源码如下

```php
<?php
    setcookie("ahash",base64_encode($secret.urldecode("admin"."admin")),time()+(60*60*24*7));
  //error_reporting(0);
  show_source("28.php");
    echo '<br>';
    require 'flag.php';
    if(!isset($_POST["username"]) || !isset($_POST["password"])){
        exit();
    }
     $username = $_POST["username"];
     $password = $_POST["password"];

     if(!empty($_COOKIE["check"])){
          if(urldecode($username) === "admin" && urldecode($password) !="admin"){
            if($_COOKIE["check"] === base64_encode($secret).urldecode($username.$password)){
              echo "Login successful .\r\n";
              die("The flag is ".$flag);
            }
            else{
              die("check your cookie again!");
            }
          }
          else{
          die("Son's of bitch? Are you admin?Fuck you!");
          }
     }

?>
```

通过阅读源码，我们可以知道我们需要、手动去调整cookie的内容

payload

```
cookie: check=ODg=admin12345

post数据: username=admin&password=12345
```