BUG BOUNTY REPORT

***AUTHORED BY*:**

AMJAD AMEEN

VAISHNAV P

MUHAMMED ALTHAF A

Table of Contents

SUMMARY TITLE (TARGET-1):

Path Traversal Vulnerability Allowing Unauthorized File Access

TARGET:

https://confituredebali.com

TECHNICAL SEVERITY :

The technical severity for this vulnerability would be classified as **P1 - Critical** under the Vulnerability Rating Taxonomy (VRT).

Reason:

- Accessing the /etc/passwd file is highly sensitive, as it contains user account details. Although this file doesn't contain passwords themselves in modern systems (those are usually in /etc/shadow), exposure of such a file can lead to system reconnaissance, potential privilege escalation, or other attacks.
- This level of access can significantly compromise the server's security, making it a **Critical** issue.

URL/LOCATIOIN OF THE VULNERABILITY:

URL: https://confituredebali.com/index.php?page=shop.php

VULNERABILITY DETAILS:

Overview

A path traversal vulnerability was identified on https://confituredebali.com, specifically in the page parameter of the index.php page. By manipulating the

parameter, an attacker can traverse directories and access sensitive files on the server, such as /etc/passwd. This vulnerability arises from improper validation or sanitization of user-supplied input, allowing unauthorized access to files outside the intended directory scope.

Walkthrough and POC (Proof of Concept)

To reproduce the issue:

1. Navigate to the following URL: https://confituredebali.com/index.php?page=shop.php
2. Modify the page parameter by injecting directory traversal sequences. For example, change the page parameter to ../../../../etc/passwd.
3. Submit the modified request:

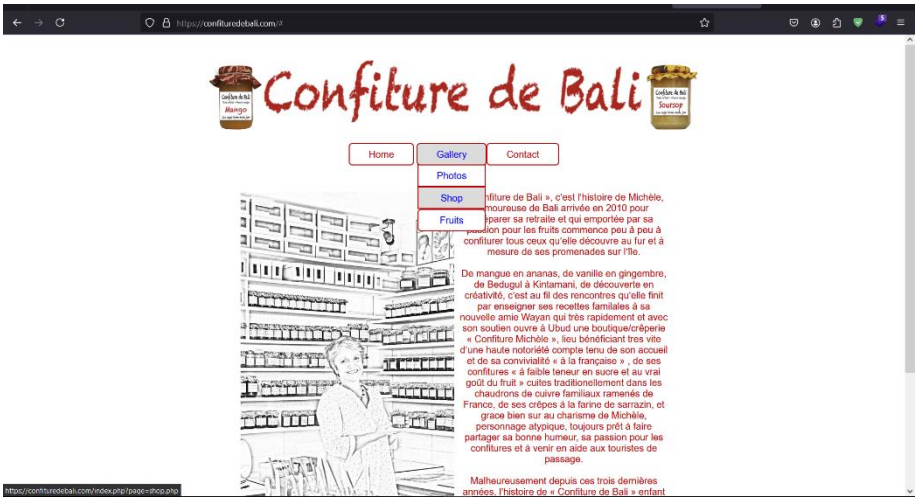
   ://confituredebali.com/index.php?page=../../../../etc/passwd
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

   This demonstrates that the application is not properly validating the input, allowing an attacker to navigate the server's file system and retrieve sensitive files.

Vulnerability Evidence:

The following evidence shows the vulnerability in action:

- A screenshot of the HTTP request sent with the page=../../../../etc/passwd payload.
- A screenshot of the server’s response containing the /etc/passwd file.



Screenshot: 1

Screenshot: 2

Screenshot: 3

Demonstrated Impact:

This vulnerability has a **Critical** impact because it allows an attacker to access sensitive files on the server, such as /etc/passwd. While this file does not contain passwords in most modern systems, it reveals information about user accounts, which can be leveraged for further attacks, such as privilege escalation or reconnaissance for additional vulnerabilities. If attackers can access other critical files (e.g., configuration files or logs), the impact could be further exacerbated, potentially leading to a complete compromise of the system

SUMMARY TTTLE- (TARGET-2):

Path Traversal Vulnerability Allowing Unauthorized File Access

TARGET:

http://testphp.vulnweb.com

TECHNICAL SEVERITY :

The technical severity for this vulnerability would be classified as **P1 - Critical** under the Vulnerability Rating Taxonomy (VRT).

Reason:

- Accessing the /etc/passwd file is highly sensitive, as it contains user account details. Although this file doesn't contain passwords themselves in modern systems (those are usually in /etc/shadow), exposure of such a file can lead to system reconnaissance, potential privilege escalation, or other attacks.
- This level of access can significantly compromise the server's security, making it a **Critical** issue.

URL/LOCATIOIN OF THE VULNERABILITY:

URL: //testphp.vulnweb.com/showimage.php?filename=./pictures1.jpg

VULNERABILITY DETAILS:

Overview

A path traversal vulnerability was identified on http://testphp.vulnweb.com in the filename parameter of the showimage.php page. By manipulating the filename parameter, an attacker can traverse directories and access sensitive files on the server, such as /etc/passwd. This vulnerability is due to improper input validation, allowing unauthorized access to files outside the intended directory.

Walkthrough and POC (Proof of Concept)

To reproduce the issue:

1. Navigate to the following URL: http://testphp.vulnweb.com/showimage.php?filename=./pictures1.jpg
2. Modify the filename parameter to traverse directories and attempt to access the /etc/passwd file by using the following payload:

   http://testphp.vulnweb.com/showimage.php?filename=../../etc/passwd
3. Submit the modified request via Burp Suite or a web browser.
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

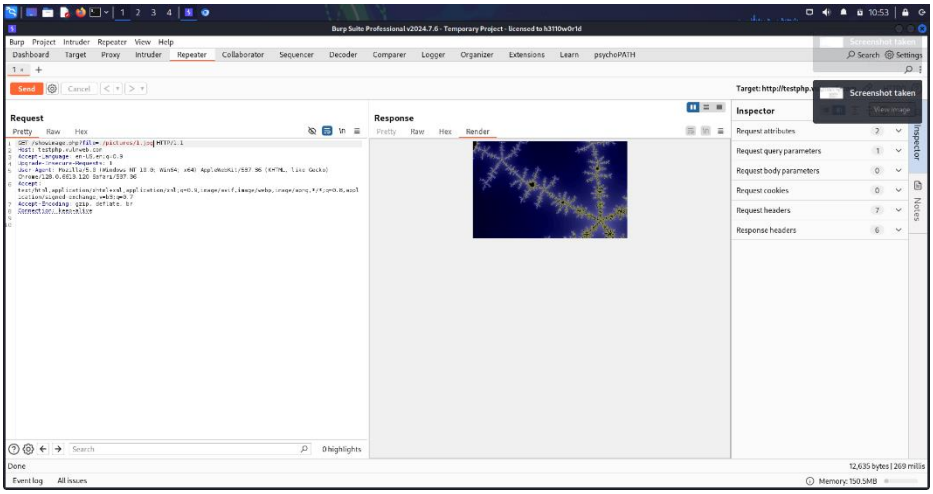
This demonstrates that the application does not properly sanitize user input in the filename parameter, allowing an attacker to access files on the server's filesystem.

Vulnerability Evidence

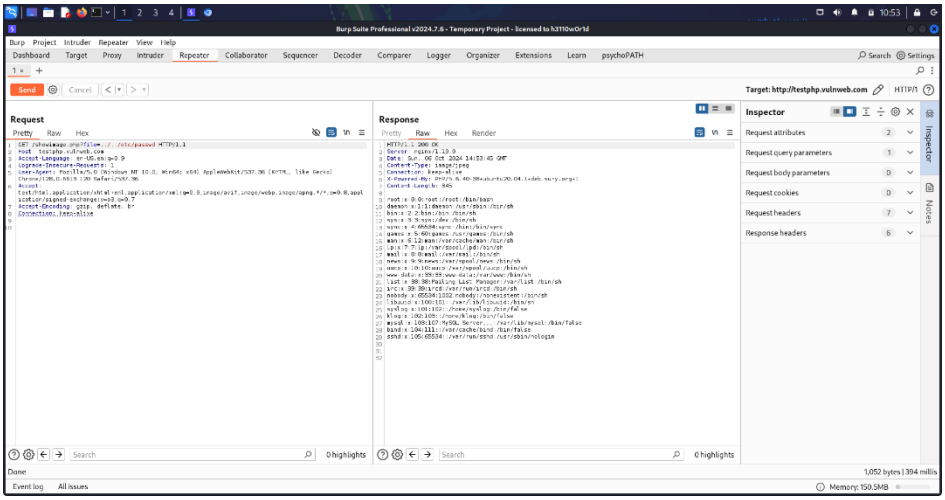
Provide evidence to support the vulnerability:

- A screenshot of the HTTP request sent with the filename=../../etc/passwd payload in Burp Suite.

- A screenshot of the server's response showing the contents of the /etc/passwd file.



Screenshot 1:



Screenshot 2:

Demonstrated Impact

This vulnerability allows attackers to access sensitive files on the server, such as /etc/passwd. Exposing this file can provide valuable information about user accounts, which may lead to further exploitation attempts such as privilege escalation. The vulnerability presents a significant risk to the security and confidentiality of the system, especially if additional sensitive files are accessible.

SUMMARY TITLE (TARGET-3):

Path Traversal Vulnerability Allowing Unauthorized File Access

TARGET:

http://otc-jbg.com

TECHNICAL SEVERITY :

The technical severity for this vulnerability would be classified as **P1 - Critical** under the Vulnerability Rating Taxonomy (VRT).

Reason:

- Accessing the /etc/passwd file is highly sensitive, as it contains user account details. Although this file doesn't contain passwords themselves in modern systems (those are usually in /etc/shadow), exposure of such a file can lead to system reconnaissance, potential privilege escalation, or other attacks.
- This level of access can significantly compromise the server's security, making it a **Critical** issue.

URL/LOCATIOIN OF THE VULNERABILITY:

URL: http://otc-jbg.com/index.php?page=society.html

VULNERABILITY DETAILS:

Overview

A path traversal vulnerability was discovered on http://otc-jbg.com in the page parameter of the index.php page. By manipulating this parameter, an attacker can traverse directories and access sensitive files on the server, such as /etc/passwd. This vulnerability is caused by inadequate validation of user input, allowing unauthorized access to files outside the intended directory.

Walkthrough and POC (Proof of Concept)

To reproduce the issue:

1. Navigate to the following URL: http://otc-jbg.com/index.php?page=society.html
2. Modify the page parameter to attempt to access the /etc/passwd file directly:

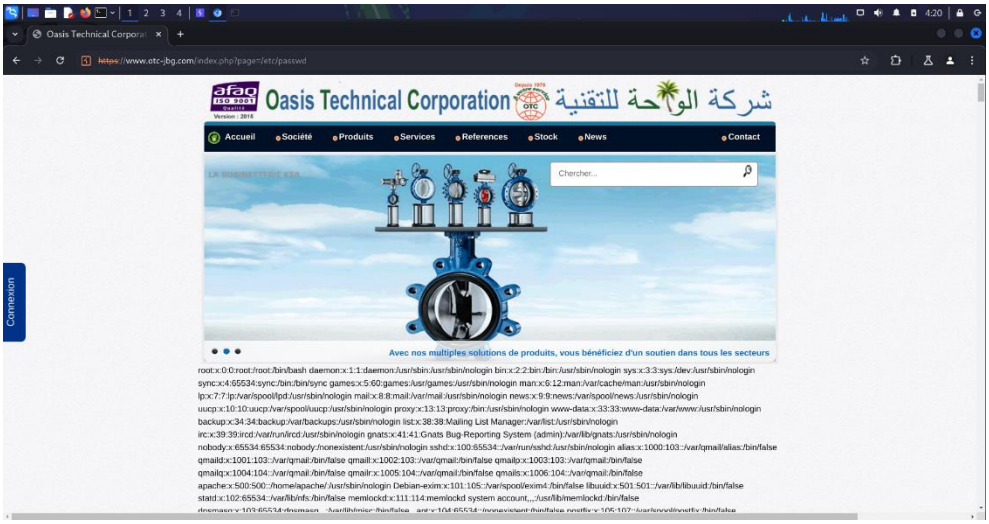
   http://otc-jbg.com/index.php?page=etc/passwd
3. Submit the modified request
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

Vulnerability Evidence

Provide evidence to substantiate the vulnerability:

- A screenshot of the HTTP request sent with the page=etc/passwd payload.
- A screenshot of the server's response containing the contents of the /etc/passwd file.

Screenshot: 1



Screenshot: 2

Demonstrated Impact

This vulnerability poses a **Critical** risk, as it allows attackers to access sensitive files on the server, such as /etc/passwd, which contains information about user accounts. Access to this file can lead to further attacks, including user enumeration and potential privilege escalation. If other sensitive files are similarly accessible, the impact could be even greater, jeopardizing the security of the entire system.

SUMMARY TITLE (TARGET-4):

Path Traversal Vulnerability Allowing Unauthorized File Access

TARGET:

http://sksc.somaiya.edu/en

TECHNICAL SEVERITY :

The technical severity for this vulnerability would be classified as **P1 - Critical** under the Vulnerability Rating Taxonomy (VRT).

Reason:

- Accessing the /etc/passwd file is highly sensitive, as it contains user account details. Although this file doesn't contain passwords themselves in modern systems (those are usually in /etc/shadow), exposure of such a file can lead to system reconnaissance, potential privilege escalation, or other attacks.
- This level of access can significantly compromise the server's security, making it a **Critical** issue.
- **URL/LOCATIOIN OF THE VULNERABILITY:**
- **URL:**http://sksc.somaiya.edu/download.php?pdf_path=xxxxxx.26020.pdf

VULNERABILITY DETAILS:

Overview

A path traversal vulnerability was identified on http://skc.soumiya.edu.in in the pdf_path parameter of the /download/php endpoint. This vulnerability allows an attacker to manipulate the pdf_path parameter to traverse directories and access sensitive files on the server, such as /etc/passwd. The lack of proper input validation enables unauthorized file access, posing a significant security risk.

Walkthrough and POC (Proof of Concept)

To reproduce the issue:

1. Navigate to the following URL: http://skc.soumiya.edu.in/download/php?pdf_path=(xxxxxxxxx_260820.pdf)
2. Modify the pdf_path parameter to access the /etc/passwd file by using the following payload:

   http://skc.soumiya.edu.in/download/php?pdf_path=///etc/passwd
3. Submit the modified request.
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

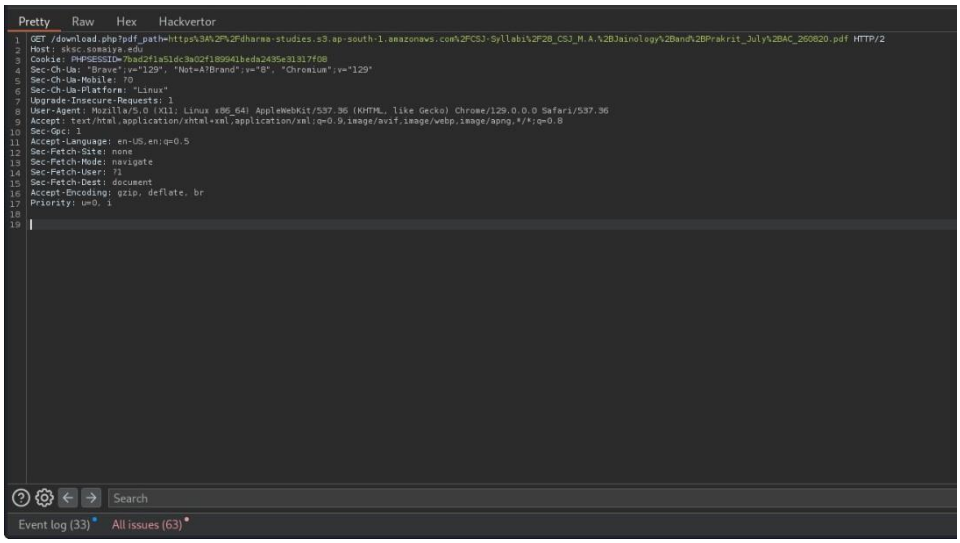
This demonstrates that the application does not adequately validate the pdf_path parameter, allowing directory traversal to sensitive files.

Vulnerability Evidence

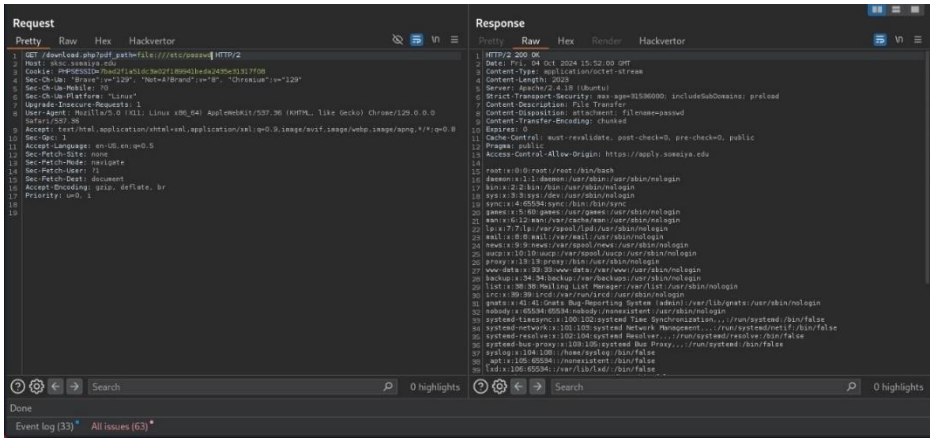
Provide evidence to support the vulnerability:

- A screenshot of the HTTP request sent with the pdf_path=///etc/passwd payload.

- A screenshot of the server's response showing the contents of the /etc/passwd file



Screenshot: 1



Screenshot: 2

Demonstrated Impact

This vulnerability has a **Critical** impact as it allows unauthorized access to sensitive files like /etc/passwd. This file contains important information about user accounts, which could be exploited by an attacker to carry out further attacks, such as user enumeration or privilege escalation. The risk is heightened if additional sensitive files are accessible through similar methods, potentially compromising the entire system.

SUMMARY TITLE (TARGET-5):

Path Traversal Vulnerability Allowing Unauthorized File Access

TARGET:

http://ravagedband.com

TECHNICAL SEVERITY :

The technical severity for this vulnerability would be classified as **P1 - Critical** under the Vulnerability Rating Taxonomy (VRT).

Reason:

- Accessing the /etc/passwd file is highly sensitive, as it contains user account details. Although this file doesn't contain passwords themselves in modern systems (those are usually in /etc/shadow), exposure of such a file can lead to system reconnaissance, potential privilege escalation, or other attacks.
- This level of access can significantly compromise the server's security, making it a **Critical** issue.

URL/LOCATIOIN OF THE VULNERABILITY:

URL: http://ravagedband.com/index.php?page=title

VULNERABILITY DETAILS:

Overview

A path traversal vulnerability was identified on http://ravagedband.com in the page parameter of the index.php file. This vulnerability allows an attacker to manipulate the page parameter to access sensitive files on the server, such as /etc/passwd. The issue stems from inadequate input validation, permitting unauthorized access to files outside the intended directory.

Walkthrough and POC (Proof of Concept)

To reproduce the issue:

1. Navigate to the following URL: http://ravagedband.com/index.php?page=title
2. Modify the page parameter to directly access the /etc/passwd file using the following payload:

   http://ravagedband.com/index.php?page=/etc/passwd
3. Submit the modified request.
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

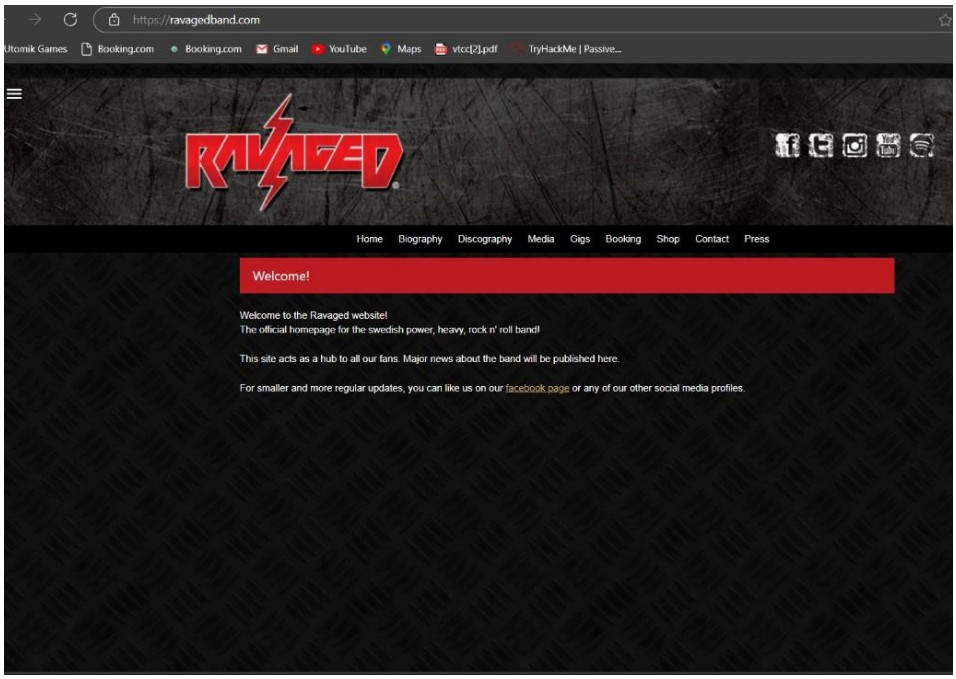
This demonstrates that the application does not properly validate the page parameter, allowing direct access to sensitive files on the server.

Vulnerability Evidence

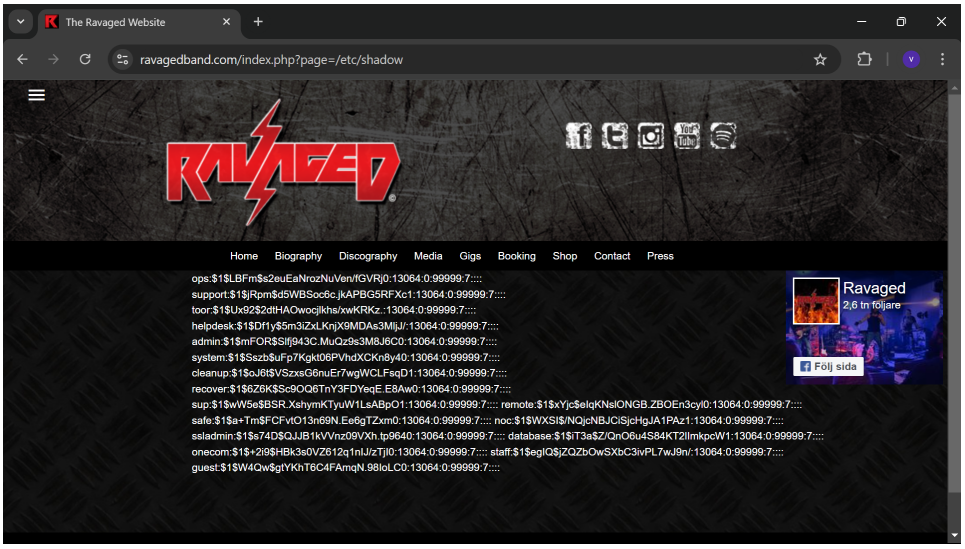
Provide evidence to support the vulnerability:

- A screenshot of the HTTP request sent with the page=/etc/passwd payload.

- A screenshot of the server's response showing the contents of the /etc/passwd file.



Screenshot 1:



Screenshot 2:

Demonstrated Impact

This vulnerability poses a Critical risk, as it allows unauthorized access to sensitive files like /etc/passwd, which contains user account information. Exposing this file can lead to further attacks, such as user enumeration or privilege escalation. If other sensitive files are similarly accessible, the impact could be significantly increased, compromising the overall security of the system.
