<?php

if( isset( $\_GET[ 'Login' ] ) ) {

// 检查token,防止CSRF攻击

checkToken( $\_REQUEST[ 'user\_token' ], $\_SESSION[ 'session\_token' ], 'index.php' );

// 接收用户名

$user = $\_GET[ 'username' ];

// 对接收到的user变量进行过滤

$user = stripslashes( $user );

// 对user变量中的特殊字符进行转义

$user = ((isset($GLOBALS["\_\_\_mysqli\_ston"]) && is\_object($GLOBALS["\_\_\_mysqli\_ston"])) ? mysqli\_real\_escape\_string($GLOBALS["\_\_\_mysqli\_ston"],$user): ((trigger\_error("[MySQLConverterToo] Fix the mysql\_escape\_string() call! This code does not work.", E\_USER\_ERROR)) ? "" : ""));

// 接受用户密码

$pass = $\_GET[ 'password' ];

// 对接收到的password变量进行过滤

$pass = stripslashes( $pass );

// 对password变量中的特殊字符进行转义

$pass = ((isset($GLOBALS["\_\_\_mysqli\_ston"]) && is\_object($GLOBALS["\_\_\_mysqli\_ston"])) ? mysqli\_real\_escape\_string($GLOBALS["\_\_\_mysqli\_ston"], $pass ) : ((trigger\_error("[MySQLConverterToo] Fix the mysql\_escape\_string() call! This code does not work.", E\_USER\_ERROR)) ? "" : ""));

// 进行MD5加密

$pass = md5( $pass );

// 进行数据库查询

$query = "SELECT \* FROM `users` WHERE user = '$user' AND password = '$pass';";

$result = mysqli\_query($GLOBALS["\_\_\_mysqli\_ston"], $query ) or die( '<pre>' . ((is\_object($GLOBALS["\_\_\_mysqli\_ston"])) ? mysqli\_error($GLOBALS["\_\_\_mysqli\_ston"]) : (($\_\_\_mysqli\_res = mysqli\_connect\_error()) ? $\_\_\_mysqli\_res : false)) . '</pre>' );

if( $result && mysqli\_num\_rows( $result ) == 1 ) {

// 得到用户信息

$row = mysqli\_fetch\_assoc( $result );

$avatar = $row["avatar"];

// 登陆成功

echo "<p>Welcome to the password protected area {$user}</p>";

echo "<img src=\"{$avatar}\" />";

}

else {

// 登陆失败，并且强制休眠三秒

sleep( rand( 0, 3 ) );

echo "<pre><br />Username and/or password incorrect.</pre>";

}

((is\_null($\_\_\_mysqli\_res = mysqli\_close($GLOBALS["\_\_\_mysqli\_ston"]))) ? false : $\_\_\_mysqli\_res);

}

//产生新的防止CSRF的token值

generateSessionToken();

?>

代码审计：首先增加了token值的验证，不仅防范了CSRF攻击，而且增加了爆破的难度。当用户登陆失败时，系统会强制休眠0-3秒，但这个时间对于暴力破解来说意义不大。