The passwords and usernames of more than 400,000 contributors to the Yahoo Voices website have been stolen and posted on the Internet.

The hack was carried out by an organization calling itself "D33Ds Company," which posted the data on the Web.

The D33Ds Web page containing the data was down when checked at press time. However, the text file is reportedly available through torrents.

The passwords were stored in clear text and not encrypted, according to TrustedSec , which disclosed news of the hack The hackers apparently used an SQL injection attack.

Safety Last

SQL injection has been used by hackers for years. This fact, and the lack of encryption of the data stolen, have led security experts to criticize Yahoo's security practices.

"The fact that they have unencrypted storage of usernames and passwords shows a lack of security practices embedded into the software lifecycle of the company," Dave Kennedy, TrustedSec's president and CEO, told TechNewsWorld.

"The only place we should be seeing SQL injection attacks today is in the classroom, as IT professionals are being trained to prevent such attacks," said Randy Abrams, research director at NSS Labs , said.

SQL injection attacks are preventable through proper filtering and sanitizing, and are "required for security," Abrams told TechNewsWorld. "The more than 300,000 results on Google for the search string 'prevent SQL injection attack' would have been useful to Yahoo."

Yahoo "did not follow the concept of least privilege, which let the hackers gain admin access to the database," Jason Rhykerd, a consult at SystemExperts , stated. This concept means giving an application the minimum of privileges it requires to conduct its business when talking to a database.

"I find it hard to believe that, if as much database information was pulled via the SQL injection as was reported, someone or better yet something, such as an intrusion detection system , did not notice it," Rhykerd continued.

Defense, Defense, Defense!

Web application security is an art rather than a science, so it's conceivable that not every type of application error or fault will be discovered, but there are mitigation techniques, SystemExperts' Rhykerd told TechNewsWorld.

For example, generic error messages that watch for SQL and other errors could warn users of such an error without leaking back application information, Rhykerd pointed out. Using a service account with least privilege and by encrypting the data would have reduced the impact of the hack.

Yahoo could have placed multiple layers of controls in place, "but this can only be done by understanding your business objectives, inventorying assets and assessing risk to recognize gaps," Rhykerd said.

Fallout From the Hack

It's not just Yahoo Voices users who are at risk. TrustedSec said the data stolen contained email addresses from other domains, including Gmail.com and AOL.com.

"This was one of many sites the hackers had access to," TrustedSec's Kennedy said. "It sounds like there are systemic issues at Yahoo."

While this kind of hack, where the data stolen is publicly posted, is usually conducted for bragging rights, "others without such neutral intent now have access to these folks' emails and passwords to use for phishing or on other sites where users may have reused their passwords," Chet Wisniewski, a senior security advisor at Sophos , told TechNewsWorld.

"The thing about SQL injection attacks is that, sometimes, the attacker gets the system root," NSS Labs' Abrams pointed out. "We don't know how deep the breach really is, or whether there is a back door lingering in the system now."

Yahoo "needs to enhance their network access controls, database security model, and to start sanitizing data input," Abrams continued. "This was preventable."

By Richard Adhikari
TechNewsWorld