Kalle Jalkanen AB8822
time used: 3 hours

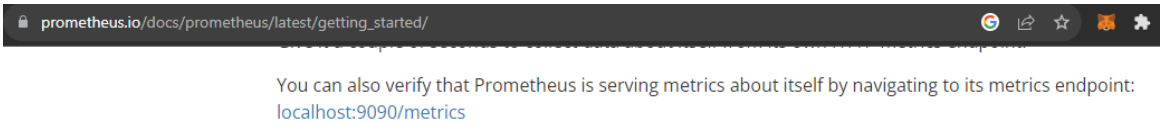
Juice Shop - Exposed Metrics

Description

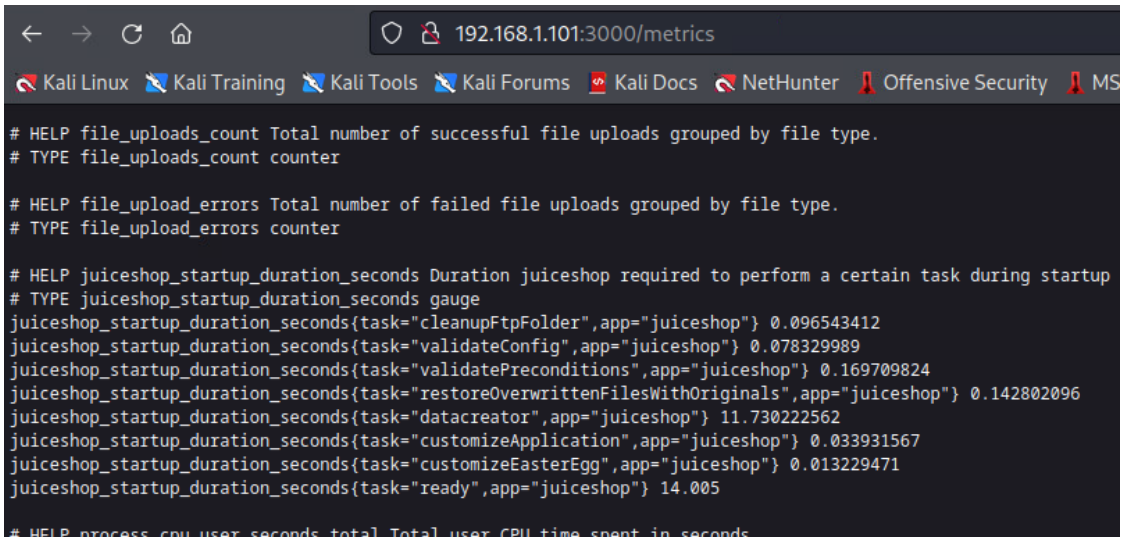
Prometheus uses default path, so it is easy to find by anyone.

Steps to produce

From Prometheus's getting started guide we can find default path to it.



Now test it on juice shop.



Impact estimation

Low severity. This gives sensitive information to attacker about how application works. It gives attacker more attack surfaces and how information how application works.

Mitigation

Make metrics data only visible to admins or/and to different port.

Main target - Insertion of Sensitive Information into Log File

Description

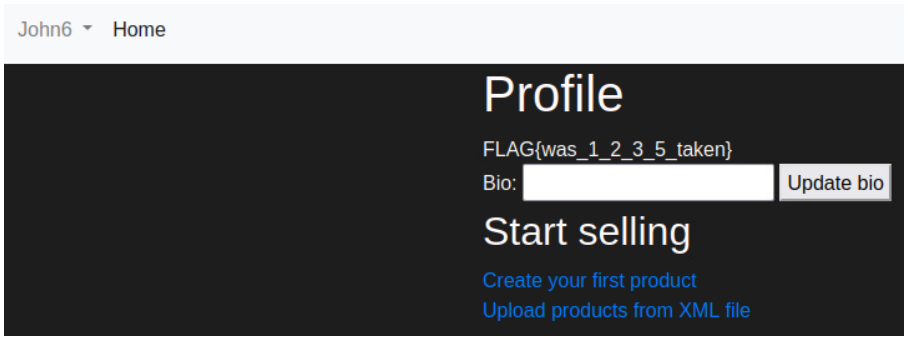
Django's log file has sensitive information which can be used to find out users' login credentials.

Steps to produce

From error log file we can see that someone has tried to make account called 'John' with password 'john88'. User has failed to create account with username 'john1-5' so maybe 'john6' was successful.

```
wasdat@wasdat:~$ docker exec -it wasdat_v2_docker-django-1 cat /var/log/django.log
<ul class="errorlist"><li>username<ul class="errorlist"><li>A user with that username already exists.</li></ul></l
i></ul> Account details: John:john88
<ul class="errorlist"><li>username<ul class="errorlist"><li>A user with that username already exists.</li></ul></l
i></ul> Account details: John1:john88
<ul class="errorlist"><li>username<ul class="errorlist"><li>A user with that username already exists.</li></ul></l
i></ul> Account details: John2:john88
<ul class="errorlist"><li>username<ul class="errorlist"><li>A user with that username already exists.</li></ul></l
i></ul> Account details: John3:john88
<ul class="errorlist"><li>username<ul class="errorlist"><li>A user with that username already exists.</li></ul></l
i></ul> Account details: John4:john88
<ul class="errorlist"><li>username<ul class="errorlist"><li>A user with that username already exists.</li></ul></l
i></ul> Account details: John5:john88
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Lisa:catdog
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Dan:apples
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Robert:qwerty
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Lyla:abc123
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Celine:default
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Harry:password123
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Fabian:12345678
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Jamie:monkey
<ul class="errorlist"><li>password2<ul class="errorlist"><li>The two password fields didn't match.</li></ul></li><
/ul> Account details: Joe:football
```

Now we login as 'John6' with password 'john88'.



Impact estimation

Low severity. This allows the attacker to obtain only the login credentials of individual customer. But it might impact the trust to the company.

Mitigation

Is there really need to save passwords to log file? Also log files should be encrypted if it has sensitive information.