Secure login?

You can try the most popular names and passwords, but it wouldn't work.

We can notice, that there is one extra folder in URL. So we can try if there is directory listing enabled. We are lucky because it is. You can explore all files. Two most important could be admin.conf, where we can find username and hash of his password, and login.php.

You can try to break the hash, but the password is really strong and this didn't work for me.

It could be useful to look at the login.php file to get info about the login process, but the .php file is already interpreted, so we can't see the php code. Fortunately, there is another folder called backup and there is the file login.php.bcp. Here we can analyze the login script and find the vulnerability.

We can find, that if the inserted name and password hash are the same like in the file admin.conf, the script will make this:

```
if ($flag==1)
{
        echo "<script language='javascript'>createCookie(\"p\", \"".md5($user)."\", 2);</script>";
        echo "<script language='javascript'>location.href='status_device.php'</script>";
}
```

We can try to get to status_device.php site, but we will be redirected back to login.

The most important knowledge from the login.php.bcp for us is, that if we successfully insert the credentials, the script will make the cookie with hash of **user name** only.

The final part is to send GET request

```
GET /Secure/status_device.php HTTP/1.1
Host: xxx.xxx.xxx.xxx
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: p=21232f297a57a5a743894a0e4a801fc3
Connection: close
Upgrade-Insecure-Requests: 1
```

(I used Burp Suite in Intercept mode and just add a cookie into the request to status_device site)

Now you are logged in so you can read the flag:

⇨ **TM17-UUMN-NjOP-kcQm-def6**

PS: This challenge is based on real situation – the login script was extracted from commercially offered device