



Bug Bytes #193 – Top 10 Web Hacking Techniques for 2022, Confessions of the Community and Filter Evasion

BY TRAVISINTIGRITI · FEBRUARY 22, 2023 · LAST UPDATED ON MARCH 6, 2025

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

This issue covers the weeks from February 13th to February 19th

[CLICK HERE TO SUBSCRIBE](#)

Intigriti News

- [We're incredibly happy to share the latest Hacker Portraits with you! Congrats to Foobar7, Renniepak and WonderU](#)
- [Intigriti's February Challenge is over! Check out the cool write ups!](#)
- [We welcome @ninjakiwigames to the platform! Ninja Kiwi Games are the creators of hit computer game franchises Bloons, Bloons TD and SAS: Zombie Assault for mobile and web.](#)
- [More game hacking programs = more game hacking videos](#)
- [Code Snippet Challenge](#) and [the solution](#)
- [Safe harbor legal framework for ethical hacker officially launches in Belgium](#)

From my notebook

This week we saw the release of the top 10 web hacking techniques for 2022. Something that jumped out at me is that they are either very technical and rely on you knowing a lot about how a piece of technology works, or very logical and require you to go through a lot of steps and break the flow. It's cool to see OAuth take the top spot here, it's always been a technology that a lot of developers implement but flows can be complex so it's often insecure! Other articles for this week include some different perspectives on Bug Bounty hunting with a triager, program manager and bug hunter, some fun news and views from Critical Thinking and a list of missing CVEs in nuclei templates in case you'd like to contribute to the community.

1. [Top 10 web hacking techniques of 2022 by Portswigger!](#)
2. [Weekly updated list of missing CVEs in nuclei templates official repository](#)
3. [Confessions of a bug bounty program manager](#) & [Confessions of a top-ranked bug bounty hunter](#)
4. [The View from the Other Side: A Security Analyst's Perspective on Bug Bounty Triage](#)

5. [Episode 7: PortSwigger Top 10, TruffleSecurity Drama, and More!](#) (I also liked this one that I forgot to include last week! [Episode 6: Mobile Hacking Attack Vectors with TeknoGeek \(Joel Margolis\)](#))

Other Amazing Things

Videos

- [How to Bug Bounty in 2023](#)
- [Deep Dive into Parsing SSH Keys](#)
- [I Saw 8 MILLION Phishing Scams](#)
- [Malicious JavaScript Vjw0rm / STRRAT Analysis](#)
- [How Hackers Can Bypass Your Security Defenses](#)
- [VPNs, Proxies and Secure Tunnels Explained \(Deepdive\)](#)
- [Evading Filters to Dump Databases \(like a hacker\)](#)
- [Let's Recon With Vaibhav | Hacker2Hacker | #osint #bugbounty](#)
- [Live TV Hacked In Iran... Again](#)

Podcasts .|||..|||

- [188 - Rusty Kernel Bugs, mast1c0re, and OpenSSH](#)
- [Srsly Risky Biz: North Korean ransomware, Biden flags US privacy reform](#)
- [Synthetic voices, ChatGPT reflections, and social skirmishes](#)
- [Risky Business #695 — North Korea is ransomwaring hospitals, Russia to make "patriotic" hacking legal](#)
- [SN 910: Ascon - Malicious ChatGPT Use, Google Security Key Giveaway, OTPAuth](#)
- [187 - Top 2022 Web Hacking Techniques and a Binance Bug](#)

- [NO. 369 | Reddit Hack, Deepfake Scams, Embracing Change...](#)
- [EP108 How to Hunt the Cloud: Lessons and Experiences from Years of Threat Hunting](#)
- [Why Do NFTs Disappear? \[ML B-Side\]](#)
- [Episode 362 – A lesson in Rust from Carol Nichols](#)

Tweets

- [Bee shares rescope](#)
- [Hussein's BSides Ahmedabad talk](#)
- [Stored XSS Leads to full org Takeover](#)
- [Zseano struggles to find a bug so he's taking a little break](#)
- [Nahmsec: You have a reverse shell/RCE and you can only run one command and one command only](#)
- [Info disclosure thanks to a .env file](#)
- [Executing Custom Database Scripts from an Un-authorized Roles.](#)
- [Linode bans Axiom and other recon tools](#)
- [DNS X updated](#)
- [Name a youtube channel whose videos you cant miss](#)

Tutorials

- [LFI -> RCE -> Escaping Docker. A TryHackMe CTF \(part 1\)](#)
- [Level Up Your Cybersecurity Game: 100 Places to Hone Your Ethical Hacking Skills](#)
- [Introduction to SSRF Exploitation: A Practical Tutorial for Ethical Hackers—StackZero](#)
- [AWS Lambda script to delete Inactive Users](#)
- [Bypass Jailbreak Detection in Flutter apps](#)

- [Demystifying CORS](#)
- [Server side prototype pollution, how to detect and exploit](#)
- [ChatGPT Hacking Prompts, SQLi, XSS, Vuln Analysis, Nuclei Templates, and more](#)
- [Building a one-shot recon script with Project Discovery tools](#)
- [Hacking the cloud](#)

Write ups

- [Hacking Apple: Two Successful Exploits and Positive Thoughts on their Bug Bounty Program](#)
- [Business logic flaw, the enemy of scanners](#)
- [How I found an IDOR that led to sensitive information leak?](#)
- [For the first time in Kurdistan and Iraq, we organized a hacking AND CTF challenge conference](#)
- [Hacking the Search Bar: The Story of Discovering and Reporting an XSS Vulnerability on Bing.com](#)
- [Found an URL in the android application source code which lead to an IDOR](#)
- [\\$\\$\\$\\$ IDOR's—How to find IDORs in Ecommerce sites?](#)
- [Stealing in motion. Immunefi bounty hunting from different ANGLE.](#)
- [The Inside Story of Finding a Reverse Transaction Vulnerability in a Financial Application](#)
- [Have a safe flight \(hacking the boarding pass\)](#)
- [A tale of a full Business Takeover—Red Team Diaries](#)
- [WAF Bypass + XSS on The MOST Popular Movie Ticket website.](#)
- [I GOT UNITED NATION'S HALL OF FAME WITH THIS SIMPLE TECHNIQUE!](#)
- [Heart Bleed Bug In An Indian Government Server](#)
- [Bypassing CORS configurations to produce an Account Takeover for Fun and Profit](#)
- [Logic Error Bug Fix Review](#)
- [Bypassing SameSite=lax cookie restrictions to preform CSRF resulting to a horizontal privilege...](#)
- [Blind Time-based SQL injection vulnerability in an Indian government website](#)

- [Facebook bug: A Journey from Code Execution to S3 Data Leak](#)

Tools

- [Reverseip_Py - Domain Parser For IPAddress.com Reverse IP Lookup](#)
- [Upload Bypass Carnage - File Upload Restrictions Bypass, By Using Different Bug Bounty Techniques!](#)
- [Fearless CORS: a design philosophy for CORS middleware libraries \(and a Go implementation\)](#)
- [Reverse shell generator](#)

Tips

- [Proxy to burp from your terminal](#)
- [Debugging by asking yourself a question](#)
- [Interesting account takeover method using a new line character](#)
- [Apache server status](#)
- [SQL injection tips](#)
- [Burp Suite certified practitioner study tips](#)
- [File upload cheatsheet](#)

REQUEST A DEMO

intigrity.com/demo

VISIT THE WEBSITE

intigrity.com

GET IN TOUCH

hello@intigrity.com