Web开发-PHP应用&弱类型脆弱&Hash加密&Bool类型&Array数组&函数转换比较



#知识点：  
1、安全开发-原生PHP-超级全局变量  
2、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
0、安全开发-原生PHP-数据库通讯  
1、安全开发-原生PHP-身份验证技术  
2、安全开发-Cookie&Session&Token  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-弱类型脆弱  
2、安全开发-原生PHP-函数&数据类型  
3、安全开发-原生PHP-代码审计案例  
  
#章节点：(待补充)  
#具体点：(待补充)

演示案例：

* WEB开发-原生PHP-超级全局变量
* WEB开发-原生PHP-代码审计案例
* WEB开发-原生PHP-通讯数据库
* WEB开发-Cookie&Session&Token
* WEB开发-身份验证-代码审计案例
* WEB开发-弱类型&函数-特性安全
* WEB开发-数据对比-代码审计案例

1、== 和 ===  
两个等号==是弱比较，使用==进行对比的时候，php解析器就会做隐式类型转换，如果两个值的类型不相等就会把两个值的类型转为同一类型进行对比。  
  
2、MD5对比缺陷  
进行hash加密出来的字符串如存在0e开头进行弱比较的话会直接判定为true  
QNKCDZO  
0e830400451993494058024219903391  
240610708  
0e462097431906509019562988736854  
s878926199a  
0e545993274517709034328855841020  
s155964671a  
0e342768416822451524974117254469  
s214587387a  
0e848240448830537924465865611904   
s214587387a  
0e848240448830537924465865611904  
s878926199a  
0e545993274517709034328855841020  
s1091221200a  
0e940624217856561557816327384675  
s1885207154a  
0e509367213418206700842008763514  
  
3 函数strcmp类型比较缺陷   
低版本的strcmp比较的是字符串类型，如果强行传入其他类型参数，会出错，出错后返回值0，正是利用这点进行绕过  
  
4、函数Bool类型比较缺陷  
在使用 json\_decode() 函数或 unserialize() 函数时，部分结构被解释成 bool 类型，也会造成缺陷，运行结果超出研发人员的预期  
  
5、函数switch 类型比较缺陷  
当在switch中使用case判断数字时，switch会将参数转换为int类型计算  
  
6、函数in\_array数组比较缺陷  
当使用in\_array()或array\_search()函数时，如果第三个参数没有设置为true，则in\_array()或array\_search()将使用松散比较来判断  
  
7、===数组比较缺陷  
注意此时遇到的是 “===” ，不过也不是代表无从下手。在md5()函数传入数组时会报错返回NULL，当变量都导致报错返回NULL时就能使使得条件成立。  
  
案例：  
CTF题目：  
https://ctf.bugku.com/challenges/detail/id/72.html  
https://ctf.bugku.com/challenges/detail/id/94.html  
代码审CMS:  
https://mp.weixin.qq.com/s/k1hRg7cmRwwJJyyX04Ipmg

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)