
TECLAND
ENCONTRO

PHP Seguro – Passos básicos

Éderson T. Szlachta
{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

Éderson

Analista e Desenv. de Sistemas.

Desenvolvimento Web:

- *PHP, MySQL*
- *JavaScript*
- *ActionScript 3.0 (quando necessário)*
- *ASP/C# .NET, SQL Server*

Desktop:

- *Java*
- *C#*

Éderson T. Szlachta

{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

Razões

- **PHP** (!”POO”), em minha humilde opinião, é fácil de aprender
- Rapidamente pequenas aplicações são lançadas na web
- Maioria delas não possui controle de segurança básico

Éderson T. Szlachta
{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

Formas

Ataques à servidores ocorrem diariamente e isso não novidade. Aqui vamos ver algumas formas de ataques e como evitá-las.

- Clickjacking
- RFI (**R**emote **F**ile **I**nclude)
- LFI (**L**ocal **F**ile **I**nclude)
- SQL injection
- Cross-Site Scripting (XSS)
  - Reflected / Stored
- File-Upload

Éderson T. Szlachta

{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

Clickjacking

Não se trata de uma forma de ataque mas sim uma forma de “Roubar Cliques” fazendo com que o usuário acredite que está clicando em um conteúdo mas na verdade está fazendo alguma outra ação.

Éderson T. Szlachta

{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

RFI - LFI

Estas duas técnicas resumem-se em inserir um arquivo, geralmente um script malicioso, para um servidor executar.
Estas falhas são, de certa forma, antigas mas ainda ocorrem e, quando encontradas, podem ser fatais para o servidor.

RFI:
Inserir um aquivo armazenado em servidor diferente do qual onde está o site alvo.

LFI:
Inserir um arquivo que está armazenado no mesmo servidor que o site.

Éderson T. Szlachta
{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

SQL Injection

Esta é uma vulnerabilidade rara de ser encontrada nos dias atuais. Rara mas não extinta. O princípio básico desta é a inserção de comando SQL para quebrar a rotina de chamada de banco de dados e ter acesso ao dados/servidor alvo.

Éderson T. Szlachta

{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

Cross-Site Scripting (XSS)

Aparentemente simples mas fatal. Diversas vezes as redes sociais foram alvo deste tipo de ataque. Consiste em inserir um script, geralmente JavaScript, o qual será executado pelo browser do usuário. O script é criado para se reproduzir entre os usuários que acessam o site e efetuam roubo de informações entre outras coisas.

Reflected:
Quando inserido em um campo de busca, por exemplo, logo é executado e descartado.

Stored:
Inserido através de formulários de cadastro, comentários de sites, etc. Fica salvo no banco de dados.

Éderson T. Szlachta
{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

File-Upload

Muitos site utilizam inserção de arquivos por parte dos usuários o que pode gerar problemas para o servidor. Um usuário mal intencionado pode mascara códigos maliciosos em arquivos e enviá-los para o servidor. Se o programador não aplicar bons filtros sobre o arquivo recebido pode entregar todo o ouro ao bandido.

Éderson T. Szlachta

{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}

Referências

https://www.owasp.org/index.php/Category:Attack
http://en.wikipedia.org/
http://www.dvwa.co.uk/
http://www.securephpwiki.com/index.php/Main_Page

Éderson T. Szlachta

{Tecnólogo em Análise e Desenv. De Sistemas – FAE 2010}


TECLAND
ENCONTRO