云演CTF: 003.ereg

转载

wangguixiu 于 2021-06-09 22:50:13 发布 138 收藏

原文链接：https://www.wangguixiu.top/%E4%BA%91%E6%BC%94/%E4%BA%91%E6%BC%94CTF-003-ereg.html

云演CTF: 003.ereg

- 作者: admin
- 时间: 2021-05-27
- 分类: 云演CTF

主页空白，没有返回有效信息。

顺手打开robots.txt，发现源码，这个文本是给搜索引擎看的，里面的收录的目录和文件不会出现在搜索结果中(然并卵)

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

if (ereg ("[1]+$", $_GET[‘password’]) === FALSE) # 只允许大小写和数字(注1)
{
echo ‘ You password must be alphanumeric ’;

}
else if (strlen($_GET[‘password’]) < 8 && $_GET[‘password’] > 9999999) # 长度小于8并且值大于9999999(注2)
{

```
if (strpos ($_GET['password'], '*-*') !== FALSE) # 查找'*-*'在password中首次出现的位置(注3)
{
    die('Flag: ' . $flag);
}
else
{
    echo('&lt;p&gt;*-* have not been found&lt;/p&gt;');
}
```

}
else
{
echo ‘ Invalid password ’;
}

}

1) ereg函数可以通过数组或者%00绕过特殊字符，例如：password[0]=666!和password=666%00!

2) 长度可以使用科学计数法绕过，1e10比9999999大

3) 第三条只要传参中包含"-"就可以

所以最终结果是password[0]=1e9-或password=1e9%00-，最终得到flag

标签: none

---

a-zA-Z0-9 ↩