Intigriti Bug Bytes #231 - December 2025

BY AYOUB • DECEMBER 18, 2025

Hi hackers,

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

- React2Shell scanner (with WAF bypasses)
- Identifying server origin IP to bypass popular WAFs
- CSRF exploitation cheat sheet
- Finding vulnerabilities in sign-ups

And so much more! Let's dive in!

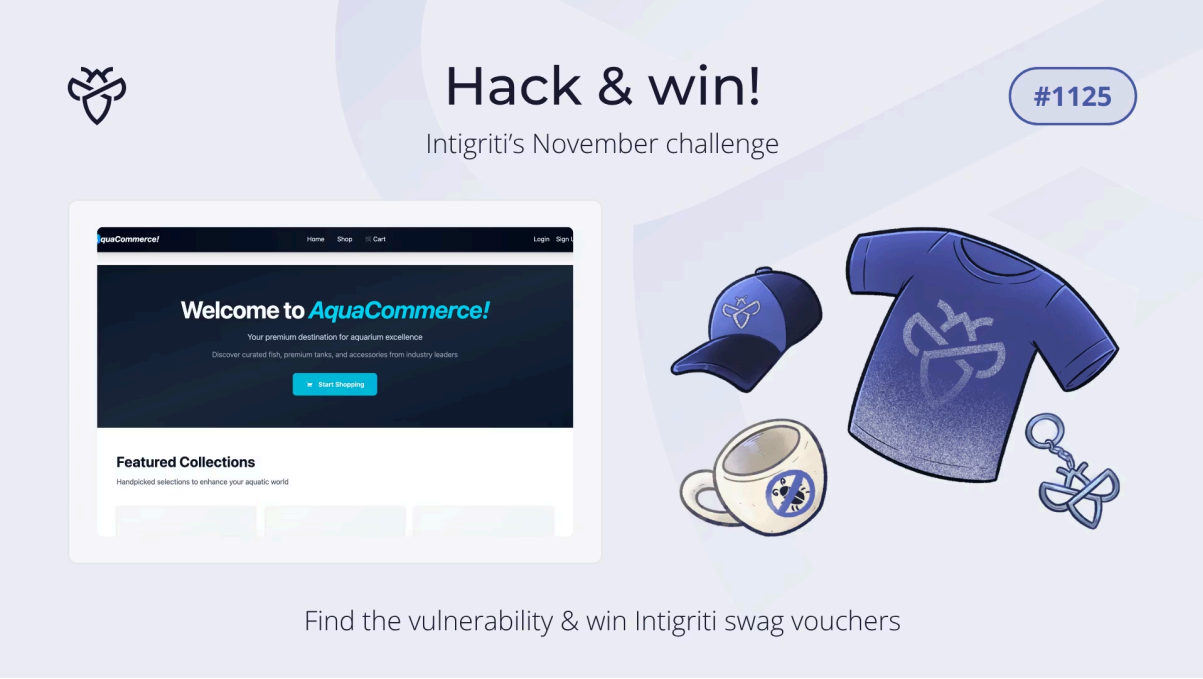
INTIGRITI 1125 results are in

November's Intigriti Challenge was on us. 1125 brought hundreds of hackers together to test a vulnerable e-commerce shop, *AquaCommerce!,* for a remote code execution vulnerability.

With over 100 solves, it effortlessly joins the list of the most solved and most popular challenges ever to be featured on Intigriti.

Quick recap:

- 145 hackers reported the correct flag
- First blood went to qualwin38000
- And 42 hackers wrote a nice write-up



INTIGRITI 1125 CTF Challenge

[Announcement post]

INTIGRITI 1125 official write-up

Challenge 1125 featured a [JSON Web Token vulnerability] that allowed for privilege escalation, resulting in accessing an admin panel vulnerable to [server-side template injection].

If you wish to learn more about JSON Web Token exploitation, make sure you have a look at our technical article.

November CTF Challenge: Exploiting JWT vulnerabilities to achieve RCE Cover Image

[Read the write-up]

Participate in INTIGRITI 1225

The holidays are approaching at a rapid pace. And this month's XSS challenge by @RenwaX23 will challenge your hacking skills and keep you busy. If you're looking for a fun activity to put your web hacking skills to the test, this is your chance.

With only 5 confirmed solves so far, there are still plenty of prizes to win. Wish to still participate? Follow the instructions on our announcement post and ensure you submit your flag before Monday, the 22nd, 11:59 PM UTC.

INTIGRITI 1225 XSS Challenge

[Participate now]

Blogs & videos

Bypassing CSPs

Bypassing Content Security Policy (CSP) Cover Image

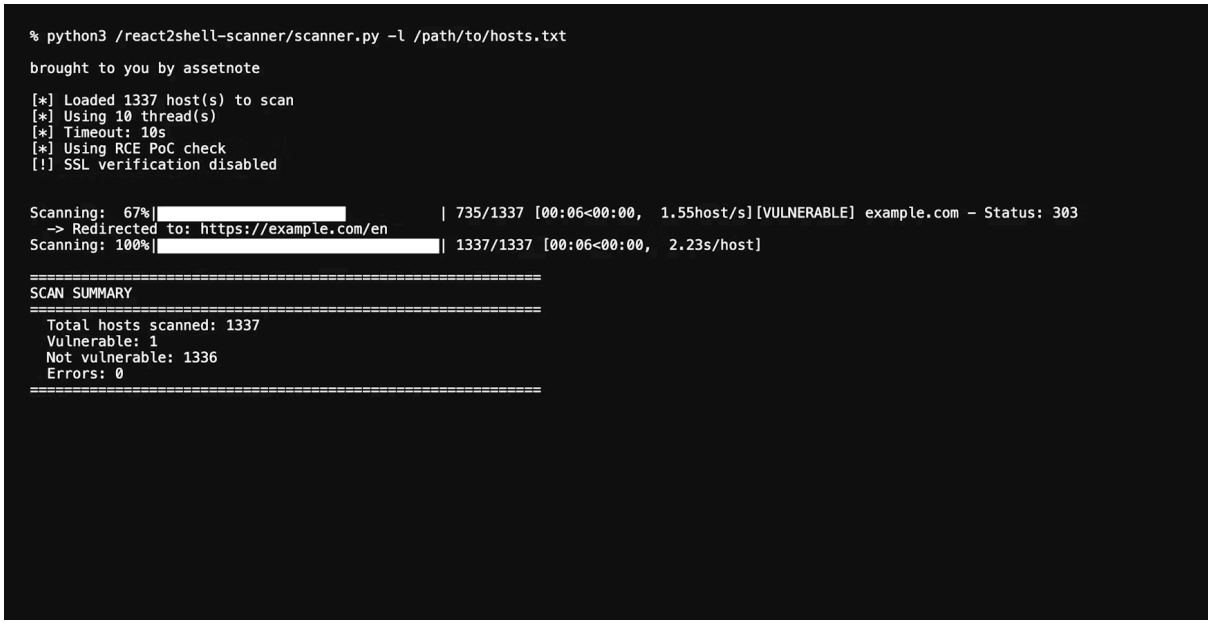
Cross-site scripting vulnerabilities can be fun to find & exploit. However, with Content Security Policy (CSP) in the way, it can make exploitation seem almost impossible... Luckily, developers frequently allow for loosely scoped (misconfigured) policies, enabling us to bypass these restrictions. In our technical article, we've documented 5 common ways to bypass Content Security Policies (CSPs) and exploit XSS vulnerabilities.

- **Applications become more complex than ever before, allowing for a wide range of bugs to arise, including logic flaws.** However, it is essential to correctly distinguish logic flaws (with impact) from functional bugs. In our comprehensive article, we outline how you should approach exploiting logic flaws in web applications, including real-world examples.
- **Imagine finding an application vulnerable to SQLi, XSS or even React2Shell, only for a Web Application Firewall (such as Cloudflare or Akamai) to be in the way...** Luckily for us, in some instances, we can bypass this WAF altogether by reaching the origin IP directly. In our article, we share several methods for identifying a server's origin IP, including a methodology for determining when this technique is applicable.

Tools & resources

Tools

React2Shell Scanner



React2Shell Scanner

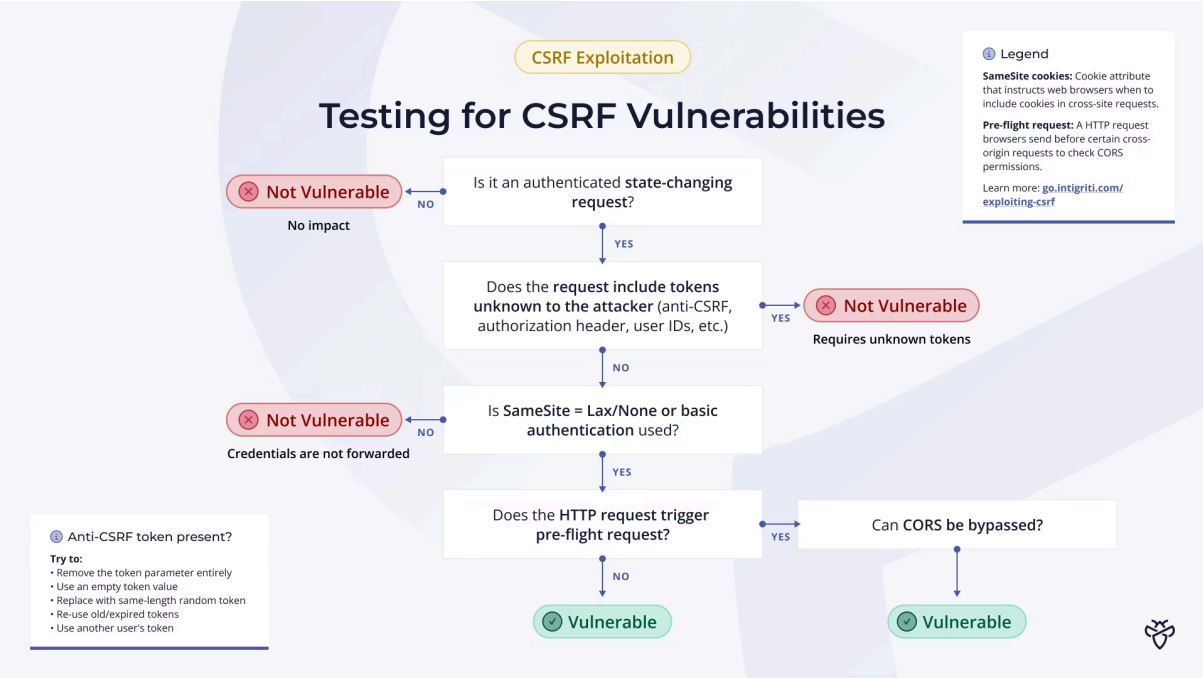
Need a simple way to scan for React2Shell (CVE-2025-55182 and CVE-2025-66478)? React2shell-scanner by Assetnote is a simple command-line tool that detects both CVE-2025-55182 and CVE-2025-66478 in vulnerable NextJS applications. It even includes support for bypassing WAF filters.

- **Scanning codebases for vulnerabilities is now possible with AI and can even yield you a few quick wins.** Securevibes is a simple tool that deploys several agents to scan your codebase for injection vulnerabilities, hard-coded secrets and other weaknesses.

- **Google dorking can help you identify new files, endpoints, and parameters previously indexed by Google.** Google Dorks for Bug Bounty is a web-based tool that helps simplify the process of effectively searching for interesting data.

Resources

CSRF exploitation cheat sheet



Testing for CSRF vulnerabilities cheat sheet

CSRFs can sometimes be escalated to account takeovers. However, as with many client-side bugs, they may be unexploitable due to browser security restrictions. We've created a simple CSRF exploitation cheat sheet to help you easily determine the exploitability of any CSRF vulnerability. If you wish to delve deeper into CSRF exploitation, be sure to read our comprehensive article.

- Watch Towr Labs documents on how .NET Framework HTTP client proxies can be tricked into writing files to the filesystem, achieving RCE in Barracuda, Ivanti, and Umbraco.
- Zakhar from PortSwigger shares new parser-level inconsistencies in Ruby and PHP SAML libraries, achieving full authentication bypass through attribute pollution and namespace confusion.
- S1r1us Ninja demonstrates how cookie tossing combined with XSS can escalate to RCE on Google Cloud JupyterLab instances, earning $3,133.70.
- HamidSj shares how he bypassed Google Identity Services (GIS) SDK protections by hooking window.open to achieve a 0-click account takeover.
- Voorivex documents a creative account takeover technique using Punycode to bypass security controls.
- SecuringBits reveals a critical authentication bypass in Google Cloud API Gateway's ESPv2 proxy using the x-http-method-override header.
- Came across a default IIS page? Never ignore it. @mugh33ra documents his journey from discovering a default IIS page to finding and exploiting an SQL injection vulnerability.

- Vitor shares insights and lessons learned from spending 3 months as a full-time bug bounty hunter. If you're just starting (or are struggling to score consistent bounties), make sure to give this article a read.
- Almost all interactive applications incorporate sign-ups and authentication. Coffinxp breaks down 12+ essential checks for testing signup flows, from duplicate registration to HTTP parameter pollution.

Intigriti at BSides London

BSides London was a feat! A day of brilliant minds sharing security wisdom. The community vibes and conversations made it unforgettable.

Quick recap:

- Our Hacker Community Lead, Alex Olsen, presented the 'Anyone Can Hack APIs' talk, where he covered practical skills, real-world examples, followed by an easy-to-apply methodology.
- Interesting conversations covering various security topics led by our community team.

Don't miss our next hacker gathering, follow us on LinkedIn and Twitter/X for upcoming event announcements.

Intigriti at BSides London

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 support@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

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com