' or 1=1 # Web Hacking 101

...

Introdução a vulnerabilidades em aplicações web

$ whoami

Diego Marques
dmarquesdev@gmail.com
https://github.com/dmarquesdev

- Bacharel em Ciências da Computação (UFSC)
- 6 anos de desenvolvimento web
- 2 anos como analista de cibersegurança
- Entusiasta do hacking desde sempre!

Conteúdo

- Primeiro dia
  - Bate-papo sobre a web e segurança no geral
  - Protocolo HTTP
  - Hands-on nas vulnerabilidades web
  - Exploração e mitigação
- Segundo dia
  - Aplicação das vulnerabilidades em cenário realístico (simulado)
  - Bate-papo sobre hacking

Disclaimer

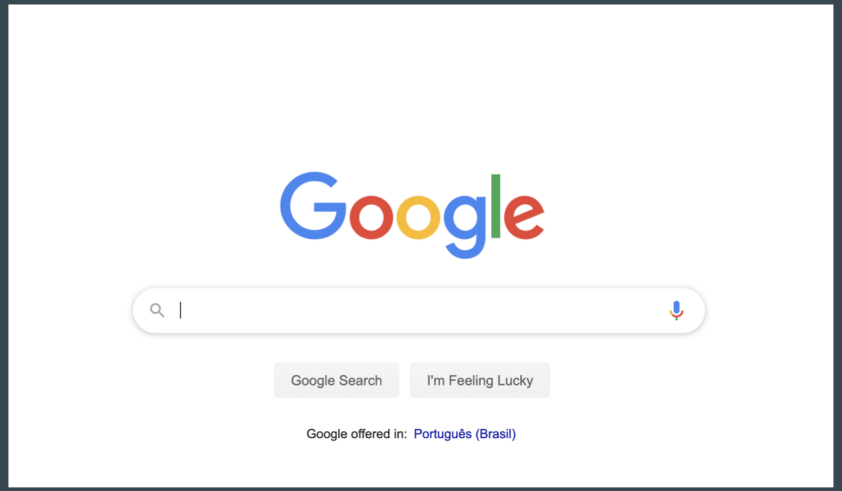
Todo o conteúdo apresentado nesse curso é para fins didáticos. Os ambientes que serão explorados são ambientes e aplicações que simulam a realidade.

A aplicação dos conteúdos ministrados cabe inteiramente aos participantes, não sendo de responsabilidade do ministrante ou da organização do evento os possíveis problemas gerados pelo mesmo.

"Uma faca serve tanto para cortar uma fruta quanto para cortar uma pessoa. Quem decide o uso é quem a maneja"

Aplicações Web

- Arquitetura mais utilizada para desenvolvimento de software
- Aplicações escaláveis
- Fácil acesso
- Fácil integração entre sistemas
- Mercado extremamente aquecido
- Comunidade gigante
- Suporte de grandes corporações



Desvantagens

- Mais propenso a bugs
- Maior quantidade de "desinformação" técnica
- Custo elevado para manter x aplicação desktop comum
- E acima de tudo....

Maior facilidade para criar vulnerabilidades de segurança!

Implicações

- Vazamento de dados
- Deface
- Máquina "zumbi"
- Extorsão
- Entre outros

OWASP

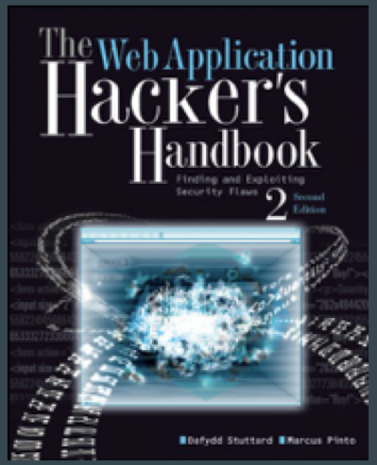
- Open Web Application Security Project
- Projeto voltado para segurança de aplicações web
- Categorizam as vulnerabilidades possíveis
- Top 10 de vulnerabilidades mais comuns e perigosas
- Trata também de aplicações mobile

Protocolo HTTP

Talk is cheap, show me the PoC!

Referências

- Open Web Application Security Project (OWASP)
  - https://www.owasp.org/index.php/Top_10-2017_Top_10
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws - 2nd Edition – Wiley - 2011 (Também conhecida como ~A bíblia do Web Hacking~)
- Web Hacking 101
  - https://leanpub.com/web-hacking-101
- Cybrary
  - https://www.cybrary.it/
- Udemy
  - https://www.udemy.com/



Referências

- PortSwigger Web Academy
  - https://portswigger.net/web-security
- Como Hackear
  - https://comohackear.com.br/
- Hackaflag Academy
  - https://hackaflag.com.br/academy.html
- Offensive Security Advanced Web Attacks and Exploitation
  - https://www.offensive-security.com/information-security-training/advanced-web-attack-and-exploitation/
- HackTheBox
  - https://www.hackthebox.eu/

Referências

- VulnHub
  - https://www.vulnhub.com/
- PentesterLab
  - https://pentesterlab.com/exercises
- eLearnSecurity
  - https://www.elearnsecurity.com/course/
- HackerOne
  - https://www.hackerone.com/
- BugCrowd
  - https://www.bugcrowd.com/