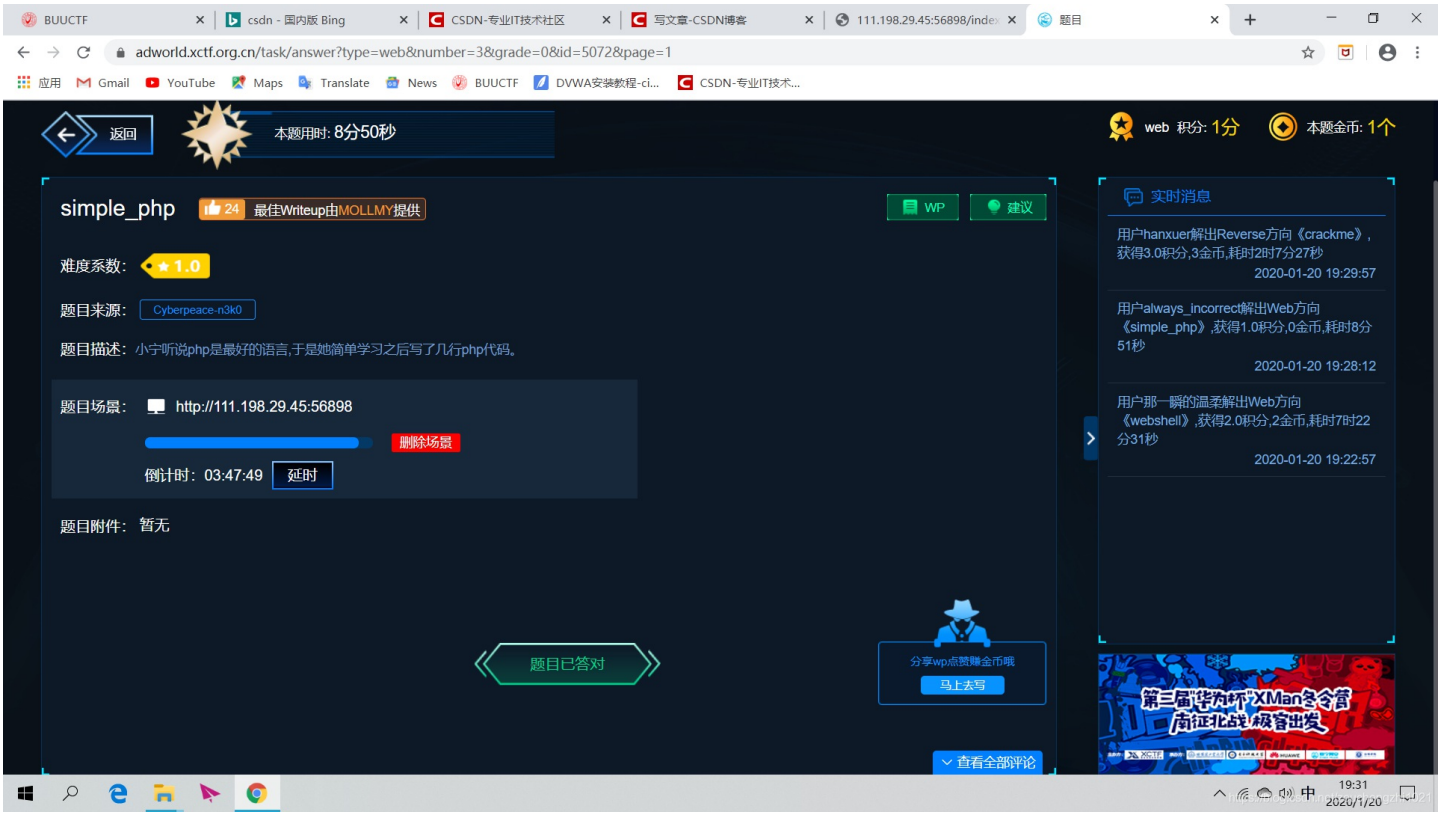
攻防世界simple_php

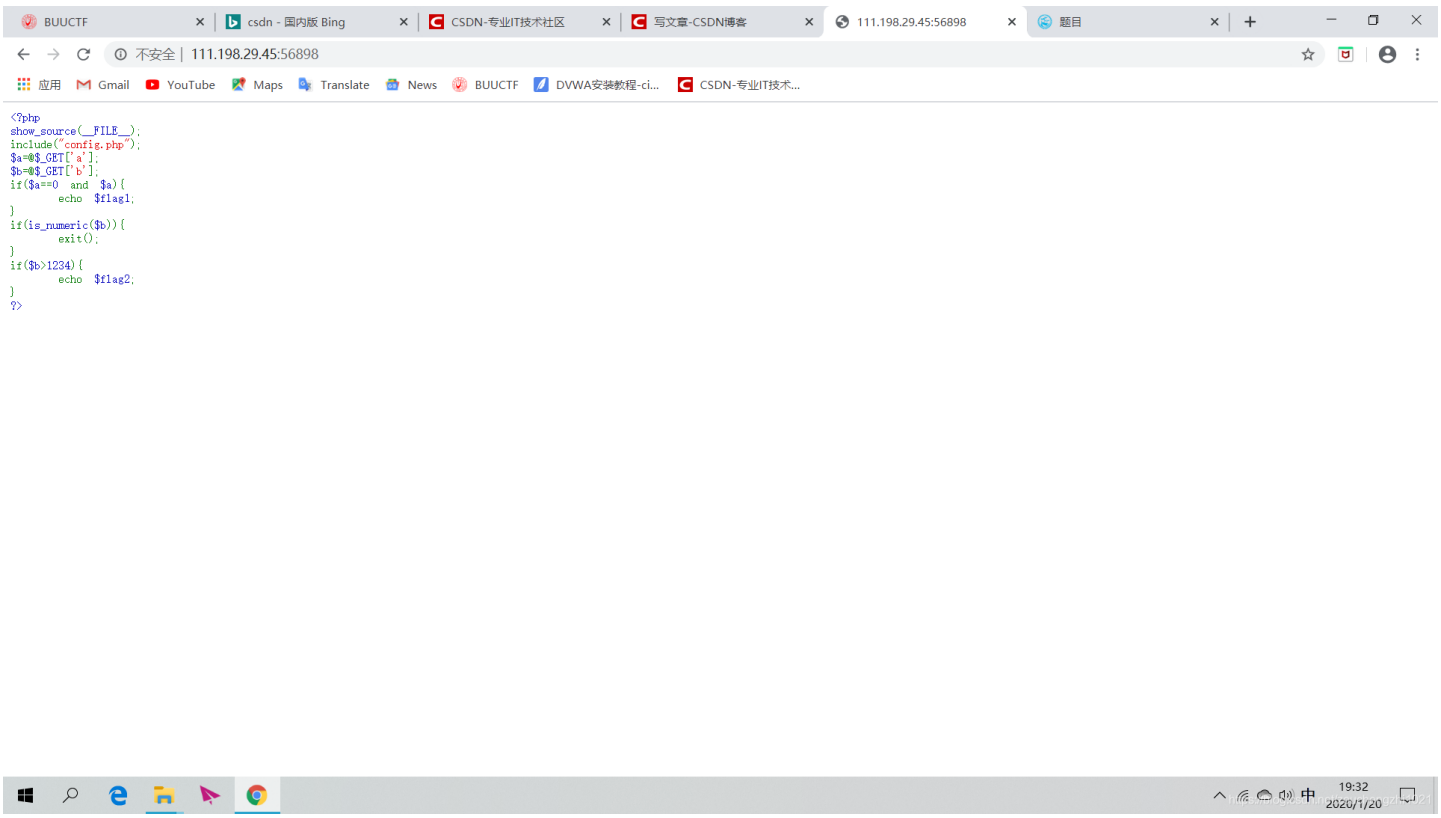
原创

LEO-max 于 2020-01-20 19:52:08 发布 2606 收藏 4

分类专栏： CTF学习

生活会辜负努力的人，但不会辜负一直努力的人——Leo的个人博客。


BUUCTF
csdn - 国内版 Bing
CSDN-专业IT技术社区
写文章-CSDN博客
111.198.29.45:56898/inde
题目
adworld.xctf.org.cn/task/answer?type=web&number=3&grade=0&id=5072&page=1
应用 Gmail YouTube Maps Translate News BUUCTF DVWA安装教程-ci... CSDN-专业IT技术...
返回
本题用时: 8分50秒
web 积分: 1分
本题金币: 1个
simple_php
24 最佳Writeup由MOLLMY提供
WP
建议
难度系数: 1.0
题目来源: Cyberpeace-n3k0
题目描述: 小宁听说php是最好的语言,于是她简单学习之后写了几行php代码。
题目场景: http://111.198.29.45:56898
删除场景
倒计时: 03:47:49
延时
题目附件: 暂无
题目已答对
分享wp点赞赚金币哦
马上去写
查看全部评论
实时消息
用户hanxuer解出Reverse方向《crackme》,获得3.0积分,3金币,耗时2时7分27秒
2020-01-20 19:29:57
用户always_incorrect解出Web方向《simple_php》,获得1.0积分,0金币,耗时8分51秒
2020-01-20 19:28:12
用户那一瞬的温柔解出Web方向《webshell》,获得2.0积分,2金币,耗时7时22分31秒
2020-01-20 19:22:57
第三届"华为杯"XMan冬令营
南征北战,极客出发
19:31
2020/1/20


BUUCTF
csdn - 国内版 Bing
CSDN-专业IT技术社区
写文章-CSDN博客
111.198.29.45:56898
题目
不安全 | 111.198.29.45:56898
应用 Gmail YouTube Maps Translate News BUUCTF DVWA安装教程-ci... CSDN-专业IT技术...
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
echo $flag1;
}
if(is_numeric($b)){
exit();
}
if($b>1234){
echo $flag2;
}
?>
19:32
2020/1/20

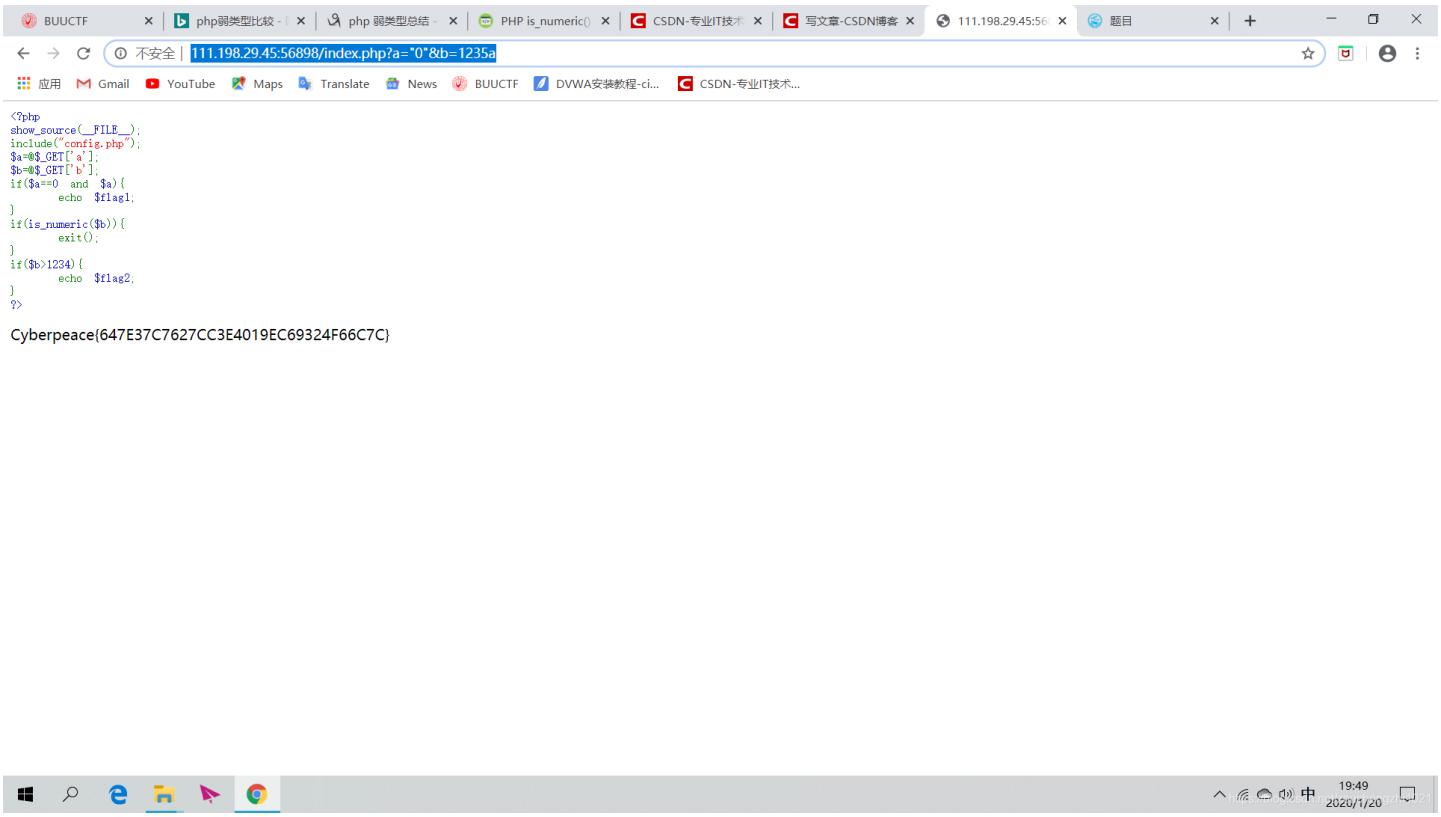
代码审计：
不难发现代码中给出了两个条件，且贱贱的把flag拆分到两个条件中。
条件1：
if($a==0 and $a){
echo $flag1;
}
说明：参数a=0且a为真才能得到半个flag.

条件2：
if(is_numeric($b)){
exit();
}
说明：is_numeric()函数可以参考https://www.runoob.com/php/php-is_numeric-function.html
如果b为数字则返回，即b不能为数字。

条件3:
if($b>1234){
echo $flag2;
}
说明：b要求大于1234才能得到另外半个flag.

条件2要求b不为数字条件3要求大于1234，此问题涉及到php弱类型比较。（可以上网搜搜）
在本题中弱类型比较时，1234=1234a。所以b=1235a时既不为数字同时也大于1234.

所以：http://111.198.29.45:56898/index.php?a=%220%22&b=1235a 补充条件就可以得到flag。



我也是刚学web，只能先从简单的开始了，加油加油！