



## Vulnerability Report



**CVE-2022-45227**

**Date: 08/12/2022**

**Author: K. Narahari**

## Vulnerability Description

DRAGINO - 18ed40 web portal has the directory listing on <https://10.10.20.74/lib/>. This has a backup file which can be downloaded without any authentication due to directory listing flaw.

## Impact

Attacker can open the URL, download the backup file, and read the contents of the backup file without requiring any authentication.

## Severity

Category	CVSS 3.0 score
High	7.0

## Weakness Enumeration

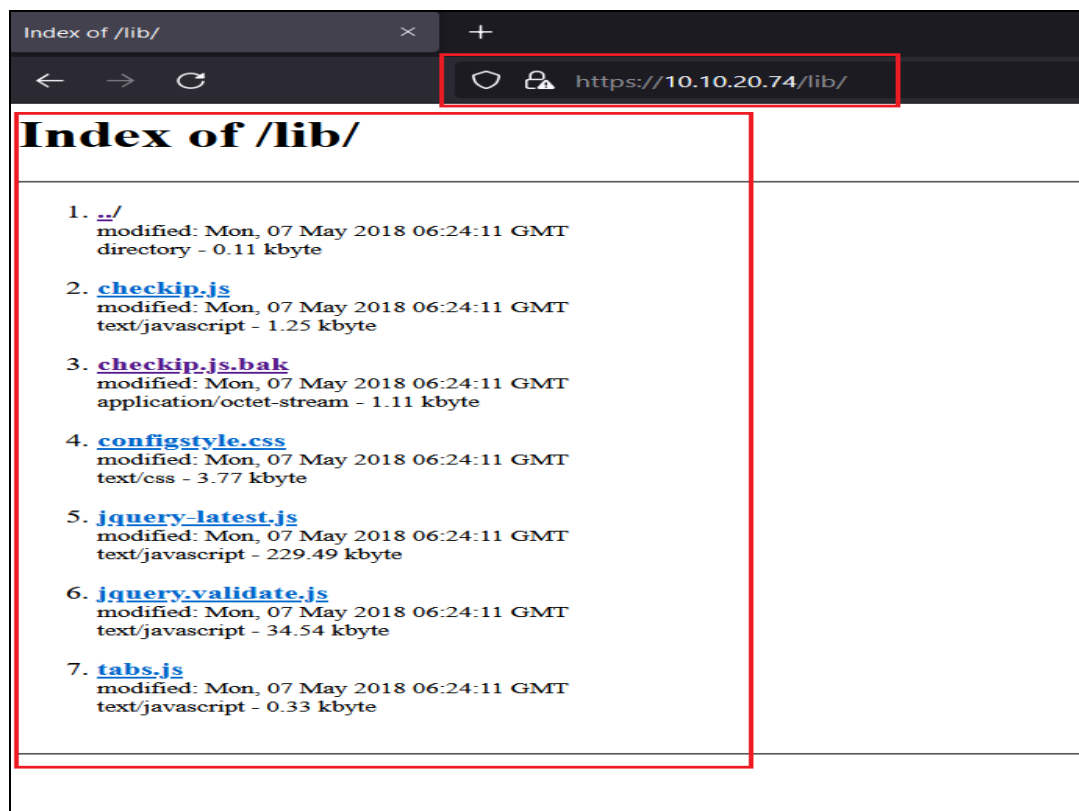
CWE-ID	CWE Name
CWE-22	Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)

## Steps to Reproduce

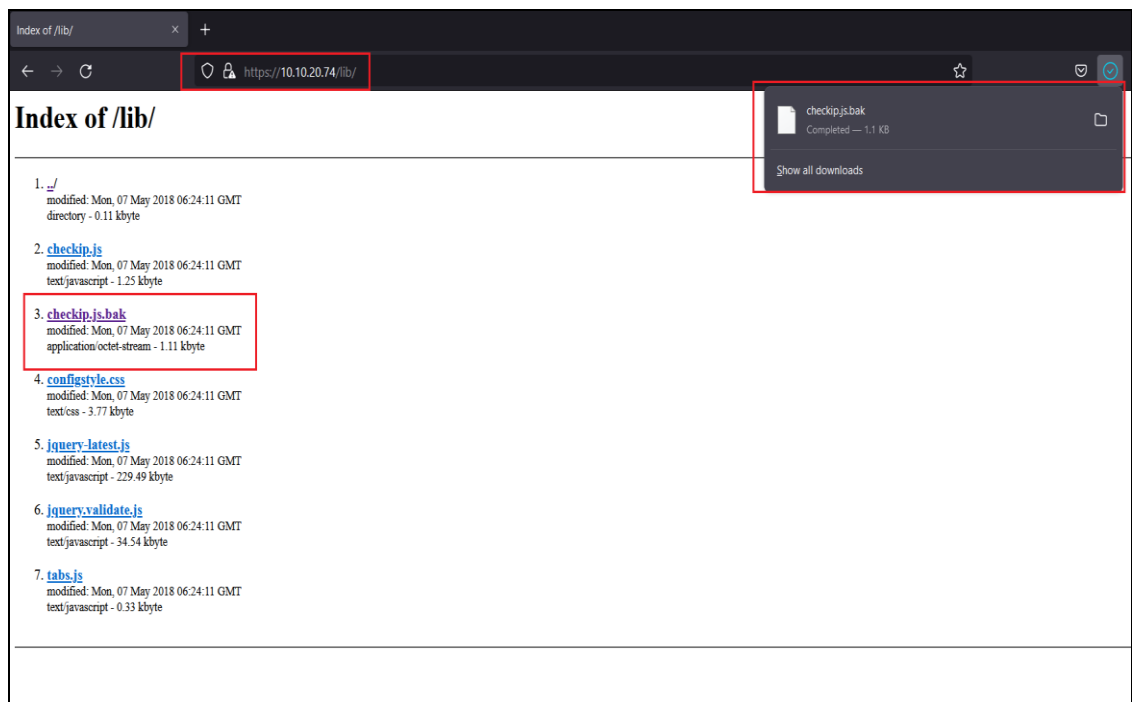
1. Perform directory enumeration using directory bruteforce tool.

```
└─# gobuster dir -u 10.10.20.74 -w /usr/share/wordlists/dirb/small.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.10.20.74
[+] Method:             GET
[+] Threads:           10
[+] Wordlist:           /usr/share/wordlists/dirb/small.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.1.0
[+] Timeout:           10s
=====
2022/05/10 13:34:42 Starting gobuster in directory enumeration mode
=====
/cgi-bin/              (Status: 403) [Size: 79]
/cgi-bin               (Status: 302) [Size: 0] [--> /cgi-bin/]
/data                 (Status: 401) [Size: 0]
/lib                  (Status: 302) [Size: 0] [--> /lib/]
/mailbox              (Status: 401) [Size: 0]
=====
2022/05/10 13:34:49 Finished
=====
```

2. Access the URL <https://10.10.20.74/lib/> using the browser and we can see the directory listing.



3. Click **checkip.js.bak**. The backup file is downloaded in a readable format.



## Mitigation:

- Configure your web server to prevent directory listings for all paths beneath the web root.
- Place a default file (such as `index.htm`) into each directory that the web server will display instead of returning a directory listing.