Lab 20 - CTF Challenge

PHP Fairy

Source code shows that we have to bypass two if conditions to get the flag. We know the `pass` variable. it's md5 of "admin1674227342" so: $pass = "0e463854177790028825434984462555";

First condition is this:

```
(((((((((($_GET['pass'] == $pass)))) && (((($pass !== $_GET['pass'])))))) || ((((($pass == $_GET['pass']))))) && ((($_GET['pass'] !== $pass))))))))
```

Summery of above condition is this:

```
$_GET['pass'] == $pass && $pass !== $_GET['pass']
```

we know that first condition($_GET['pass'] == $pass) is using `equal operator`,

While second condition($pass !== $_GET['pass']) uses `Not Identical Operator`

We can bypass both condition by using "0" as input,

```
"0" == "0e463854177790028825434984462555"   => True

"0e463854177790028825434984462555" !== "0"  => True
```

Second condition is:

```
(strlen($pass) == strlen($_GET['pass']))
```

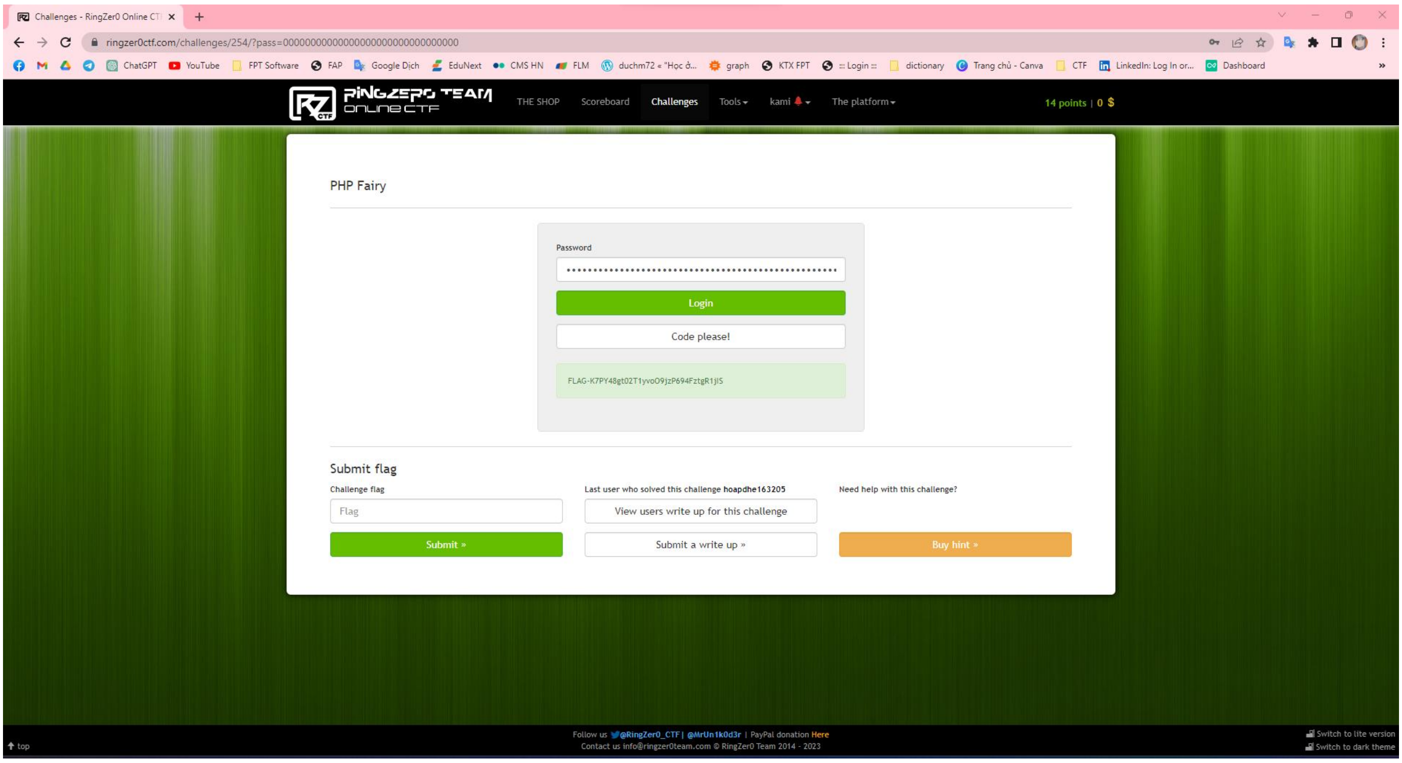
or

```
(32 == strlen($_GET['pass']))
```

So to bypass second one, we just have to use 32 zeros ("0" * 32)

Our final payload looks like this:

```
00000000000000000000000000000000
```



ringzer0ctf.com/challenges/254/?pass=000000000000000000000000000000

PHP Fairy

Password

FLAG-K7PY48gt02T1yvoO9jzP694FztgR1jlS

Submit flag

Challenge flag

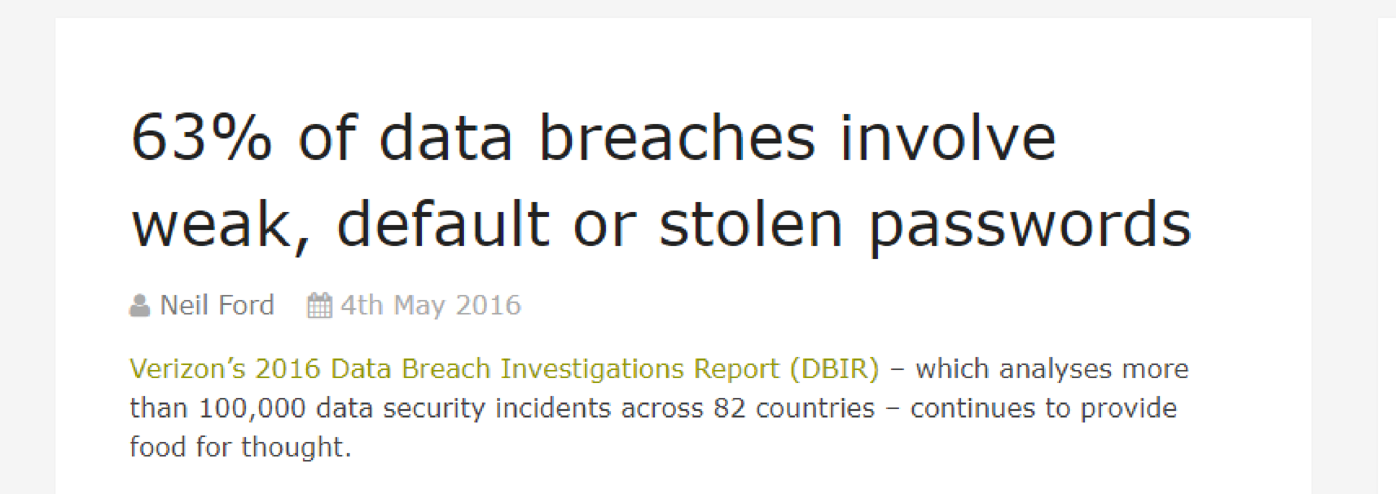
Flag

Last user who solved this challenge hoapdhe163205

Need help with this challenge?

Follow us @RingZer0_CTF | @MrUn1k0d3r | PayPal donation Here
Contact us info@ringzer0team.com © RingZer0 Team 2014 - 2023

Hacking skill are optional

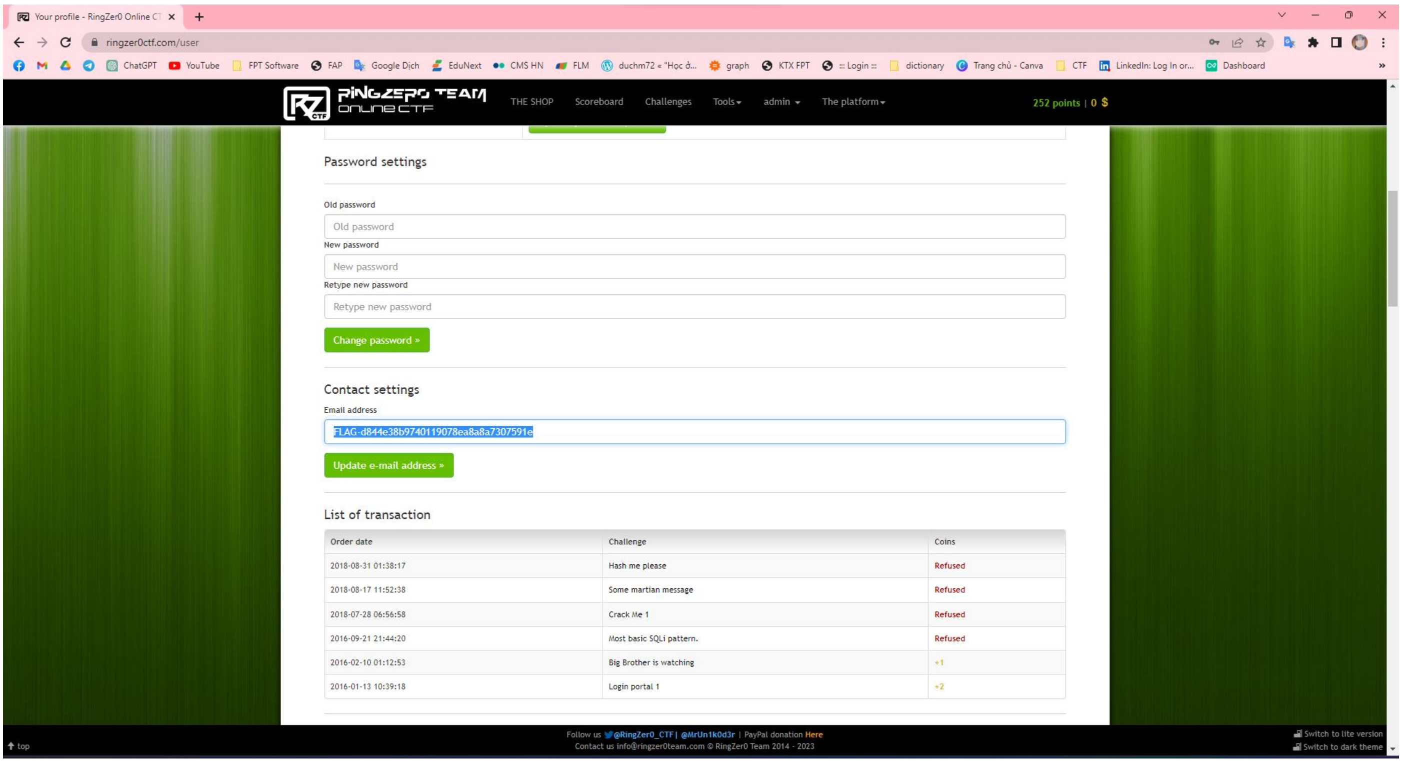


63% of data breaches involve weak, default or stolen passwords

Neil Ford 4th May 2016

Verizon's 2016 Data Breach Investigations Report (DBIR) – which analyses more than 100,000 data security incidents across 82 countries – continues to provide food for thought.

The article is about data theft with more than half due to love password, default password or stole n password but after looking through the website we don't see any place to log in then I think go to ringzer0's login page and try through default or guessable accounts and passwords and when trying admin/admin i got into admin account then i searched in admin account and found the flag in my profile this account



Password settings

Old password

Old password

New password

New password

Retype new password

Retype new password

Change password »

Contact settings

Email address

FLAG-d844e38b9740119078ea8a8a7307591e

Update e-mail address »

List of transaction

Order date	Challenge	Coins
2018-08-31 01:38:17	Hash me please	Refused
2018-08-17 11:52:38	Some martian message	Refused
2018-07-28 06:56:58	Crack Me 1	Refused
2016-09-21 21:44:20	Most basic SQLi pattern.	Refused
2016-02-10 01:12:53	Big Brother is watching	+1
2016-01-13 10:39:18	Login portal 1	+2

Follow us @RingZer0_CTF | @MrUn1k0d3r | PayPal donation Here
Contact us info@ringzer0team.com © RingZer0 Team 2014 - 2023