Contents

Learning to Appreciate the Tao of the Hack

Hackers can be categorized into a series of different types, for instance: Crackers, Script Kiddies or Kidiots, Phreakers, White Hats, Black Hats, and many more. Hackers can be many things—however one thing that all hackers have is a love of a challenge and the ability to stretch their computing knowledge—whether it be for noble or ignoble motivations.

The Seven Classes of Attack

- Denial of service
- Information leakage
- Regular file access
- Misinformation
- Special file/database access
- Remote arbitrary code execution
- Elevation of privileges

Well-Formed XML Documents

When developing an XML document, certain rules must be followed:

- The document must have exactly one root element.
- Each element must have a start-tag and end-tag.
- The elements must be properly nested.
- The first letter of an attribute's name must begin with a letter or with an underscore.
- A particular attribute name can appear only once in the same start-tag.

Answers to Your Frequently Asked Questions

Q: Can DTDs and schemas be used together?

A: Yes, they can. It's perfectly acceptable to define the structure of data with a DTD and constrain the contents of the structure with a schema.

XML Signatures Can Be Applied in Three Basic Forms

- **Enveloped form** The signature is within the document.
- **Enveloping form** The document is within the signature, as shown in the following example.
- **Detached form** The signature references a document that is elsewhere through a universal resource identifier (URI).

Tools & Traps…

IBM's XML Security Suite

Although IBM is planning to release a new version relatively soon, we cover some points of XML Security Suite here:

- **XML signatures** Verify a digital signature, canonicalize a document, and verify its form as well as XPATH transformations.
- **Nonrepudiation** It is designed to provide nonrepudiation.
- **Java** It is written in Java, hence, you must be running Java to use the security suite.

Tools & Traps…

Viewing XML Files

If you want to view an XML file as it would be parsed, simply use your Web browser to open the file. Most current Web browsers have built-in XML parsers that allow you to view XML files in an expandable/collapsible format. In addition, some even support the use of DTD files to verify the format of your XML file.

.NET Code Access Security Model

The .NET code access security model is built around a number of characteristics:

- Stack walking
- Code identity
- Code groups
- Declarative and imperative security
- Requesting permissions
- Demanding permissions
- Overriding security checks
- Custom permissions

Deciding How Much Detail to Publish

- Take great care in deciding whether or not you want to provide exploit code with your NSF report. Be aware that there are times when exploit code is necessary for reporting the problem.
- You must be prepared to take a slight risk when reporting security flaws. You could end up facing the vendor's wrath or imposing undue risk on the public at large.
- Be extra cautious in describing any security flaw that requires the circumvention of a vendor's copyright protection mechanisms, as this is a very gray area for the time being.