PHP (2)

李博杰 2011-11-26

内容一览

超全局数组
类与对象
数据库
    关系型数据库简介

    SQL

    PHP 的 MySQL 扩展

PHP 超全局数组

$GLOBALS
$_SERVER
$_GET
$_POST
$_REQUEST
$_FILES
$_SESSION
$_ENV
$_COOKIE

$_SERVER

phpinfo();

$_GET

forum.php?board=10&post=2
$_GET['board'] = 10
$_GET['post'] = 2

$_POST

<form action= "login.php method= "post" >
<input type= "text" name= "username" />
<input type= "password" name= "password" />
<input type= "button" value= " 提交" >
</form>

```php
<?php
$username = $_POST[ 'username' ];
$password = $_POST[ 'password' ];
$success=mysql_query ( "SELECT * FROM users WHERE `username`= '$username' AND `password`= '$password' " );
```

SQL 注入

SELECT * FROM users WHERE `username` = 'hack';' AND password = 'fake';
SELECT * FROM users WHERE `username` = 'hack'; DROP TABLE users;' AND password = 'fake';

addslashes

$password = addslashes($_POST['password']);
hack'; => hack\';

$_REQUEST

$_REQUEST = array_merge($_GET, $_POST);

$_FILES

$_SESSION

$_ENV

$_COOKIE

PHP 面向对象

数据库

SQL

PHP+MySQL