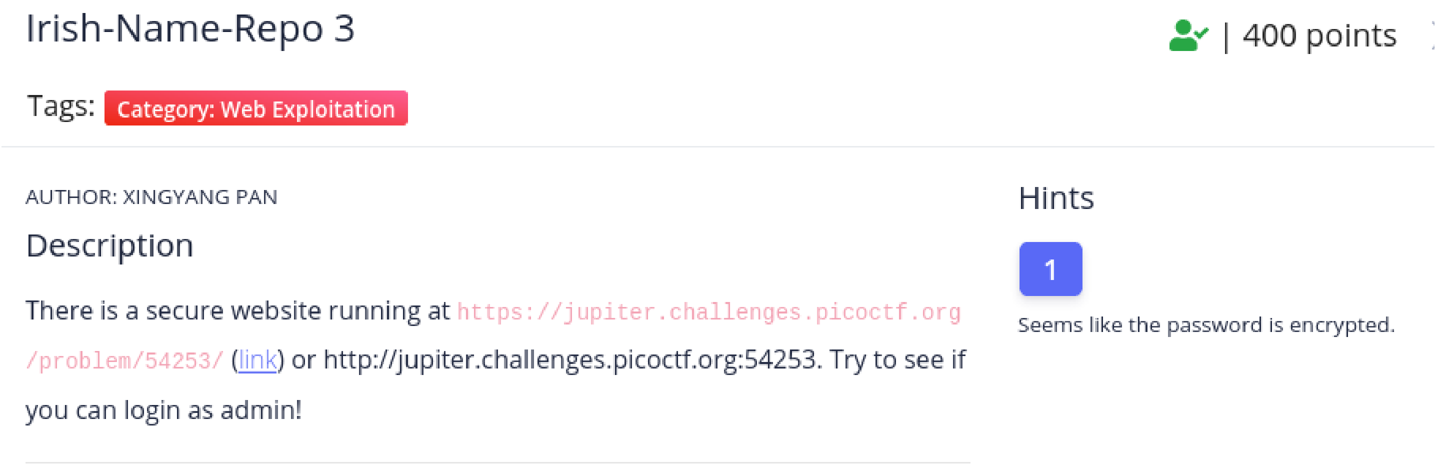
Mark Seliternikov

picoCTF - Irish Name Repo 3 [400 points]

Challenge details:



Irish-Name-Repo 3

✓ | 400 points

Tags: Category: Web Exploitation

AUTHOR: XINGYANG PAN

Description

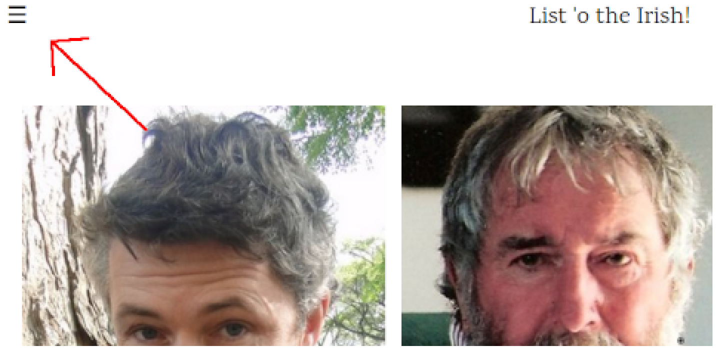
There is a secure website running at `https://jupiter.challenges.picoctf.org/problem/54253/` (link) or http://jupiter.challenges.picoctf.org:54253. Try to see if you can login as admin!

Hints

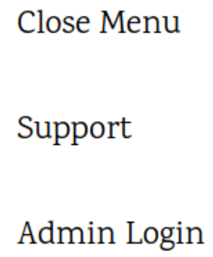
1

Seems like the password is encrypted.

Note that the hint is that the the password is encrypted. (This is the third challenge for this website).
The website: (just images of irish people)



Navigating to the admin login page

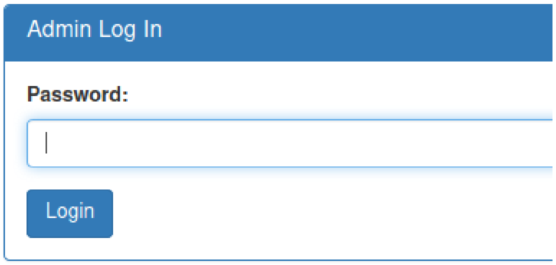


Close Menu

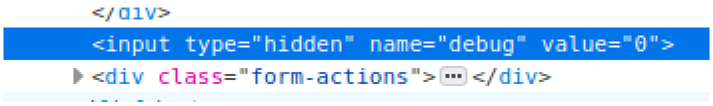
Support

Admin Login

Next we see that this time it doesn’t even as for a username and just the password. We are also hinted that the password is encrypted.

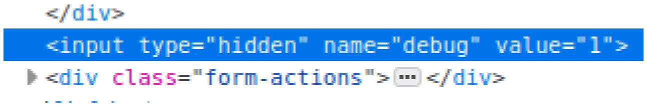


Like last time I should change the “debug mode” to true inside the hidden form value.
before:



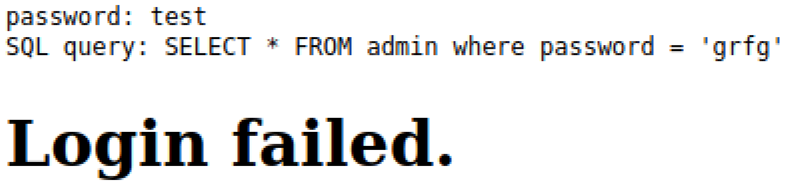
```
    </div>
    <input type="hidden" name="debug" value="0">
  ▸ <div class="form-actions">…</div>
```

After:



```
  </div>
  <input type="hidden" name="debug" value="1">
▸ <div class="form-actions">…</div>
```

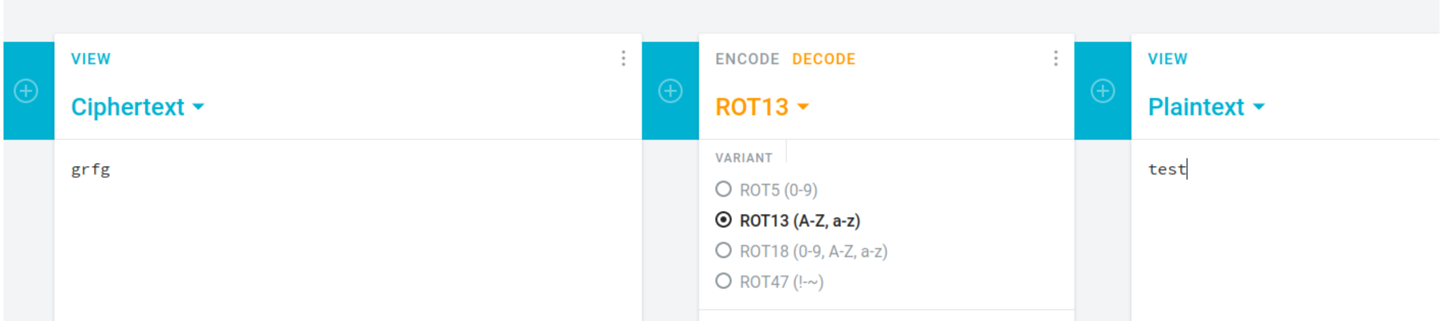
Now, lets see what the debug mode shows when I type “test” as the password.



```
password: test
SQL query: SELECT * FROM admin where password = 'grfg'
```

Login failed.

I thought to myself, The letter “t” got “g” for all times, So there was some sort of letter replacement in this encryption. The first thing that came to mind was ROT13 (which is rotating the alphabet letters 13 places).
So what I’ve done before I started writing a script was to check what “test” will return in an online ROT13 decoder.
This was the result:



Ciphertext

grfg

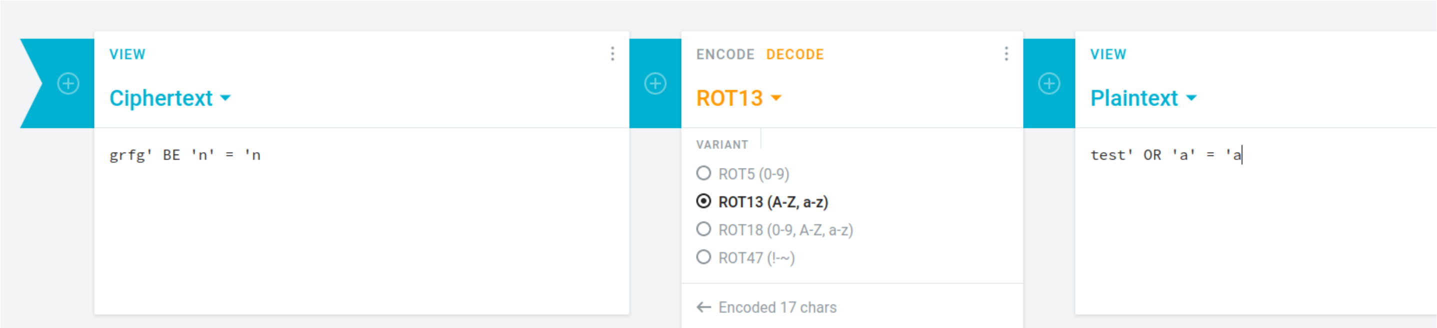
ROT13

VARIANT
○ ROT5 (0-9)
● ROT13 (A-Z, a-z)
○ ROT18 (0-9, A-Z, a-z)
○ ROT47 (!-~)

Plaintext

test

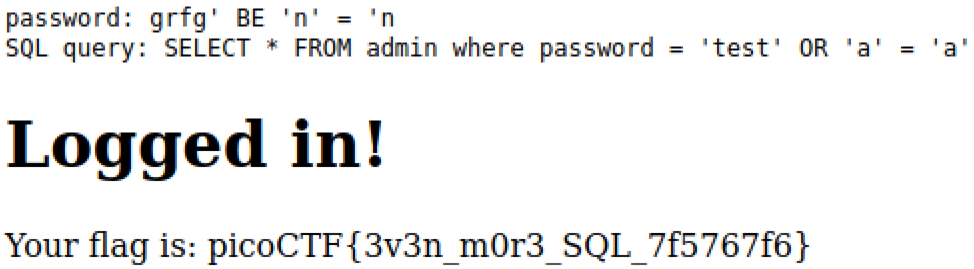
At that moment I smiled because I knew that I can wrap it up and finish the challenge. So what I’ve done next is to extend the SQL query in order to make the password irrelevant, meaning to place an OR statement which would always be true so I can login regardless of the password.
(I wanted the query to be: SELECT * FROM admin WHERE password = ’test’ OR ‘a’ = ‘a’, This lets me log in when either statement is true, either password is correct or a=a is correct, which is always true)



```
grfg' BE 'n' = 'n
```

```
test' OR 'a' = 'a
```

As you can see on the right was the statement I wanted to be inserted, So in order for it to be inserted and be encrypted but get the plaintext, I had to put the ciphertext which is on the left (If you ROT13 twice you get back to the original because there are 26 letters.)



```
password: grfg' BE 'n' = 'n
SQL query: SELECT * FROM admin where password = 'test' OR 'a' = 'a'
```

Logged in!

Your flag is: picoCTF{3v3n_m0r3_SQL_7f5767f6}

As you can see the query was successful and there's the flag :)