Week 2 - XXE

Introduction to Offensive Security

XXE?

- XML eXternal Entity (attacks)
- Turns out XML is really *really* overcomplex…
  - XSLT (Extensible Stylesheet Language Transformations) is Turing complete
  - Others have written formal programming languages based on XML

XML 101

- Tree of tags
- Tags have attributes, and inner data/children

```
<html>
	<body>
		<p style="font-size: 10px">Hello</p>
	</body>
</html>
```

XML Entities

- Essentially placeholders
  - Commonly see & > < in HTML
  - "Replaced" with &, >, <
- Defined with

  `<!ENTITY name value>` inside of a `<!DOCTYPE […]>`

XML Entities

- Somebody had the wonderful idea to let you include other files in entities…

```
<!ENTITY foo SYSTEM "file://file.txt">
<p>&foo;</p>
```

XML Entities

- That's about all you'll ever need to know

ASIS CTF Demo