Começando no Bug Bounty

Israel Comazzetto dos Reis

@DCG5554 / @z3xddd

Quem sou eu?

- Nome: Israel Comazzetto dos Reis
- Profissão: Pentester no Grupo Randon
- Fundador da DEF CON Caxias do SUL @DCG5554
- Bug Hunter nas horas vagas, Voluntário da OWASP :)

- Linkedin: Israel Comazzetto dos Reis
- Github: @z3xddd

Revisão

- O que é Bug Bounty;
- Programas públicos / privados;
- CTF HackerOne;
- Escolha do programa;
- Materiais de Estudo / Como Praticar;
- Perguntas / Respostas.

Afinal, o que é Bug Bounty?

- Programa oferecido por algumas empresas, no qual o pesquisador pode receber por falhas de segurança encontradas.
- Empresas conhecidas que oferecem programas de Bug Bounty:
  - HackerOne;
  - BugCrowd.

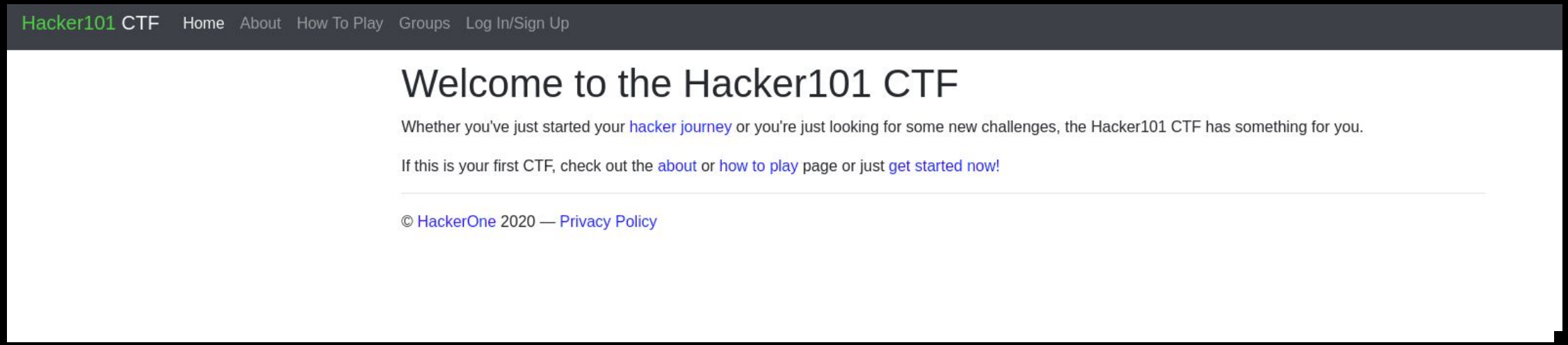
Tipos de Programas para Bug Bounty

- Públicos:
  - Tipo de programa onde qualquer pesquisador que contenha uma conta criada na HackerOne pode ter acesso.

- Privados:
  - Tipo de programa onde o pesquisador só tem acesso após possuir reputação no site / ter finalizado alguns CTFs da plataforma.

CTF HackerOne

- ***URL: https://ctf.hacker101.com***
- Porque realizar os CTFs?
  - Aumento do seu conhecimento e mindset;
  - Acesso a programas privados.



Escolha do seu primeiro programa

- Procure no ínicio por programas ***White Scope***;
  - O que são programas ***WhiteScope***? São programas onde o pesquisador é permitido para testar todos os domínios / subdomínios do cliente.

- Leia atentamente o escopo e preste atenção em quais vulnerabilidades são aceitas no programa;

- Não se importe com o dinheiro no ínicio e sim em conseguir uma boa reputação em seus relatórios;

- Leia os relatórios que estão abertos ao público;

- Reporte somente o que for realmente “explorável”.

Materiais para Estudo

- OWASP – https://owasp.org
- Defcon – https://media.defcon.org
- Black Hat - https://www.blackhat.com/html/archives.html
- Exploit DB – https://exploit-db.com
- PortSwigger - https://portswigger.net

Como Praticar?

- Hack the Box – HTB: https://hackthebox.eu
- CTF – Capture the Flag – https://capturetheflag.com.br
- Damn Vulnerable Web Application - DVWA: http://dvwa.co.uk/

DEMO

Perguntas?