Breadcrumbs

Synopsis

Laboratory is an easy difficulty Linux machine that features a GitLab web application in a docker. This application is found to suffer from an arbitrary read file vulnerability, which is leveraged along with a remote command execution to gain a foothold on a docker instance. By giving administration permissions to our GitLab user it is possible to steal private ssh-keys and get a foothold on the box. Post-exploitation enumeration reveals that the system Laboratory has an executable program set as setuid. This is leveraged to gain a root shell on the server.

Skills

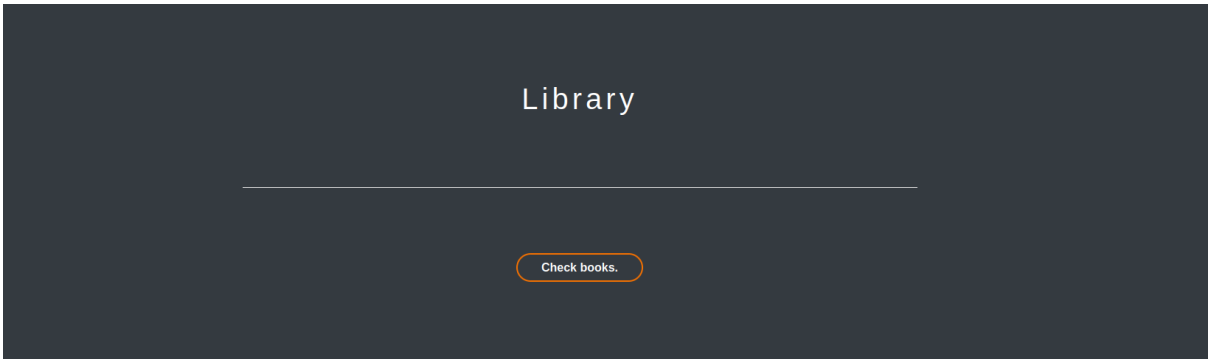
- Enumeration
- Scripting
- Code review
- Forging PHP session
- SQL injection

Exploitation

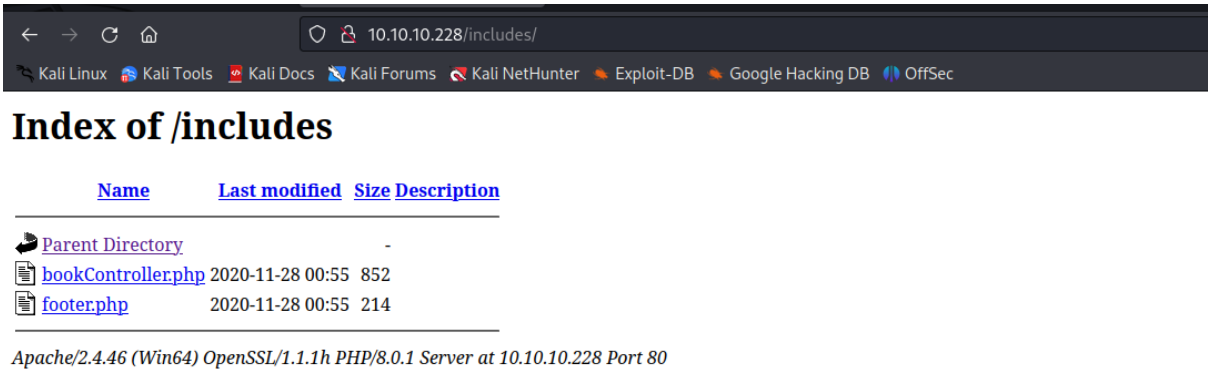
As always we start with the nmap to check what services/ports are open

```
└─# nmap -A 10.10.10.228
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 23:27 EDT
Nmap scan report for localhost (10.10.10.228)
Host is up (0.034s latency).
Not shown: 993 closed tcp ports (reset)
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-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Library
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)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| tls-alpn:
|_  http/1.1
| 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
|_ssl-date: TLS randomness does not represent time
|_http-title: Library
445/tcp  open  microsoft-ds?
3306/tcp open  mysql?
```

We see quite a few ports open,
Opening the browser gave us the books searching page

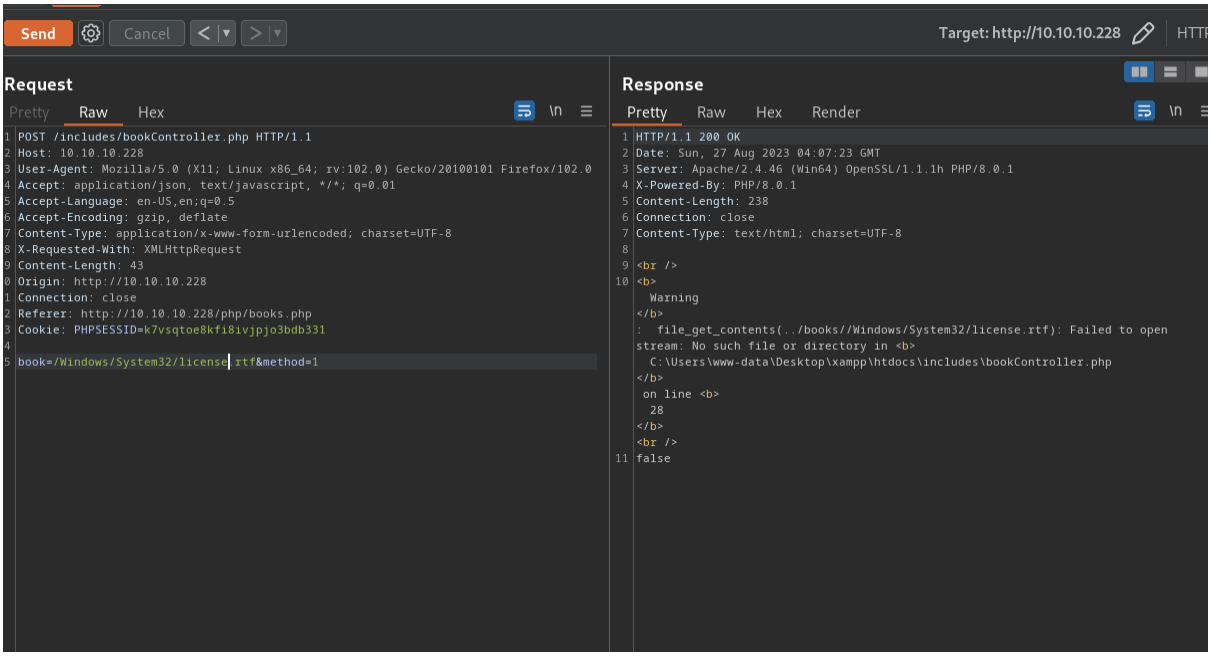


Aftera bit of enumeration we discovered that it’s possible for us to access web root directory where php files are stored

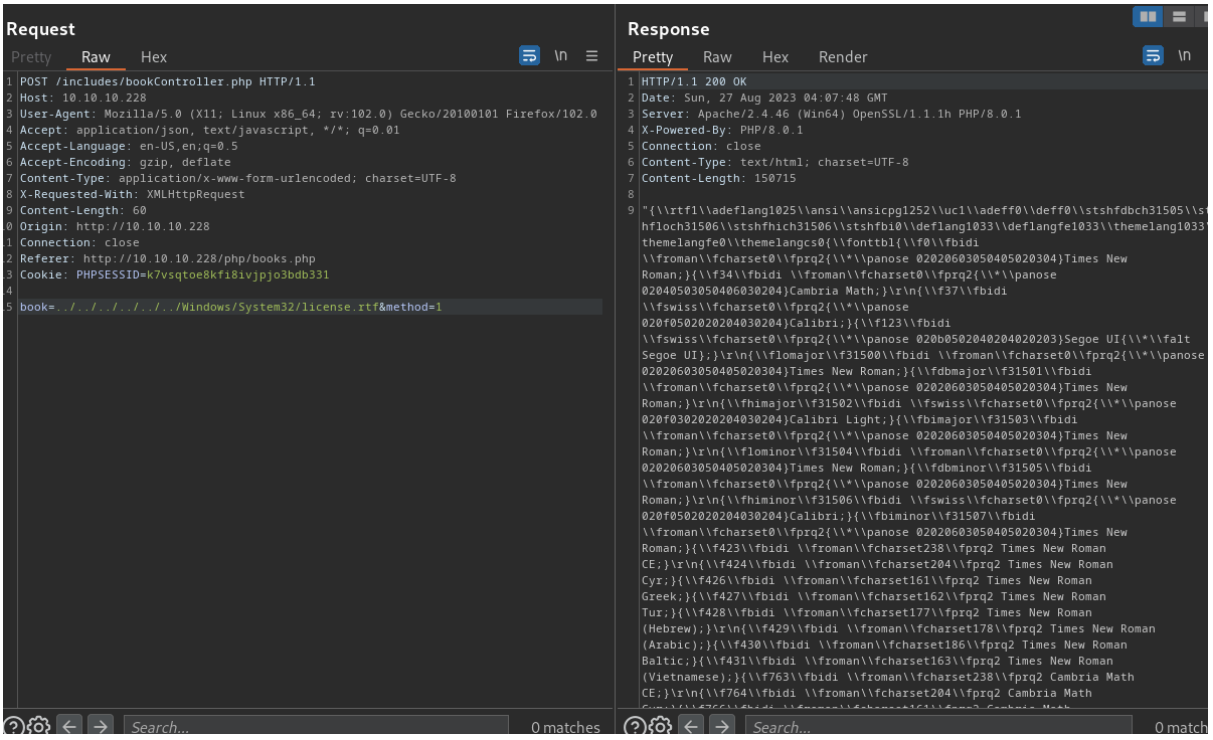


yet , except this information disclosure there was nothing else we could do, so we moved on

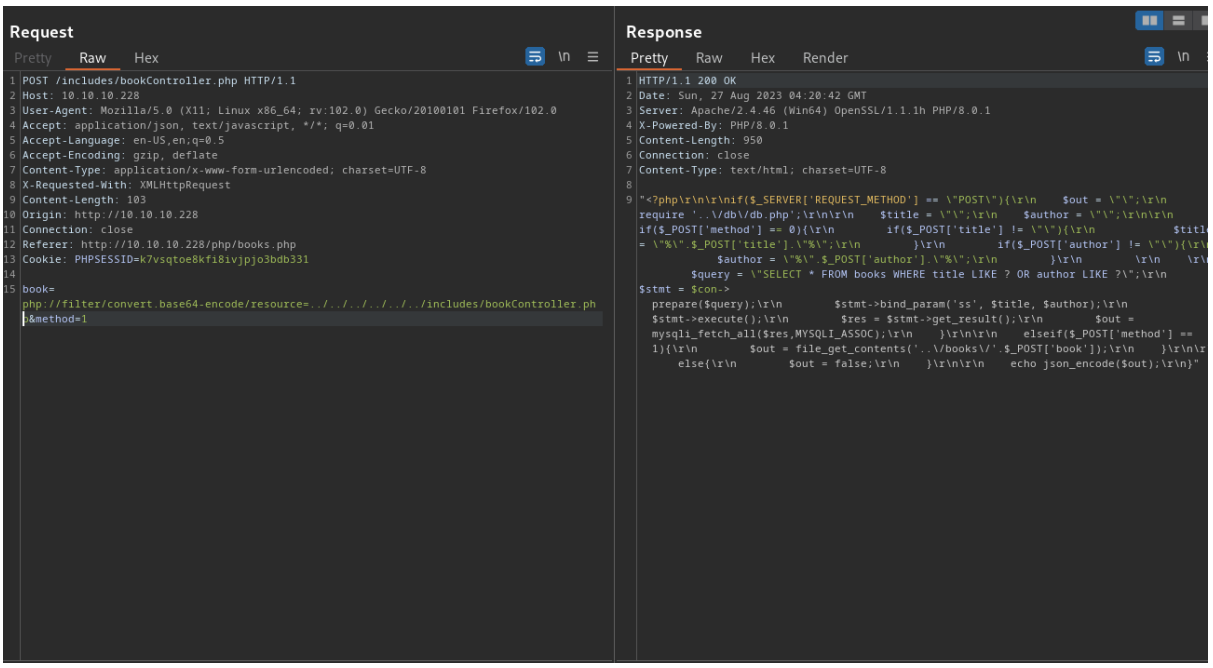
We captured the request via BurpSuit and started tampering with parameters values, we got a few error messages, what indicates that the page may be vulnerable to local file inclusion



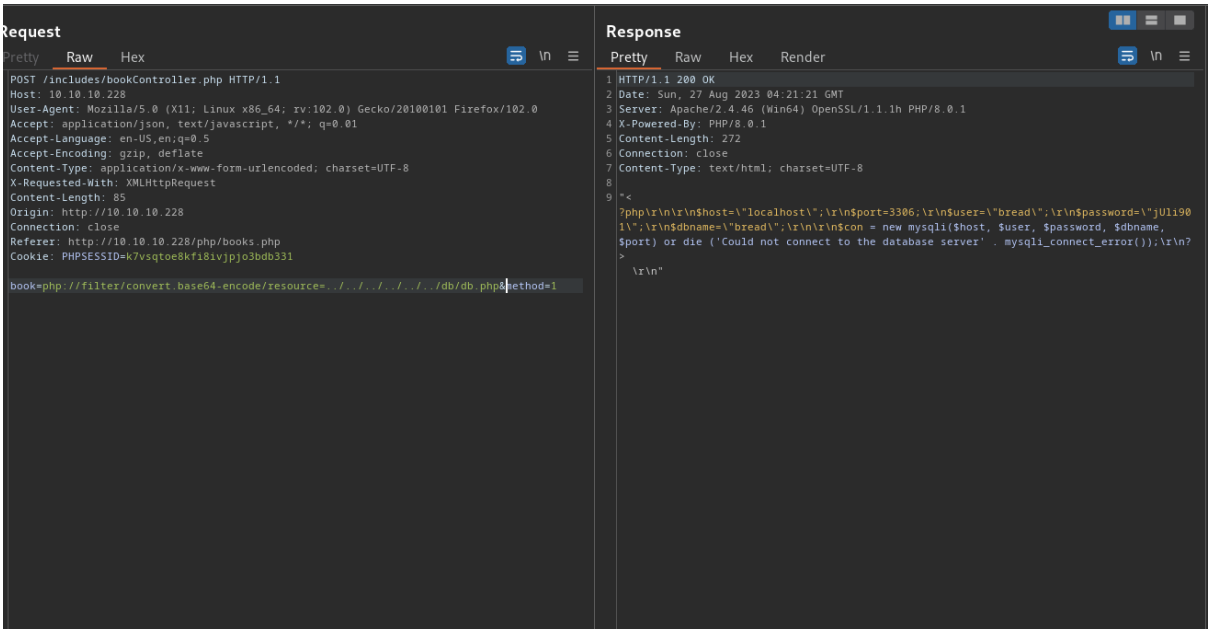
After a few more trials we confirmed LFI vulnerability that allowed us to read system files

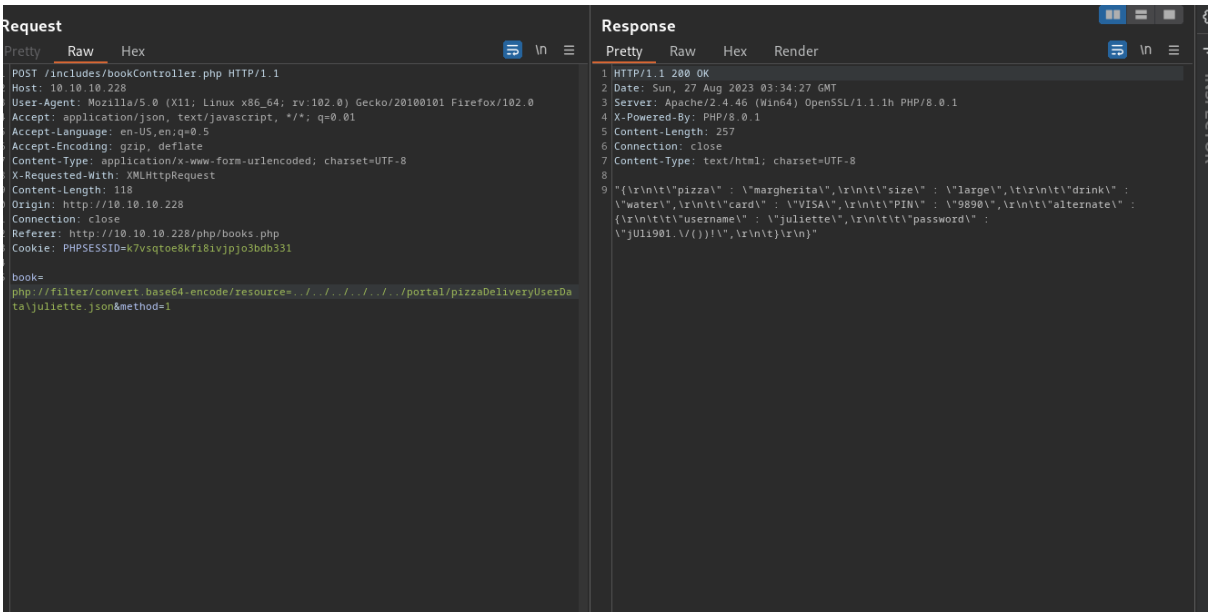


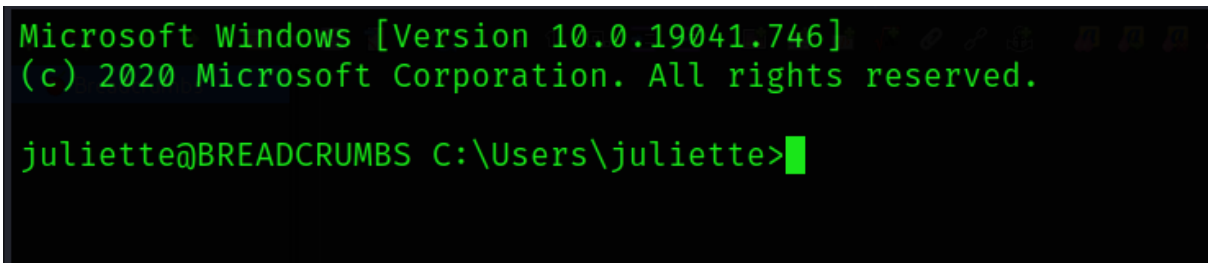
Reading system files also provided us with the database credentials



And user credentials that were used to SSH to the target machine







And we got a low privilege shell
We started our enumeration process from accessing the sqlite database associated with sticky notes

```
 Directory of C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState

01/15/2021  05:10 PM    <DIR>          .
01/15/2021  05:10 PM    <DIR>          ..
01/15/2021  05:10 PM            20,480 15cbbc93e90a4d56bf8d9a29305b8981.storage.session
11/29/2020  04:10 AM             4,096 plum.sqlite
01/15/2021  05:10 PM            32,768 plum.sqlite-shm
01/15/2021  05:10 PM           329,632 plum.sqlite-wal
               4 File(s)        386,976 bytes
               2 Dir(s)   6,522,228,736 bytes free

juliette@BREADCRUMBS C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState>
```

Opening the file, gave us credentials for a another user, so we SSH as the user development

```
└─# sqlite3 plum.sqlite
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> select * from Node
   ...> ;
Parse error: no such table: Node
sqlite> select * from NOTE;
\id=48c70e58-fcf9-475a-aea4-24ce19a9f9ec juliette: jUli901./())!
\id=fc0d8d70-055d-4870-a5de-d76943a68ea2 development: fN3)sN5Ee@g
\id=48924119-7212-4b01-9e0f-ae6d678d49b2 administrator: [MOVED]|ManagedPosition=|1|0||Yellow|0||||||0c32c3d8-7c60-48ae-939e-798df198cfe7|8e814e57-9d28-4288-961c-31c806338c5b|637423162765765332||637423163995607122
sqlite>
```

```
development@BREADCRUMBS C:\Users\development>dir
 Volume in drive C has no label.
 Volume Serial Number is 7C07-CD3A

 Directory of C:\Users\development

01/26/2021  10:11 AM    <DIR>          .
01/26/2021  10:11 AM    <DIR>          ..
12/07/2019  02:14 AM    <DIR>          Desktop
01/17/2021  02:41 AM    <DIR>          Documents
12/07/2019  02:14 AM    <DIR>          Downloads
12/07/2019  02:14 AM    <DIR>          Favorites
12/07/2019  02:14 AM    <DIR>          Links
12/07/2019  02:14 AM    <DIR>          Music
12/07/2019  02:14 AM    <DIR>          Pictures
12/07/2019  02:14 AM    <DIR>          Saved Games
12/07/2019  02:14 AM    <DIR>          Videos
               0 File(s)              0 bytes
              11 Dir(s)   6,518,169,600 bytes free

development@BREADCRUMBS C:\Users\development>
```