



# Open **W**eb **A**pplication **S**ecurity **P**roject

## Segurança em Web – Aula 4

Maycon Maia Vitali ( OutOfBound )

[maycon@hacknroll.com](mailto:maycon@hacknroll.com)

Hack'n Roll



Centro Universitário Vila Velha

# Agenda

- Revisão da Última Aula
  - Execução de Arquivos Remotos
  - Referência a Objetos Inseguros
  - Cross Site Request Forgery
- Vazamento de Informações
  - Mensagens de Erro
  - robots.txt, seu (segundo) melhor amigo
- Furos de Autenticação e Gerência de Sessão
- Armazenamento Criptográfico Inseguro
- Comunicação Insegura
- Falha de Restrição de URL
- Conclusão

# AVISO

## ATENÇÃO

**O instrutor do curso (Maycon Maia Vitali) tão pouco o Centro Universitário Vila Velha não se responsabilizam pela má utilização das informações fornecidas neste curso.**

**O Curso de Extensão Tecnológica em Segurança Web tem a única finalidade de formar profissionais aptos a desenvolver um ambiente Web seguro, protegendo-o de ataques que porventura viriam acontecer.**

**Qualquer ato ilícito ou ilegal acarretado devido a má utilização das informações apresentadas no curso serão de inteira responsabilidade do autor, estando o mesmo completamente sujeito as mais severas penalidades cabíveis pela lei.**

# Revisão da Última Aula



Centro Universitário Vila Velha

# Execução de Arquivos Remotos

- Produtividade vs Qualidade
- Possibilidades:
  - Apagar Arquivos
  - Instalar programas (keyloggers, sniffers, rootkit, etc)
  - Compromete o servidor inteiro
  - Repositório de Virus e servidor Zumbi (DDoS)
- Ocorrência com `include*` e `require*`
- Exemplos

# Vazamento de Informação



Centro Universitário Vila Velha

# Princípios de *Information Leak*

- Informação de desinteresse para o usuário são úteis para um atacante.
- Debugging só se utiliza em tempo de desenvolvimento.
- Não utilize mecanismos não padrões de proteção, pois você pode estar dando um tiro no próprio pé.

# Informações de Desinteresse

Usuário Inválido + Senha inválida

X

Usuário/Senha inválidos

- 200 Sobrenomes
- Prefixo e Sufixo → 5.200
- Senhas = 010160 ... 311208 (17.520 pos.)

# Usuário/Senha Inválido

- Total de Usuários:
  - 5.200
- Total de Senhas:
  - 17.520
- Total de tentativas:
  - $5.200 * 17.520 = 91.104.000$  (~ 3 anos)

# Usuário Inválido + Senha inválida

- Total de Usuários:
  - 5.200 (encontramos N válidos em ~ 1h30)
- Total de Senhas:
  - 17.520
- Total de tentativas (Ex: para 5 usuários):
  - $5 * 17.520 = 8.760$  (~ 24h08)

# Debugging Desnecessário

- Erro de SQL:
  - Erro em: `Select * from noticias where id='`
- Erros do PHP
  - Failed to include file `/var/www/site.com/hack.php`
- Directory Indexing
  - Index of `/arquivos/`

# Recursos mal-utilizados

- Robots.txt

User-Agent: \*

Disallow: /bd/banco.mdb

Allow: /

- Utilize meta tags:

```
<META
```

```
  NAME="ROBOTS"
```

```
  CONTENT="NOINDEX,NOFOLLOW"
```

```
>
```

# Autenticação e Gerência da Sessão



Centro Universitário Vila Velha

# Princípios de Sessão

- O que é sessão?
- O que é *cookie*?
- Como fazer um ataque à sessão?

# *Session Hijacking*

- Através de falhas de XSS
- Através de Sniffer de rede (local)
- Através de cookies armazenados

# *Session Fixation*

- Não é necessário estar logado
- Gera-se uma sessão para o usuário
- Espera-se ele autenticar e utiliza-se a sessão já conhecida.

# Não utilize cookies (?)

- Nunca armazene informações que não podem ser modificadas:
  - admin=false
  - logado=false
  - userid=1001
- Nunca utilizem algoritmos próprios de geração de *tokens* de *cookie*

# Proteção contra Sequestro de Sessão por XSS

- A falha não está na sessão
- Tokens em formulários
- HttpOnly
- Utilizar criptografia (https)

# Armazenamento Criptográfico Inseguro



Centro Universitário Vila Velha

# Definições

- Funções Hash
- Funções Criptográficas
  - Criptografia Simétrica
  - Criptografia Assimétrica
- Hash + Criptografia

# Tipos de Ataques

- Senhas fracas
  - *Brute-force*
- Senhas fortes
  - *Wordlist*
- *Rainbowcrack + hash sites*

# Tipos de Ataques RainbowCrack

- Brute-force Normal:
  - 350 milhões de senhas (texto puro) por segundo.
- Rainbow
  - 62.223 milhões de senhas em texto puro por segundo

# Tipos de Ataques BOTNets

- Servidor: irc.plain-text.info
- Canal: #RainbowCrack

[02:12] <OutOfBound> .C3P0 addmd5 8c52b2a2bea46c2f74579bff96175474

[02:12] <@C3P0> OutOfBound: add ok... at 06:12:03

[02:12] <@C3P0> MD5 Hash:**8c52b2a2bea46c2f74579bff96175474** passwd:**beringela** hex:626572696e67656c61

[02:12] <OutOfBound> .C3P0 addmd5 91f5167c34c400758115c2a6826ec2e3

[02:12] <@C3P0> OutOfBound: add ok... at 06:12:08

[02:12] <@C3P0> MD5 Hash:**91f5167c34c400758115c2a6826ec2e3** passwd:**administrador** hex:61646d696e6973747261646f72

[02:12] <OutOfBound> .C3P0 addmd5 9de07c176f15b02da6694f1ac518af6f

[02:12] <@C3P0> OutOfBound: add ok... at 06:12:53

[02:12] <@C3P0> MD5 Hash:**9de07c176f15b02da6694f1ac518af6f** passwd:**cascadura** hex:636173636164757261

# Tipo de Ataque Md5 Web Crackers

- <http://www.md5crack.com/>



# Proteção de Dados

- Armazenamento de Senha?
- Dados a serem recuperados?
- *Hash* puro?
- E criptografia? Proteja bem a chave.

# Comunicação Insegura



Centro Universitário Vila Velha

# Comunicação Insegura

## Gerenciamento de Sessão

- Criptografar não somente para armazenar
- Processo de Autenticação em HTTP
  - Sniffer + MiTM = roubo de senhas
- SSL + HTTP = HTTPS
  - Não é 100% eficás

# Boas Práticas

- SSL em tráfegos com informações sigilosas
- SSL em tráfegos que utilizam sessões
- Boa infra-estrutura de rede (evitar MiTM)

# Falha de Restrição de URL



Centro Universitário Vila Velha

# Princípios da Falha de Restrição de URL

- Controle de sessão para acessar as páginas
- Sem qualquer controle de permissão entre as páginas.
- Se tiver uma sessão é possível acessar qualquer página.



# Open **W**eb **A**pplication **S**ecurity **P**roject

Fim. Será?!?!

Maycon Maia Vitali ( OutOfBound )

[maycon@hacknroll.com](mailto:maycon@hacknroll.com)

Hack'n Roll



Centro Universitário Vila Velha