

## Description of the Path Traversal Vulnerability

Vulnerability found on the web server: Path Traversal

Tool used to execute the vulnerability: Burp Suite

### Description:

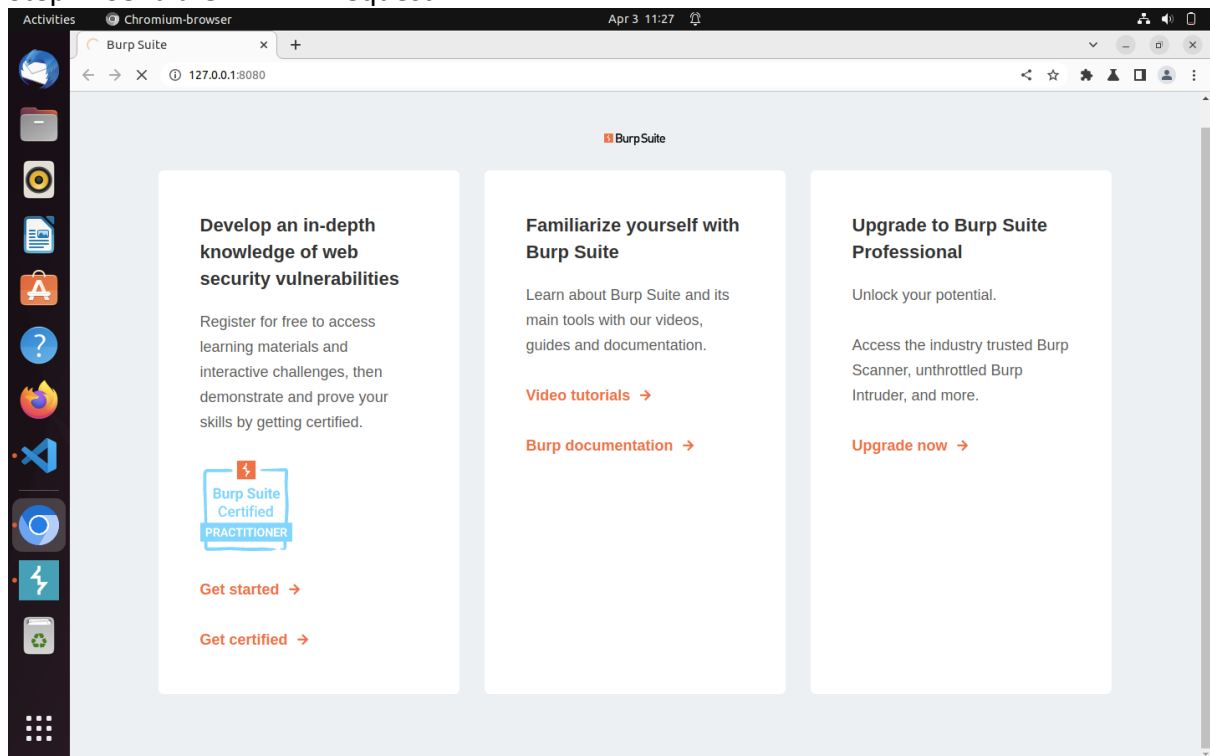
This attack works on web servers with little to none access control set in place and no input validation of the URI Path in the HTTP request. It works by chaining relative directory paths to its parent directories using this pattern `"../..../..../..../"`. This allows the attacker to navigate and access files outside the directory of the web application which compromises the security of the application.

Steps to reproduce the attack:

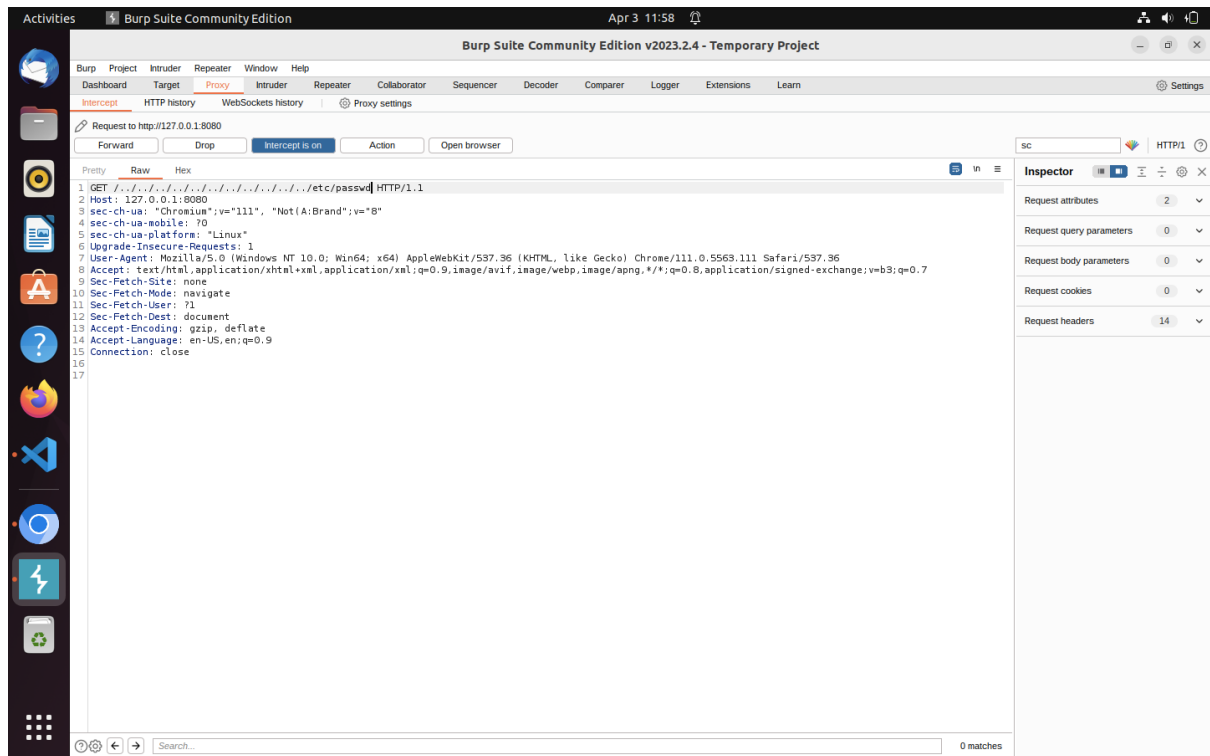
### Prerequisite:

Burp suite must be running at this time and either the built-in browser or the proxy must be used to execute this attack since the HTTP request must be intercepted.

Step 1: Send a GET HTTP request.



Step 2: Intercept the HTTP request in burpsuite and modify the URI path in this pattern `"../..../..../<dir>/<file>"`. In this case, it is requesting the passwd file from the etc directory in Linux.



Step 3: Obtain the content of the file from the HTTP response.

