SECTRIO

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

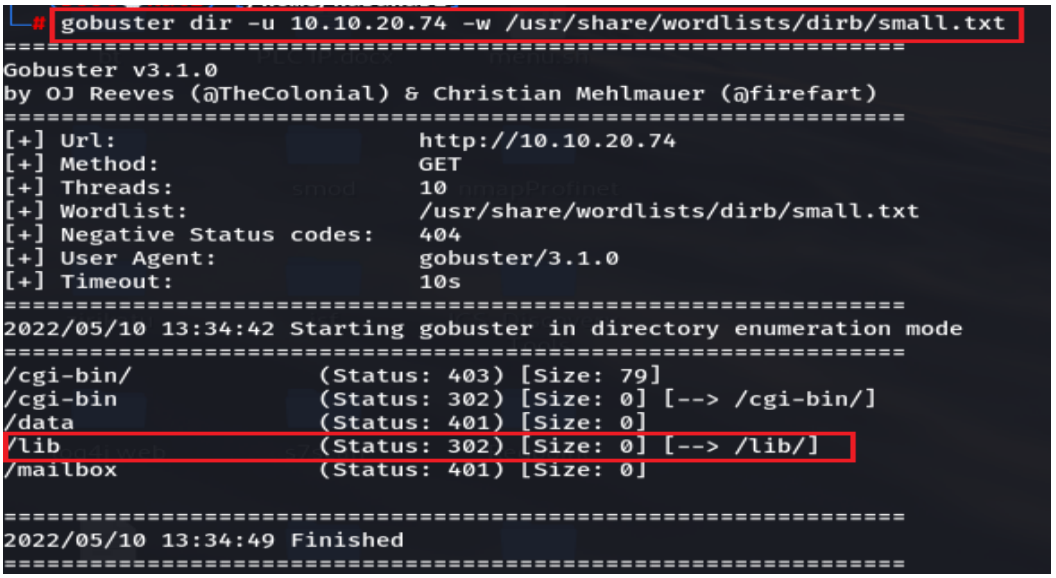
Category	CVSS 3.0 score
High	7.0

Weakness Enumeration

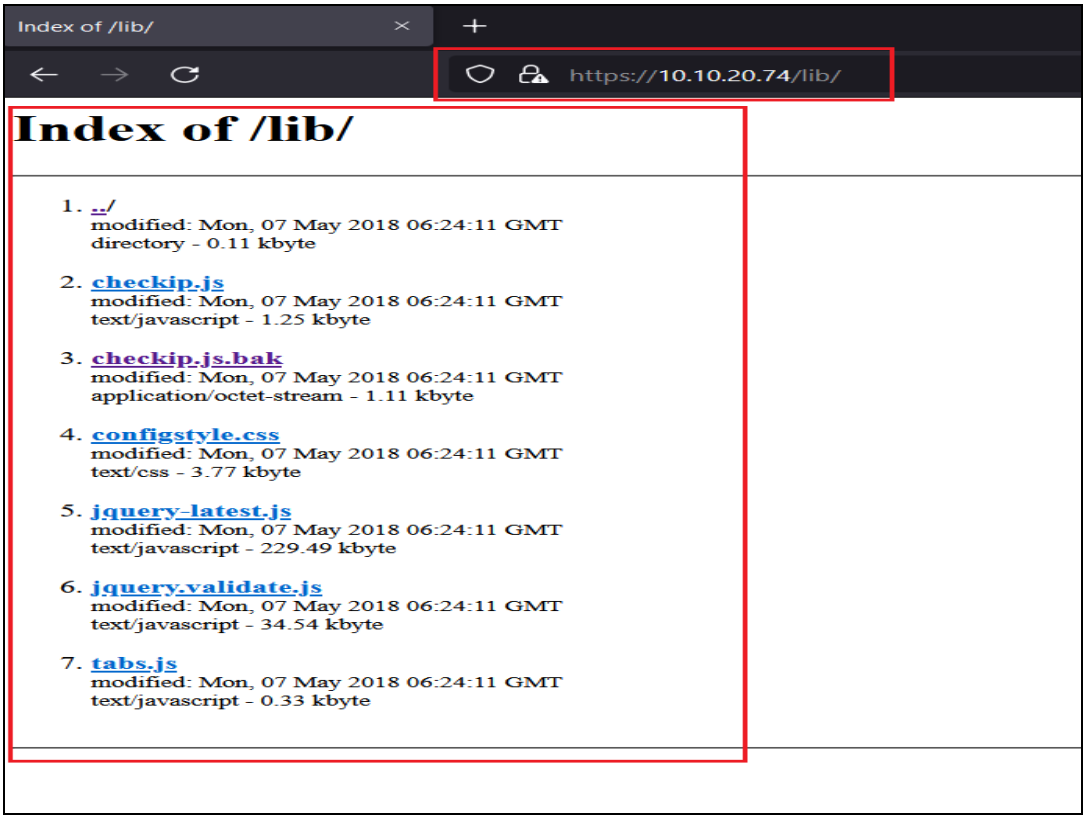
CWE-ID	CWE Name
CWE-22	Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)

Steps to Reproduce

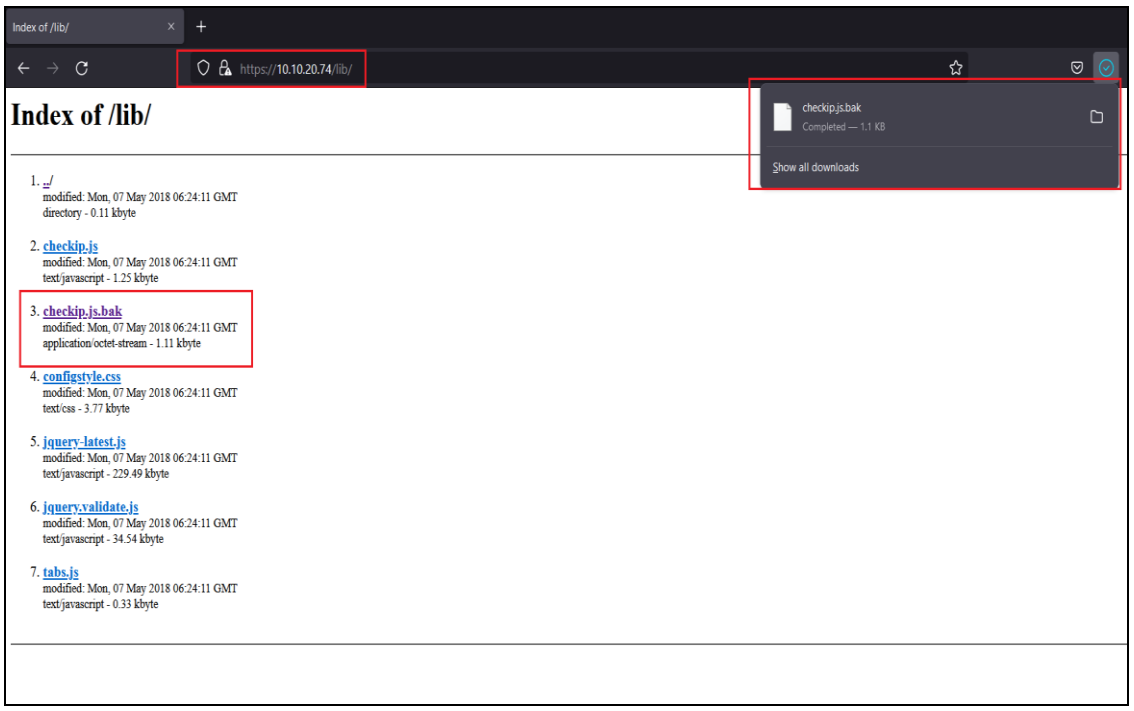
1. Perform directory enumeration using directory bruteforce tool.



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.