REPÚBLICA FEDERATIVA DO BRASIL UNIVERSIDADE *HACKER* INTRODUÇÃO A SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS MÓDULO VII – DESENVOLVIMENTO *WEB*

Considerações finais

Prof. Alex Dias Camargo

alexcamargoweb@gmail.com





I. Plano de aula

Na aula anterior foi visto:

- Conceito de execução de comandos em sites cruzados
- □ Exemplo prático: PHP e *JavaScript*



I. Plano de aula

Nesta aula será apresentado:

- Considerações finais do Módulo
- Principais abordagens de desenvolvimento Web seguro



1. Introdução

Nas **inúmeras aplicações Web** desenvolvidas atualmente, os invasores precisam obter acesso a apenas algumas contas ou apenas uma conta de administrador para comprometer o sistema.

- Validar as entradas de todas as fontes de dados externas, incluindo arquivos controlados pelo usuário.
 - Ex.: formulários, APIs, etc.
- Projetar a aplicação para implementar políticas de segurança.
 - Ex.: logs de acesso e atividade, níveis de permissão, etc.
- Ter uma defesa em camadas com múltiplas camadas.
 - Ex.: validação no front-end e back-end, em nível de SO, etc.



1. Introdução

Caso você **queira aprender mais** sobre os tópicos aqui abordados, há uma série de vídeos no *Youtube* muito interessante (em português).

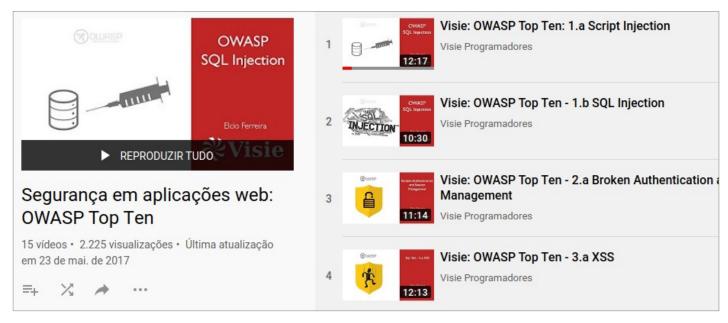


Figura. Segurança em aplicações web: OWASP Top Ten.

Link: https://bit.ly/2KyTl8g



Referências básicas

OWASP, Top. Top 10-2017. **The Ten Most Critical Web Application Security Risks. OWASP™ Foundation. The free and open software security community.** URL: https://www.owasp.org/index.php/Top_10-2017_Top_10, 2017.