Sc0p3 Hack3r Follow
Sep 16 · 3 min read · Listen

CVE-2022–37700 Directory Transversal in ZenTao Easy soft ALM v16.5

I am Shubham Sudhir Sawant a Security Researcher, super thrilled to write my very first blog. Medium is one of my favorite platform where I can read on Security Bug blogs. I came across so many great contents which made me write one today. It not only helps us grow our knowledge or built our skill set in a particular field but also in exploring new ideas and think out of the box.

This article gives a walk through on what directory traversal is, explains how to perform path traversal attack, and elucidate how to prevent directory traversal vulnerability.

What is Directory Traversal?

Path Traversal alias Directory Traversal, is a web related vulnerability that allows an attacker to read arbitrary files on the server running an application. (Example: application assets, backend systems credentials, and sensitive operating system files). In certain cases, an attacker can potentially tamper the arbitrary file on the server, which eventually give full control over the server running the application.

Read arbitrary file through directory traversal

The Basic Steps are given below:

1. Shoot up **Burp Professional** Suite/ **Burp Community** Edition Tool on your browser.

2. Open The Web Application which has to be intercepted in burp Intercept **proxy tab.**

3. Now before intercepting, set the proxy in web browser **network setting.**

4. Open the burp tool and enable the **proxy intercept** tab.

5. The request URL will be captured and send it to the **repeater** to launch the attack.

6. Look for an Crawled Website(performed in repeater tab)

In Crawled Website I found the below URL:-

https://demo15.zentao.pm/user-login.html/zentao/index.php?mode=getconfig

Figure 1: File Path Traversal Simple Example

{“version”:”16.5",”requestType”:”PATH_INFO”,”requestFix”:”-”,”moduleVar”:”m”,”methodVar”:”f”,”viewVar”:”t”,”sessionVar”:”zentaosid”,”systemMode”:”new”,”sprintConcept”:”0",”URAndSR”:”0",”sessionName”:”zentaosid”,”sessionID”:”vgpgn3knuc5g2jod6uptc8db42",”random”:7923,”expiredTime”:”1440",”serverTime”:1663360511,”rand”:7923}

I found it is a sensitive config file which is getting executed for which was assigned a CVE-2022–37700

How to prevent a directory traversal attack?

Although there are many ways in which the security professionals can avoid the possibility of path traversal attack some preventive measure are listed below: which includes..

1. User supplied dynamic input should be strictly validated before being passed to any filesystem operation. After validating user input, the application can use a suitable filesystem API to verify that the file to be accessed is actually located within the base directory used by the application.

2. Input containing dot-dot-slash sequences should be blocked.

3. Also, the directory used to store files that are accessed using user supplied dynamic input can be located on a separate logical volume to other sensitive application and operating system files, so that these cannot be reached via path traversal attacks.

4. If user provided data passed to input filesystem APIs is unavoidable then 2 layers of defense should be used together such as:

- 1st step : The application should validate user input before processing it. This done by comparing to the whitelist of permitted values. If this is not possible then it should be validated based of “alphanumeric characters.”

 

For example: A java code to validate the canonical path of a file based on user input:

```
File f = new File (base_Dir, user_Input);

If (f.getCanonicalPath() .startsWith(base_Dir))

{

//process file

}
```

5. The developer should avoid storing sensitive data in the web root of the application.

6. It is advisable to run the latest version of these web servers because by default it will have good directory security, if possible one can make sure that they are running the latest version (up- to-date with current patches).

References

1. https://portswigger.net/web-security/file-path-traversal

2. https://www.acunetix.com/websitesecurity/directory-traversal/

3. https://portswigger.net/daily-swig/patched-wordpress-plugin-still-susceptible-to-attacks

4. https://portswigger.net/daily-swig/vulnerability-found-in-oracle-pos-terminals

5. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/01-Testing_Directory_Traversal_File_Include