

Natas Wargame Level20 Writeup (会话状态注入/篡改)

转载

a_18067 于 2017-05-20 14:35:00 发布 71 收藏

文章标签: [php](#)

原文地址: <http://www.cnblogs.com/liquhao/p/6882068.html>

版权

You are logged in as a regular user. Login as an admin to retrieve credentials for natas21.

Your name:

[Change name](#)

[View sourcecode](#)

```
▼ <form action="index.php" method="POST">
  Your name:
  <input name="name" value=""></input>
  <br><br>
  <input value="Change name" type="submit"></input>
</form>
```

sourcecode核心代码:

```
1 <?
2
3 function debug($msg) {
4     if(array_key_exists("debug", $_GET)) {
5         print "DEBUG: $msg<br>";
6     }
7 }
8
9 function print_credentials() {
10    if($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1) {
11        print "You are an admin. The credentials for the next level are:<br>";
12        print "<pre>Username: natas21<\n";
13        print "Password: <censored></pre>";
14    } else {
15        print "You are logged in as a regular user. Login as an admin to retrieve credentials for natas21." ;
16    }
17 }
18
19
20 /* we don't need this */
21 function myopen($path, $name) {
22     //debug("MYOPEN $path $name");
23     return true;
24 }
25
26 /* we don't need this */
27 function myclose() {
28     //debug("MYCLOSE");
29     return true;
30 }
31
```

```

32 function myread($sid) {
33     debug("MYREAD $sid");
34     if(strspn($sid, "1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") != strlen($sid))
{
35     debug("Invalid SID");
36     return "";
37 }
38 $filename = session_save_path() . "/" . "mysess_" . $sid;
39 if(!file_exists($filename)) {
40     debug("Session file doesn't exist");
41     return "";
42 }
43 debug("Reading from ". $filename);
44 $data = file_get_contents($filename);
45 $_SESSION = array();
46 foreach(explode("\n", $data) as $line) {
47     debug("Read [".$line "]");
48     $parts = explode(" ", $line, 2);
49     if($parts[0] != "") $_SESSION[$parts[0]] = $parts[1];
50 }
51 return session_encode();
52 }
53
54 function mywrite($sid, $data) {
55     // $data contains the serialized version of $_SESSION
56     // but our encoding is better
57     debug("MYWRITE $sid $data");
58     // make sure the sid is alnum only!!
59     if(strspn($sid, "1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") != strlen($sid))
{
60     debug("Invalid SID");
61     return;
62 }
63 $filename = session_save_path() . "/" . "mysess_" . $sid;
64 $data = "";
65 debug("Saving in ". $filename);
66 ksort($_SESSION);
67 foreach($_SESSION as $key => $value) {
68     debug("$key => $value");
69     $data .= "$key $value\n";
70 }
71 file_put_contents($filename, $data);
72 chmod($filename, 0600);
73 }
74
75 /* we don't need this */
76 function mydestroy($sid) {
77     //debug("MYDESTROY $sid");
78     return true;
79 }
80 /* we don't need this */
81 function mygarbage($t) {
82     //debug("MYGARBAGE $t");
83     return true;
84 }
85
86 session_set_save_handler(
87     "myopen",
88     "myclose",
89     "myread"

```

```

85     "myread",
86     "mywrite",
87     "mydestroy",
88     "mygarbage");
89 }
90
91 session_start();
92
93 if(array_key_exists("name", $_REQUEST)) {
94     $_SESSION["name"] = $_REQUEST["name"];
95     debug("Name set to " . $_REQUEST["name"]);
96 }
97
98 print_credentials();
99
100
101 $name = "";
102 if(array_key_exists("name", $_SESSION)) {
103     $name = $_SESSION["name"];
104 }
105
106
107 ?>
108
109 <form action="index.php" method="POST">
110 Your name: <input name="name" value=<?=$name?>"><br>
111 <input type="submit" value="Change name" />
112 </form>

```

关键部分已经用红色标出，mywrite和myread是两个管理会话状态的关键函数，以下是一些参考资料：

<http://php.net/manual/zh/function.session-set-save-handler.php>

<http://php.net/manual/zh/function.strspn.php>

http://www.w3school.com.cn/php/func_string_explode.asp

<http://php.net/manual/zh/function.session-encode.php>

简单来说，myread首先对sid（第一次由服务器自动生成并保存在cookie中）进行校验，若非字母/数字则不返回会话状态。

若sid合法，则进入相关目录寻找/读取文件，若是老的会话/文件已经删除会新建文件保存会话，文件读取完后将session的最后一对键值覆盖到第一的位置。

mywrite则会在会话结束的时候重新读取session，并对session进行一次ksort，将排序后的键值对重新写入文件。

一开始我的思路是通过使sid带有目录路径（改cookie），使得debug输出的时候将/etc/...../natas20的文件内容读出来，但是在myread和mywrite里面都进行了检验，所以很难通过sid进行注入。

另一个思路就是，源码里面其实没有向session里面添加admin的键值对，这也提示我们可以通过“唯一”的一个name键值对进行注入：将data里面的值变为：name xxxx\nadmin 1\n

如何添加这个\n呢？既然通过get方式提交，也要用URL编码编码后进行提交。（这里有个插曲，一开始我对mywrite的写入和myread的读取没有理解好，以为注入name xxx admin 1就可以了，实际上如果让mywrite这么写入，myread读取会话状态时\$parts = explode(" ", \$line, 2)，只会将这仅有的一行的第一个键值对name xxx添加到session里面）。\n对应%0A（\r对应%0D，但在linux下用换行号就够了）。所以应该输入xxxx\nadmin 1，第一次会显示regular，因为没有文件/状态可以读取，session里还是没有Admin的，会话关闭后xxxx\nadmin 1就会被写入到状态中，下次登录后session就会被加入admin 1了。

但是，这里的输入并不能直接在form中输入并提交：

Request Body:

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

Content-Length: 19

name=xxx%5Cnadmin+1

因为\n即回车并不会被编码为%0A这个字节存入到file中，可以直接url中输入并提交或者改postbody。

<http://natas20.natas.labs.overthewire.org/index.php?name=xxx%0Aadmin%201&debug=1> (%20为空格 直接空格也行)

DEBUG: MYREAD nuvqerfrem6hik089umsdf0m84

DEBUG: Reading from /var/lib/php5/sessions

//mysess_nuvqerfrem6hik089umsdf0m84

DEBUG: Read [name xxx]

DEBUG: Read [admin 1]

DEBUG: Read []

DEBUG: Name set to xxx admin 1

You are an admin. The credentials for the next level are:

Username: natas21

Password: IFekPyrQXftziDEsUr3x21sYuahypdgJ

Your name:

总结：如果用户的输入要保存为会话状态，服务端读取和写入会话时要进行防注入处理，，否则存在提权或劫持等注入问题。

flag:**IFekPyrQXftziDEsUr3x21sYuahypdgJ**

转载于:<https://www.cnblogs.com/liqiuhan/p/6882068.html>