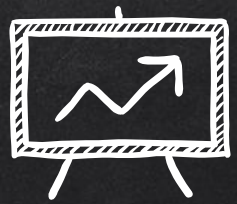

Detecção de vulnerabilidades em aplicações WEB

Bruno Padilha

Bruno Padilha

Graduando em Sistemas de informação pela Universidade Tecnológica Federal do Paraná. Entusiasta em segurança da informação. É desenvolvedor de software na Identifique Artigos Personalizados e é co-fundador da startup CriarCartao.com.br.

“Art. 154-A. Invadir dispositivo informático alheio, conectado ou não á rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
”

Motivação

- Rápida evolução da computação WEB
- Desenvolvedores se apoiam muito em frameworks / CMS
- Muitas aplicações carregando informações atrativas para ataques (números de cartões de créditos, informações bancárias, informações pessoais e privadas)

Aplicação WEB

Definições, conceitos, arquitetura, protocolo HTTP

Uma aplicação WEB é um software que é acessado através da rede utilizando o protocolo HTTP. Geralmente, o browser é utilizado como cliente.

Arquitetura geral de uma aplicação WEB

- Front-end / Client side
- Back-end / Server side
- Protocolo HTTP(S)

Arquitetura Three-tier

Protocolo HTTP

STATUS	DESCRIÇÃO
1xx	Classe informativa
2xx	Indica sucesso.
3xx	Classe de redirecionamento.
4xx	Classe de erros ocorridos no cliente.
5xx	Classe de erros ocorridos no servidor.

COMANDO	DESCRIÇÃO
GET	Solicita um recurso ao servidor WEB.
POST	Envia dados ao servidor WEB.
HEAD	Solicita o cabeçalho de um recurso ao servidor WEB.
PUT	Envia dados para o servidor WEB.
DELETE	Remove um recurso armazenado em um servidor WEB.

Vulnerabilidades

OWASP, Ferramentas, Vulnerabilidades

OWASP

The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software.

Vulnerabilidades

- Cross-site scripting (Front-end)
- SQL Injection (Back-end)

Cross-site scripting (XSS)

Ocorre em duas situações:

- Dados entram em uma aplicação WEB através de uma fonte não confiável (WEB Request)
- Dados incluídos pelo usuário (conteúdo dinâmico) sem serem corretamente validados

Demonstração

SQL-Injection

- Consiste na injeção de código SQL na aplicação através de uma entrada de dados não confiável.

```
ID = FONTE_INSEGURA;
db->query("SELECT * FROM tabela WHERE id = ' id' ");
```

SQL-Injection

Demonstração

Obrigado

linkedin.com/in/brunopadilha
github.com/bpadilha
http://www.bpadilha.com