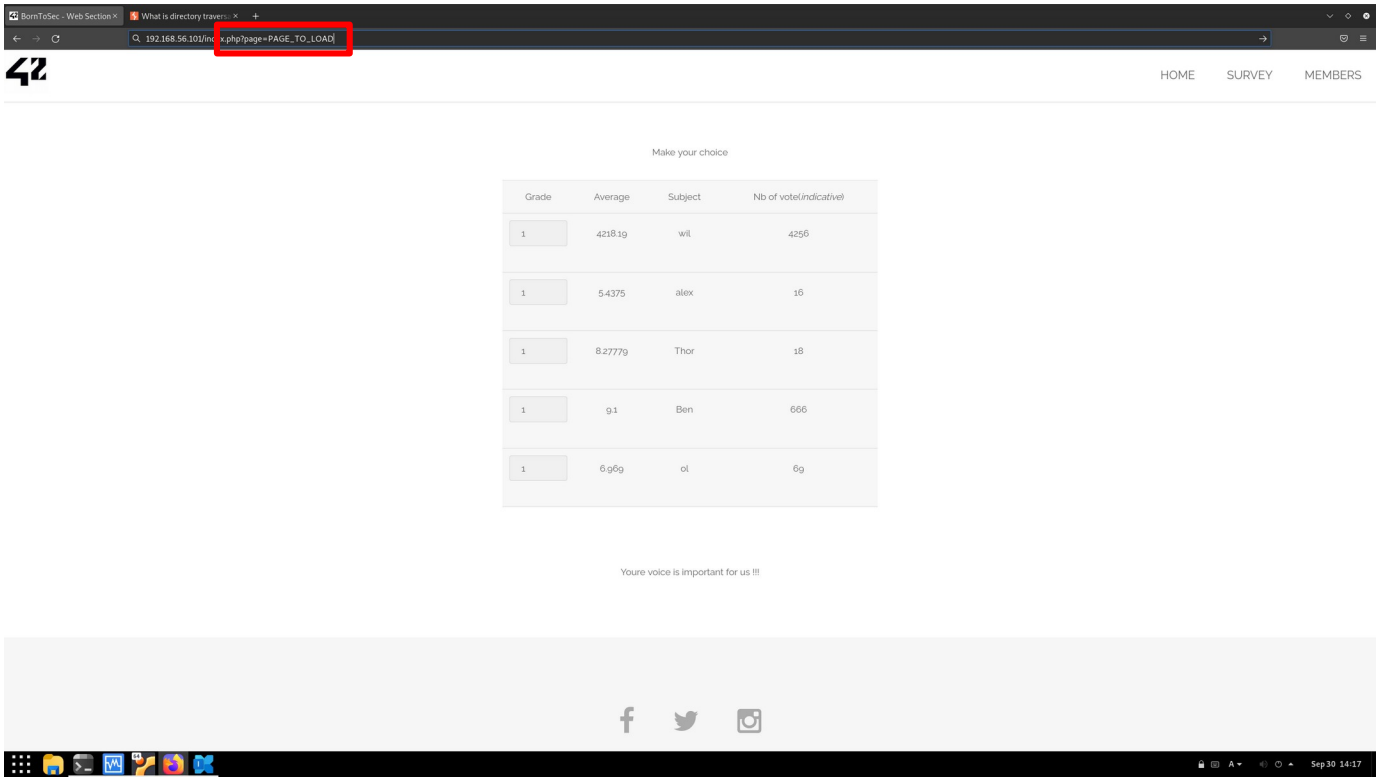
Directory traversal

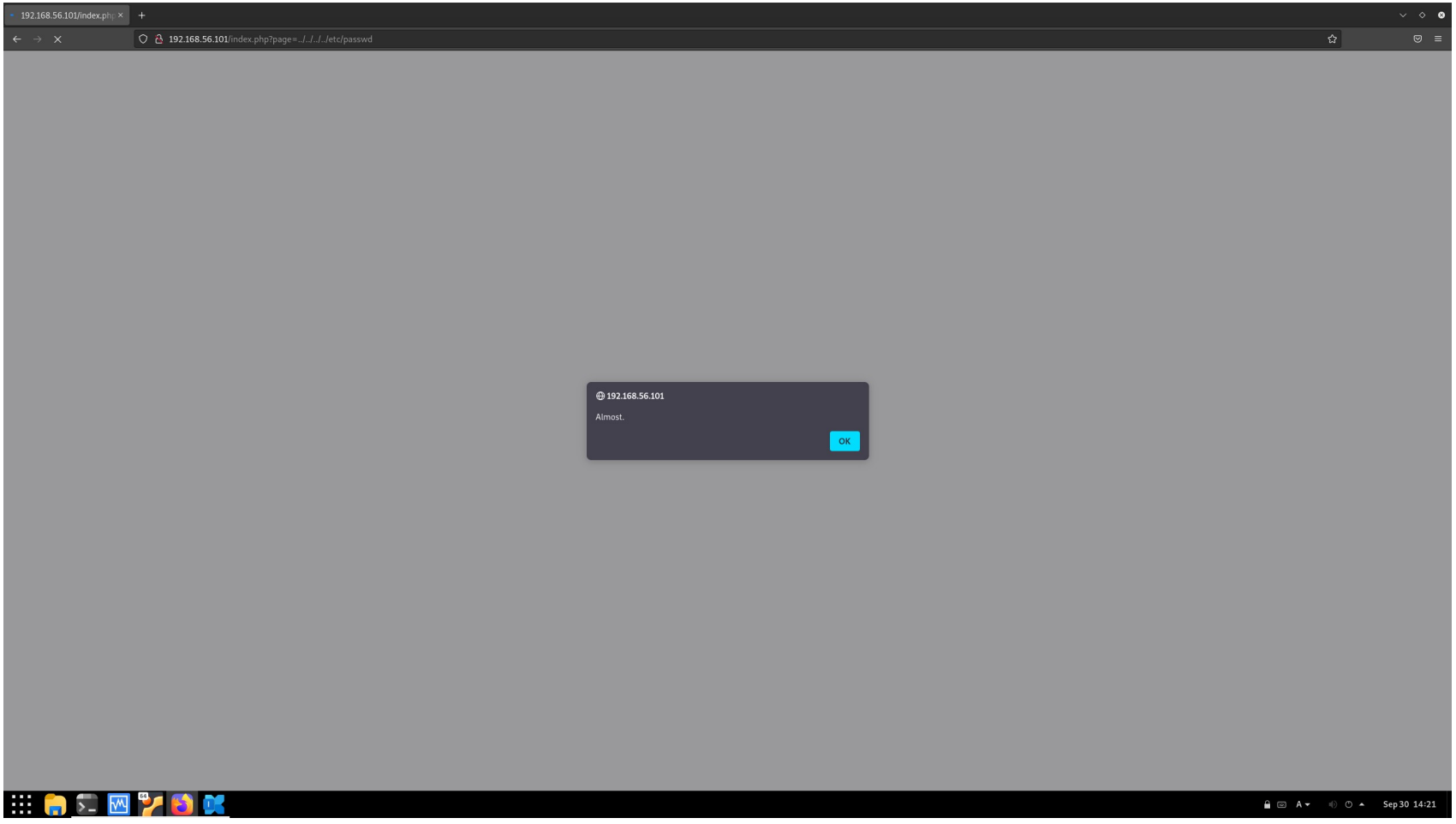
Directory traversal (also known as file path traversal) is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application. This might include application code and data, credentials for back-end systems, and sensitive operating system files. In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server.

Walk through

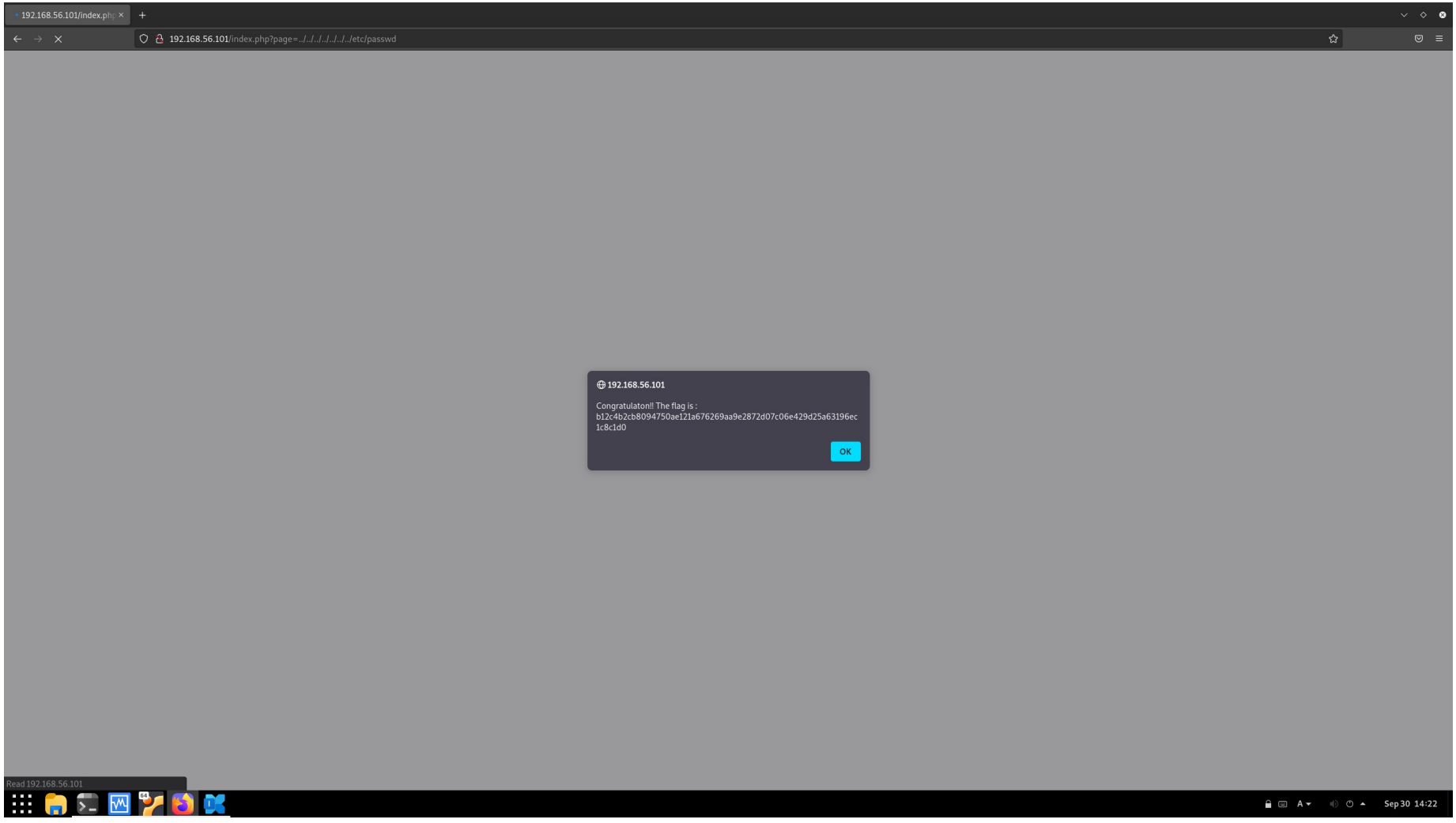
Step 1 : We saw an argument ?page=x in the URL typical entry point to directory traversal flaw



Step 2 : Change the path to back up to the root of the webserv and try to read a sensible file like passwd or shadow



Step 4 : Get the flag !



How to fix

- The backend should validate the user input
- Have a whitelist of valid inputs
- Chroot the accessible path