Referral Beware, Your Rewards Are Mine



Exploring insecurity in incentive rewards programs

whoami

- Whit Taylor (un1tycyb3r)
- Application Pentester at **Rhino Security Labs**
- Bug Bounty Hunter / Security Researcher
- Proud father and husband
- Pianist, Powerlifter, and gamer
    - Halo, Helldivers, Splitgate, etc.





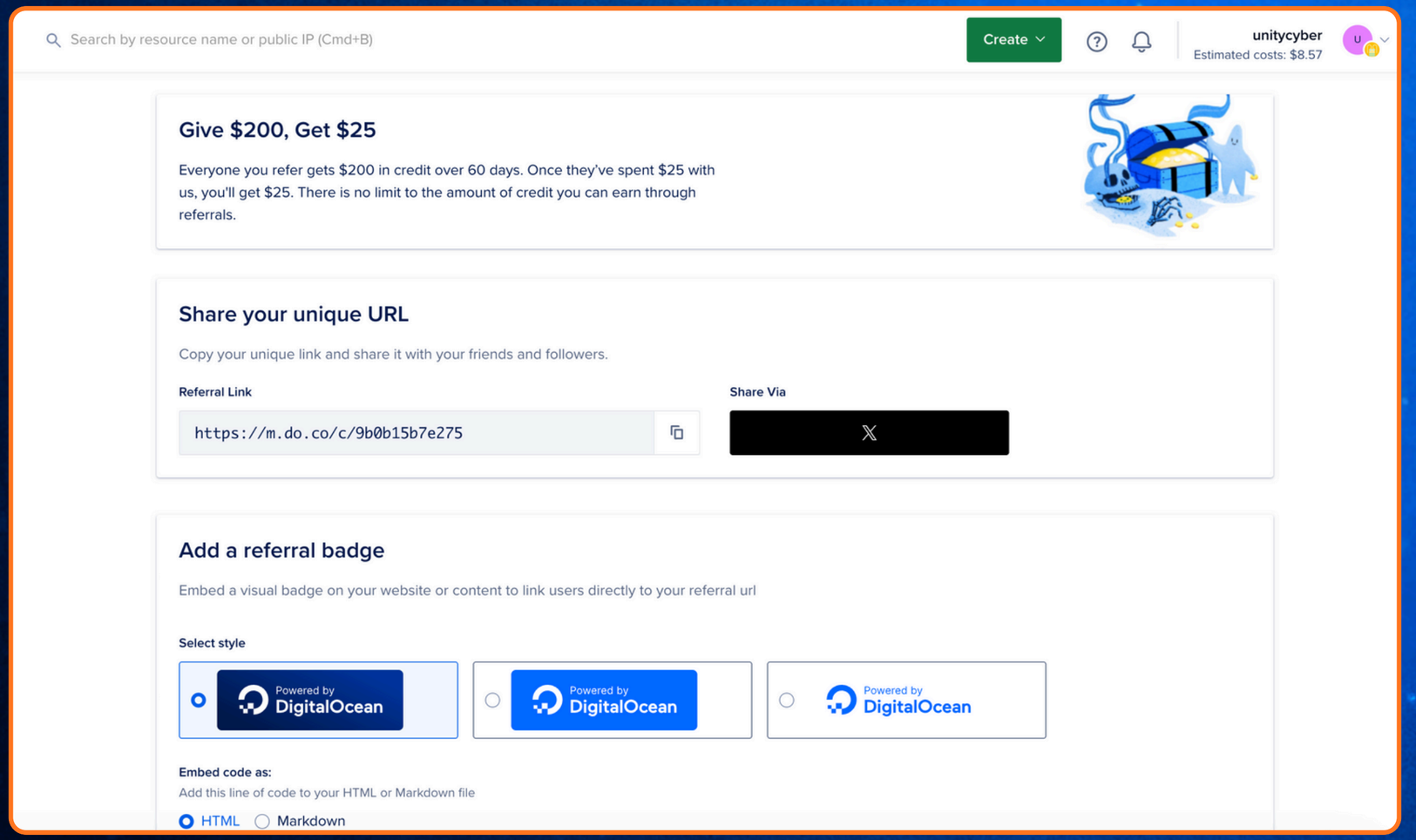



ROGUE

So...Why Referral Rewards?



Referral rewards programs




instacart
THREDUP
HELLO FRESH
Vinted
Gemini
robinhood
Etsy
DigitalOcean
DOORDASH
Proton Mail

Technical Implementations



URL to Cookie



URL to Cookie

Prospective User Receives
Referral Link



URL to Cookie

Prospective User Receives
Referral Link

User navigates to link



URL to Cookie

Prospective User Receives Referral Link

User navigates to link

Referral Code is extracted from the URL and added as a cookie



URL to Cookie

Prospective User Receives Referral Link

User navigates to link

User begins signup

Referral Code is extracted from the URL and added as a cookie



URL to Cookie

Prospective User Receives Referral Link

User navigates to link

User begins signup

User submits signup. referral code is sent along via the cookie that was set

Referral Code is extracted from the URL and added as a cookie



URL to Client-Side Initiated Request(s)

URL to Client-Side Initiated Request(s)

Prospective User Receives
Referral Link



URL to Client-Side Initiated Request(s)

Prospective User Receives Referral Link

User navigates to link and begins signup



URL to Client-Side Initiated Request(s)

Prospective User Receives Referral Link

User navigates to link and begins signup

Referral Code is extracted from query param or URL Path



URL to Client-Side Initiated Request(s)

Prospective User Receives Referral Link

User navigates to link and begins signup

Referral Code is extracted from query param or URL Path

Value is sent in validation request created by client-side JS



URL to Client-Side Initiated Request(s)

Prospective User Receives Referral Link

↓

User navigates to link and begins signup

→

Referral Code is extracted from query param or URL Path

↓

Value is sent in validation request created by client-side JS

↓

If valid, the code is applied in a secondary request created by the client-side JS



URL to Client-Side Initiated Request(s)

Prospective User Receives Referral Link

User navigates to link and begins signup

Referral Code is extracted from query param or URL Path

Value is sent in validation request created by client-side JS

If valid, the code is applied in a secondary request created by the client-side JS

User Completes Signup



Referral Code as Promo Code



Referral Code as Promo Code

Prospective user is either sent referral code or referral link.



Referral Code as Promo Code

Prospective user is either sent referral code or referral link.

User begins signup or begins shopping



Referral Code as Promo Code

Prospective user is either sent referral code or referral link.

↓

User begins signup or begins shopping

↓

User starts checkout



Referral Code as Promo Code

Prospective user is either sent referral code or referral link.

User begins signup or begins shopping

User starts checkout

Code is applied as a promo code and discount is applied.



Referral Code as Promo Code

Prospective user is either sent referral code or referral link.

User begins signup or begins shopping

User starts checkout

User completes checkout and referral reward is applied to referring user.

Code is applied as a promo code and discount is applied.



Mobile Implementation



Typical Code Pattern

```
public final void m12977c(String emailHeader, String emailBody) {
        Intent intent = new Intent("android.intent.action.SEND");
        intent.setType("message/rfc822");
        intent.putExtra("android.intent.extra.SUBJECT", emailHeader);
        intent.putExtra("android.intent.extra.TEXT", emailBody);
        Activity activity = this.activity;
        activity.startActivity(Intent.createChooser(intent, activity.getString(lk
        m12976b("invites_email_android_share_page");
    }
```



From un1tycyb3r@gmail.com

To

Here's 45% off your first thredUP order!

Hi!

Thrifting is better with company! 👯 That's why I'm gifting you a super exclusive offer at thredUP: 45% off + free shipping on your first . It's their best offer yet and it's only for ited time.

Make sure you use my link to shop: https://www.thredup.com/r/OBJWVI



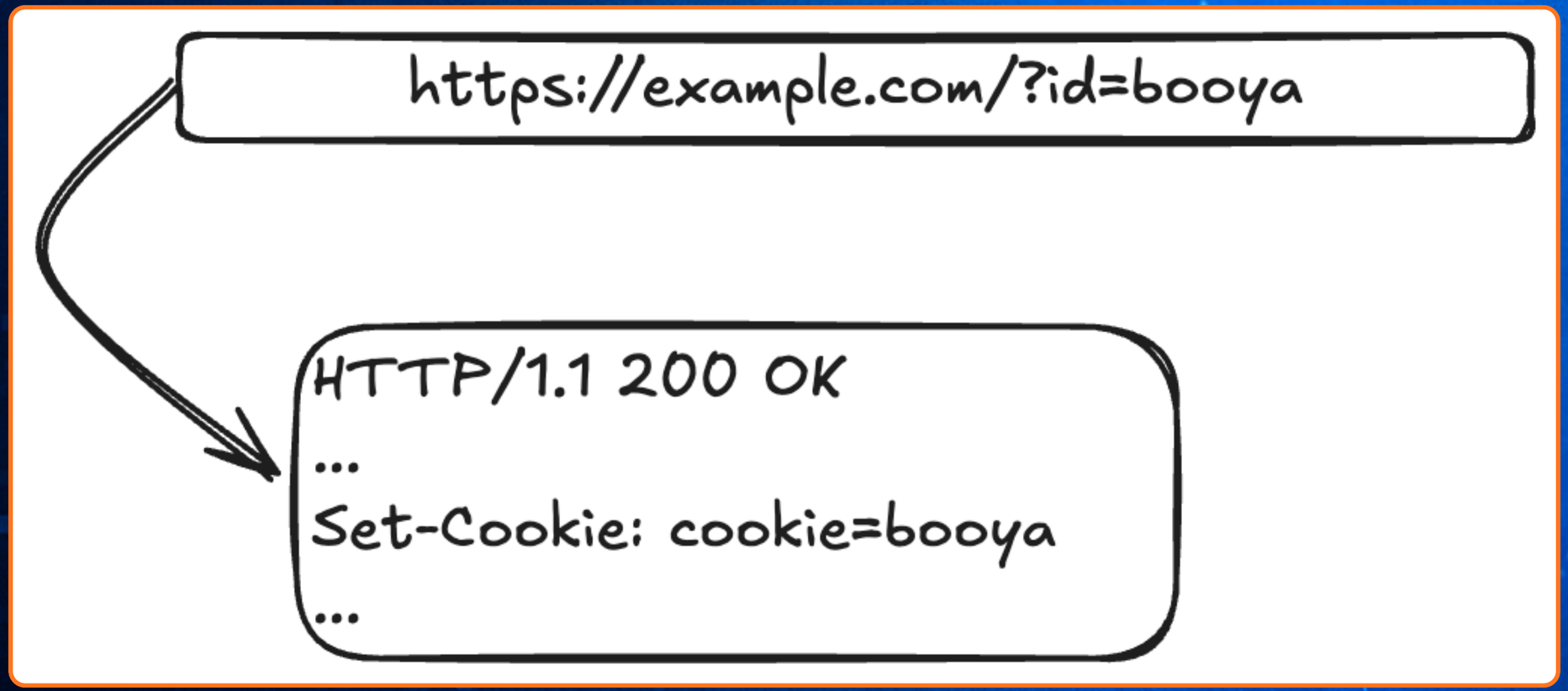
Why should companies care?



Can I find client-side gadgets?



Cookie Injection



CSPT



https://blog.doyensec.com/2025/03/27/cspt-resources.html

Can I find client-side gadgets?

Can I abuse the logic?



Infinite Credit Flaw

Requirements

- Application allows signup with alias emails
- No requirement for new users to start referring users
- Reward for referral is greater than spending requirement for referral.

Referral Program Details

- Current user refers friend
- New user signs up and makes a purchase of X dollars
- Referring user receives reward of store credit several times greater than the required spend.



Infinite Credit Flaw

User 2 → Refer user 1 → Buy and trigger reward



Infinite Credit Flaw





Infinite Credit Flaw

User 2 → Refer user 1 → Buy and trigger reward

User 1 → Refer User 2 → Buy and trigger reward

Create user 3 → Refer User 1 → Buy and trigger reward



Infinite Credit Flaw



Infinite Credit Flaw

User 2 → Refer user 1 → Buy and trigger reward

User 1 → Refer User 2 → Buy and trigger reward

Create user 3 → Refer User 1 → Buy and trigger reward

User 1 → Refer User 3 → Buy and trigger reward

And repeat



Order Cancellation Flaw

Requirements

- Application requires order before referral
- Orders are not automatically processed
- Order cancellation allowed

Referral Program Details

- User’s required to make an order before referral code is unlocked
- Referral code is used to discount orders



Order Cancellation Flaw

Attacker signs up first account

Attacker Signs up second account



Order Cancellation Flaw

Attacker signs up first account

Attacker Signs up second account

User 1 shops and checks out with scheduled delivery

Referral Code is unlocked



Order Cancellation Flaw

Attacker signs up first account

User 1 shops and checks out with scheduled delivery

Referral Code is unlocked

Attacker Signs up second account

User 2 begins shopping

User 2 checks out using user 1's referral code. Order is discounted



Order Cancellation Flaw

Attacker signs up first account

User 1 shops and checks out with scheduled delivery

Referral Code is unlocked

User 1 cancels scheduled order

Attacker Signs up second account

User 2 begins shopping

User 2 checks out using user 1's referral code. Order is discounted



Self Referral/Self Discount Flaw

Requirements

- Application utilizes referral code as promo code implementation
- Some way to retrieve referral code before subscription.

Referral Program Details

- Referral code is used to discount subscription and award credit to referring user



Self Referral/Self Discount Flaw

Attacker signs
up for account



Self Referral/Self Discount Flaw

Attacker signs up for account

↓

Attacker cancels subscription flow



Self Referral/Self Discount Flaw

Attacker signs up for account

↓

Attacker cancels subscription flow

→

Attacker navigates to account settings

↓

Attacker finds API request with referral code in response



Self Referral/Self Discount Flaw

Attacker signs up for account

↓

Attacker cancels subscription flow

→

Attacker navigates to account settings

↓

Attacker finds API request with referral code in response

←

Attacker restarts subscription flow

↓

Attacker completes subscription signup using their own referral code as a promo code



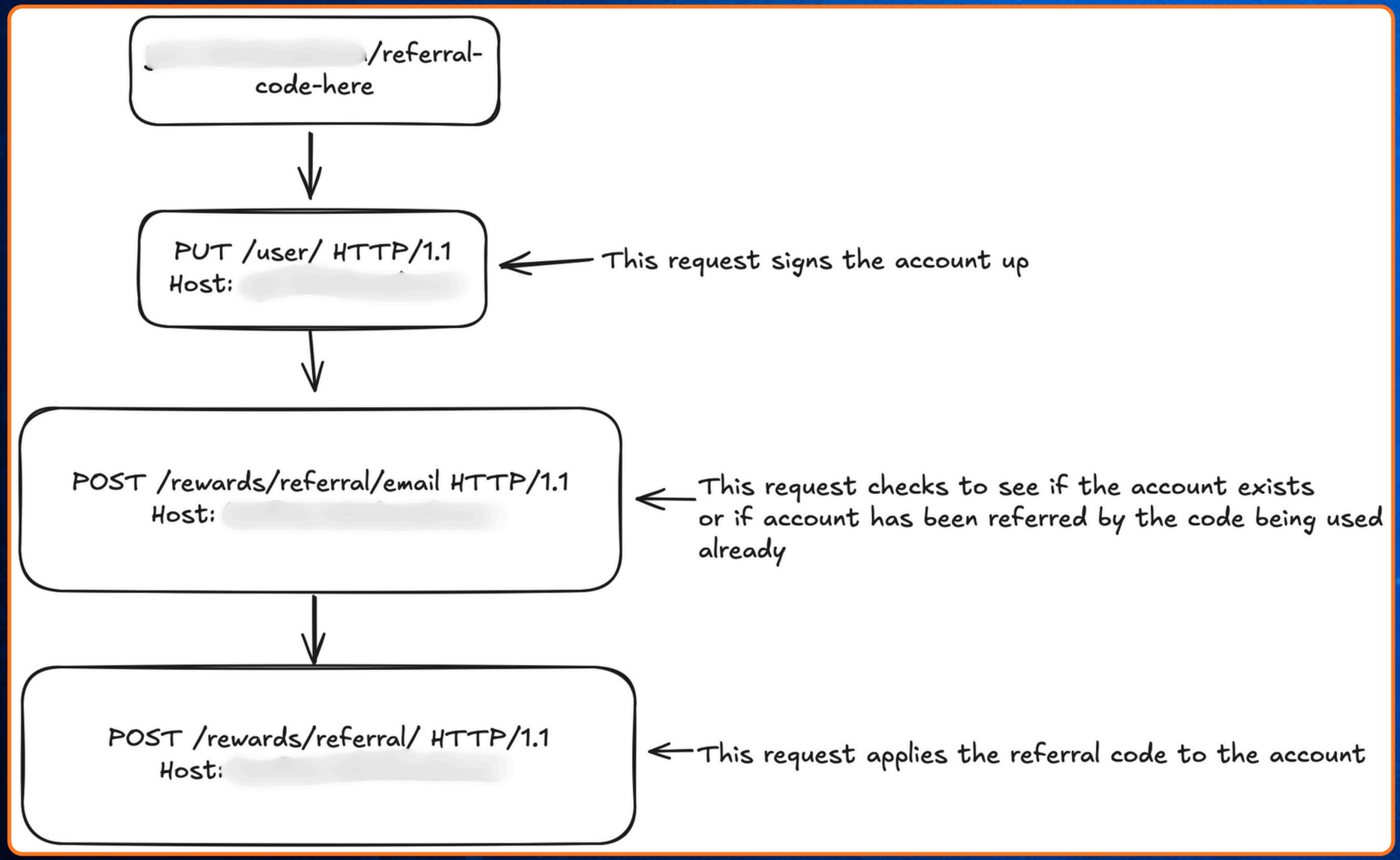
Can I find client-side gadgets?

Can I abuse the logic?

Can I Get Multiple Rewards for a Single Referral?



Race Condition



Race Condition

Pending

Referral of Whit T. Apr 1, 2025	Reminded
Referral of Whit T. Apr 1, 2025	Reminded
Referral of Whit T. Apr 1, 2025	Reminded
Referral of Whit T. Apr 1, 2025	Reminded
Referral of Whit T. Apr 1, 2025	Reminded



Can I find client-side gadgets?

Can I abuse the logic?

Can I Get Multiple Rewards for a Single Referral?

Can I steal referrals?



Referral Hijacking via Cookie Fixation

Attacker sends crafted link to victim



Referral Hijacking via Cookie Fixation

Attacker sends crafted link to victim

→

Victim visits link. Cookie is stored with the specified path



Referral Hijacking via Cookie Fixation

Attacker sends crafted link to victim

Victim visits link. Cookie is stored with the specified path

Victim receives referral link from friend.



Referral Hijacking via Cookie Fixation

Attacker sends crafted link to victim

Victim visits link. Cookie is stored with the specified path

Victim receives referral link from friend.

Victim completes signup, but the attacker cookie is prioritized



Referral Hijacking via Cookie Fixation

Attacker sends crafted link to victim

Victim visits link. Cookie is stored with the specified path

Victim receives referral link from friend.

Victim completes signup, but the attacker cookie is prioritized

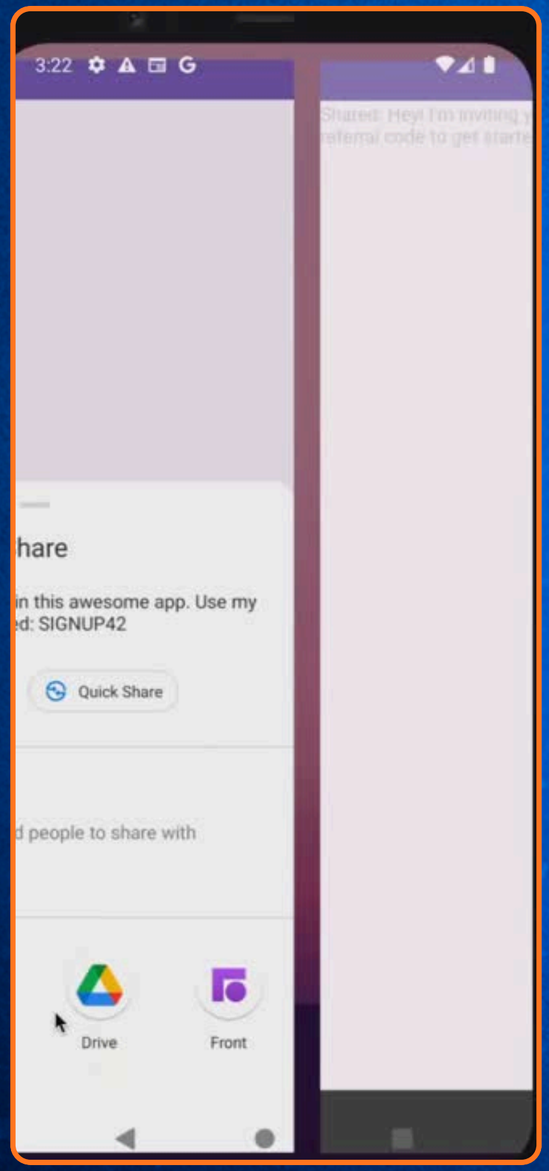
Attacker receives the reward



Referral Hijacking by Mobile Design

```
public final void m12977c(String emailHeader, String emailBody) {
        Intent intent = new Intent("android.intent.action.SEND");
        intent.setType("message/rfc822");
        intent.putExtra("android.intent.extra.SUBJECT", emailHeader);
        intent.putExtra("android.intent.extra.TEXT", emailBody);
        Activity activity = this.activity;
        activity.startActivity(Intent.createChooser(intent, activity.getString(lk
        m12976b("invites_email_android_share_page");
    }
```




3:22
hare
n this awesome app. Use my
d: SIGNUP42
Quick Share
d people to share with
Drive
Front

Takeaways



The dark side of bug bounty...

- 25+ Submissions across various programs
- Less than $1,000 in bounties
- Triagers didn’t understand impact and closed as informative
  - Also never responded to further explanations
- Some companies cited “expected behavior”
- Other companies eventually fixed but did not pay
- Those that did paid super low bounties



Big thank you to everyone who made this research possible

