


Path Traversal Report- 16.8.2 - 16

Tester's Name: Stanley Ford

Lab No. 16.8.2 Path Traversal

- General information:
 - Testing period: 07.02.2023
 - Test object: <http://51.250.73.193:8086/>
- Instructions: The first step, looking at the code of the page, only gave me the information that the Google Maps API is being used. It might come in handy.

Next, there is a form for feedback at the bottom. I tried to enter something there, it gave an error in HTML

 **Leave A Message.**

Name

Email

Message


<!doctype html> <html lang=en> <title>405 Method Not Allowed</title> <h1>Method Not Allowed</h1> <p>The method is not allowed for the requested URL</p>

SEND MESSAGE

:In general, there are no more complaints. The site is raw, that's normal. The next step was to go to the LEARN MORE section, after which I was redirected to another page with

[this URL:http://51.250.73.193:8086/files/](http://51.250.73.193:8086/files/)

The word "files" appealed to me. I wonder why he was left so openly. After that, I clicked on one of the links and the URL was converted to this:

 Not secure | 51.250.73.193:8086/files/?dir=informationSecurity

What if I try to put something of my own in there? For example, the name of some admin folder or other place where I, as a simple user, should not be? I'll walk through the server folders with the help of "steps back" .. /: Just two steps back and I've found the right flag:

This page in progress, but you can download some materials about [../..](#).

```
bin
dev
etc
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
.dockerenv
app
flag{D1r3ct0ry_is_d@ng3r0us}
```

Lab Done!

Self-Assessment Questions:

- List the tools (programs and utilities) that you used to solve this lab: Web browser (Google Chrome)
- List the vulnerabilities you discovered:
Path Traversal
- Give advice on how to improve security: Store site assets on a separate central database, rather than directly in the file system of a web server. It also doesn't hurt to update the software you're using. This is generally work advice in most cases.