XML EXTERNAL ENTITY INJECTION

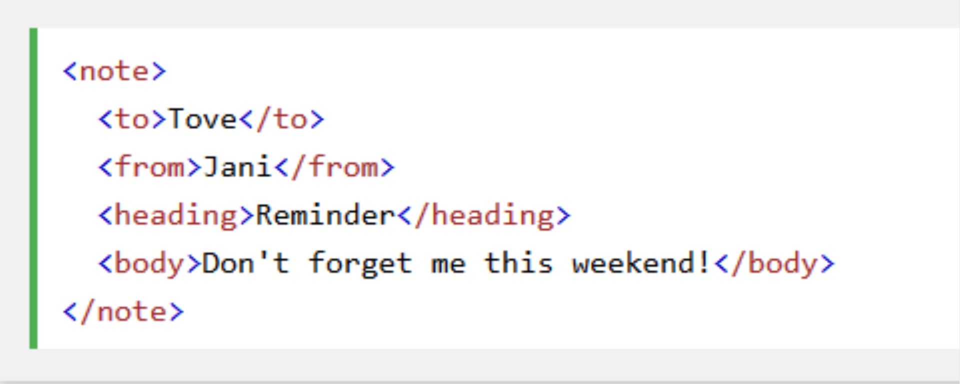
Rupam Bhattacharya

Whoami?

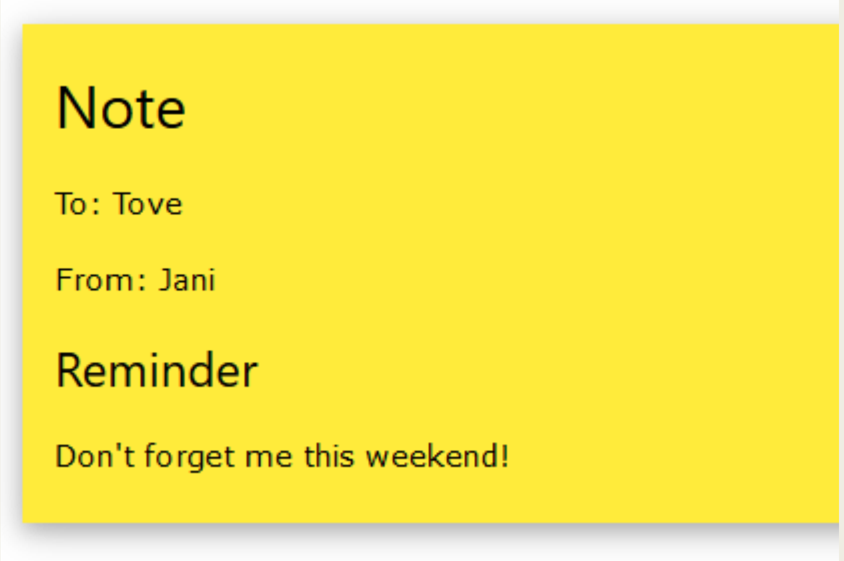
- Security Researcher
- Head of Offensive Security Practice at Spectrami
- Twitter – ru94mb

XML?

- Extensible Mark-up Language (XML)
- XML was designed to store and transport data
- No pre-defined tags



```
<note>
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```



Note

To: Tove

From: Jani

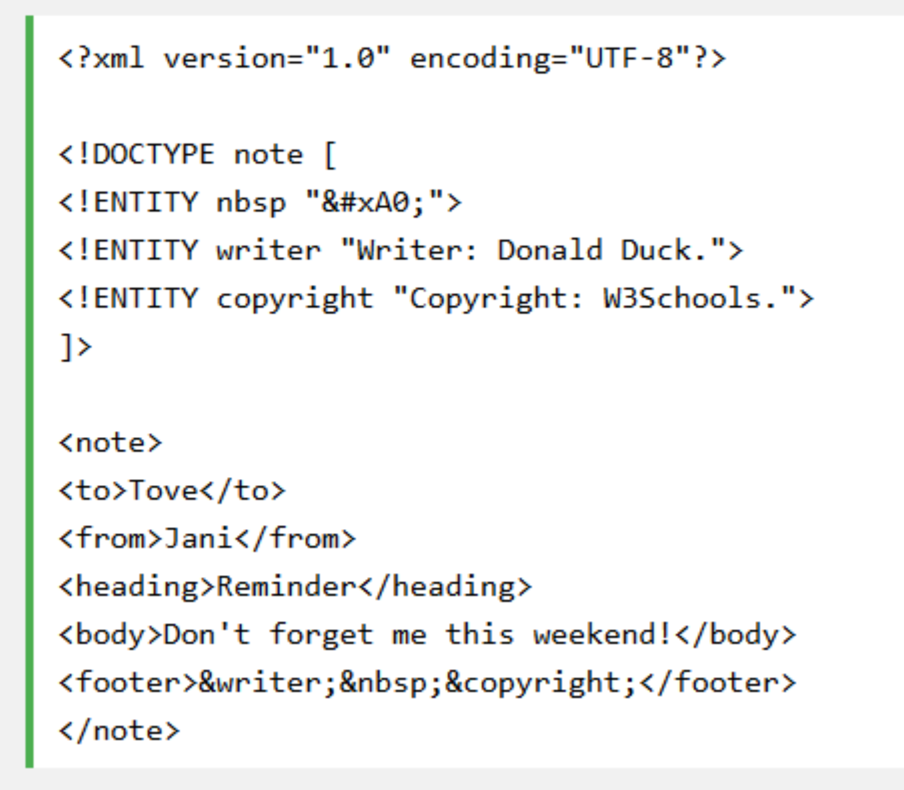
Reminder

Don't forget me this weekend!

Courtesy - www.w3schools.com

XML DTD?

- Document Type Definition (DTD) - The purpose of a DTD is to define the structure of an XML document. It defines the structure with a list of legal elements:



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

<!DOCTYPE note [
<!ENTITY nbsp "&#xA0;">
<!ENTITY writer "Writer: Donald Duck.">
<!ENTITY copyright "Copyright: W3Schools.">
]>

<note>
<to>Tove</to>
<from>Jani</from>
<heading>Reminder</heading>
<body>Don't forget me this weekend!</body>
<footer>&writer;&nbsp;&copyright;</footer>
</note>
```

- Independent groups of people can agree to use a standard DTD for interchanging data.
- You can verify that the data you receive from the outside world is valid.
- You can also use a DTD to verify your own data.
- DTD is added feature and not mandatory for XML.

Courtesy - www.w3schools.com

Can you see the security risk?

XXE

- Top 10-2017 A4-XML External Entities (XXE)
- An XML External Entity attack is a type of attack against an application that parses XML input.
- XML input containing a reference to an external entity is processed by a weakly configured XML parser
- Extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack etc.

Fix?

- The XML processor should be configured to use a local static DTD.
- Disable XML external entity and DTD processing in all XML parsers.
- Patch or upgrade all XML processors and libraries in use by the application or on the underlying operating system.
- Use JSON instead… 😉

LET'S PRAY
TO THE DEMO GODS
memegenerator.net

References

- https://www.w3schools.com/xml/xml_whatis.asp
- https://www.w3schools.com/xml/xml_dtd.asp
- https://www.owasp.org/index.php/Top_10-2017_A4-XML_External_Entities_(XXE)
- https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing
- https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet