Login as Admin:

這題考的是php == 跟 === 的”feature”，就是在php中 == 跟 ===是不一樣的，用==判斷時左邊跟右邊不一定要完全一樣，用===才要完全依一樣，

例如：

$a = “127.0.0.1”

if ($a === “127.0.0.1) {

echo ‘inndy: php suck!’

}

if ($a == true){

echo ‘orange: are u sure?’

}

結果是：

inndy: php suck

orange: are u sure?

那看到source code ，我們有兩個事情要做第一是要進入admin account，第二要讓admin account印出flag，那剛好判斷這兩件事的code都有上面講的 ’feature’

code:

    $username = $data['username'];  
    $password = $data['password'];  
     
    if($users[$username] && $users[$username] == $password) {  
        $user = $username;  
    }

----------------------------------------------------------------------------------------------------------------

if($user === 'admin'){  
            if( strcmp( $\_POST['keyA'], base64\_encode($flag) ) == 0 &&  
                strcmp( $\_POST['keyB'], md5($flag) ) == 0           &&  
                sha1($\_POST['keyA']) === sha1($\_POST['keyB']) ){  
                  printf("<code>%s</code>", htmlentities($flag));  
            }  
            else{  
                  echo '<div class="alert">Wrong Key !</div>';  
            }  
  
          }

那第一部分就將$users[$username]設為admin，然後將$password設為true就能進admin了。

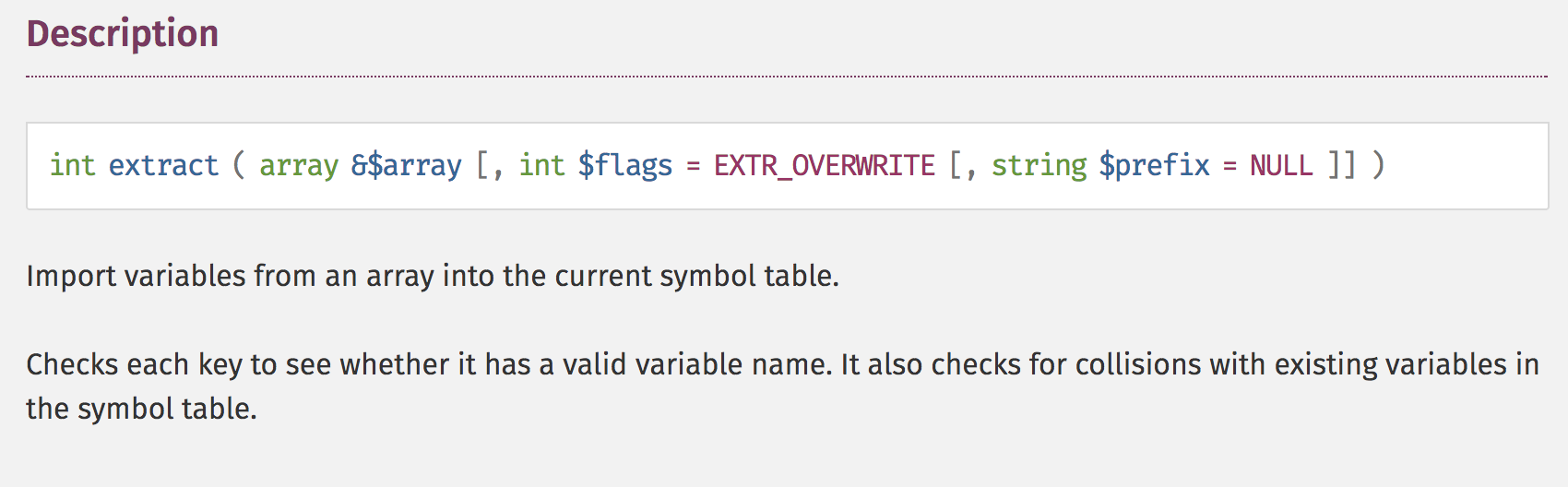
第二部分除了==之外還要知道strcmp的特性應為我們最後是要讓strcmp(…) == 0

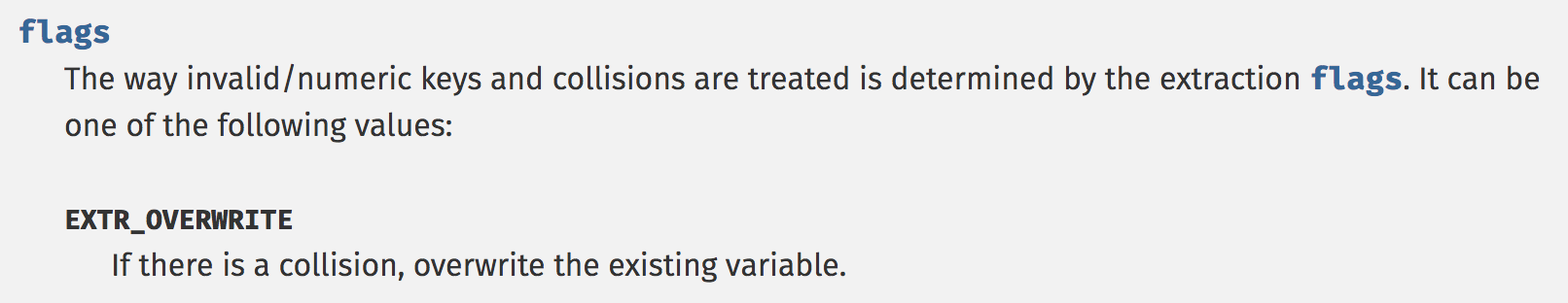
那，所以我們要想辦法讓strcmp(…)變成null or false，查了一下資料發現如果strcmp裡面的兩個參數型態不一樣的話會噴null，所以就將keyA, keyB變成陣列的型態即可。

Login as Admin2:

那這一題跟上一題差不多只是利用的洞不一樣，這題是利用了extract的”feature”

來看到extract的document:





所以直接送出json data將$user改成admin然後$\_SERVER['REMOTE\_ADDR']改成127.0.0.1就完成了