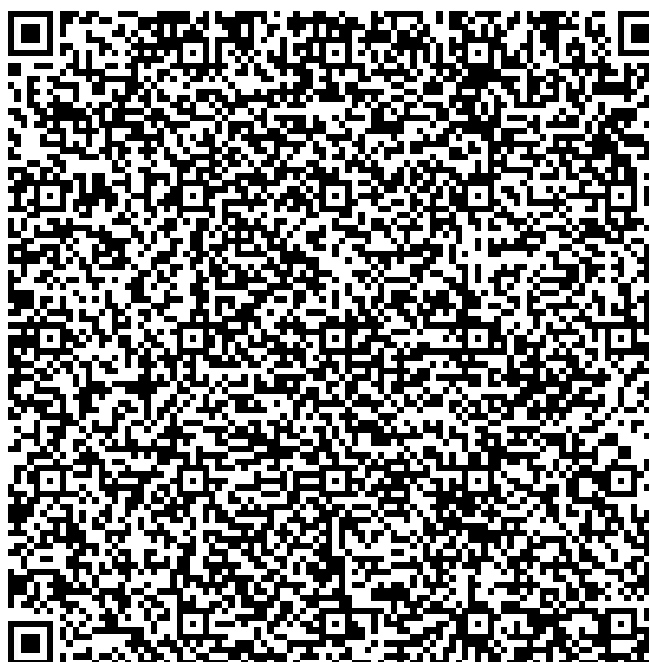




# O QUE É BUGBOUNTY?



kauenavarro







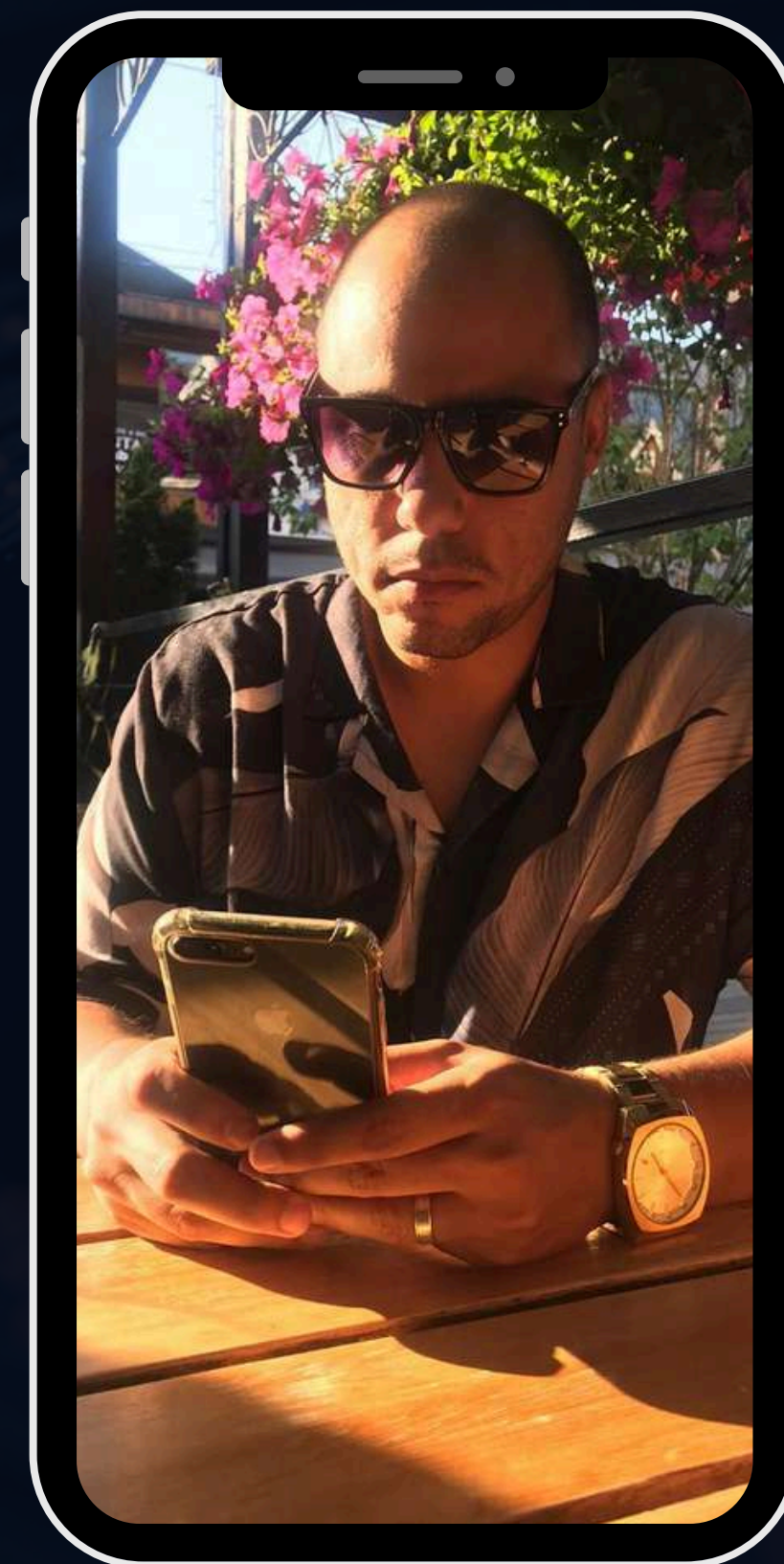
# WHO AM I

Atuação: Analista de Segurança da Informação e Bughunter.

Plataformas de bugbounty: Intigriti, Bugcrowd, Hackerone, Yeswehack, bugbase, Openbugbounty

Cves: 12

Hall da fama: NASA, REDHAT, DELL, COCA-COLA, CISCO, ADIDAS, OPERA, BINANCE.....







# O QUE É BUGBOUNTY?

O Bug Bounty é um programa de recompensas pelo descobrimento de falhas em sistemas, aplicativos ou dispositivos físicos.. O objetivo é incentivar hackers éticos a analisarem, de forma independente, o sistema de uma empresa para que encontrem vulnerabilidades ali. Dessa forma, a organização pode contar com mão de obra especializada para identificá-los e tomar as providências necessárias para corrigir os erros. Quando esses profissionais encontram falhas e as relatam para a empresa, são recompensados – a remuneração varia de acordo com a quantidade e a criticidade do problema.

A mecânica do Bug Bounty surgiu em 1983, quando a empresa estadunidense Hunter & Ready criou um programa de recompensas para quem encontrasse bugs e vulnerabilidades em seus sistemas. O nome que conhecemos hoje, entretanto, só começou a ser usado em 1995 pela empresa de serviços de computadores Netscape Communications Corporation.



<https://vantico.com.br/o-que-e-bug-bounty-qual-a-diferenca-pentest/>







# COMO SE TORNAR UM HUNTER?

Para iniciar o processo de se tornar um Bughunter, você precisa ter habilidades técnicas avançadas, sendo as principais, redes, programação e arquitetura de sistemas operacionais.

Após adquirir essas habilidades você pode se vincular a plataformas de Bugbounty ou realizar as pesquisas e reportar diretamente as empresas como por exemplo os programas do Google, Apple e Microsoft.

As plataformas utilizam o sistema de Crowdsourcing. (Crowdsourcing é um modelo de produção e de estruturação de processos que utiliza a sabedoria e os aprendizados coletivos para a resolução de problemas ou desenvolvimento de uma solução.), as mais famosas são (Hackerone, Bugcrowds, Intigriti, Synack, Yogosha e Openbugbounty).

Feito isso você está apto a reportar de forma ética bugs em aplicativos mobile, code review, web e hardware.

O processo funciona da seguinte forma:

- Envio do relatório
- Triagem
- Validação
- Correção
- Liberação do Pagamento ou Hall da fama

# TIPOS DE PROGRAMA

Temos dois tipos de programas, programa de divulgação de vulnerabilidades (VDP) ou Programa de Recompensa por Bugs (BBP), cada um possui suas particularidades. E possuem um escopo público ou privado, neste caso são enviados aos pesquisadores os convites para ter o acesso, assim reduzindo o número de Hunters que possuem acesso ao alvo.

Os programas públicos normalmente possuem muitos relatórios e isso acaba restringindo encontrar alguma falha inicialmente por um Hunter iniciante.

Os programas VDP são uma ótima estratégia para empresas pois ela não tem um custo financeiro quando o pesquisador encontra uma falha. Muitas vezes apenas ela disponibiliza brindes e/ou um hall da fama público em seu site.

Os programas BBP que pagam um valor monetário são mais disputados, esses por sua vez podem ser pagos em reais, dólares, euros, libras ou outra moeda de origem do país da plataforma.



<https://docs.hackerone.com/en/articles/8368965-vdp-vs-bbp>

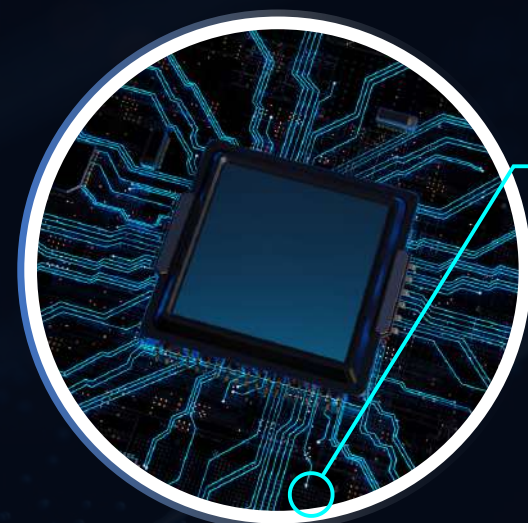






# DORKS BUGBOUNTY

inurl /bug bounty  
inurl : / security  
inurl:security.txt  
inurl:security "reward"  
inurl : /responsible disclosure  
inurl : /responsible-disclosure/ reward  
inurl : / responsible-disclosure/ swag  
inurl : / responsible-disclosure/ bounty  
inurl:'/responsible disclosure' hoodie  
responsible disclosure swag r=h:com  
responsible disclosure hall of fame  
inurl:responsible disclosure \$50  
responsible disclosure europe  
responsible disclosure white hat  
white hat program  
insite:"responsible disclosure" -inurl:nl



### Enviando Relatório

Nessa etapa montamos a prova de conceito também conhecida como POC, com detalhes técnicos, e informações de como realizar a correção se disponível.



### O QUE PRECISA TER?

- Resumo da vulnerabilidade
- Classificação cvss
- Link ou raw do alvo
- Imagens da exploração ou video
- Impacto
- Recomendações de correção

# ENVIANDO RELATÓRIO





### TRIAGEM

Nessa etapa a equipe da empresa ou da intermediária que cuida do programa como a hackerone, testam a POC e validam se é verdadeira e explorável.

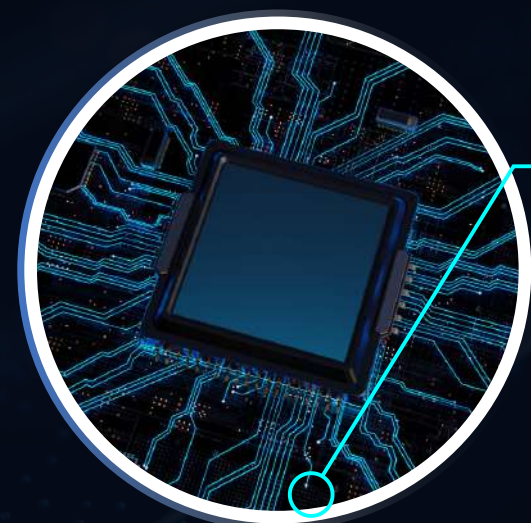


### PÓS TRIAGEM

Nesse momento será analisado se é um relatório único ou duplicado de outro pesquisador, pode ainda ocorrer da falha já ser conhecida internamente pela equipe.

# TRIAGEM





### **CORREÇÃO**

Após a triagem aceitar o report e passar para empresa, ela inicia o processo de correção, nesse momento pode já ser liberado o pagamento, brindes ou hall da fama.

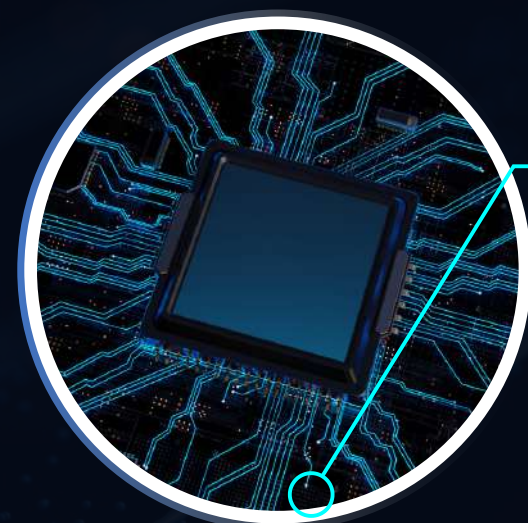


### **DURANTE A CORREÇÃO**

A empresa pode devolver a poc para validarmos se foi corrigido, e assim encerrar o relatório como resolvido. Ou voltar para esteira de correção.

# **CORREÇÃO**





### RECOMPENSAS

As recompensas podem ser pagas via transferência bancária, paypal em alguns casos criptomoedas.



### IMPOSTO

Como pessoa física temos que pagar os 27,5 %, porém pode se abrir uma LTDA para que seja pago um valor menor de imposto.

# RECOMPENSAS





# HALL OF FAME



access.redhat.com/articles/66234

with the application vendor and acknowledgements maybe given by t

- We expect you to make a good faith effort to avoid privacy violations. Please avoid using tools that are likely to automatically generate sign sites.

## 2024 Acknowledgements:

- Omri Inbar (<https://www.linkedin.com/in/omri-inbar/>)
- Ariel Rachamim (<https://www.linkedin.com/in/ariel-rachamim/>)
- Hritom Bhattacharya (<https://www.linkedin.com/in/hritom-bhattacharya>)
- Aviv Keller (<https://linkedin.com/in/redyetidev>)
- Allan Swanepoel (<https://linkedin.com/in/allanice001>)
- Vaibhav Jain (<https://www.linkedin.com/in/vaibhav-jain-aa5680254/>)
- Kauenavarro (<https://www.linkedin.com/in/kau%C3%AA-navarro>)





# BRINDES






# RECOMPENSAS



 Swedavia / XSS REFLECTED  
Code: [redacted] X • Paid on: 24/01/2024, 10:57:53

 [redacted] XT

PayPal [redacted]

Bounty €325

Paid

[redacted]

2024-08-08

Reward

€100.00

Succeeded

-

Spotify

April 12, 2023

\$250

las

XSS REFLECTED  
Reference [redacted] R

\$500.00

5 Jan 2023





KEEP HACKING