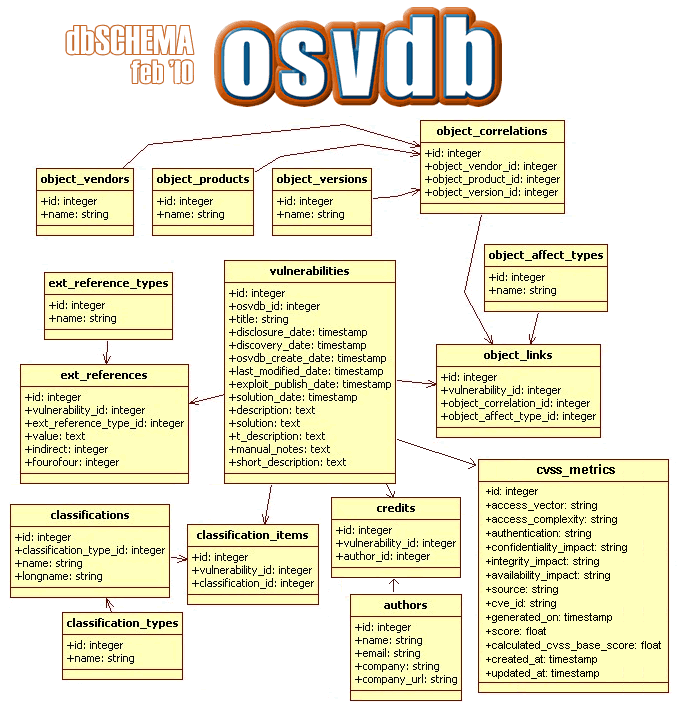
Báo cáo về Open Source Vulnerability Database<OSVDB>

Đây là một kho dữ liệu mã nguồn mở về các lỗ hổng bảo mật được xây dựng từ năm 2002 , đến nay cơ sở dữ liệu hiện tại gồm hơn 60.000 vuls<tính đến 11-2009-> ,được sử dụng trong một số ứng dụng quét vuls <quen thuộc là Nessus>.

Đây là cấu trúc dữ liệu lưu trong OSVDB<http://osvdb.org/database\_info>:



Ví dụ về Vul dưới định dạng XML

“”””””

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

<vulnerability>

<complete type="integer">5</complete>

<created-on type="datetime">2003-02-21T02:10:00-05:00</created-on>

<cve-description></cve-description>

<description></description>

<disclosure-date type="datetime">2000-02-27T00:00:00-05:00</disclosure-date>

<disclosure-source-id type="integer"></disclosure-source-id>

<discovery-date type="datetime">1970-01-01T00:00:00-05:00</discovery-date>

<exploit-publish-date type="datetime">1970-01-01T00:00:00-05:00</exploit-publish-date>

<keywords></keywords>

<manual-notes></manual-notes>

<osvdb-id type="integer">1234</osvdb-id>

<promoted-on type="datetime"></promoted-on>

<short-description></short-description>

<solution></solution>

<solution-date type="datetime">1970-01-01T00:00:00-05:00</solution-date>

<t-description></t-description>

<title>Lynx Long URL Overflow Vulnerabilities</title>

<updated-on type="datetime">2007-12-12T00:25:12-05:00</updated-on>

<user-id type="integer"></user-id>

<ext-references>

<ext-reference>

<ext-reference-type-id type="integer">3</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>2000-0209</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">5</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>1012</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">19</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>28149</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">24</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>http://downloads.digium.com/pub/security/AST-2007-027.pdf</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">3</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>2007-6430</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">30</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>http://www.securityfocus.com/archive/1/archive/1/485287/100/0/threaded</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">33</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>http://downloads.digium.com/pub/security/AST-2007-027.html</a></value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">5</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>26928</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">38</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>ADV-2007-4260</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">31</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>1019110</value>

</ext-reference>

<ext-reference>

<ext-reference-type-id type="integer">13</ext-reference-type-id>

<fourofour type="boolean">false</fourofour>

<indirect type="boolean">false</indirect>

<value>39124</value>

</ext-reference>

</ext-references>

</vulnerability>

””””””

Về truy suất dữ liệu trên OSVDB:

Dữ liệu trên OSVDB sẽ được cập nhật vào 1AM mỗi sáng theo giờ chuẩn quốc tế.

Dữ liệu có thể xuất ra dạng XML ,CSV ,MySQL dump file…

Cách thức xây dựng cơ sở dữ liệu từ file XML của OSVDB

Trước hết sử dụng đoạn mã SQL trong link sau <http://osvdb.org/OSVDB-tables.mysql> để xây dựng hệ thống các bảng dữ liệu cần thiết

Down file XML của OSVDB từ link <http://osvdb.org/exports>

Sử dụng tool sau <http://osvdb.org/files/xmldbImport.pl> <đây chẳng qua là đoạn mã perl> để import nội dụng từ file XML vừa down vào trong hệ thống các bảng dữ liệu đã tạo sẵn..

Finish…..

Question:

1. [Thi] Cấu trúc dữ liệu trong OSVDB là như thế nào? Nó không giống với cấu trúc các table trong cơ sở dữ liệu được tạo ra bằng đoạn SQL.