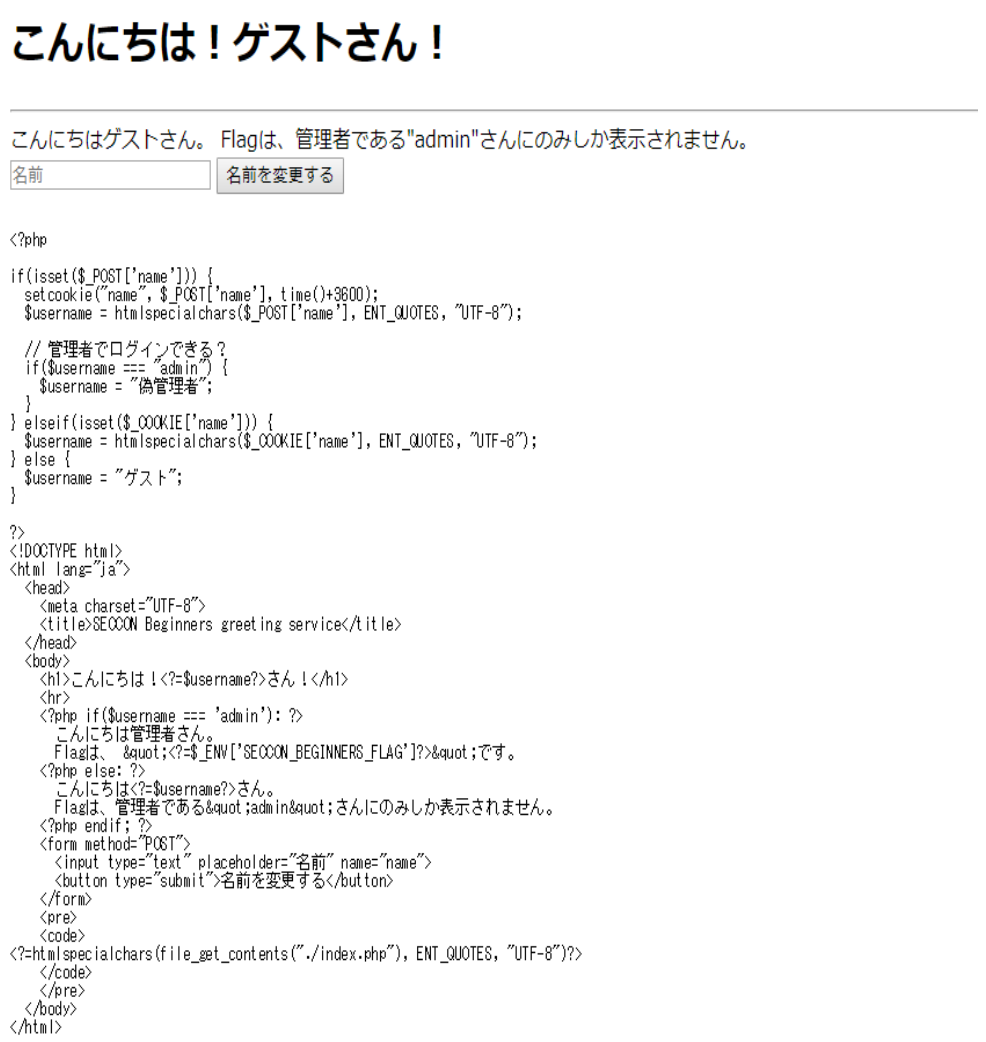
SECCON for Beginners2018
Web

[Warmup]Greeting

Write up

問題

- ようこそ！
  http://greeting.chall.beginners.seccon.jp/
- 名前をadminにすればflagが表示されるらしい。しかし、愚直にadminと打つとifに引っかかって偽管理者という名前に書き換えられてしまう。



こんにちは！ゲストさん！

こんにちはゲストさん。 Flagは、管理者である"admin"さんにのみしか表示されません。

名前 名前を変更する

```
<?php

if(isset($_POST['name'])) {
  setcookie("name", $_POST['name'], time()+3600);
  $username = htmlspecialchars($_POST['name'], ENT_QUOTES, "UTF-8");

  // 管理者でログインできる？
  if($username === "admin") {
    $username = "偽管理者";
  }
} elseif(isset($_COOKIE['name'])) {
  $username = htmlspecialchars($_COOKIE['name'], ENT_QUOTES, "UTF-8");
} else {
  $username = "ゲスト";
}

?>
<!DOCTYPE html>
<html lang="ja">
  <head>
    <meta charset="UTF-8">
    <title>SECCON Beginners greeting service</title>
  </head>
  <body>
    <h1>こんにちは！<?=$username?>さん！</h1>
    <hr>
    <?php if($username === 'admin'): ?>
      こんにちは管理者さん。
      Flagは、 &amp;quot;<?=$_ENV['SECCON_BEGINNERS_FLAG']?>&amp;quot;です。
    <?php else: ?>
      こんにちは<?=$username?>さん。
      Flagは、管理者である&amp;quot;admin&amp;quot;さんにのみしか表示されません。
    <?php endif; ?>
    <form method="POST">
      <input type="text" placeholder="名前" name="name">
      <button type="submit">名前を変更する</button>
    </form>
    <pre>
    <code>
<?=htmlspecialchars(file_get_contents("./index.php"), ENT_QUOTES, "UTF-8")?>
    </code>
    </pre>
  </body>
</html>
```

解法

- コードを眺めてると、$_POST['name']が空なら下のelse ifに引っかかるようになってることに気づく。

```
if(isset($_POST['name'])) {
  setcookie("name", $_POST['name'], time()+3600);
  $username = htmlspecialchars($_POST['name'], ENT_QUOTES, "UTF-8");

  // 管理者でログインできる？
  if($username === "admin") {
    $username  = "偽管理者";
  }
} elseif(isset($_COOKIE['name'])) {
  $username = htmlspecialchars($_COOKIE['name'], ENT_QUOTES, "UTF-8");
} else {
  $username  = "ゲスト";
}
```

解法

- else ifの条件に引っかかるためには、$_POST['name']が空でcookieに値が入っている必要があるのが分かる。この条件に引っかかるとcookieの値がusernameに代入されるので、cookieの値をadminにすればよいとわかる。
- EditThisCookieを使い、cookieの値をadminに固定する

- あとはformを空にした状態でページを更新するだけ

解法(flag)

こんにちは！adminさん！

こんにちは管理者さん。 Flagは、 "ctf4b{w3lc0m3_TO_ctf4b_w3b_w0rd!!}"です。

名前 名前を変更する

```
<?php

if(isset($_POST['name'])) {
  setcookie("name", $_POST['name'], time()+3600);
  $username = htmlspecialchars($_POST['name'], ENT_QUOTES, "UTF-8");

  // 管理者でログインできる？
  if($username === "admin") {
    $username = "偽管理者";
  }
} elseif(isset($_COOKIE['name'])) {
  $username = htmlspecialchars($_COOKIE['name'], ENT_QUOTES, "UTF-8");
} else {
  $username = "ゲスト";
}

?>
<!DOCTYPE html>
<html lang="ja">
  <head>
    <meta charset="UTF-8">
    <title>SECCON Beginners greeting service</title>
  </head>
  <body>
    <h1>こんにちは！<?=$username?>さん！</h1>
    <hr>
    <?php if($username === 'admin'): ?>
      こんにちは管理者さん。
      Flagは、 &amp;quot;<?=$_ENV['SECCON_BEGINNERS_FLAG']?>&amp;quot;です。
    <?php else: ?>
      こんにちは<?=$username?>さん。
      Flagは、管理者である&amp;quot;admin&amp;quot;さんにのみしか表示されません。
    <?php endif; ?>
    <form method="POST">
      <input type="text" placeholder="名前" name="name">
      <button type="submit">名前を変更する</button>
    </form>
    <pre>
    <code>
<?=htmlspecialchars(file_get_contents("./index.php"), ENT_QUOTES, "UTF-8")?>
    </code>
    </pre>
  </body>
</html>
```