



## Tag de Web-Hacking

- 1) O que é o protocolo HTTP? Explique como ele funciona
- 2) O que é um Response Code? Cite um exemplo de um programa que você pode fazer com ele.
- 3) O que é um HEADER? Cite um uso INSEGURO desse cabeçalho.
- 4) O que é um Método HTTP? Explique o funcionamento do método POST, o funcionamento do método GET. Explique qual é considerado mais seguro e por que.
- 5) O que é Cache e como ele funciona? Cite os principais HEADERS de Request e Response responsáveis pelo controle de Cache.
- 6) O que é Cookie? Qual é o principal ataque relacionado a ele?
- 7) O que é OWASP-Top-Ten?
- 8) O que é Recon e Por que ela é importante?
- 9) Command Injection (SO-Injection)
  - a) O que é Command Injection?
  - b) Mostre um exemplo de Command Injection ( PoC da exploração )



- 10) SQL INJECTION
  - a) O que é SQL injection?
  - b) O que é Union Based Attack?
  - c) O que é Blind-SQL-I?
  - d) Mostre um exemplo de um Blind SQL-Injection ( PoC da exploração ).
  
- 11) XSS
  - a) O que é XSS?
  - b) Quais são os tipos de XSS? Explique-os.
  - c) Mostre um exemplo de um XSS Stored ( PoC da exploração ).
  - d) Mostre um exemplo de um DOM-XSS ( PoC da exploração ).
  
- 12) LFI , RFI e Path Traversal
  - a) O que é LFI?
  - b) O que é RFI?
  - c) O que é Path Traversal?
  - d) Como aliar Path Traversal e LFI
  - e) Mostre um exemplo de LFI utilizando a contaminação de LOGS ( PoC da exploração ).



- 13) CSRF e SSRF
- a) O que é CSRF?
  - b) Mostre um exemplo de CSRF  
( PoC da exploração )
  - c) O que é SSRF?
  - d) Mostre um exemplo de SSRF  
( PoC da exploração )
  - e) Como evitar ataques de CSRF?