Date: 10/19/2012

Case Study: PENETRATION TESTING AUDIT

Preface: Penetration testing AKA pen-testing is a process where a tester looks for exploitable vulnerabilities from within an IT infrastructure that may allow the tester to subvert, modify and extract information.

The Case: A Hedge Fund client with more than $21 billion assets under management, was looking to perform a pen test for their public facing Web Application. In almost every Web Application you will find "password reset" function allowing users to reset their account password using secret questions. Our tester could successfully bypass this mechanism by using SQL-Injection that allowed him to finish this process successfully. To solve this, we suggested the following:

1. Used parameterized queries (also known as prepared statements) for all database access(es).
2. Doubled up any single quotation marks appearing within user input before incorporating that input into a SQL query.
3. Used stored procedures for database access.

The client got a full detailed report of how to mitigate our findings with screenshots and client/server Reponses.

In Conclusion: With our expertise, the client saved *time & money* and now has greater security, visibility and control over its Web Application.

About 2Secure Corp

2Secure is a Cyber Security firm that takes a PROACTIVE approach to solving network problems. We provide the right tools to fix problems the first time around – in fact, we guarantee it!

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355