Oracle Security Issues
To Consider

CERT Shows a Difference

Established in 1988, the CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. This organization consistently shows ***many, many*** more reported security incidents and vulnerabilities for Oracle than for DB2. (When this research was taken, it was 230 to 5! See attached screen shots.) Why does Oracle have so many real-world problems? After all, it claims to be the "worlds most secure database" and has many security evaluations. Could it be that marketing claims and evaluations are no substitute for actual performance? We invite you to please research this for yourself.

The OS security question

UNIX is an inherently secure OS. It was one of its early claims to fame and a major factor in being readily adopted. Why do many organizations that rely on UNIX to secure so much of their other IT systems suddenly get scared into thinking they need "special" security for database authentication?

Oracle userids and passwords sync problem

Oracle database authentication userids have no way to sync with each other from database to database. Your end users must remember and juggle multiple userids and passwords for all databases, even if they are on the same server. Using OS authentication in Oracle takes care of this problem, but then you are right where DB2 is. However, you still have to define the user in each Oracle database, while you don't have to with DB2.

The Oracle schema dilemma

Each new schema in Oracle ***always requires*** another userid and password for it; in DB2 this is ***not*** the case as it uses "true" schema support. How does your shop manage all these passwords among all the DBAs who must deal with them? Many shops we've encountered have a "secret" file hidden in a certain location on the UNIX filesystem with all userids and passwords maintained by all DBAs because they need to keep track of them for every repository, every schema, every special user id, etc. Is ***this*** really safe? If your shop doesn't handle them this way, find out how your DBAs do handle this… really… with no double talk. Isn't it logical that the more userids and password you create, especially ones with DBA authority, the ***less*** safe your database is? DB2 does not require that you make so many userids with passwords just for schemas.

The Oracle default userids & passwords exposure

On a similar note: does having 32 ***default*** users with default passwords really make your database more secure?
See: http://www.tusc.com/oracle/download/author_loneyk.html and look for the article "How I broke your database" which is an exploration of this issue by Kevin Loney, an Oracle 10g expert. He shows just how many backdoors exist in the Oracle security architecture right out of the box.

The Oracle user switcheroo exposure

Oracle allows a DBA to change a user's password, log on as that user, make changes that makes it look like that user did those changes and change the password back. With DB2, this is not possible as the DBA would have to log in as that user on the OS. Having "special" DB2 knowledge alone will not enable a DBA to do this.

Oracle Security Issues
To Consider

Cost comparison: a losing proposition for Oracle

If an Oracle rep presents extra cost as a problem for DB2 because you may need to purchase Tivoli for enterprise wide security or Kerberos or some other third party security package, then ask yourself if cost is a DB2 problem or an Oracle one. It is not debatable really: Oracle is more expensive than DB2 is with equivalent offerings, sometimes by a factor of 2 or 3! Remember too, if you do want to use third party security like Kerberos for database authentication, Oracle charges you an extra fee to support it! Oracle "locks you in" to their security methodology in doing so.

The bottom line is your company is either already using an enterprise security software package or not. If it is not, you probably rely on the OS and skilled administration to deliver "secure enough" systems for all your applications and data outside your RDBMS. Securing your new DB2 database won't be any different from them. If you ***are*** using enterprise security, then you are OK too, because DB2 supports them without an extra fee. So, this should tell you not to be scared into thinking you need to buy extra software to support DB2 authentication!

On the other hand, if you are using Oracle and ***don't*** have enterprise wide security, ask yourself why the database security has to be different than all other OS secured systems? If you ***are*** using enterprise wide security, then why not use it for your Oracle database too? Could it be that Oracle charges you ***extra*** to support these other security packages so Oracle is forcing your hand ***away*** from that? Don't let Oracle security ideology force your hand to only using their methodologies.

Database security is not enterprise security

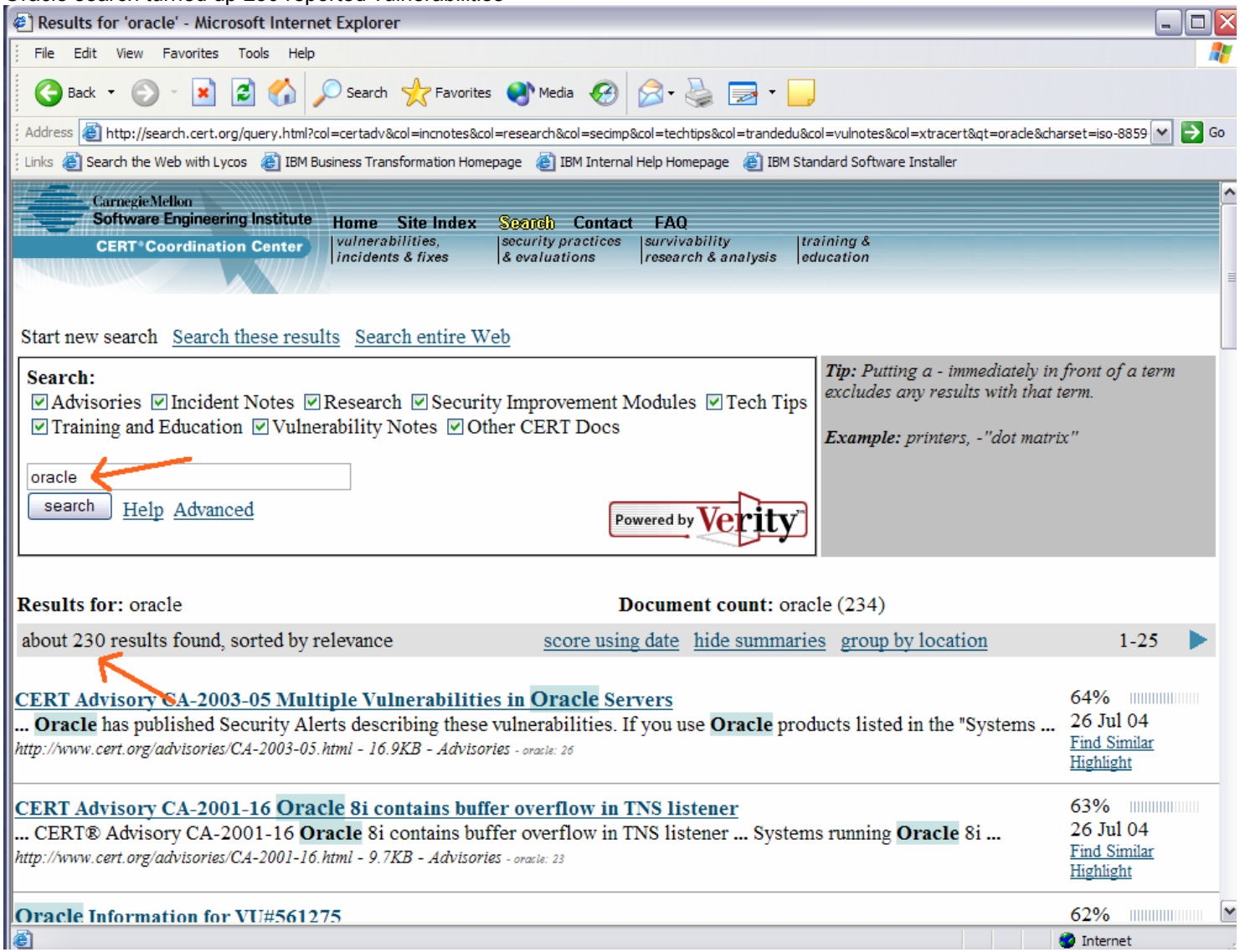
On a similar note, remember that Tivoli is an ***enterprise wide*** security solution, not just a database security solution. Don't let Oracle make you think that the cost of Tivoli for database authentication alone compares to what Oracle provides, even if you were to decide to purchase Tivoli in addition to purchasing DB2. Oracle database authentication will never compare to a Tivoli security product and doesn't even begin to play in that space.

In the light of all this, what do you think? Which database is "more secure"?

IBM sees security at the enterprise level first, as a "best of breed" solution issue that must be addressed separately from just a data base alone issue. Oracle built its company on the database first, so it inherently thinks security at the database level is all-important. Remember: *IBM has more overall security experience than Oracle does*. Oracle fixates on the database for all security and IBM does not. By the points outlined in this paper and by the www.cert.org numbers you see in the attached screen shots, you should probably be able to ascertain whose approach is succeeding.

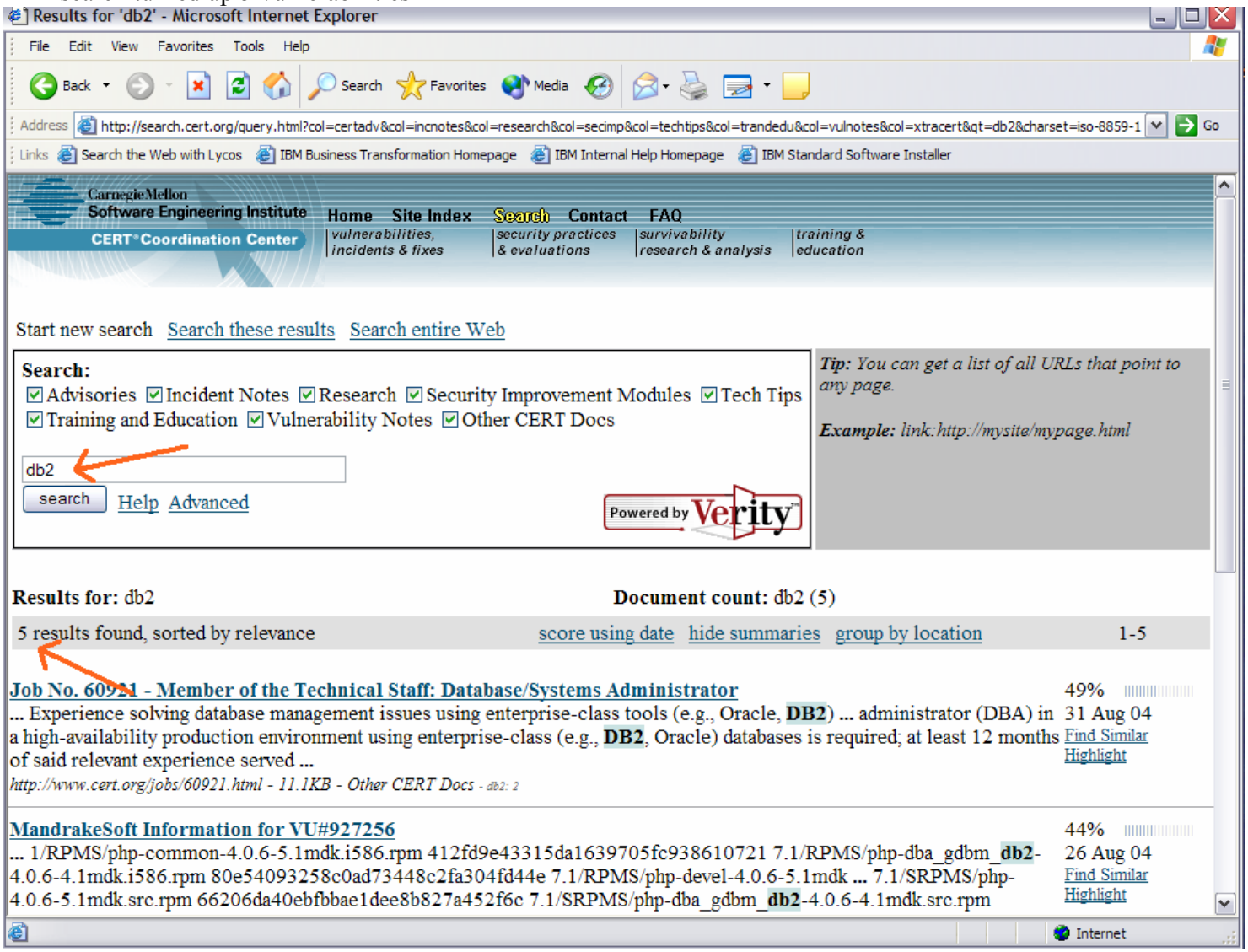
Oracle Security Issues
To Consider

WWW.CERT.ORG search on Oct 8, 2004
Oracle search turned up 230 reported vulnerabilities



Oracle Security Issues
To Consider

DB2 search turned up 5 vulnerabilities



Document by Burt Vialpando, Oct 8, 2004.