



FROM BUG TO BOUNTY

\$ WHOAMI

Gustavo (Fepame) Oliveira

Desenvolvedor
Bug hunter por hobby

Co-fundador do maior grupo de
bug bounty do brasil no telegram
(só existe 1)

\$ echo “O QUE É BUG
BOUNTY?”

\$ O QUE É BUG BOUNTY?

- Programas de recompensas onde as empresas recompensam os hunters pelas suas descobertas

\$ O QUE É BUG BOUNTY?

- **Programas de recompensas onde as empresas recompensam os hunters pelas suas descobertas**
- **A recompensa pode ser em dinheiro \$, swags (brindes) ou hall da fama.**

\$ echo “COMO
E POR ONDE
COMEÇAR”



\$ COMO E POR ONDE COMEÇAR?

- Não existe receita de bolo

\$ COMO E POR ONDE COMEÇAR?

- Não existe receita de bolo
- Encontre um escopo que você se sinta confortável

\$ COMO E POR ONDE COMEÇAR?

- Não existe receita de bolo
- Encontre um escopo que você se sinta confortável
- Crie laboratórios

\$ COMO E POR ONDE COMEÇAR?

- **Não existe receita de bolo**
- **Encontre um escopo que você se sinta confortável**
- **Crie laboratórios**
- **Pratique!**

\$ COMO E POR ONDE COMEÇAR?

- Não existe receita de bolo
- Encontre um escopo que você se sinta confortável
- Crie laboratórios
- Pratique!
 - CTF

\$ COMO E POR ONDE COMEÇAR?

- Não existe receita de bolo
- Encontre um escopo que você se sinta confortável
- Crie laboratórios
- Pratique!
 - CTF
 - DVWA

\$ echo “PLATAFORMAS”

\$ PLATAFORMAS

- **Hackerone**
- **Bug Crowd**
- **Intigriti**
- **Bug Hunt**
- **Synack (só com processo seletivo)**
- **YesWeHack**

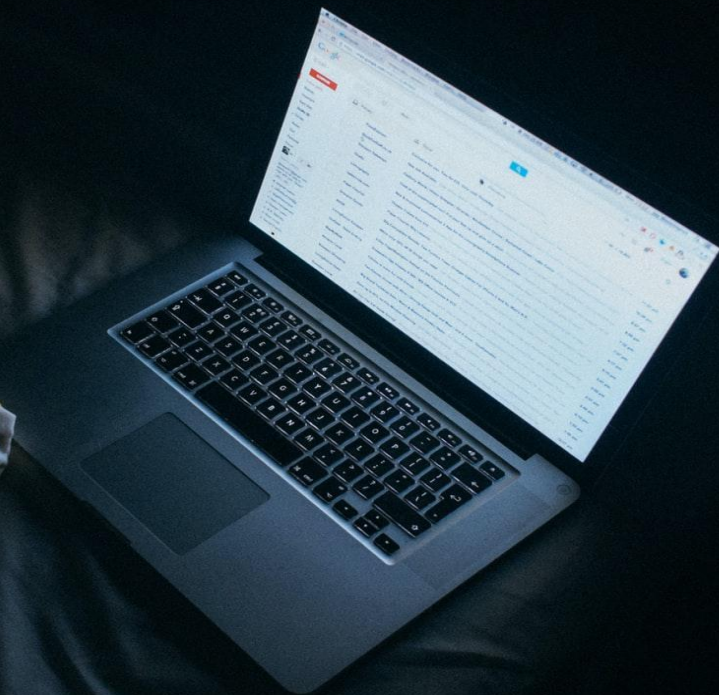
**\$ echo “COMO
ESCOLHER UM
PROGRAMA”**



\$ COMO ESCOLHER UM PROGRAMA

- Ler e Entender BEM o escopo
- Se sentir confortável com o escopo
- Se divertir

\$ echo
“PROGRAMAS
PÚBLICOS /
PRIVADOS”



\$ PROGRAMAS PÚBLICOS / PRIVADOS

- **Públicos:**
 - Qualquer um pode entrar e enviar reports
 - Alguns são necessários ter o mínimo de reputação
- **Privados:**
 - Necessário ser convidado para participar

\$ PROGRAMAS PÚBLICOS / PRIVADOS

- **Públicos:**
 - Qualquer um pode entrar e enviar reports
 - Alguns são necessários ter o mínimo de reputação
- **Privados:**
 - **Necessário ser convidado para participar**
 - Conseguindo reputação com programas públicos
 - Participando do CTF (<https://ctf.hacker101.com/>)



ORAN.design

\$ echo “COMO
REPORTAR”

SIRO
& RIBELLE
CANTIERE

\$ COMO REPORTAR

- Triagers são gente como a gente
- Demonstre um impacto para a empresa
- Aprenda Markdown
- Monte uma PoC de respeito
- Assista as lives do Manoelt (Principalmente a com o glassofbeer)

\$ echo "TIPS & TRICKS"

```
if(target != null) {
    p.sendMessage(main.prefix + "§5You have added §6" + amount + "§5 to your account.");
    money.addmoney(target, amount);
    System.out.println(target);
    System.out.println(amount);
} else {
    p.sendMessage(main.prefix + "§cDer Sp
}
}
if(args[0].equalsIgnoreCase("removemoney")) {
    Player target = Bukkit.getPlayer(args[1]);

    int amount = Integer.parseInt(args[2]);

    p.sendMessage(main.prefix + "§7Du hast ha
    money.removemoney(target, amount);
}
```

\$ TIPS & TRICKS

- Recon:
 - Google / Github / Bitbucket / etc dorks
 - Gitminer
 - Gitleaks
 - Git-all-secrets
 - LinkedIn
- Subdominios:
 - DNSGrep
 - crt.sh
 - Sublist3r
 - Knock Subdomain Scan
 - Assetfinder
 - Subfinder

\$ TIPS & TRICKS

- **Assets / Diretorios / Fuzzing:**
 - ffuf
 - DirBuster
 - gobuster
 - fukon
 - Arjunp
- **Automatização:**
 - Burp Suite
 - json-beautifier
 - ContentTypeConverter
 - authorize
 - upload-scanner
 - reflector
 - param-miner
 - Nuclei

**\$ echo “TALK IS
CHEAP SHOW ME
THE MONEY”**



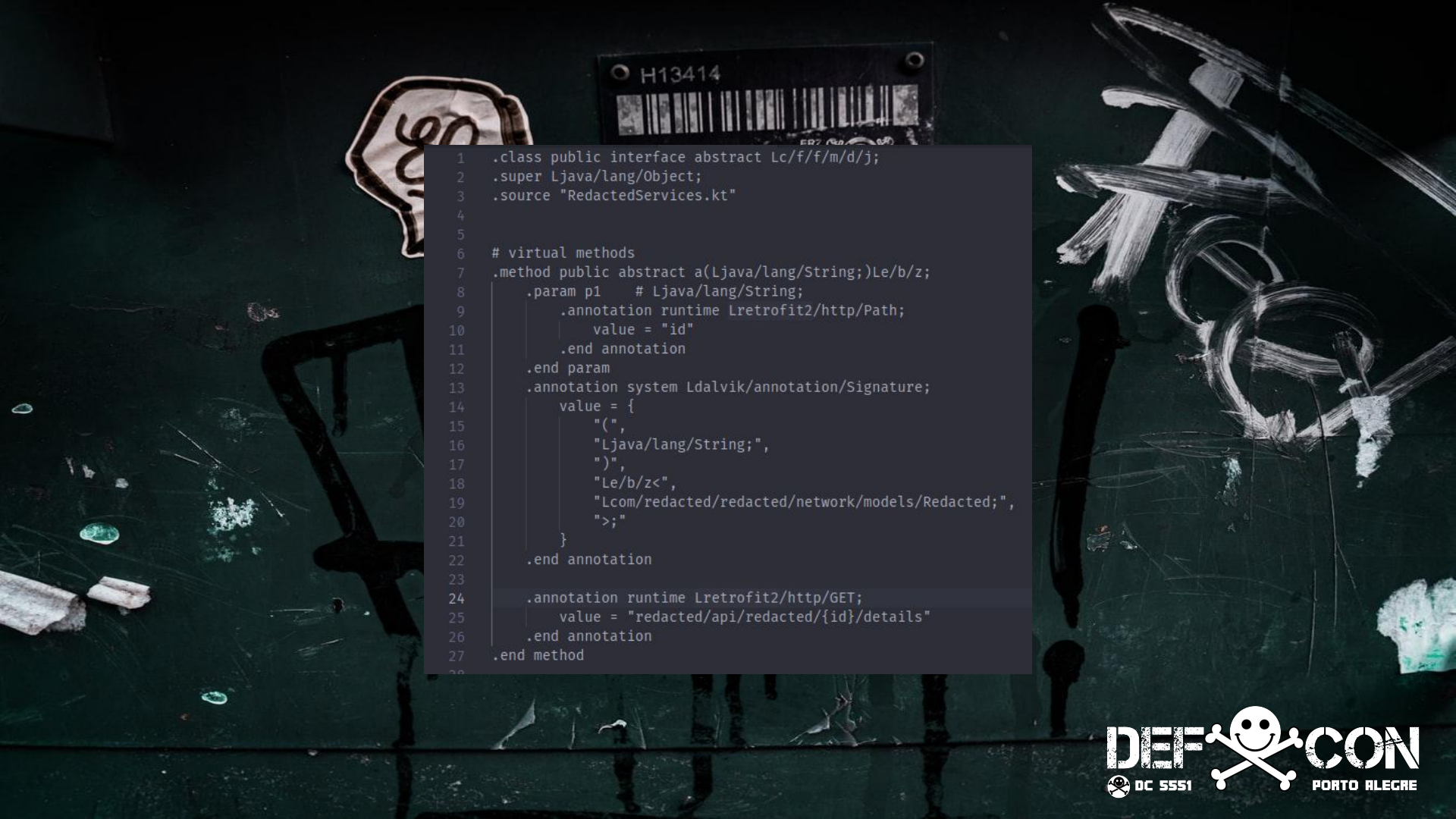
H13414

No report selected

[Directory](#) [Security](#) [Leaderboard](#) [Blog](#) [Docs](#) [Support](#) [Disclosure Guidelines](#) [Press](#) [Privacy](#) [Terms](#)

\$1 - IDOR





```
1 .class public interface abstract Lc/f/f/m/d/j;  
2 .super Ljava/lang/Object;  
3 .source "RedactedServices.kt"  
4  
5  
6 # virtual methods  
7 .method public abstract a(Ljava/lang/String;)Le/b/z;  
8     .param p1 # Ljava/lang/String;  
9         .annotation runtime Lretrofit2/http/Path;  
10             value = "id"  
11         .end annotation  
12     .end param  
13     .annotation system Ldalvik/annotation/Signature;  
14         value = {  
15             "(",  
16             "Ljava/lang/String;",  
17             ")",  
18             "Le/b/z<",  
19             "Lcom/redacted/redacted/network/models/Redacted;",  
20             ">;"  
21         }  
22     .end annotation  
23  
24     .annotation runtime Lretrofit2/http/GET;  
25         value = "redacted/api/redacted/{id}/details"  
26     .end annotation  
27 .end method  
28
```



```
1  [
2    "id": "1",
3    "name": "mission1 ",
4    "priority": 1,
5    "type": "single",
6    "redacted_id1": "1",
7    "executer_id": "59156",
8    "redatect_id3": "900101951",
9    "state": "finished",
```


H13414

```
6 # virtual methods
7 .method public abstract a(I)Lb/z;
8     .param p1    # I
9         .annotation runtime Lretrofit2/http/Path;
10             value = "executerId"
11         .end annotation
12     .end param
13     .annotation system Ldalvik/annotation/Signature;
14         value = {
15             "(I)",
16             "Lb/z<",
17             "Lcom/redacted/redacted/network/models/redacted/redacted;",
18             ">";
19         }
20     .end annotation
21
22     .annotation runtime Lretrofit2/http/GET;
23         value = "redacted/api/redacted/{redactedId}/active"
24     .end annotation
25 .end method
```

H13414

```
8605 },
8606 "address": {
8607     "lat": "1.3518",
8608     "lng": "-48.5182",
8609     "tag": "house",
8610     "address": "R. da Paz, 100",
8611     "address_id": "100",
8612     "description": ""
8613 },
8614 "user": {
8615     "id": "1",
8616     "vip": "0",
8617     "email": "user@example.com",
8618     "phone": "11 9999-9999",
8619     "last_name": "User",
8620     "first_name": "User"
8621 },
8622 }
```



xxx rewarded [fepame](#) with a \$1,000 bounty.
Enjoy reward!!


Apr 28th (2 days ago)

BECAUSE FUCK BANKS



\$1 - Misconfiguration



 Sign in with Google

Sign in

to continue to [auth0.com](#)

Email or phone

[Forgot email?](#)

To continue, Google will share your name, email address, language preference, and profile picture with [auth0.com](#).

[Create account](#)

Next

English (United States) ▼

[Help](#)

[Privacy](#)

[Terms](#)



404

Can't find the page you're looking for

BECAUSE FUCK BANKS

▼ General

Request URL: [https://api.github.com/repos/defcon/defcon/branches](#)
Request Method: POST
Status Code: 401
Referrer Policy: no-referrer-when-downgrade

▶ Response Headers (20)

▼ Request Headers

:scheme: https
accept: application/json, text/plain, */*
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVVRRek16UkN0emhHUXpCQ05rRTRRdyJ9.eyJpc3MiOiJodHRwczovLmV4MTM4NzY2VyaW5mb3JldCJpYXQ1OjE100cmMzZmJksImV4cCI6MTU1a2I1BmUc1LCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIGVtYWlsIn0.VzWMQiqMT_mFDs1L7tmqkDZeQosJl0wfEqezDppCZVGXegieNvGatm7-fEbEVDPEnrtp7hrQ6L2JyxoTRf5vSU7KS26E_T_I62cH1MLqnjnG1lM9MZ68nc1X6A4Bmv_WvDncj0ihDY-m36a00sPpvcvzKINZ2A
content-length: 2
content-type: application/json
sec-fetch-mode: cors
sec-fetch-site: same-site

▼ Request Payload [view source](#)

▼ {}

No properties

```
getOrder(order: any): Observable<any> {
  const country = CommonUtils.getCountry(order);

  const url = 'http://api.localhost:3000/orders';

  const params = {
    ...this.defaultRelations,
    searchBy: 'support-order',
    searchText: order.id,
    userId: localStorage.getObject('user').id
  };

  return this.httpClient.get(url, { params });
}

getOrderExtendedInfo(order: any): Observable<any> {
  const country = CommonUtils.getCountry(order);

  const url = 'http://api.localhost:3000/orders';

  return this.httpClient.get(url);
}
```


JSON ▼

Auth ▼

Query

Header 1

Docs

Preview ▼

Header 19

Cookie

Timeline

≡ authorization

Bearer eyJhbGciOiJSUzI1NiIsInR5cC

 New Header



mimacher rewarded [fepame](#) with a **\$1,000** bounty.

Apr 20th (10 days ago)

Once again thanks for your help [@fepame](#) . Enjoy your reward and happy hacking!

BECAUSE FUCK BANKS



Please note that for any IDOR related reports, we will be paying \$50 at this time. We will review each report and award an additional bonus on a case-by-case basis.

BECAUSE FUCK BANKS

\$ echo “Perguntas?”