Estudo e Análise de Vulnerabilidades Web

Apresentação: Vagner Kaefer Dos Santos
Adaptado de (Monteverde et al. 2014)

Conceitos Fundamentais (CID)

- Confidencialidade (Disponível somente para pessoas autorizadas)
- Integridade (Informação correta)
- Disponibilidade

Vulnerabilidade Web

Prazos curtos de entrega das aplicações aliados a processos falhos de desenvolvimento resultam em maior taxa de falhas de segurança nas aplicações.

A **qualificação técnica** dos desenvolvedores e uma política de revisão constante e de melhoria contínua.

Configurações padrões

A configuração dos servidores e/ou equipamentos de rede, quando feitas de maneira padrão, podem oportunizar brechas graves de segurança independentemente da qualidade e dos padrões de segurança aplicadas no processo de desenvolvimento.

Principais tipos de ataques conhecidos

- SQL Injection
- Roubo de Sessions e Cookies
- XSS
- Níveis de acesso
- CSRF (Falsificação de solicitações)
- Man in the middle

Como são encontradas e exploradas?

- Manualmente
- Scanners

Windows: Acunetix

Linux: Nikto, Nessus, Uniscan, Grabber, W3af, WebScarab, Sqlmap, Wireshark, etc.

Sql Injection

```php
<?php

//url.com.br/noticias/1542

$parametro = get(1); //1542

$query  = "SELECT id, name, texto FROM noticias where id = '".$parametro."'";

//[Executa a query...]

?>
```

Sql Injection

```php
<?php

//url.com.br/noticias/1542'; DROP table noticias;--

$parametro = get(1); //1542'; DROP table noticias;--

$query  = "SELECT id, name, texto FROM noticias where id = '".$parametro."'";
//SELECT id, name, texto FROM noticias where id = '1542'; DROP table noticias;--
//[Executa a query...]

?>

```

Sql Injection

```php
<?php
//[...]

$parametro = (int)get(1);

//[...]
?>
```

Sql Injection

90% das vulnerabilidades classificadas como severas são de injeção de código SQL na aplicação.

Apenas **UM** parâmetro não validado em uma aplicação Web, expõe ao risco várias outras aplicações e, consequentemente, toda uma infraestrutura de servidor de banco de dados incorretamente configurado.

Cross-site Scripting (XSS)

Este ataque permite que códigos sejam inseridos de maneira arbitrária no navegador do usuário alvo.

pesquisar.php?s=busca do usuário

Roubo de Sessão

O roubo de sessão normalmente utiliza em conjunto o ataque Man in The Middle.

```php
<?php
$_SESSION['usuario'] = 'Thiago';
```

Roubo de Sessão

Qual o problema do código?

```php
<?PHP
session_start();

//Caso o usuário não esteja autenticado, limpa os dados e redireciona
if ( !isset($_SESSION['login']) and !isset($_SESSION['senha']) ) {
    //Destrói
    session_destroy();

    //Limpa
    unset ($_SESSION['login']);
    unset ($_SESSION['senha']);

    //Redireciona para a página de autenticação
    header('location:login.php');
}
?>
```

Tratamento arquivos

- **Upload**

Validar e filtrar todas as extensões dos arquivos e salvar com nome randômico.

arquivo_bonitinho.jpg.php

- **Download**

Filtrar o que pode o servidor está enviando para o usuário.

baixar.php?f=relatorio_lucros_2016.pdf ➜ baixar.php?f=index.php

Níveis de Acesso

Verificar não somente se o usuário está logado corretamente, mas também se ele tem acesso para as solicitações.

alterar_dados_usuario.php?id=5 ← Página do usuário.

alterar_dados_usuario.php?id=1 ← Página do administrador.

Configuração incorreta

No ataque realizado no trabalho de referência, o roubo de UMA senha, possibilitou o acesso ao banco de dados de 177 aplicações. Comprometendo a confidencialidade de todas elas.

Exposição de dados sensíveis

Um dos testes em um site que utilizava o sistema moodle sem **https** possibilitou a visualização de todos os dados da rede, inclusive todos os dados de logins dos usuários que utilizavam o sistema.

- Man in the middle

Componentes de terceiros

A instalação de um tema no Wordpress tornou o sistema vulnerável a Sql Injection. A versão original do sistema não possuía a brecha de segurança, mas o software de terceiros tornou todo o sistema vulnerável.

Sites testados

Tabela 1. Visão geral das varreduras.

Tipos de Sítios Web	Tempo Médio de Varredura	Quantidade de Sítios Web
Comércio Eletrônico	6 horas	4
Religiosos	30 minutos	1
Acadêmicos	3 horas	2
Grandes Portais	6.3 horas	1
Sítios que Utilizam CMS	56 minutos	2
Governamentais	30 minutos	1
Regionais	40 minutos	4
Conteúdo Adulto	1 hora	1

Resultados encontrados

Tabela 2. Distribuição dos Sítios e as Vulnerabilidades Encontradas.

Sítios/Tipo de Sítios	Vuln. Severa	Vuln. Moderada
Sítio 1 / Regional	0	1
Sítio 2 / Comércio Eletrônico	0	2
Sítio 3 / Regional	1	2
Sítio 4 / Grande Portal	0	1
Sítio 5 / Regional	0	2
Sítio 6 / Comércio Eletrônico	1	2
Sítio 7 / Comércio Eletrônico	1	1
Sítio 8 / Acadêmico	1	2
Sítio 9 / CMS	1	2
Sítio 10 / Religioso	1	2
Sítio 11 / Acadêmico	1	1
Sítio 12 / Governamental	1	1
Sítio 13 / Regional	1	1
Sítio 14 / CMS	0	1
Sítio 15 / Comércio Eletrônico	1	1
Sítio 16 / Conteúdo Adulto	1	2

Discussões

TODOS os sítios analisados apresentaram vulnerabilidades, o que ressalta a falta de preocupação com segurança.

A vulnerabilidade explorada poderia comprometer seriamente a aplicação e o negócio vinculada a mesma.

NUNCA confie no usuário

Simplesmente filtre tudo. Onde houver uma chance de o usuário gerar problemas, será o primeiro lugar que ele irá ir. (Murphy's Law)

Conclusões

Muitas empresas de desenvolvimento ainda não aplicam os principais conceitos de segurança no desenvolvimento de suas aplicações.

Fatores como esse contribuem para um crescente número de falhas básicas e simples de serem exploradas, conforme foi apresentado no trabalho.

Há a urgência de conscientizar e treinar os desenvolvedores de software sobre a importância de programação segura com o intuito de diminuir as vulnerabilidades nas aplicações Web.

Links interessantes

- Running an SQL Injection Attack - Computerphile
- Hacking Websites with SQL Injection
- Roubo de sessão com xss

Referências

MONTEVERDE, Wagner; CAMPIOLO, Rodrigo. **Estudo e Análise de Vulnerabilidades Web**. SB Seg 2014 (pg 415-423).