Directory Traversal Attacks

Directory traversal or Path traversal attack is web security vulnerability, using this this vulnerability an attacker can read arbitrary files on the server that is running an application.

Attacker can get the application code and data, sensitive information like credentials for back-end systems, and sensitive operating system files.

There are the cases where in an attacker was able to write in files on the server. Attacker was able to modify application data and he was able to take full control of the server. That is dangerous ☹.

Here is the example of directory traversal attack, when DT vulnerability is present in the application then attacker can use [**filename=../../../etc/passwd**] in the url path to read from the following file path: **/var/www/images/../../../etc/passwd**

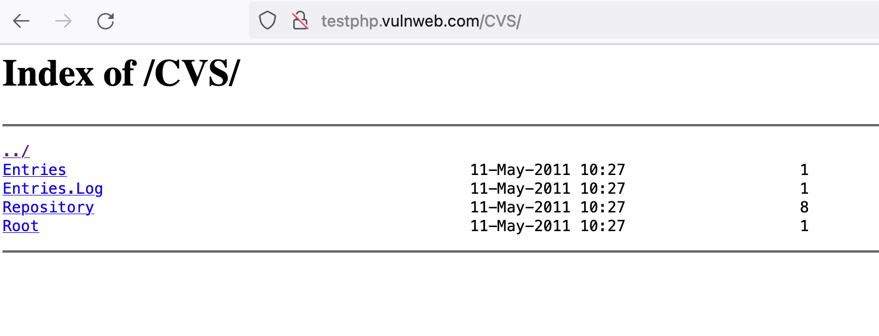
Let’s have a look into real time example:

The **testphp.vulnweb.com** is the vulnerable website provided by Acunetix

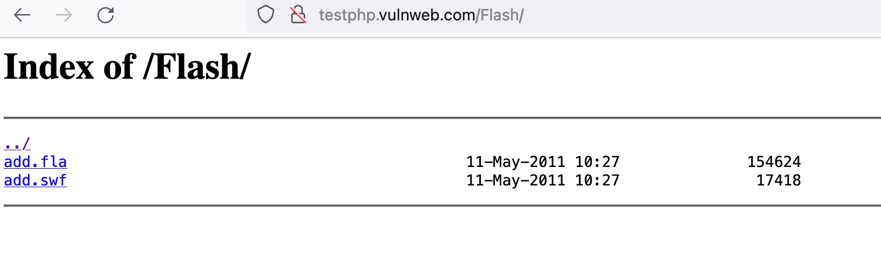
When you access below website and it path /cvs/

<http://testphp.vulnweb.com/CVS/>

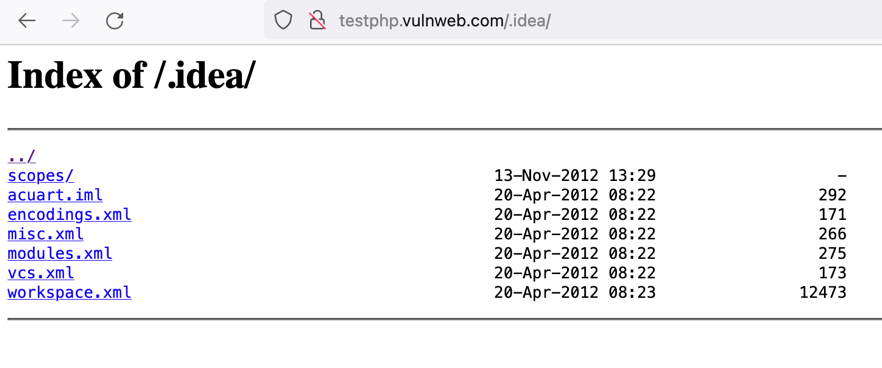
You are able to access their files which are on their server and nobody from outside should have access to these sensitive files:



Try to access another url with path /Flash/ - <http://testphp.vulnweb.com/Flash/>



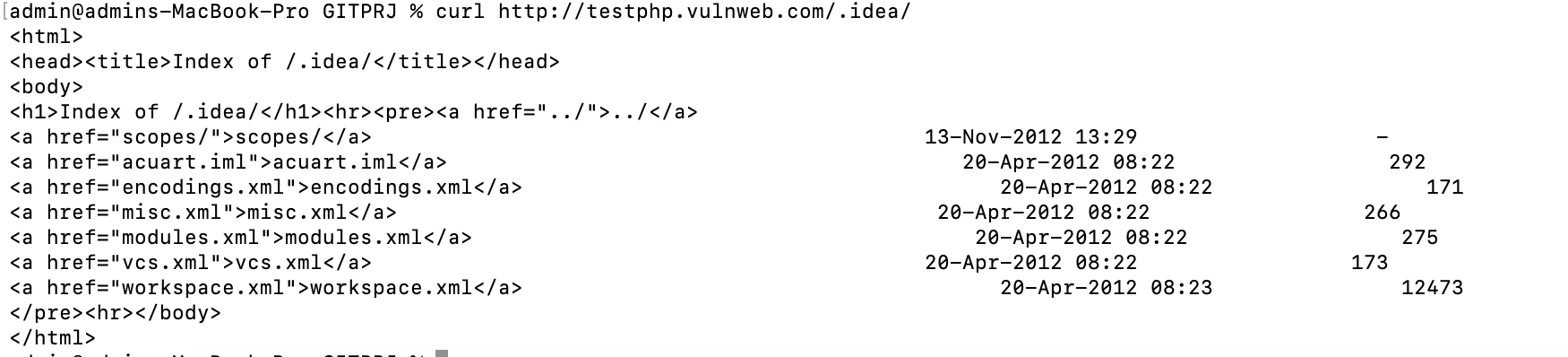
Similarly try to access <http://testphp.vulnweb.com/.idea/>



You can also use curl command to test your application for directory traversal

**curl** [**http://testphp.vulnweb.com/.idea/**](http://testphp.vulnweb.com/.idea/)

**Response:**



**How to Mitigate/Prevent:**

1. **Input Validation:** Do not trust any user input, filter any user input, remove everything but the known good data and filter meta characters from the user input. Use whitelisting of permitted values.
2. **Web Application Firewall [WAF] :** You can implement WAF to protect your environment from directory traversal attack. WAF has rules[Signatures] for directory traversal attack.

WAF will inspect the http request against directory traversal rules, if any http request has the directory traversal payload, then it will be matched and then WAF will block the request.

1. **Disabling directory listing for selected web servers:** If the attacker finds the secret folder by crawling or fuzzing, when he tries to access it directly, he can gain access to the secret files.

So directory listing can be disabled in the web server configuration file. There are different web server like tomcat, apache, IIS, NGNIX etc. basen on your webserver you can disable the directory listing in their config file.