to Assetnote's glossary of blind SSRF chains
- The Kelvin sign 'K' becomes 'k' when lowercased
- Need help with a vuln? Ask @Masonhck3571!

Misc. pentest & bug bounty resources

- GCP pentesting methodology (HackTricks)
- Living Off Trusted Sites (LOTS) Project
- @0xAwali's methodology for testing File Generation & Sensitive Response
- K8S Nuclei Templates
- Web Attack Cheat Sheet

Challenges

- HackTheBox Secret CTF 2021 (December 1-5)
- TryHackMe's Advent of Cyber 3 (2021) (December 1-25)
- 2021 Metasploit Community CTF (December 3-6)
- XSS challenge by @ankursundara

Articles

- New Type of Supply Chain Attack Could Put Popular Admin Tools at Risk
- Identity Security Authentication Vulnerability
- GitHub Apps – How to avoid leaking your customer's source code with GitHub apps
- Abusing Google Drive's Email File Functionality
- Spoofing Calendar Invites Using .ics Files

Bug bounty & Pentest news

- Black Friday
  - InfoSec Black Friday Deals 2021
- Bug bounty
  - Inside the Mind of a Hacker 2021 Edition
- Upcoming events
  - YASCON 2021 (November 28)
- Tool updates
  - Eyeballer 2.0 Web Interface and Other New Features
  - Semgrep: New, high-signal rules for the JavaScript ecosystem
  - Dalfox 2.6 Released
  - dnsx v1.0.7

Non technical

- Todayisnew And Hx01 On Collaboration
- Scanning Millions of Publicly Exposed Docker Containers – Thousands of Secrets Leaked