New issue

Jump to bottom

SImiik <=v1.6.2.1 xss + rce #123

Closed deFming opened this issue on Apr 15, 2019 · 1 comment

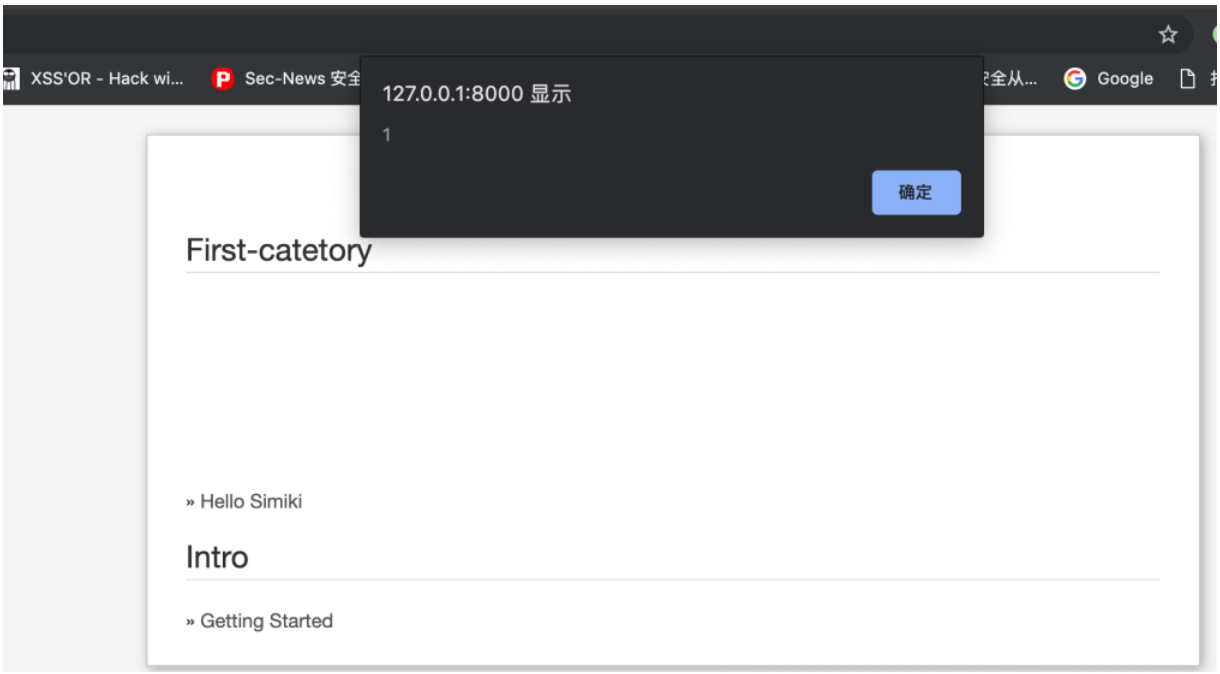
deFming commented on Apr 15, 2019 • edited

1.XSS

Examples:

```
python3 -m simiki.cli new -t "Hello Simiki<svg/onload=alert(1)>" -c first-catetory

python3 -m simiki.cli g
python3 -m simiki.cli p
```



The affected file appears to be
https://github.com/tankywoo/simiki/blob/master/simiki/generators.py Line 54

By default, jinja2 sets autoescape to False. Consider using autoescape=True or use the select_autoescape function to mitigate XSS vulnerabilities.

2.RCE

https://github.com/tankywoo/simiki/blob/master/simiki/config.py line 64
Use of unsafe yaml load. Allows instantiation of arbitrary objects. Consider yaml.safe_load().

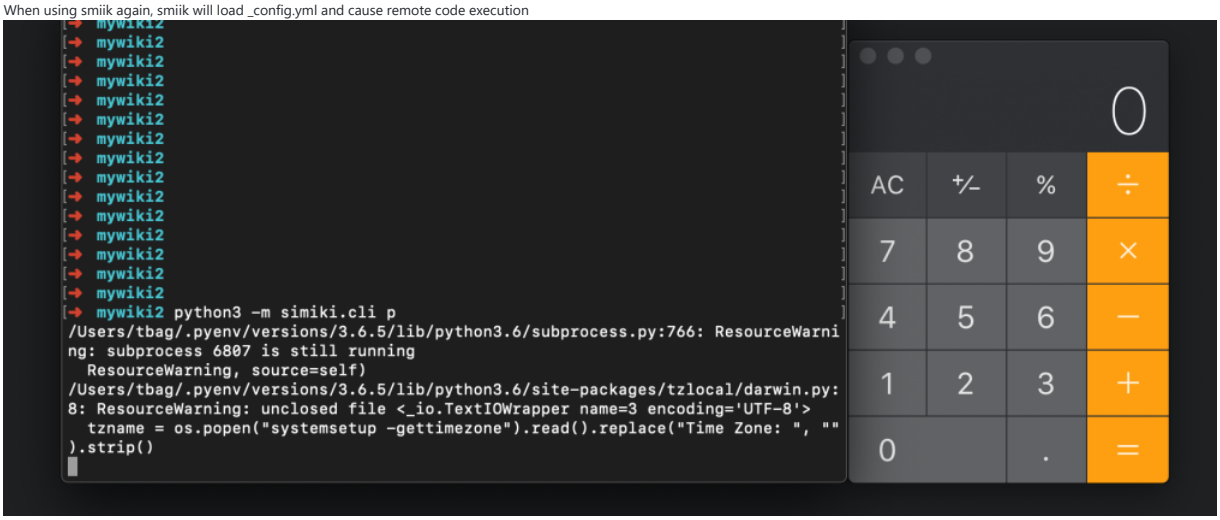
This can lead to remote code execution.

When simiki loads a malicious _config.xml file.

Payload:

```
!!python/object/new:os.system ["/Applications/Calculator.app/Contents/MacOS/Calculator"]
```

When using smiik again, smiik will load _config.yml and cause remote code execution



deFming changed the title ~~Smiik v1.6.2.1 xss + rce~~ Smiik <=v1.6.2.1 xss + rce on Apr 15, 2019

deFming changed the title ~~Smiik <=v1.6.2.1 xss + rce~~ SImiik <=v1.6.2.1 xss + rce on Apr 15, 2019

tankywoo commented on Apr 21, 2019 — Owner

Thanks for your report.

The first problem, enable `autoescape` need theme also add `safe`, and I will fix it later.

The second problem was fixed in version 1.6.2.2.

tankywoo closed this as completed on Apr 21, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants