Intigriti Bug Bytes #234 - March 2026

BY AYOUB · MARCH 27, 2026 · LAST UPDATED ON APRIL 23, 2026

Hello hackers,

Welcome to the latest edition of Bug Bytes! In this month's issue, we'll be featuring:

- Earning $180K via SSRFs
- Free Burp Suite Pro licenses for top hackers
- Bypassing tricky file upload restrictions
- Injecting malicious code into AI coding assistants

And so much more! Let's dive in!

New: PortSwigger collaboration with Intigriti

We've teamed up with PortSwigger to reward high-performing researchers on our platform. Any hacker who earns 400+ valid reputation points in a single quarter will receive a free 6-month Burp Suite Professional license.

This is our way of equipping the community with professional-grade tooling so you can hunt deeper, work faster, and focus on what matters, while finding impactful bugs. Licenses are checked quarterly and are available once per researcher per year.

Intigriti collaborates with PortSwigger to support ethical hacking excellence

Learn more

New: Intigriti Hacker Ambassador program

We've launched the Intigriti Hacker Ambassador Program, a new initiative designed to support the people who are already helping the community grow. Whether you run local meetups, mentor newcomers, create content, or organize study groups, this program gives you the recognition, resources, and access to take your community efforts further.

It's a one-year commitment with flexible participation, and we're starting with a pilot group across different regions before expanding through a structured application process.

If you're passionate about growing your local hacker scene, you may apply through the following link.

Intigriti launches new global Hacker Ambassador Program

Learn more

Hacker Spotlight: Marc-Oliver Munz (c1phy)

Our second Hacker Spotlight features Marc-Oliver Munz (c1phy), an ethical hacker from Germany who got into bug bounty during COVID after spending time on HackTheBox.

In this interview, we chatted with him about how curiosity shaped his journey, the trends he's seeing in the industry, and his approach to finding critical bugs across a global range of targets.

If you're looking for inspiration or practical insights from an experienced hunter, be sure to read the full interview.

From curiosity to critical bugs: Interview with Marc-Oliver Munz (c1phy)

[Read the full interview]

Upcoming: Intigriti Bug Bounty Meetup in Stuttgart

Our newest Hacker Ambassador, c1phy, is hosting the first Intigriti bug bounty meetup in Germany! Whether you're just getting started or you're a seasoned hunter, join us for talks, hands-on hacking, and community networking.

Event details:

April 19, 2026

Shackspace, Stuttgart

14:00 – Open End

Please note that registration is required (link below).

Upcoming: Intigriti Bug Bounty Meetup in Stuttgart, Germany

Register today

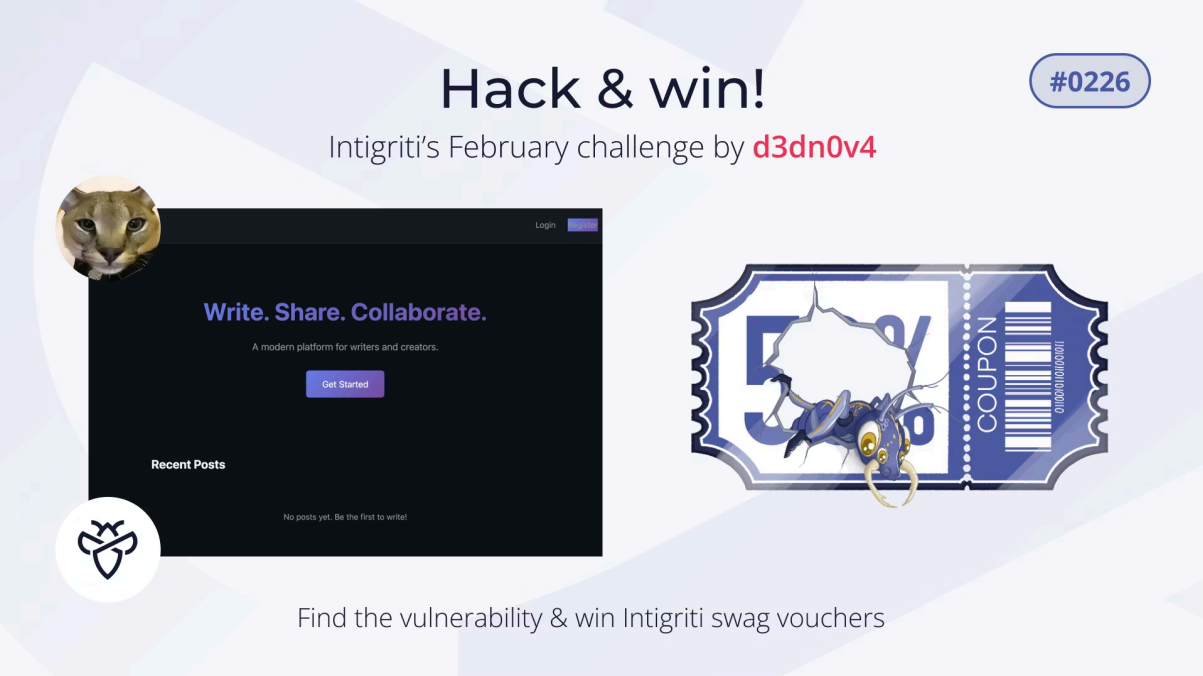
Intigriti 0226 InkDrop CTF results are in

February's CTF challenge featured a collaborative writing platform, deliberately vulnerable to a DOM-based XSS vulnerability. Since a strict CSP prevented code execution from malicious sources, the trick was to bypass the CSP to ultimately capture the admin's flag.

Quick recap:

- 182 hackers reported the correct flag
- First blood went to arturs911
- And 30 hackers wrote a nice write-up

If you want to put your hacking skills to the test, be sure to give Inkdrop 0226 CTF a go before heading over to the Bugology, where you can find all the researchers' submitted solutions.

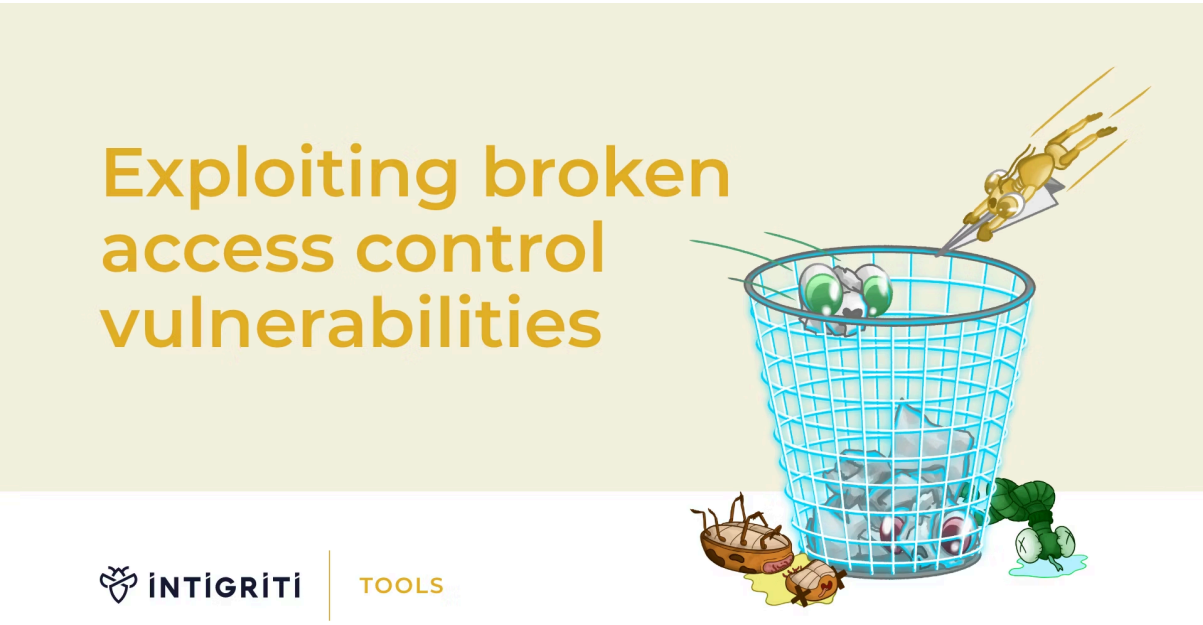


Intigriti 0226 InkDrop CTF Challenge

[Read the write-ups]

Blogs & videos

Exploiting broken access control vulnerabilities



Exploiting broken access control vulnerabilities Cover Image

Broken access control vulnerabilities have consistently remained at the top of the OWASP Top 10, and for a good reason. In our latest technical guide, we break down how these vulnerabilities arise from flawed authorization logic and walk you through some practical exploitation scenarios, ranging from simple

IDORs to more advanced scenarios. If you're looking to sharpen your methodology for testing broken access control vulnerabilities, this one's a must-read.

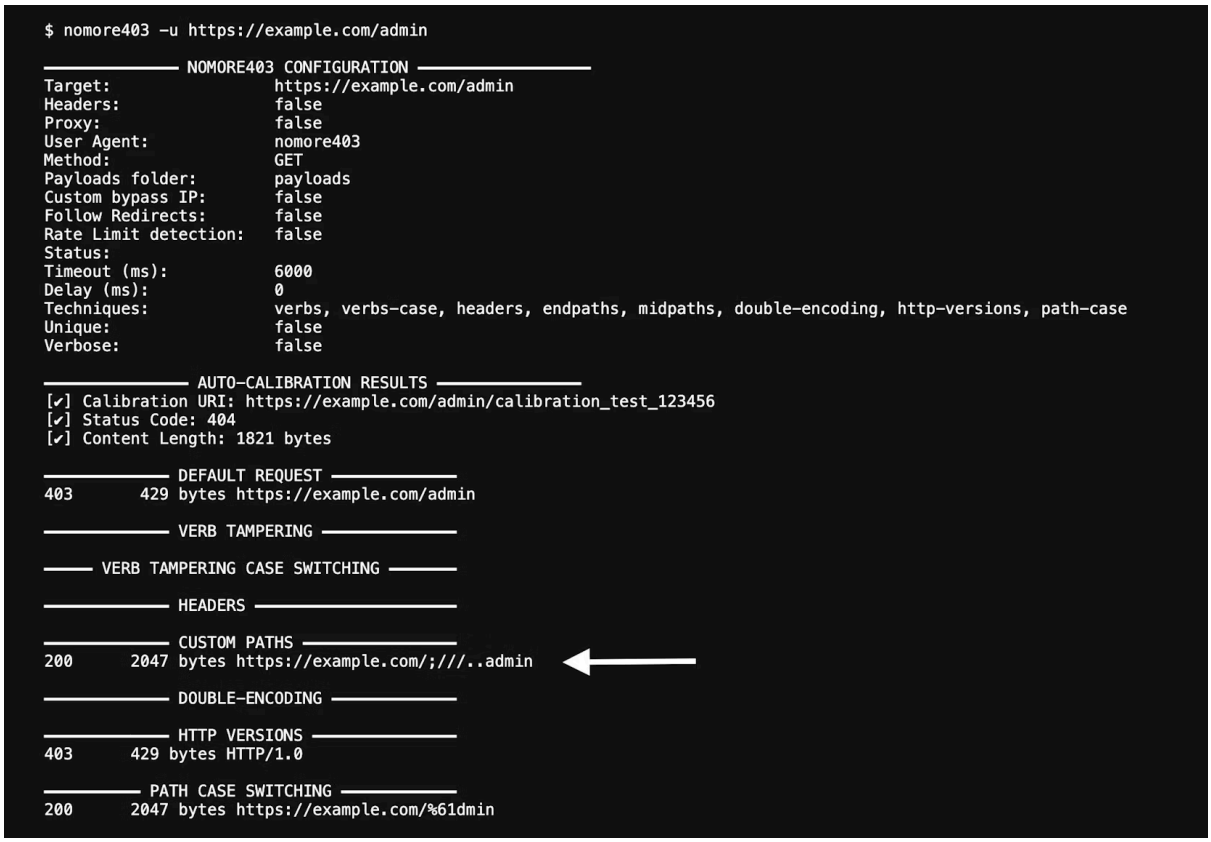
- **We've noticed a spike in AI-generated vulnerability reports.** Some are great, others sadly never met the bar. In our latest article, we share practical tips on how to use LLMs effectively to craft better reports without falling into common pitfalls, such as submitting unvalidated proofs of concept, including hallucinated payloads, or generic responses to feedback requests.

- **March's CTF challenge featured another surprisingly vulnerable target, with the goal of capturing the flag using an XSS.** Despite a strict CSP and restricted DOMPurify implementation, it was still possible for us to achieve XSS and read the flag. Our official write-up walks you through the entire exploitation chain step by step.

Tools & resources

Tools

Nomore403



Nomore403

Being blocked by 403 isn't fun. Nomore403 by @devploit automates several different bypass techniques, from header manipulation to HTTP request method tampering. It also incorporates smart auto-calibration that helps with fuzzing at scale and filtering out false positives.

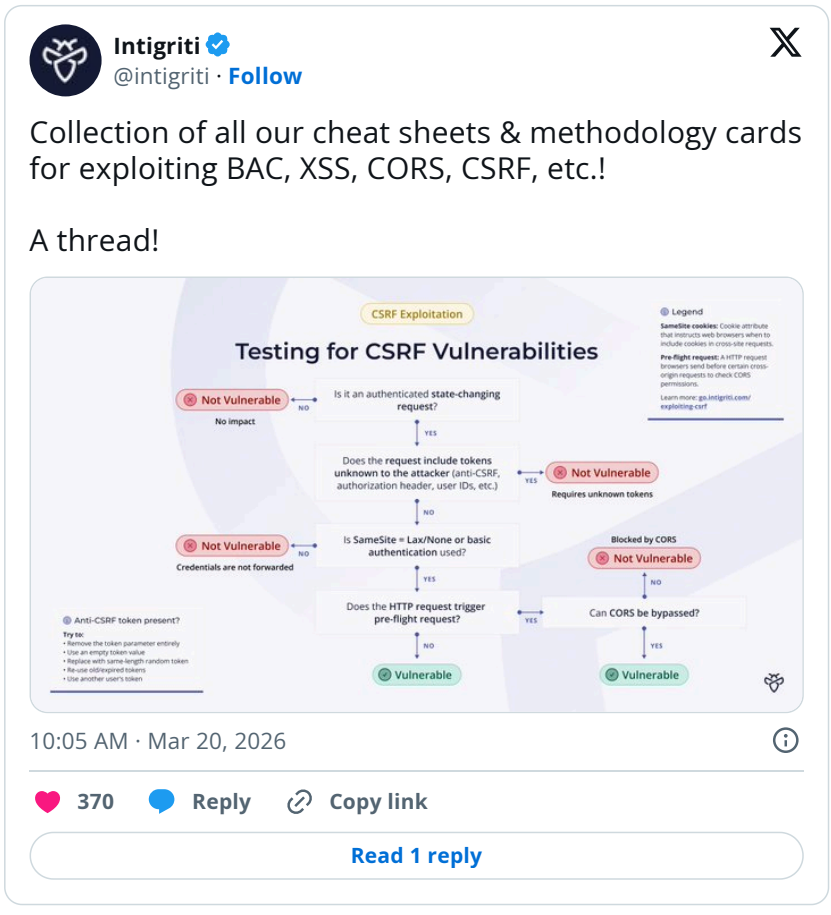
- **Need a quick way to pull in-scope targets from all major bug bounty platforms?** bbscope by @sw33tLie just received a major update with a new web-based interface and API for browsing aggregated scopes from all major bug bounty platforms, including ours! It now

includes a PostgreSQL backend for tracking scope changes over time and even supports LLM-based cleanup of messy scope strings.

- **Struggling to enumerate more subdomains using traditional wordlists?** CewlAI by @rez0__ uses AI to analyze patterns in seed domains and generate new domain name variations, based on your target's naming conventions.
- **Targeting Salesforce Lightning applications?** Auraditor by @irsdl is a Burp Suite extension built specifically for security testing Salesforce Aura framework apps, featuring advanced action management, context editing, and comprehensive audit checks.
- Sj by @BishopFox **automates the process of auditing all defined API endpoints in Swagger docs** for weak authentication, brute-forcing any other undocumented endpoints, and generating ready-to-use curl and SQLMap commands for additional testing.
- Vulnerability Spoiler Alert by @spaceraccoon is a cool GitHub Action based on his latest research that uses LLMs to monitor repositories for commits that look like they're patching vulnerabilities, **alerting you before a CVE is ever assigned.**

Resources

Collection of all our cheat sheets & methodology cards



We recently compiled all our cheat sheets and methodology cards for exploiting BAC, XSS, CORS, CSRF, and more into a single thread. If you enjoy our content, be sure to give us a follow and bookmark this thread for future reference!

- PortSwigger published their annual Top 10 Web Hacking Techniques of 2025, featuring the most innovative and impactful research from the past year as voted by the community.
- Anthropic announced they've been using Claude to find vulnerabilities in Mozilla's codebase, continuing the trend of AI-driven vulnerability discovery in major open-source projects.
- Adnan shares Clinejection, a research piece on injecting malicious code into AI coding assistants through crafted repository content.
- Flatt Security discovered a remote command execution in Google Cloud triggered by a single directory deletion — a subtle but critical cloud infrastructure vulnerability.
- Voorivex disclosed a UXSS in Samsung Browser (tracked as CVE-2025-58485), achieving universal cross-site scripting through a flaw in the browser's security model.
- Vsevolod explores smuggling payloads through AI outputs, showing how LLM-generated content can be weaponized to bypass security filters downstream.
- SL Cyber researchers disclosed an unauthenticated file upload to RCE in Magento using a polyshell technique to bypass upload validation and achieve code execution.
- Lauritz documents a collection of XSS-to-ATO gadgets, practical techniques for escalating cross-site scripting vulnerabilities into full account takeovers across various common frameworks and authentication flows.
- @spaceraccoon shares his journey of getting a shell on a Tapo C260 webcam, covering hardware hacking, firmware extraction, and ultimately achieving code execution on the IoT device.
- @castilho101 demonstrates how to steal Salesforce OAuth tokens using the WAF to achieve account takeover on Salesforce-integrated applications.
- Adrian presents FontLeak, a technique that uses CSS font rendering quirks to exfiltrate sensitive data from web applications without JavaScript execution.
- A single path traversal in Grafana was chained into XSS, open redirect, and SSRF (CVE-2025-4123). A good example of how one vulnerability can unlock multiple other attack vectors.
- @_bergee_ documents finding multiple critical bugs in Red Bull, including a chain of vulnerabilities that led to high-severity impact across their assets.
- Patrik shares an honest reflection on being outperformed by AI in a vulnerability research task and what it means for the future of manual security research.
- Check Point Research published an in-depth article on using generative AI for reverse engineering, demonstrating how LLMs can assist in binary analysis and malware deobfuscation.
- @hamidonsolo details how he bypassed a strict CSP to achieve XSS on a main target page, resulting in a significant bounty payout.
- The CTBB Podcast also features one of the many stories of @thedawgyg, who earned $180K in bounties by bypassing SSRF protections, detailing the methodology and mindset behind his journey.

- @the_IDORminator explains how second-order broken access control via session stuffing can be used to overwrite user sessions and identify even more IDORs.
- Another write-up from @castilho101 where he demonstrates how to convert a limited DOM Clobbering into a full CSPT, turning a seemingly low-impact finding into a meaningful client-side attack.
- This article walks through exploiting XSS with JavaScript/JPEG polyglots, crafting files that are simultaneously valid images and executable JavaScript to bypass upload restrictions.
- A rare file upload bypass in FreeScout was discovered by @J0R1AN, where uploading a ".png" file containing SVG contents with a manipulated content type allowed for stored XSS.
- @Wakedxy1 shares a clever file upload bypass via a parsing flaw, using "application/ php/jpeg" as the content type to trick the server into executing uploaded files.
- Voorivex documents how an Android hook led to RCE and a $5,000 bounty, chaining mobile-specific techniques into server-side code execution.
- Sebsrt explores how trailing characters in URLs can lead to unexpected behavior, including authentication bypasses and access control issues.
- This researcher shares how they earned their first $13,500 bounty through HTTP Parameter Pollution (HPP), demonstrating that some exploitation techniques are still worth testing on modern targets.
- The CTBB Podcast covers some practical tips on building Claude Skills as a bug bounty hunter, including integrating AI into your hacking workflow for recon, code review, and automation.
- This researcher documents how they earned $76,000 from a single Bugcrowd program, sharing insights on focus, persistence, and methodology that kept the bounties coming.
- @hamidonsolo shares his $15,129 bug bounty challenge, earning $10K in a single month as part of a focused 7-month sprint.
- If you want to deeply understand how browsers enforce security, this researcher has published a free online book, Beyond XSS, which provides an excellent in-depth dive into the browser security model and client-side attack techniques.
- @GodfatherOrwa shares a useful methodology for hunting vulnerabilities in Google services, covering recon approaches and common misconfigurations.
- This researcher discovered an Instagram Notes audio leakage vulnerability where audio URLs could be extracted without authentication. An example of how simple broken access control vulnerabilities can be.
- Looking to level up your SQL injection skills? This SQLi exploitation guide walks through practical techniques for identifying and exploiting SQL injection vulnerabilities step by step.
- New to mobile testing? This guide covers intercepting iOS traffic with Burp Suite, including certificate pinning setup and common troubleshooting tips.

Company news

Intigriti at RootedCON 2026

We attended RootedCON 2026 in Madrid, where we organized a Hacker Night featuring exclusive targets for the community to hack on. The competition was fierce! Congratulations to alvarodh5 for taking the top spot with 120 points, followed by devploit (creator of Nomore403), and remot3 landing on the leaderboard with 65 points.

We also had the pleasure of being joined by two of our newest Hacker Ambassadors, Cristian (@CristiVlad25) and Süleyman (@slymn_clkrsln), who helped make the event one to remember. Big thanks to everyone who participated!

RootedCON 2026 HackerNight

Intigriti named runner-up for Cyber Security Company of the Year

We're proud to share that Intigriti was named runner-up for Cyber Security Company of the Year at the Teiss Awards 2026. Standing out among 21 finalists in a category dedicated to recognizing excellence in information security is a huge honour. Thank you to our amazing community, customers, and team for making this possible.

Intigriti named runner-up for Cyber Security Company of the Year in Teiss Awards 2026

Feedback & suggestions

Before you click away: Do you have feedback, or would you like your technical content to get featured in the next Bug Bytes issue? We want to hear from you. Feel free to send us an email at community@intigriti.com or DM us on X/Twitter, and we'll take it from there.

Did you like this Bug Bytes issue? Consider sharing it with your friends and tagging us along on X/Twitter, Instagram, or LinkedIn.

Wishing you a bountiful month ahead,

Keep on rocking!

AUTHOR

Ayoub

Senior security content developer