Capture the Flag:

O que é?

Por onde começar?

Pode ser útil?

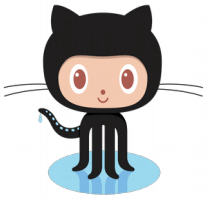
Capture the Flag

- **Quem sou eu?**
- **O que é *CTF*?**
- **Benefícios de jogar *CTF*?**
- **Por onde começar a jogar?**
- **Objetivo da apresentação**

Whoami?

- **Discente de LC 2015.1**
- **Técnico em Informática – LEIAUT Cariele 2014-2016**
- **Entusiasta em segurança da informação**

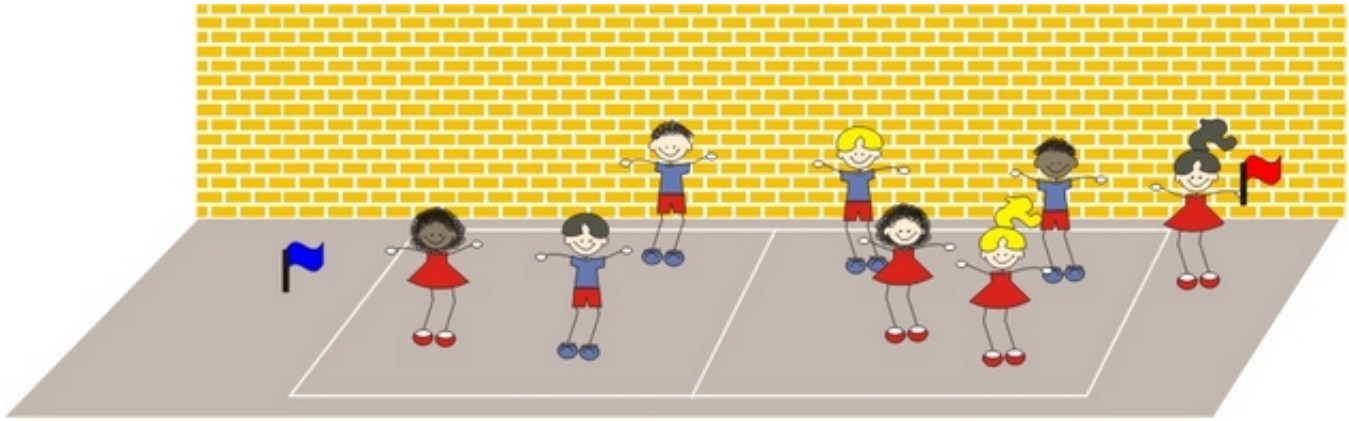
https://gitlab.com/EwertonQueiroz/



https://github.com/EwertonQueiroz/

O que é CTF?

- **Competições que envolvem diversas competências dos jogadores para a resolução de desafios relacionados à segurança da informação, com o objetivo de capturar a bandeira e pontuar.**
- **Dois tipos:**
  - Jeopardy
  - Attack/Defense

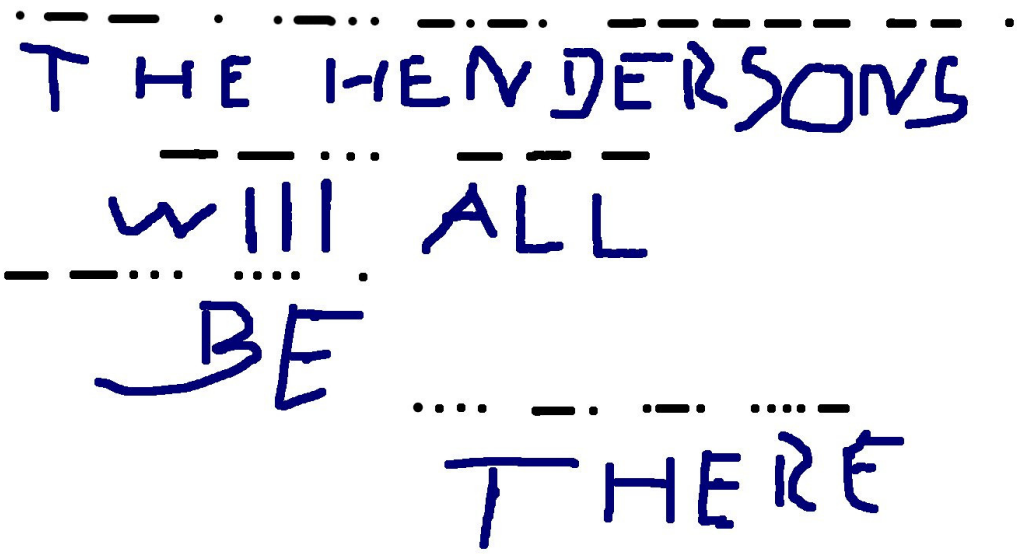


O que é CTF?

- **Capturar a bandeira?**
  - welc0me 7o 7he hnr4
  - stringsRules
  - SECCON{3678cbe0171c8517abeab9d20786a7390ffb602d}
  - flag{ld4p_inj3ction_i5_a_th1ng}

O que é CTF?

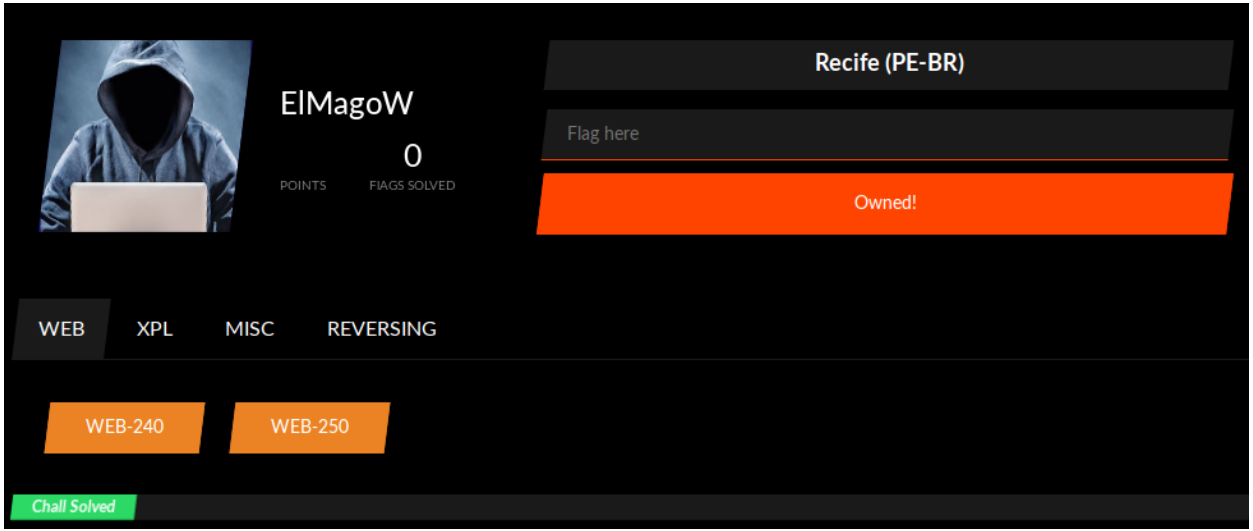
- **Jeopardy:**
  - Engenharia reversa
  - Criptografia
  - Forense (investigação)
  - *Miscellaneous* (diversos)
  - Web hacking
  - Análise de tráfego de redes
  - Exploração de software
  - Programação
  - Trívias

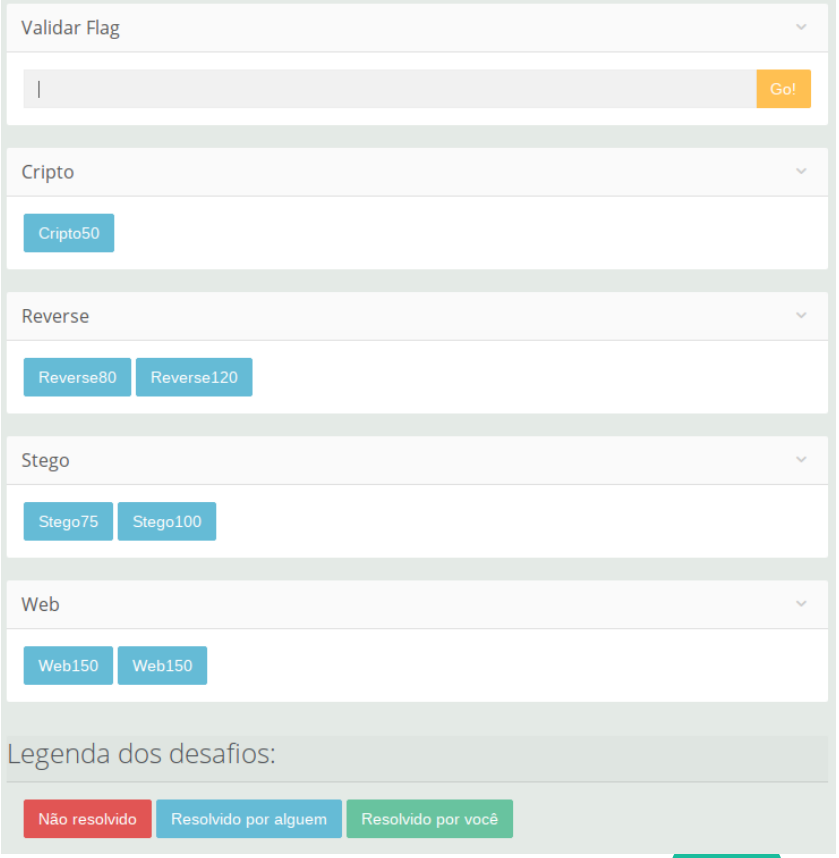


0x41444354465f57334c43304d335f37305f414443374632303134

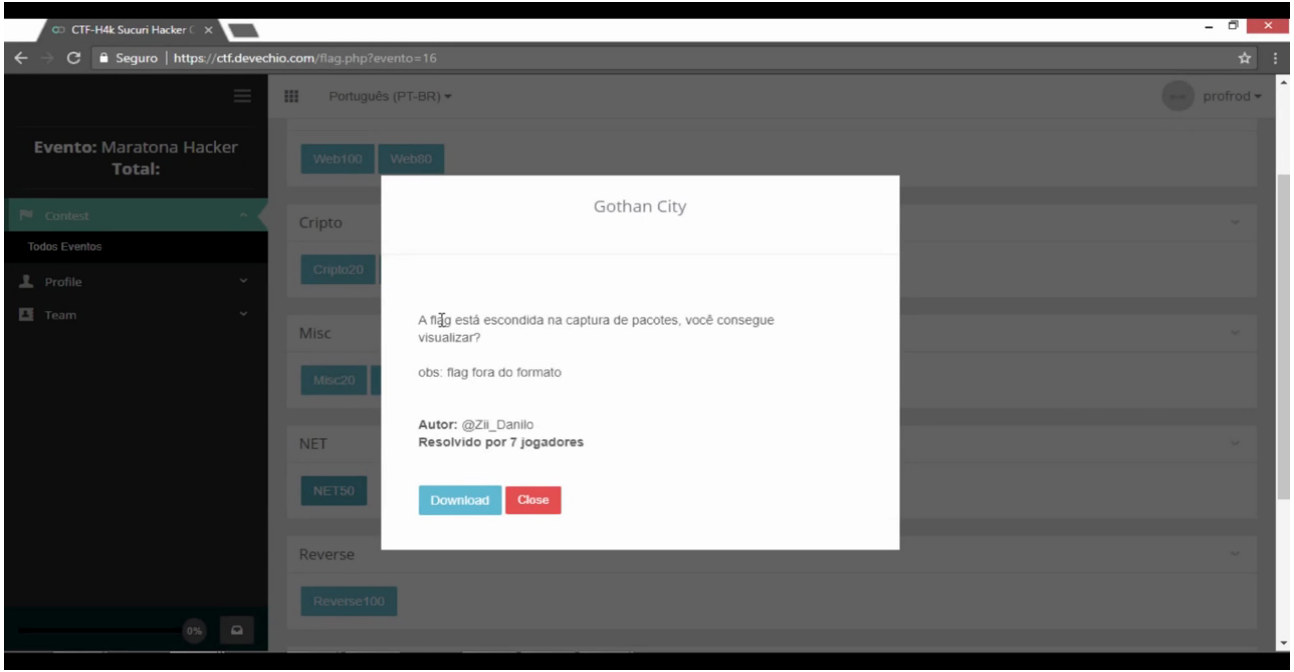
O que é CTF?

- **Jeopardy:**





O que é CTF?



https://www.youtube.com/watch?v=8SbWLg-TmBk

O que é CTF?

- **Attack/Defense:**
  - Jogado em times
  - Cada equipe recebe uma máquina virtual
  - A máquina virtual possui alguns serviços com ou sem vulnerabilidades
  - O time se divide em grupos de ataque e defesa
  - O grupo de ataque busca explorar as vulnerabilidades da *VM* do time adversário *(red team / pentest)*
  - O grupo de defesa busca corrigir as vulnerabilidades da sua *VM (blue team / hardening)*

Benefícios de jogar CTF?

- **Ver a aplicação dos assuntos aprendidos teoricamente**
  - Utilizando álgebra linear para burlar a assinatura de um arquivo:
  - Pt. 2: https://www.youtube.com/watch?v=EOlddNofKxo
  - Pt. 1: https://www.youtube.com/watch?v=Vgdhlh6evjI
- **Obter familiaridade com documentação técnica**
- **Obtenção de fundamentos importantes de segurança da informação**
- **Há uma crescente preocupação com SegInfo devido ao avanço do IoT**

Benefícios de jogar CTF?

- **Desenvolver uma base que diminuirá o primeiro impacto de disciplinas mais técnicas como:**
  - Programação I e II
  - Algoritmos e estruturas de dados
  - Banco de dados
  - Circuitos digitais
  - Arquitetura e organização de computadores
  - Redes de computadores
  - Sistemas operacionais

Benefícios de jogar CTF?

- **E em último caso, ficar rico com bug bounty**

Por onde começar?

- **Material de estudo:**
  - Muitos cursos gratuitos na internet
  - Muito conteúdo bom em inglês também de graça
  - Conteúdo em português?
  - Pirataria?
  - Livros?
- **Ajuda da comunidade**
- **Fóruns**
- **Contatos em eventos**

Por onde começar?

- **Plataformas para treinar os conceitos aprendidos**
- **Sistemas web com vulnerabilidades para explorar**
- **Distribuições Linux também com vulnerabilidades**

Por onde começar?

- **Cursos em português:**
  - https://solyd.com.br/treinamentos/
  - https://esecurity.com.br/cursos/
  - https://www.4linux.com.br/cursos
  - https://desecsecurity.com/treinamentos/
  - https://cursomalware.blogspot.com/?m=0
- **Cursos em inglês:**
  - http://liveoverflow.com/
  - http://www.fuzzysecurity.com/index.html
  - https://www.udemy.com/

Por onde começar?

- **Livros online:**
  - https://mentebinaria.gitbook.io/engenharia-reversa/
  - https://fundacion-sadosky.github.io/guia-escritura-exploits/

Por onde começar?

- **Forum:**
  - http://caveiratech.com/forum/
- **Canais do YouTube:**
  - Ricardo Longatto: https://www.youtube.com/user/ricardolongatto
  - Xtreme Security: https://www.youtube.com/user/daybsonbruno
  - Papo Binário: https://www.youtube.com/channel/UCuQ8zW9VmVyml7KytSqJDzg
  - Roadsec: https://www.youtube.com/channel/UCxHzA-Z97sjfK3OISjkbMCQ
  - Black Hat: https://www.youtube.com/channel/UCJ6q9Ie29ajGqKApbLqfBOg
  - Brasil Pentest: https://www.youtube.com/channel/UCJBj5qNoHQ9H7MqxZYiXEhw

Por onde começar?

- Bóson Treinamentos: https://www.youtube.com/user/bosontreinamentos
- Computerphile: https://www.youtube.com/user/Computerphile
- DEFCON Conference: https://www.youtube.com/user/DEFCONConference
- Live Overflow: https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w
- HackerSploit: https://www.youtube.com/channel/UC0ZTPkdxlAKf-V33tqXwi3Q
- MalwareAnalysisForHedgehogs: https://www.youtube.com/channel/UCVFXrUwuWxNlm6UNZtBLJ-A

Por onde começar?

- Colin Hardy: https://www.youtube.com/channel/UCND1KVdVt8A580SjdaS4cZg
- GynvaelEN: https://www.youtube.com/user/GynvaelEN
- IppSec: https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA
- Webpwnized: https://www.youtube.com/user/webpwnized
- Penetration Testing in Linux: https://www.youtube.com/channel/UC286ntgASMskhPIJQebJVvA
- Pentester Academy TV: https://www.youtube.com/channel/UChjC1q6Ami7W0E71TzPZELA

Por onde começar?

- Murmus CTF:
  https://www.youtube.com/channel/UCUB9vOGEUpw7IKJRoR4PK-A
- rev3rse security:
  https://www.youtube.com/channel/UCzvJStjySZVvOBsPl-Vgj0g
- Null Byte:
  https://www.youtube.com/channel/UCgTNupxATBfWmfehv21ym-g
- Filipe Balestra:
  https://www.youtube.com/channel/UCcbclCkQytwH1YCQLla-0WQ
- Free Training:
  https://www.youtube.com/channel/UC3RYdKzMQmdz8I8IU2iQDZA

Por onde começar?

- JJ Lima: https://www.youtube.com/channel/UCN82sPMFOLuM30BuTMZ8Mfg
- Malware Reverse: https://www.youtube.com/channel/UCl9lriUoIc6l03UhOISJdqQ
- OYS Academy: https://www.youtube.com/user/oyssecurity
- Prof. Rodrigo Costa: https://www.youtube.com/channel/UCYZXD54pNOJEuChfzQJ_sIg
- Danscourses: https://www.youtube.com/user/danscourses
- SecurityCast: https://www.youtube.com/channel/UCTEAZTTJ69yatuMd70k2Wow

Por onde começar?

- **Livros:**
  - Editora Novatec
- **Eventos:**
  - Roadsec
  - Cryptoparties
  - JampaSec
  - Hackers2Hackers Conference
  - SBSeg - Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais

Por onde começar?

- **Eventos:**
  - BSides
  - NullByte Security Conference
- **Distribuições Linux com vulnerabilidades:**
  - Metasploitable
- **Sistemas Web para explorar:**
  - OWASP Mutillidae
  - Damn Vulnerable Web Application – DVWA

Por onde começar?

- **Plataformas para treinar:**
  - Shellter labs: https://shellterlabs.com/pt/
  - Hackaflag: https://ctf.hackaflag.com.br/
  - CTF-H4k: https://sucurihc.maratonahacker.net.br/
  - OverTheWire: http://overthewire.org/wargames/
  - Maratona Hacker: https://www.maratonahacker.net.br/
  - Hack the Box: https://www.hackthebox.eu/
  - Cryptopals: http://cryptopals.com/
  - Smash the stack: http://smashthestack.org/

Por onde começar?

- **Plataformas para treinar:**
  - HackThisSite: https://www.hackthissite.org/
  - Try2Hack: http://www.try2hack.nl/
  - Vuln Hub: https://www.vulnhub.com/
  - PentesterLab: https://pentesterlab.com/
  - CTF365: https://ctf365.com/
  - Root Me: https://www.root-me.org/
  - RingZer0 Team Online CTF: https://ringzer0team.com/
  - WeChall: https://www.wechall.net/challs

Por onde começar?

- **Plataformas para treinar:**
  - Pentest it: https://lab.pentestit.ru/
  - Attack/Defense: https://public.attackdefense.com/
  - Eng. Reversa para iniciantes: https://www.begin.re/
  - CTF Learn: https://ctflearn.com/
  - Lista com mais CTFs: http://captf.com/practice-ctf/
- **Projetos importantes:**
  - https://ctf-br.org/
  - https://ctftime.org/

Objetivo da apresentação

- **Hype do e-sport na universidade**
- **Despertar o interesse sobre SegInfo no curso**
- **Promover uma maior aproximação entre as turmas**
- **Treinarmos juntos para participarmos das competições representando o curso e a universidade**

UFRPE vence Jogos Universitários Brasileiros na primeira edição de League of Legends

Dúvidas?

Obrigado pela atenção! :)

Contato:

 **@EwertonQueiroz**

ewerton.queiroz@outlook.com