

php代码审计基础篇

第1课 基础语法讲解

php简介

PHP能做任何事，PHP主要是用于服务端的脚本程序

php语法<?php ?>; .php文件扩展名

```
<?php
```

```
echo "hello world":?>
```

php的注释介绍 // /* */

php的变量规则：变量以\$开始，后面接变量名称 变量名必须以字母或者下划线字符开始 变量名只能包含字母数字

字符以及下划线 变量名只能包含字母数字字符以及下划线(A-z,0-9和_) 变量名是区分大小写!

php语句和php变量全都区分大小写变量覆盖\$one = "aaa";\$a= "one" ;



- var_dump函数用于输出变量的相关信息
- echo,print,print_r()是内置函数
- string--字符串
- int--整型
- float--浮点型
- boolean--布尔型
- array--数组
- object--对象
- null--空值



- 字符串

- ' ' , ' '

- "hello world"

- 单双引号能声明字符串

- 字符串没有长度限制

- 在双引号声明的字符串中即可以直接解析变量，又可以使用转义字符，

- 在单引号声明的字符串中不可以直接解析变量，也不可以使用转义字符

- 转义字符\只能用来转义它自己和单引号



- **数组分类** `array()`
- **数值数组** `$men=array("red""green" ,"blue")`
- **key是自定义** **索引数组**
- **关联数组** `$age=array( "ren "=>" 19" ,"yi"=> "20" , "men"=>"21" );`
- **多维数组-** **包含一个或多个数组的数组**
- **print_r 打印数组**
- **foreach**

数组的遍历



php的控制结构

if条件成立执行

if else条件成立执行，不成立时执行另一个

if elseif else若干条件之一成立时执行一个

switchc在若干条件之一成立时执行一个代码块

首先对一个简答表达式n,进行条件判断，将其中的值与结构中每个case的值

去比较，如果存在匹配则执行与case关联的代码，代码执行后，用break阻止代

码跳入到下一个case中执行，default语句用于不存在匹配，即case为真时执行

<code>x == y</code>	等于
<code>x === y</code>	绝对等于
<code>x != y</code>	不等于
<code>x <> y</code>	不等于
<code>x !== y</code>	绝对不等于
<code>x > y</code>	大于
<code>x < y</code>	小于
<code>x >= y</code>	大于等于
<code>x <= y</code>	小于等于



php的变量与作用域

PHP有四种不同的变量作用域：

local global static parameter

全局变量可以被脚本中的任何部分访问，要在一个函数中访问一个全局变量，需要使用global关键字。在PHP函数内部声明的变量是局部变量，

仅能在函数内部访问

isset()—检测变量是否设置

```
<?php      $y
```

```
function a(){
```

```
    定义变量 global $x
```

```
}?>
```



常量是一个简单值的标识符。该值在脚本中不能改变。

一个常量由英文字母、下划线、和数字组成，但数字不能作为首字母出现

设置常量，使用define()函数

name:必选参数，常量名称，即标志符。

value:必选参数，常量的值。

caseinsensitive:可选参数，如果设置为TRUE,该常量则大小写不敏感。默认是大小写敏感的常量在定义

后，默认是全局变量，可以在整个运行的脚本的任何地方使用

魔术常量 __LINE__ __FILE__ __DIR__



php超全局变量

\$GLOBALS SGLOBALS是PHP的一个超级全局变量组，在一个PHP脚本的全部作用域中都可以访问

\$SERVER

\$_REQUEST \$_POST \$_GET用于收集HTML表单提交的数据

\$_FILES

\$_ENV

\$_COOKIE \$_SESSION 会话技术

\$_COOKIE变量用于取回cookie的值



php的函数

```
function函数名(){    //要执行代码  
  
}
```

函数的名称应该提示出它的功能

函数名称以字母或下划线开头(不能以数字开头)

如需让函数返回一个值，请使用return语句

有参函数也可以叫形参和实参

```
function函数名($a,$b){    //执行代码}
```



Object-oriented programming, 缩写: OOP

类使用class关键字后加上类名定义

类名后的一对大括号({})内可以定义变量和方法

类的变量使用var来声明, 变量也可以初始化值

函数定义类似PHP函数的定义, 但函数只能通过该类及其实例化的对象访问

\$this代表当前类的对象

self代表类本身

访问控制:

public表示全局, 类内部外部子类都可以访问;

private表示私有的, 只有本类内部可以使用;

protected表示受保护的, 只有本类或子类或父类中可以访问



php是一门弱类型语言

==只是对值得比较(将两边值转化为同类型再比较),而===则是对值和类型的比较。

var_dump(0== "admin")结果是true因为0是数字类型, admin是字符串类型这里的admin不是数字开头默认为0

var_dump(1== "ladmin")结果是true数字开头把它当做1来看待

var_dump(1 == "admin1")结果是false不是数字开头把他当做0来看待

转换成布尔类型的值, 整型值0,浮点型, 空字符串, 字符串 "0" 都会转为false

其他值则会被转为true 布尔型转换为整型值, 布尔值true转换成整数1布尔false转换为0

字符串转换为整型, 若字符串是以数字开始, 则使用改数值, 否则就是0

布尔型转换为字符串布尔值true转换成字符串1,布尔值false转换为空字符串

整型或浮点型转换为字符串, 直接将数字转换为字符串形式





谢谢观赏