Global Information Assurance Certification Paper

Aggregating Vulnerability Information from Current White-Hat Databases

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Sriram Polepeddi
January 18, 2005

Abstract/Summary

Where does one go to find information on a vulnerability? Quite often it is to an online vulnerability database. Unfortunately, an all-encompassing, consolidated vulnerability database does not currently exist. So this begs the question, "Which vulnerability databases are the best sources for the vulnerability information I need?"

This work surveys the state of current, white-hat vulnerability databases, enumerating the vulnerability information available on each and discussing possible drawbacks and limitations of some databases. This guide will thus allow one to limit their search to only those databases that hold the information they desire. Next, methods of aggregating vulnerability information based on CVE ID are given. Lastly, a summary of information currently missing from all vulnerability databases and other open issues in the field is provided. The main goal of this paper is to illustrate ways to gather as complete information as possible on a vulnerability using current tools and databases.

Table of Contents

List of Tables

List of Figures

Introduction

Today's computers and networks are plagued by an increasing number of software vulnerabilities. The heterogeneity of vulnerable software and the multitude of providers of error-ridden software result in a myriad exploits by which computers can be compromised. Information about these vulnerabilities is collected and disseminated via various large publicly available databases. However, one comprehensive vulnerability database, which holds all information on a vulnerability does not exist at present.

Reasons why a single such database of vulnerabilities has not been available till today, include[1]:

1. Non-uniform methods by which current vulnerability database providers receive information from vendors, white-hat hackers, and the public, requiring the modifying of each input to their particular database schema.
2. General disagreement over which features of a particular vulnerability are important and how best to present them.

Many databases claim to consolidate all available information, yet miss out on one aspect or the other. Currently the best way to get all required information is to manually query each of the databases in turn. However, given the vast variety of vulnerability databases, it is necessary to know which database or how many databases to query to find required vulnerability information.

Contribution of This Paper

This work will review current popular, white-hat vulnerability databases and discuss the information currently available in each database. A "white-hat" is defined by wikipedia© as: "a name that describes a person who is ethically opposed to the abuse of computer systems.[2]" In this context, I use "white-hat databases" to refer to the many good vulnerability information sites that exist, in which the public place a high level of trust. In addition, these are databases that would not likely be blocked by an organization's web surfing policy. Once the current major white-hat vulnerability databases have been presented and compared, I will walk the reader through two methods of aggregating vulnerability information desired from those databases.

The five databases presented here were chosen based on their relevance to the industry and/or vendor-neutrality. The SecurityFocus, ICAT, CERT Vulnerability Notes, OSVDB and X-Force databases have been chosen for review due to their popularity. Microsoft's Security Bulletin database though commonly referenced and containing useful insights into Microsoft's products, was not chosen for review here as it presented vulnerabilities in only their products. A notable

[1] OSVDB: Aims.
[2] "Whitehat Definition."

mention, not surveyed in this work, is Lawrence Livermore National Labs' CAIC database. Upon reviewing the information presented in the other databases, it was felt that the CIAC database contained no additional data.

Importance of CVE

Before the vulnerability databases are introduced, it is important to understand the CVE concept. CVE stands for Common Vulnerabilities and Exposures[3], and is possibly the *de facto* naming convention for vulnerabilities as, currently, over 200 products and services from over 100 organizations are CVE-compatible[4]. The stated goal of the CVE project is merely to be a vulnerability dictionary[5], which can provide a unique ID for a particular vulnerability. Other vulnerability databases and products can then reference this unique ID. CVE adoption by the reviewed vulnerability databases will be important in the two vulnerability data aggregation sections below as it serves as the glue to bind data from different sources together.

[3] CVE Home Page.
[4] CVE-Compatible Products and Services.
[5] About CVE.

Vulnerability Database Survey

Individual Vulnerability Database Summary

An in-depth look at each of the vulnerability databases is given below, along with:

1. The number of references by CVE. The manner of arriving at this data is given in the appendix.
2. Its acceptability to the industry, one measure being the number of products and services that reference it.
3. The vulnerability information presented in each.

The information presented is accurate up to the date this work was submitted. However, other than OSVDB, which may still tweak its schema over the coming years, the rest of the database schemas should remain more or less steady in the future.

US-CERT:

Though the US-CERT Vulnerability Notes Database (CERT-VN) contains useful information on a vulnerability, including additional features such a severity metric, this database was not highly referenced by CVE. Of CVE's 39,534 external references, only 465 entries refer to CERT Vulnerability notes. Though CERT-VN contains a lot of valuable information, and is highly respected in the industry, its low reference by CVE suggests that information presented in it is available elsewhere. A likely reason for this is the conservative approach taken by CERT in releasing vulnerability information to the public. CERT's full disclosure guidelines state that they will release vulnerability information "45 days after its initial report, regardless of the existence or availability of workarounds", unless "extenuating circumstances require an earlier or later disclosure."[6] The reality tends towards a later disclosure. It must be noted that CERT maintains a larger, internal list of vulnerabilities, even prior to public disclosure, but these entries were not available for review in this work. The effect of CERT's goal and ,perhaps, a duty to act in the "best interests of the community overall" is a public database updated much later than others.

Table 1: Vulnerability information in CERT Vulnerability Notes database

Vulnerability Title	A short description of the vulnerability.
Overview	A text description of possible affected targets and the cause of the vulnerability.
Impact	A text description of the consequence of an exploit.
Solution	Descriptions of workarounds or links to patches, when available.
Systems Affected	Information on vulnerable products and versions.
CVE Name	The vulnerability's CVE ID, when available.

[6] CERT/CC Vulnerability Disclosure Policy.

Metric	CERT's severity rating. A vulnerability alert is sent out if this rating is above 40.0.

Full descriptions of these fields can be found at: http://www.kb.cert.org/vuls/html/fieldhelp#metric

BugTraq:

The SecurityFocus Database, which uses BugTraq IDs is also well-respected by the industry. However, Symantec bought it in 2002 and while they have regularly posted a few Symantec product vulnerabilities per month[7], no guarantee exists that they will continue to do so in the future. Also, while BugTraq IDs are well-known, no list of products asserting BugTraq-compatibility was found. However, judging by the 4122 external references from CVE, I feel it is a safe call to say SecurityFocus is a very accepted vulnerability database.

Table 2: Vulnerability information in SecurityFocus database

Object	No description is given for this field.
Class	The class of vulnerability, which can be among any of the following: Boundary Condition Error, Access Validation Error, Input Validation Error, Origin Validation Error, Failure to Handle Exceptional Conditions, Race Condition Errors, Serialization Errors, Atomicity Errors, Environment Errors, Configuration Errors.
Remote/Local	Whether remotely or locally exploitable.
Vulnerable/Not Vulnerable	Whether particular software is or is not vulnerable to exploit.
CVE ID	The vulnerability's CVE ID, when available. BugTraq has done an excellent job of referencing back to CVE in most of their records.
Discussion	A text description of possible affected targets and consequences.
Exploit Code	Provided when available.
Solution	Descriptions of workarounds or links to patches are given when available.

Full definitions of these fields is available at: http://www.securityfocus.com/bid/11965/help/

ISS X-Force:

The Internet Security Systems' X-Force database, publishing vulnerability information since 1994, is one of the oldest repositories of vulnerability information. ISS is one of the founding members of CVE, and is referred to by CVE 4920 times.

It is under proprietary control; ISS alone manages the structure and entries in the database. As ISS is also a vendor of software products, the potential for reporting discrepancies may arise wherein X-Force may release competitor's information early, without proper checking, and be slower to add vulnerabilities in its own products claiming they are verifying the accuracy of the vulnerability claim. While no proof is available this is the case, the X-Force FAQ[8] clearly allows for potentially adding inaccurate information. In Section 2.6, it admits that X-Force will add a third-party product's vulnerability data "based on the credibility of the source reporting the issue." It further states that it will only remove such an entry if the "non-existence of the security issue" is reported by a credible source. Therefore, a great deal of ambiguity regarding what constitutes

[7] "Symantec Vendor Search."

[8] X-Force FAQ.

a "credible source" exists, and is solely determined by the needs of X-Force. The only possible value-add the X-Force database represents is in terms of its Risk Level Ratings. Yet, from X-Force FAQ's description, the criteria for choosing between the three risk levels is ambiguous and arbitrary.

Table 3: ISS X-Force Risk Level Criteria from X-Force FAQ[9]

High	Security issues that allow immediate remote or local access, or immediate execution of code or commands, with unauthorized privileges. Examples are most buffer overflows, backdoors, default or no password, and bypassing security on firewalls or other network components.
Medium	Security issues that have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures, or low risk issues applied to major Internet components. Examples are cross-site scripting, man-in-the-middle attacks, SQL injection, denial of service of major applications, and denial of service resulting in system information disclosure (such as core files).
Low	Security issues that deny service or provide non-system information that could be used to formulate structured attacks on a target, but not directly gain unauthorized access. Examples are brute force attacks, non-system information disclosure (configurations, paths, etc.), and denial of service attacks.

Table 4: Vulnerability information in X-Force database

Title	A short description of the vulnerability.
Description	A text description of possible affected targets and the cause of the vulnerability.
Risk Level	Can be Low, Medium or High.
Consequences	A text description of the consequence of an exploit. Can be any of: Gain Access, Gain Privileges, Bypass Security, File Manipulation, Data Manipulation, Obtain Information, Denial of Service (DoS), Configuration, Informational, Other or None.
Remedy	Descriptions of workarounds or links to patches are given when available.
Platforms Affected	Information on vulnerable products and versions.

Descriptions of these fields can be found at: http://xforce.iss.net/xforce/xfaq/#3

OSVDB:

The Open Source Vulnerability Database project was started in 2002 in order to satisfy the industry's need for an "independent and open source[10]" vulnerability database and opened to the public on March 31, 2004. While still a young database, it is gaining in acceptance. Currently, OSVDB IDs are supported by 3 open-source products: Nikto, Snort and Nessus[11]. OSVDB is referenced 718 times by CVE.

The OSVDB schema is still in a state of flux. I loaded the OSVDB on my local system in June 2004. They then modified the schema in July 2004, changing the way they represented vulnerable products, requiring the local schema to be re-loaded from scratch. While the schema has not changed since then and I do

[9] X-Force FAQ.
[10] OSVDB Home Page.
[11] OSVDB: Compatibility.

not expect this instability to continue for long, another schema change cannot be ruled out in the near future. The current schema is available at: http://osvdb.org/database-info.php#databaseschema

Table 5: Vulnerability information in OSVDB database

Title	A short description of the vulnerability
Location	Can be any one of the following: Physical, Local, Remote, Telephony or Unknown.
Attack Type	Can be any one of: Authentication Management, Cryptographic, Denial Of Service, Hijacking, Information Disclosure, Infrastructure, Input Manipulation, Misconfiguration, Race Condition, Other or Unknown
Impact	Can be: Loss of Confidentiality, Integrity or Availability
Exploit	The current status of the exploit for this vulnerability. Can be either: Available, Unavailable, Rumored / Proof or Unknown
OSVDB Specific	OSVDB's rating of the certainty of the information. Can be: Verified, Myth/Fake, Best Practice, Concern or Web Check
Solution	Descriptions of workarounds or links to patches are given when available
External References	The other databases which list information on this vulnerability.
External Text	Where the long, free form text details on a vulnerability are stored. Includes Vulnerability Descriptions, Technical Descriptions (clarifications), Manual Testing Notes and/or Solution Descriptions
Products	Information on vulnerable products.

Full descriptions of these fields can be found at: http://osvdb.org/vuln-standards.php#5

ICAT:

The ICAT database is maintained by the National Institute of Standards and Technology and uses CVE IDs for its primary key, hence every CVE ID is also an ICAT ID. ICAT once was the acronym of an Internet Hacker attack database, but shifted its function to simply an index of computer vulnerabilities[12], with the original meaning long forgotten. ICAT claims not to be a vulnerability database, but a "searchable index leading one to vulnerability resources and patch information[13]," yet it has all the trappings of any other vulnerability databases reviewed here. So, if it looks like a database, quacks like a database and walks like a database, then …

Though tightly integrated with CVE, ICAT suffers a lesser acceptance than the other databases, with currently only one ICAT-based product, CERIAS's Cassandra available[14]. In fact, that CVE is slow to add new vulnerabilities and that ICAT is even slower in updating its CVE version mappings could be the reason it is not as accepted as BugTraq or even OSVDB.

[12] ICAT Frequently Asked Questions.
[13] ICAT Metabase Documentation.
[14] ICAT Based Vulnerability Notification Systems.

Table 6: Vulnerability information in ICAT database

Published Before	Indicates where when this vulnerability was discovered. Is often not populated.
Summary	A short description of the vulnerability. Is most often the same as the CVE Title for that vulnerability
Severity	Can be: Low, Medium or High
Vulnerability Type	Can be: Access Validation Error, Input Validation Error, Design Error, Exceptional condition handling error, Race Condition, Environmental Error, Configuration Error or Other.
Loss Type	Can be: Loss of Confidentiality, Integrity, Availability or Security Protection.
Exposed Component	Can be any of these: Operating system, Protocol stack, Server application, Non-server application, Hardware, Communication protocol, Encryption module, and/or Other.
Exposed System Type	Can be any of these: Server, Workstation, Networking/Security device and/or Other.
Vulnerable Software	Information on vulnerable products and versions.

Full descriptions of these fields can be found at: http://icat.nist.gov/icat_documentation.htm

Database Comparison and Rankings

Each of the databases covered in this paper have their pros and cons. Table 7 highlights the differences is based on the individual database summaries above. The databases are ranked in Table 2 in terms of the best overall database, then the second best, etc. This section should be used as a ready reference for quickly deciding on which vulnerability database to turn to first.

Table 7: Vulnerability Database Overview

	Data Sources				
Vulnerability Database Criteria	**CERT**	**SecurityFocus**	**ISS X-Force**	**OSVDB**	**ICAT**
Up-to-date?	Slow	Yes	Yes	Yes	Mostly
Control over database	Proprietary	Proprietary & Vendor	Proprietary & Vendor	Open	Proprietary
Number of Vulnerability Features listed	5	6	5	8	7
Number of records	1327	12,276	18,937	6019 (stable)	7463
References by other products & services	DNK	DNK	DNK	3	1
DB Export files available?	No	No	No	Yes	Yes
My Ranking	**5**	**1**	**4**	**2**	**3**

Note: "DNK" means that the information was not easily available. For the "Number of features listed" value, data fields such as dates and titles were not included.

Table 8: Vulnerability Database Rankings

Rank	Database	Rationale
#1	**SecurityFocus**	After X-Force, SecurityFocus contains the second largest number of vulnerabilities, but holds more information on each vulnerability than X-Force. In addition, SecurityFocus's search capability is more powerful than X-Force. The combination of these factors and the industry's familiarity with SecurityFocus are more than enough to overcome its proprietary nature and possible questions of conflict-of-interest due to its ownership by a software vendor.
#2	**OSVDB**	Stores the most information per vulnerability and is referenced by at least 3 other vulnerability scanning tools.
#3	**ICAT**	ICAT's IDs are fully CVE-compatible and it covers a wide range of vulnerability attributes.
#4	**ISS X-Force**	The large number of vulnerability records is difficult to overlook at this point.
#5	**CERT**	Can be trusted to provide reliable information, but is simply too slow to add vulnerabilities.

The information for Table 7 above can be found at the following locations:

- BugTraq: http://www.securityfocus.com/bid/
- ICAT: http://icat.nist.gov/icat.cfm
- OSVDB: http://www.osvdb.org/search.php
- CERT: http://www.kb.cert.org/vuls/
- X-Force: http://xforce.iss.net/xforce/search.php

Vulnerability Data Aggregation

Method 1: Manually Querying Web Databases

Now that we've seen what information is available on each vulnerability database, we need to bring together required information. Each database has a search page from which one can lookup information in that database.

There are 3 types of searches available on vulnerability sites:

1. General Search: This search allows one to search on multiple characteristics of a vulnerability, such as vendor, class and affected component at once.
2. Keyword Search: This search is comprised of a simple text area, and any words entered here will be queried for in every field of the database.
3. Single Criteria search: This is a search which narrows down the records based on only 1 characteristic of a vulnerability, such as affected software, vendor, CVE ID or publish date. These searches often only allow this 1st level of query, returning very long lists of results if there are many matches.

Table 7 presents the URLs to the search pages of each vulnerability database.

Table 9: Vulnerability Database Search Page URLs

Database	Type	Search Page
Security Focus	Keyword	http://www.securityfocus.com/bid/keyword/
	Vendor-based	http://www.securityfocus.com/bid/vendor/
OSVDB	General	http://osvdb.org/search.php
ICAT	General	http://icat.nist.gov/icat.cfm
CERT	General	http://www.kb.cert.org/vuls/html/search
X-Force	Keyword	http://xforce.iss.net/xforce/search.php/

For illustration, let us suppose we suspect a vulnerability in the ACME Labs web server, Acme.serve™, and we want the following information on it: exploit code, solution information and severity. This requires querying each database in turn for the vulnerability with the desired CVE ID. We could start with any one the major databases: SecurityFocus, OSVDB, ICAT, etc., but SecurityFocus has the cleanest way to query based on vendor.

Here is a potential series of steps that can be followed:

Database 1: For exploit code and solution information, we visit SecurityFocus's Vendor vulnerabilities page: http://www.securityfocus.com/bid/vendor/ and select ACME Labs from the "vendor" pull-down menu and "Acme.serve" from the Title pull-down menu. We can set the version pull-down menu as well, but this is optional.

This search returns 1 result:

2002-07-02: Acme.Serve v1.7 Arbitrary File Access Vulnerability

Clicking on this result takes us to a INFO page listing the vulnerability's basic details. We see in Figure 1 that the Vulnerability's CVE ID is: CVE-2001-0748. However, we only need concern ourselves with the "2001-0748" portion, as the prefix, CVE or CAN only suggests whether this vulnerability is on the permanent list of CVE vulnerabilities or not[15].

Figure 1: Info page for BugTraq ID #2809[16]

VULNERABILITIES

Acme.Serve v1.7 Arbitrary File Access Vulnerability

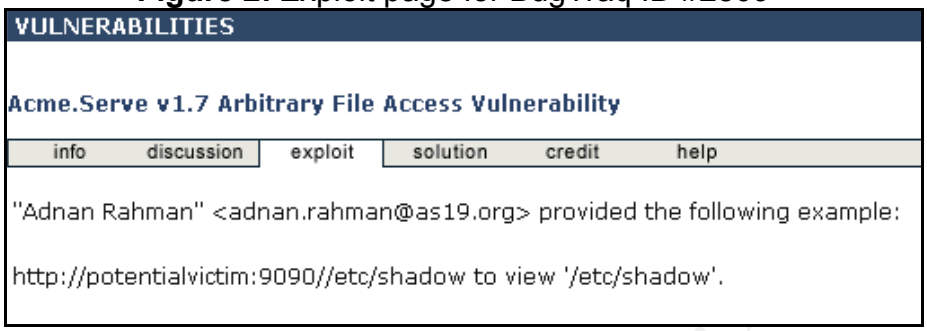
info | discussion | exploit | solution | credit | help

bugtraq id	2809
object	Acme.Serve.Serve
class	Design Error
cve	CVE-2001-0748
remote	Yes
local	No
published	May 31, 2001
updated	Jul 02, 2002
vulnerable	ACME Laboratories Acme.Serve 1.7 Cisco Secure ACS for Unix 2.0 Cisco Secure ACS for Unix 2.3 Cisco Secure ACS for Unix 2.3.5 .1
not vulnerable	Cisco Secure ACS for Unix 2.3.6 .1

[15] The CVE Naming Process.
[16] "BID 2089 - Acme.Serve v1.7 Arbitrary File Access Vulnerability," Info Page.

Next, we click on the EXPLOIT link and get the following page.

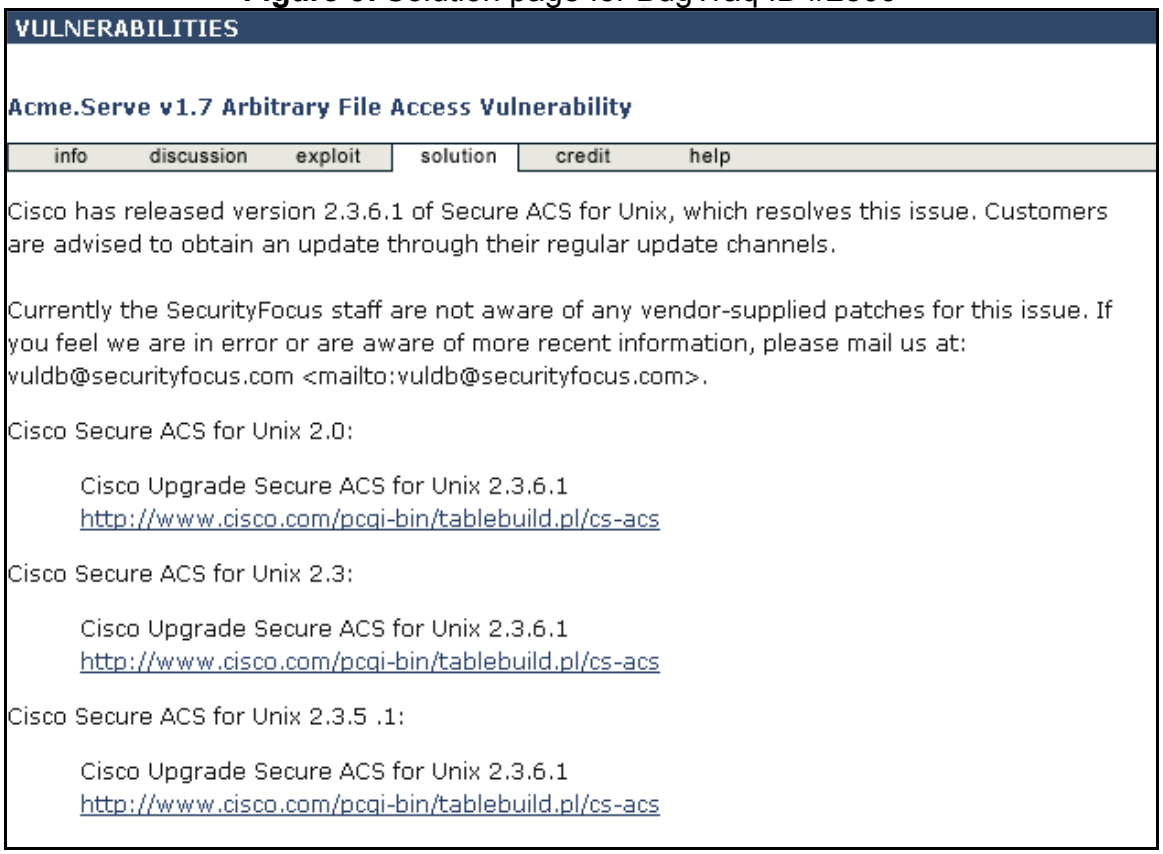
Figure 2: Exploit page for BugTraq ID #2809[17]



In this case, there is no exploit code, but only a proof-of-concept of what an affected system would be capable of.

Next, we click on the SOLUTION link for possible patches or workarounds and get the following page.

Figure 3: Solution page for BugTraq ID #2809[18]



In this case, the only solution is to upgrade to the next version.

[17] "BID 2089 - Acme.Serve v1.7 Arbitrary File Access Vulnerability," Exploit Page.
[18] "BID 2089 - Acme.Serve v1.7 Arbitrary File Access Vulnerability," Solution Page.

Database 2: To verify this information or to search for more information, we visit OSVDB' search page: http://osvdb.org/search.php. Now that we have the vulnerability's CVE ID, we simply enter "2001-0748" in the references textbox, which returns the following.

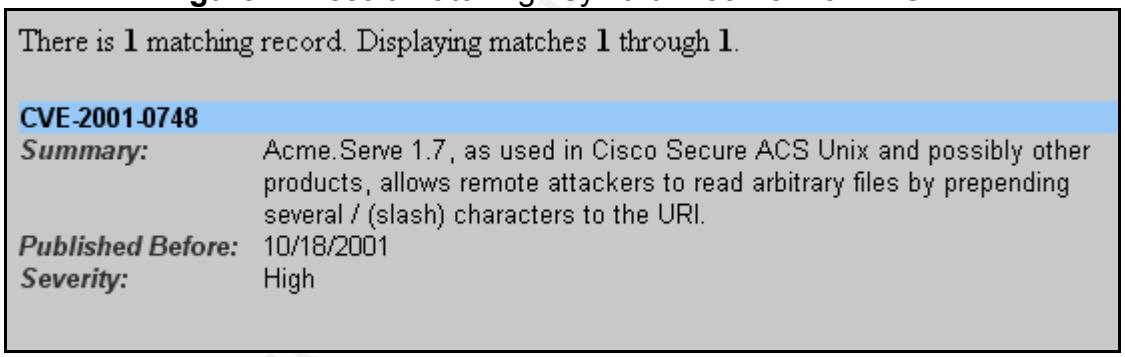
Table 10: OSVDB Search Page: Keyword "2001-0748" Result

OSVDB ID	Title	Disclosed	Status
5544	Acme.Serve URI Slash Arbitrary File Access	May 31, 2001	Stable

Clicking on OSVDB ID #5544 takes us to a page containing more details on the vulnerability[19]. We find there most of the same information as SecurityFocus, thus verifying the information found there. At times, however, additional information may be found and it is always important to check. In the External References section of this page, the BugTraq ID is 2089, which matches the BugTraq ID in Figure 1. This is additional confirmation that we are dealing with the same vulnerability.

Database 3: To find out this vulnerability's severity rating, we visit ICAT's search page: http://icat.nist.gov/icat.cfm. We again enter the CVE ID: "2001-0748" in the Keyword Search text box, which returns the following result.

Figure 4: Result matching keyword "2001-0748" in ICAT



Summary: Thus we see that this vulnerability is of High severity and has no workarounds or patches with upgrade being the only solution. Note that the order of databases we visited was not important; a similar procedure could have been begun at OSVDB or ICAT for instance.

Method 2: Loading Database Export Files Locally

Another option exists if visiting each website seems like too painstaking a process. Vulnerability databases such as ICAT and OSVDB provide daily/monthly exports of their databases, which can be loaded into a local database for easier query. Both databases provide a straightforward method of accessing the information once downloaded.

[19] "OSVDB ID 5544 - Acme.Serve URI Slash Arbitrary File Access."

ICAT: Provides a Microsoft Access 2000-ready MDB file. Simply download the latest file from http://icat.nist.gov/icat.zip and query it for the desired data. This is not much different than querying on the ICAT site, except that the information is local. ICAT also provides basic and full database exports in Tab-delimited files, but these require some scripts to be written to load into a database.
The text and Access–ready ICAT exports can be downloaded here: http://icat.nist.gov/icat.cfm?function=download.

OSVDB: Provides ready-made database schema creation and loading scripts for PostgreSQL/mySQL and XML exports of the database. Once those particular database servers are installed, one simply runs the relevant scripts as the administrator for that database, and the database is loaded locally. The database scripts and XML exports for OSVDB can be downloaded here: http://osvdb.org/database-info.php.

If one can load the ICAT and OSVDB data into the same database, one can create applications to extract information from both at the same time. For example, we could have simply queried for all ICAT information for a CVE ID that a particular OSVDB vulnerability had.

Missing Information

No Causal Information:
Current databases are missing causal information on the pre-conditions that vulnerabilities require to be exploited. While basic "location of exploit" information is available, the data about the pre-conditions for a vulnerability to be exploitable, such as requiring a denial of service, is still not available.

Poor Information on Preventative Measures:
"Protection barriers" are the components that may protect or isolate assets from particular attacks[20]. Very little information can be found in any of the databases on which components or procedures need to be in place to prevent a particular vulnerability or class of vulnerability from being exploited.

Incomplete CVE Adoption by the Major Databases:
The vulnerability databases covered in this paper, with the exception of ICAT, do not include a CVE ID for every vulnerability record they contain. This will lead to some records not being linkable to data existing on other databases.

No Linking of Software Products with Known, Vulnerable Libraries:
While lists of affected software are available, a more fine-grained view is required. Often, a vulnerability exists in a shared package or library between

[20] Hollingworth, p.25.

multiple applications and at times on even multiple operating systems. A detailed list of libraries and functions called by an application would yield a startlingly pinpointed view of the actual 'location' of a vulnerability. A fix at this level would trickle up and secure the higher-level packages as well. The possibility of acquiring this data is highly unlikely with COTS software, though open source developers may be more inclined to provide this data.

Open Issues

Using Non-CVE IDs as Primary Key:
Above we considered how well referenced each of the vulnerability databases were by CVE and used it to aggregate vulnerability data. This could also be done using BugTraq and OSVDB IDs, as they are also well-referenced by other sources. The use of ICAT IDs however would be irrelevant as ICAT uses CVE as its primary key.

Canonicalization of Additional Vulnerability Information:
Data from disparate fields such as vulnerability titles, descriptions and solution information, hold valuable information, yet are in different formats. For example, the vulnerability title for a buffer overflow in Sun's rpc daemon has the following titles in various data sources:

Table 11: Vulnerability Titles in Various Databases

ICAT	Buffer overflow in NIS+, in Sun's rpc.nisd program[21]
SecurityFocus	Multiple Vendor NIS+ Buffer Overflow Vulnerability[22]

They each convey the same idea easily for a human reader, yet, differences still exist among them. Likewise, certain OSVDB and SecurityFocus records contain solutions for their respective vulnerability, yet they are not in a common or standardized format.

Canonicalizing this data requires, first, that templates are agreed upon to store desired information in a vulnerability title, description or solution text. Then, a decision tree must be created to unambiguously populate these templates from the existing data. At present, this would be most accurately accomplished manually. Valuable information can, however, be gleaned from these fields by applying an intelligent data mining tool. This tool needs to know both the syntactic and a semantic meaning of the information in order to accurately parse it for keywords[23]. Once keyword parsing is complete, the templates would be automatically populated based on more intelligent decision trees in order to feed

[21] "CVE-1999-0008."
[22] "BID 104 - Multiple Vendor NIS+ Buffer Overflow Vulnerability."
[23] Liang, slide 4.

it into a database.

Appendix: Determining the Number of CVE External References to a Vulnerability Database

In the "Vulnerability Database Survey" section, we stated the number of external references to each database from CVE. The numbers in that section were derived by loading CVE data into a database and running straightforward `SELECT count(*)` SQL queries on it. CVE-MITRE provides comma-separated files for CVE and CANDIDATE vulnerabilities at: http://cve.mitre.org/cve/downloads/full-allitems.csv. The current CVE version is 20040901. The results of the queries are in Table 12.

Table 12: CVE Export External Reference Queries

External References	#
To OSVDB	718
To CERT-VN	465
To X-Force	4920
To SecurityFocus	4122
To ICAT	n/a
Total	39534

The ICAT database uses CVE IDs as its primary key and therefore has no external links here.

References

About CVE. 2005. The Mitre Corporation. 18 Jan 2005 <http://cve.mitre.org/about/>.

"BID 104 - Multiple Vendor NIS+ Buffer Overflow Vulnerability." SecurityFocus Vulnerability Database. 1999. 18 Jan 2005 <http://securityfocus.com/bid/104>.

"BID 2089 - Acme.Serve v1.7 Arbitrary File Access Vulnerability." SecurityFocus Vulnerability Database. 2002. 18 Jan 2005 <http://securityfocus.com/bid/2809>.

CERT/CC Vulnerability Disclosure Policy. 2005. CERT/CC. 18 Jan 2005 <http://www.cert.org/kb/vul_disclosure.html>.

"CVE-1999-0008." ICAT Metabase. 1998. 18 Jan 2005 <http://icat.nist.gov/icat.cfm?cvename=CVE-1999-0008>.

CVE-Compatible Products and Services. 2005. The Mitre Corporation. 18 Jan 2005 < http://cve.mitre.org/compatible/>.

CVE Home Page. 2005. The Mitre Corporation. 18 Jan 2005 <http://cve.mitre.org/>.

Hollingworth, Dennis. Towards Threat, Attack, and Vulnerability Taxonomies. Network Associates Labs, 2004. 18 Jan 2005 <http://www.laas.fr/IFIPWG/Workshops/44/W1/02-Hollingworth.pdf>.

ICAT Based Vulnerability Notification Systems. 2005. National Institute of Standards and Technology. 18 Jan 2005 <http://icat.nist.gov/icat.cfm?function=notification>.

ICAT Frequently Asked Questions. 2005. National Institute of Standards and Technology. 18 Jan 2005 <http://icat.nist.gov/icat.cfm?function=faq#1>.

ICAT Metabase Documentation. 2005. National Institute of Standards and Technology. 18 Jan 2005 <http://icat.nist.gov/icat_documentation.htm>.

Liang, Je Wei. Text Mining and Web Mining. Database Laboratory. Database Lab., Dept. of Computer & Information Science, National Chiao-Tung University. 18 Jan 2005 <http://www.database.cis.nctu.edu.tw/seminars/2003F/TWM/slides/p.ppt>.

OSVDB:Aims. 2005. Open Source Vulnerability Database. 18 Jan 2005 <http://osvdb.org/OSVDB-Aims.php>.

"OSVDB ID 5544 - Acme.Serve URI Slash Arbitrary File Access." OSVDB. 2001. 18 Jan 2005 <http://osvdb.org/displayvuln.php?osvdb_id=5544>.

OSVDB: Compatibility. 2005. Open Source Vulnerability Database. 18 Jan 2005 <http://osvdb.org/compatibility.php#products>.

OSVDB: FAQ. 2005. Open Source Vulnerability Database. 18 Jan 2005 <http://osvdb.org/faq.php#osvdbpurpose>.

"Symantec Vendor Search." 2005. SecurityFocus Vulnerability Database. 18 Jan 2005 < http://www.securityfocus.com/bid/vendor/>.

The CVE Naming Process. 2005. The Mitre Corporation. 18 Jan 2005 <http://cve.mitre.org/docs/docs2000/naming_process.html>.

"Whitehat Definition." Wikipedia Free Encyclopedia. 2005. 18 Jan 2005 <http://en.wikipedia.org/wiki/Whitehat>.

X-Force FAQ. 2005. Internet Security Systems, Inc. 18 Jan 2005 <http://xforce.iss.net/xforce/xfaq/#3>.