This document will describe the OWASP DEF (Data Exchange Format).

1st. Let me say that i suck at writing documentation so bare with me on this.

q. What is the purpose of OWASP DEF?

a. Well the purpose of the OWASP DEF is to have a unified format that should cover any / all information related to Dynamic, Static, Information gathering and Attack / Brute force scanning software.

q. Will this format be free for anyone to use?

a. Yes it will be free for any one to adapt and use in their projects.

OK lets descripe the format as it looks today (14-05-2014).

This is the Root, and it should hold the information about the version of DEF.

<DEF SpecVersion=*"0.1"*>

Then we have the Session-refrence, this should hold an overall refrence the the session that is contained in this XML file.

<Session-reference>Scan of this and that web application</Session-reference>

Then we have Date-Time refrence, this is when the scan was done, atm. in any date time format.

<Date-time>*12/14/2010 3:42:16 AM -06:00*</Date-time>

Then we have the Scan refrence, this holds the type of scan that is done, and atm. it can be either dynamic, static or info. And I will start with describing the Dynamic format.

<Scan type=*"dynamic"*>

In the Dynamic section of this format we will have some basic information about the target that we scanned, for this we have a Host section, wich holds the name of the host, and the IP Address.

<Host name=*"www.example.com"* ip-address=*"1.1.1.1"*>

Then we have the Port section, this is used for the basic information about the protocol and port the scan was done against.

<Port protocol=*"tcp / udp"* portid=*"80"*>

Then we have the Service section, and this holds some basic information about the service name, service product and the service product version.

<Service name=*"http"* product=*"Apache httpd 2.2.3"* version=*"1.0"* />

Then we have the Software-name section, and this holds the name of the Software that did the scan.

<Software-name>ZAProxy</Software-name>

Then we have the Software-version section, and this should hold the version of the software that did the scan.

<Software-version>2.2.2</Software-version>

Then we have the Software-arguments, and this should hold the arguments that where used to preform the scan.

<Software-arguments>Arguments used to perform the scan</Software-arguments>

Then we have the Vulnerability section, and this holds the severity of the current vulnerability, wich can be one of: Critical, High, Medium, Low, Informational, (and Best Practies (Ath time of writing this it is not decided if the latter should be included or not, this is dependent on how many of the softwares that actually uses this).

<Vulnerability Severity=*"Critical"*>

Then we have the Finding section, and this hold the NativeID and IdentifiedTimestamp, wich are the unique plugin / test ID from the software, and a time stamp of when this vulnerability was found.

<Finding NativeID=*"12345"* IdentifiedTimestamp=*"12/14/2010 3:42:16 AM -06:00"*>

Then we have the Summary section, and this holds a short one line summary of the vulnerability.

<Summary>A sort (one line) description</Summary>

Then we have the Description section, and this hold a longer description of the vulnerability.

<Description>More detailed description</Description>

Then we have the Further-info section, and this hold further information about the vulnerability, and could for example hold a link to the OWASP Top Ten or any other ressource.

<Further-info>More information about this specific issue</Further-info>

Then we have the Confidence section, this hold the confidence level that the software have about this vulnerability, and can be a number between 0 and 10, where 0 equal not provided, and 10 equals the highest confidence we have.

<Confidence>0 thru to 10</Confidence>

Then we have the Background section, and this hold some background information about the vulnerability.

<Background>More info on the type of issue</Background>

Then we have the Remediation section, and this hold remediation information for the vulnerability.

<Remediation>Advise on how to fix the issue</Remediation>

Then we have the Classification section, and this hold the classification type, id and url to the specified id for this vulnerability, this could as the example shown be the CWE classification.

<classification type=*"CWE"* id=*"CWE79"* url=*"http://www.cvedetails.com/cwe-details/79/Failure-to-Preserve-Web-Page-Structure-039-Cross-site-Scr.html"* />