# The Cracker Technology

## Report: Principais vulnerabilidades em sites

Relatório oficial da The Cracker Technology sobre as principais vulnerabilidades web

Baseado em experiencias de trabalho e observações na internet.

Weidsom Nascimento – The Cracker Technology

# The Cracker Technology

## Categorias:

- Injection flaws
- Broken Authentication
- Cross Site Scripting (XSS)
- Insecure Direct Object References
- Security misconfiguration
- Sensitive data exposure
- Missing function level access control

# The Cracker Technology

## Command Injection

```
<?php
print("Please specify the name of the file to delete");
print("<p>");
$file=$_GET['filename'];
system("rm $file");
?>
```

http://vulserver.com/delete.php?filename=test.txt;id

Caracteres usados para cmd injection:

;  - ponto e virgula.
&&  - 2 símbolos 'E' comercial.
|  - pipe.

# The Cracker Technology

## SQL Injection

Mesmo se tratando de uma falha muito trivial e explorada ainda é possível encontrar muitas aplicações com essa vulnerabilidade.

SQL Injection ocorre quando a aplicação falha em filtrar os caracteres em consultas ao banco de dados.

Apesar de simples SQL Injection pode comprometer todo o banco de dados e também a aplicação.

# The Cracker Technology

## LFI/RFI

Local File Inclusion e Remote File Inclusion são vulnerabilidades que permitem que arquivos sejam incluídos de forma arbitraria na aplicação.

Vulnerabilidades comuns e bastante perigosas pois no caso de LFI (Local File Inclusion) permite que o atacante possa ler, baixar, executar... arquivos do servidor de forma simples, se tratando de RFI (Remote File Inclusion) é ainda pior por que em alguns casos pode ate mesmo executar remotamente uma shell ou exploit no servidor corrompendo a integridade da aplicação.

# The Cracker Technology

## session hijacking

Falha comum em aplicações web que permite roubar uma sessão valida devido a falhas de autenticação

Sessões podem ser roubadas caso a aplicação confie totalmente nos cookies e não execute uma validação da origem real da requisição, um atacante pode se posicionar no meio da rota dos pacotes e capturar o id de sessão e assim acessar a aplicação sem nenhuma forma adicional de validação.

# The Cracker Technology

## Cross-site scripting (XSS)

Vulnerabilidade que raramente afeta a aplicação mais tem o foco nos usuários do sistema

XSS abre uma porta para diversos tipos de ataques como praticamente todos os sites da internet usam javascript mais da metade destes são vulneráveis a xss.

XSS permite a execução de código javascript para um usuário por meio de links infectados ou objetos na página, em alguns casos pode ser de classe: stored, nesse caso o código é inserido em bancos de dados ou arquivos de configurações.

# The Cracker Technology

## Cross-site request forgery

Vulnerabilidade que permite ao atacante manipular ações na aplicação vulnerável.

Com CSRF requisições podem ser forjadas forçando o browser executar uma ação em uma pagina que esteja logado, se a aplicação for vulnerável os dados repassados pelo navegador serão aceitos no sistema.

# The Cracker Technology

## Directory traversal

Vulnerabilidade que permite o acesso a arquivos em outros diretórios.

Potencialmente perigosa pois pode fornecer acesso a arquivos com informações sensíveis tais como: scripts php, arquivos de configuração, arquivos de senhas...

```
<?php
$template = 'red.php';
if (isset($_COOKIE['TEMPLATE']))
   $template = $_COOKIE['TEMPLATE'];
include ("/home/users/phpguru/templates/" . $template);
?>
```

```
GET /vulnerable.php HTTP/1.0
Cookie: TEMPLATE=../../../../../../../../../../etc/passwd

HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:fi3sED95ibqR6:0:1:System Operator:/:/bin/ksh
daemon:*:1:1::/tmp:...
```

# The Cracker Technology

## Listagem de diretórios

Um grande erro dos programadores que pode ser um backport para futuros ataques

Com a listagem de diretórios ativa um atacante pode identificar facilmente as estruturas internas dos arquivos na aplicação dessa forma fica mais simples um ataque direto a paginas administrativas por exemplo, essa vulnerabilidade pode ser combinada a outras como LFI e etc.

# The Cracker Technology

## Páginas administrativas

Com páginas administrativas simples como "/admin" possibilita uma rápida descoberta em seguida abre espaço para quebra de senhas, alguns desenvolvedores não se preocupam com a segurança das páginas de administração, muitas outras vulnerabilidades podem ser combinadas para atacar uma pagina de administração insegura.