




云演-Web信息篇-writeup

原创

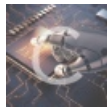
秋风瑟瑟...  于 2020-06-14 16:27:03 发布  598  收藏

分类专栏: [云演](#)

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/qq_45628145/article/details/106746819

版权



[云演](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

key在哪

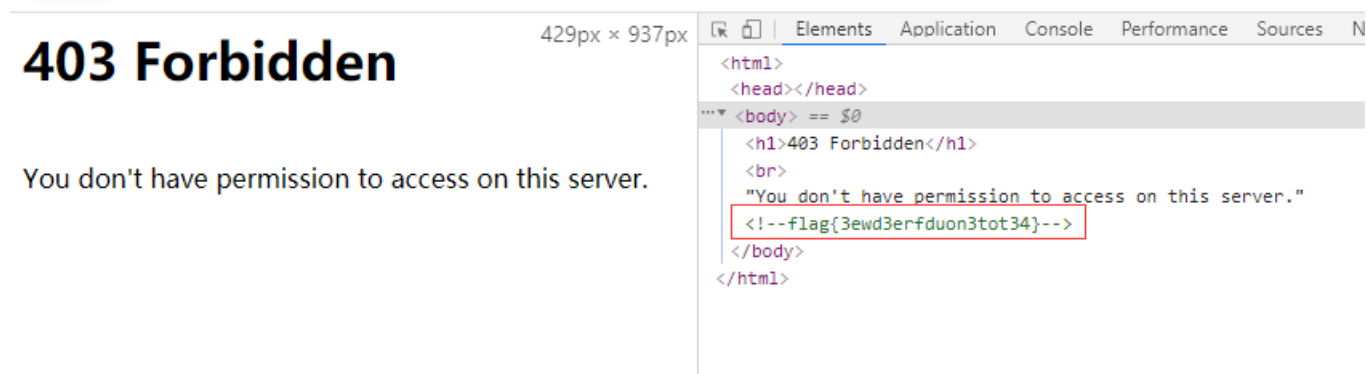
f12

Forbidden

看源码发现一段ajax请求，里面有一个 `/asetxtd/loginffff1111aaaagggggg.php`

```
686     });
687     $(function() {
688         var $login = $("#login");
689         $login.on(
690             "click",function(){
691                 try{
692                     $.ajax({
693                         url: '/asetxtd/loginffff1111aaaagggggg.php',
694                         type: 'POST',
695                         dataType: 'json',
696                         cache: false,
697                         data: new FormData($("#form-login")[0]),
698                         processData: false,
699                         contentType: false
700                     }).done(function(res) {
701                         if (data.result == 'true') {
702                             alert('登陆成功');
703                         } else {
704                             alert('登陆失败');
705                         }
706                     }).fail(function(res) {
707                         alert('登陆失败');
708                     });
709                 } catch (e) {
710                     alert(e);
711                 }
712             });
713     });
714 </script>
715 <script>
716     $(document).ready(function() {
717         /*
718         var defaults = {
719             containerID: 'toTop', // fading element id
720             containerHoverID: 'toTopHover', // fading element hover id
721             scrollSpeed: 1200,
722             easingType: 'linear'
723         };
724         */
725         $.UItoTop({
726             easingType: 'easeOutQuart'
727         });
728     });
729 </script>
730 <!--// end-smoth-scrolling -->
```

访问得到flag



429px × 937px

403 Forbidden

You don't have permission to access on this server.

```
<html>
<head></head>
<body> == $0
  <h1>403 Forbidden</h1>
  <br>
  "You don't have permission to access on this server."
  <!--flag{3ewd3erfdun3tot34}-->
</body>
</html>
```

运维失误

一个登陆框，题目是叫做运维失误，运维失误那就很大可能是源码泄露了，访问check.php.bak得到备份文件

欢迎您的到来，请登录

用户名:

密码:

验证码:

x4dn

提交 清除

58/px × 93/px

```
Elements Application Console Performance Sources Net
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
<html>
<head>...</head>
<body> == $0
  <form method="post" action="check.php">
    <div class="div">...</div>
  </form>
</body>
</html>
```

```
else
{
  if(('admin' == $name) && ('617b4cb7a816636d0b3aaf9273accad4' ==
$password))
  {
    //echo "验证成功! <br>";
    echo "<script type='text/javascript'>alert('登录成
功!');location='login_ok.php';</script>";
    $_SESSION["login"] = md5('login_ok');
  }
else
```

文件里面有用户名和密码，登录得到flag

JS



The screenshot shows a web page with a dark background and a white text box labeled "输入开门口令" (Enter the opening password). Below the text box is a "开门" (Open) button. To the right, the browser's developer tools are open, showing the source code. A JavaScript file named "check.js" is highlighted in the source code, with its path partially visible as "src='check.js'".

有一个check.js文件

```
function Check()
{
t = "118,97,114,32,77,121,80,97,115,115,32,61,32,100,111,99,117,109,101,110,116,46,103,101,116,69,108,101,109,101,110,116,66,121,73,100,40,39,73,110,99,97,110,116,97,116,105,111,110,39,41,46,118,97,108,117,101,59,32,10,9,118,97,114,32,102,105,108,101,95,49,61,34,55,56,49,53,54,57,54,101,99,98,102,49,99,57,54,34,59,10,9,105,102,40,34,34,43,112,97,114,115,101,73,110,116,40,77,121,80,97,115,115,41,32,61,61,32,77,121,80,97,115,115,41,32,10,9,123,10,9,32,32,32,32,32,32,105,102,40,112,97,114,115,101,73,110,116,40,77,121,80,97,115,115,41,43,55,57,56,55,56,57,61,61,49,48,48,48,48,48,41,32,10,9,9,123,32,10,9,9,9,118,97,114,32,102,105,108,101,95,50,61,34,101,54,56,57,52,98,55,55,57,52,53,54,100,51,51,48,34,59,9,10,9,9,9,118,97,114,32,102,105,108,101,95,51,61,34,101,54,52,102,101,53,34,59,10,9,9,9,118,97,114,32,102,105,108,101,95,51,95,116,109,112,61,102,105,108,101,95,51,46,115,112,108,105,116,40,34,34,41,46,114,101,118,101,114,115,101,40,41,46,106,111,105,110,40,34,34,41,59,10,9,9,9,118,97,114,32,102,105,108,101,95,50,61,40,102,105,108,101,95,51,95,116,109,112,46,99,111,110,99,97,116,40,34,52,56,55,56,101,49,98,34,41,41,46,99,111,110,99,97,116,40,34,97,97,57,52,57,53,102,97,50,49,50,53,50,100,52,53,57,98,50,34,41,59,10,9,9,9,118,97,114,32,103,101,116,95,102,108,97,103,95,104,101,114,101,32,61,32,102,105,108,101,95,49,32,43,32,102,105,108,101,95,50,32,43,32,39,46,112,104,112,39,59,10,9,9,9,97,108,101,114,116,40,34,20320,25214,21040,102,108,97,103,20102,20040,65311,34,41,59,10,9,9,125,10,9,9,101,108,115,101,10,9,9,123,32,9,10,9,9,9,97,108,101,114,116,40,39,19981,22909,24847,24605,65292,20320,22833,36133,20102,39,41,59,32,9,9,9,9,9,9,10,9,9,9,100,111,99,117,109,101,110,116,46,71,101,116,95,75,101,121,46,73,110,99,97,110,116,97,116,105,111,110,46,118,97,108,117,101,32,61,32,39,39,59,32,10,9,9,125,32,10,9,32,32,125,10,9,101,108,115,101,10,9,123,10,9,9,32,97,108,101,114,116,40,39,19981,22909,24847,24605,20320,22833,36133,20102,39,41,59,32,100,111,99,117,109,101,110,116,46,71,101,116,95,75,101,121,46,73,110,99,97,110,116,97,116,105,111,110,46,118,97,108,117,101,32,61,32,39,39,59,10,9,32,125";
t=eval("String.fromCharCode("+t+")");
eval(t);
}
```

把eval改成alert，丢进控制台执行

4e304dd0.yunyansec.com 显示

```
***var
file_2=(file_3_tmp.concat("4878e1b")).concat("aa9495fa21252d459b2");
***var get_flag_here = file_1 + file_2 + '.php';
***alert("你找到flag了么? ");
**}
**else
**{
***alert("不好意思，你失败了");
***document.Get_Key.Incantation.value = "";
```

得到源码，但是就算口令正确了，也没有显示flag，而是有一个get_flag_here没有被显示出来

```
var MyPass = document.getElementById('Incantation').value;
var file_1="7815696ecbf1c96";
if(""+parseInt(MyPass) == MyPass) {
  if(parseInt(MyPass)+798789==1000000) {
    var file_2="e6894b779456d330";
    var file_3="e64fe5";
    var file_3_tmp=file_3.split("").reverse().join("");
    var file_2=(file_3_tmp.concat("4878e1b")).concat("aa9495fa21252d459b2");
    var get_flag_here = file_1 + file_2 + '.php';
    alert("你找到flag了么? ");
  }else{
    alert('不好意思，你失败了');
    document.Get_Key.Incantation.value = '';
  }
}else{
  alert('不好意思，你失败了');
  document.Get_Key.Incantation.value = '';
}
```

稍微改一点，继续丢进控制台执行

```
var file_1="7815696ecbf1c96";
var file_2="e6894b779456d330";
var file_3="e64fe5";
var file_3_tmp=file_3.split("").reverse().join("");
var file_2=(file_3_tmp.concat("4878e1b")).concat("aa9495fa21252d459b2");
var get_flag_here = file_1 + file_2 + '.php';
alert(get_flag_here);
```

得到 [7815696ecbf1c965ef46e4878e1baa9495fa21252d459b2.php](#)



芝麻开门

请输入数据

输入框:
请输入口令开门:zhimakaimen

提示输入zhimakaimen，但是输入的时候发现有长度限制，发现是表单里的maxlength属性设置的，改一下，输入就好了

A screenshot of a web browser with developer tools open. The browser shows the form from the previous image. The developer tools pane is open to the 'Elements' tab, showing the HTML structure of the form. The following code is highlighted in the source view:

```
<input type="password" name="text1" maxlength="9999"> == $0
```

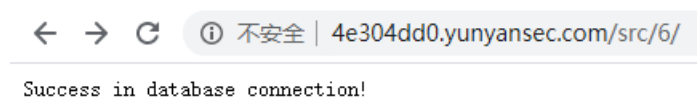
得到 [flag{CodecEe3A87c92C2}](#)

flag{CodecEe3A87c92C2}

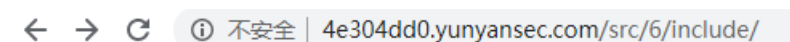
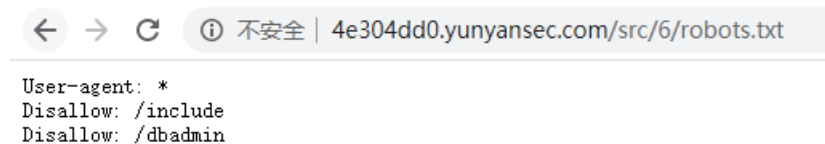
输入框:
请输入口令开门:zhimakaimen

管理员的愤怒




什么都没有，只是显示了数据库连接成功



在robots.txt里面发现东西



Index of /src/6/include

Name	Last modified	Size	Description
 Parent Directory		-	
 db.php	2019-10-24 08:02	205	
 db.phps.bak	2019-10-24 08:02	205	

存在备份文件，有数据库的账号和密码

```
<?php
define ( 'Z_DB_NAME', 'dbappweb1' );
define ( 'Z_DB_USER', 'root' );
define ( 'Z_DB_PASSWORD', 'root' );
define ( 'Z_DB_HOST', 'localhost' );
define ( 'Z_DB_CHARSET', 'utf8' );
$table_prefix = 'z_';
```



Welcome to phpMyAdmin

Log in

Username:

Password:

phpMyadmin, 登录, 在dbappweb1的数据库的flags表里面发现 `flag{49b121dfg76jtafe8231}`

Server: localhost » Database: dbappweb1 » Table: flags

Browse | **Structure** | **SQL** | **Search**

⚠ Current selection does not contain a unique column. Grid ec

✔ Showing rows 0 - 0 (1 total, Query took 0.0003 seconds.)

```
SELECT * FROM `flags`
```

Show all | Number of rows: 25 | Filter rows:

+ Options

flag

flag{49b121dfg76jtafe8231}

Show all | Number of rows: 25 | Filter rows:

愚人节的礼物

发现网页标题是cookie，看下cookie，发现admin的值为0，抓包改成1，得到flag

正在使用的 Cookie

允许 已禁止

以下 Cookie 是系统在您查看此网页时设置的

- 4e304dd0.yunyansec.com
 - Cookie
 - PHPSESSID
 - admin

名称	内容	域名	路径
admin	0	4e304dd0.yunyansec.com	/src/8

禁止 删除 完成

愚人节的礼物

4月1日这天，小黑想给大家个惊喜——让我们来找到这个彩蛋吧!!!，

恭喜你，你得到了想要的

flag{5NXruh4s4g5trwsVwOYsjKzi}

一个假的404页面，访问的时候被重定向了，在index.php响应头里面发现flag

The screenshot shows a web browser window with the address bar displaying '4e304dd0.yunyansec.com/src/10/1.php'. The main content area shows a '404 Not Found' error from 'nginx'. The Network tab is open, showing a list of requests. The 'index.php' request is selected, and its headers are displayed. The 'Response Headers' section contains the following information:

- Request URL: http://4e304dd0.yunyansec.com/src/10/index.php
- Request Method: GET
- Status Code: 302 Found
- Remote Address: 1.85.2.120:80
- Referrer Policy: no-referrer-when-downgrade
- Content-Length: 164
- Content-Type: text/html
- Date: Sun, 14 Jun 2020 08:16:29 GMT
- Flag: flag{35yhdt3gery3wwerf4f4}
- Location: ./1.php
- Server: Apache
- X-Powered-By: PHP/5.5.9-1ubuntu4.29

单身20年的手速

又是一个重定向，在search_key.php里面发现flag

The screenshot shows a web browser window with the address bar displaying 'view-source:4e304dd0.yunyansec.com/src/11/search_key.php'. The source code is displayed as follows:

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <script>>window.location="2.php"; </script>
5   <title>key</title>
6 </head>
7 <body>
8   flag{46tgs1ff22f0f929f94d9424ca5eb} </body>
9 </html>
```

单身100年也没用

又是一样的东西，在响应头里面发现一段base64，解码得到flag