Ett känt problembarn för säkerhet:

Databaser

Databaser

Webtillämpningar behöver någonstans att lagra data

Detta görs ofta med relationsdatabaser

ISBN_NO	SHORT_DESC	AUTHOR	PUBLISHER	PRICE
0201703092	The Practical SQL, Fourth Edition	Judith S. Bowman	Addison Wesley	39
0471777781	Professional Ajax	Jeremy McPeak, Joe Fawcett	Wrox	32
0672325764	Sams Teach Yourself XML in 21 Days, Third Edition	Steven Holzner	Sams Publishing	49
0764557599	Professional C#	Simon Robinson and Jay Glynn	Wrox	42
0764579088	Professional JavaScript for Web Developers	Nicholas C. Zakas	Wrox	35
1861002025	Professional Visual Basic 6 Databases	Charles Williams	Wrox	38
1861006314	GDI+ Programming: Creating Custom Controls Using C#	Eric White	Wrox	29

Rows

Columns

SQL-språket

Databaser accessas normalt med SQL *(Structured Query Language)*

Exempel:

```
SELECT * from users WHERE userName='admin';
```

Detta returnerar alla rader i databasen `users` som matchar förfrågan.

Alla SQL-förfrågningar avslutas med semikolon.

SQL-servrar tillåter flera rader i en enda förfrågan, uppdelade med semikolon.

SELECT på urval av kolumner

Du kan också fråga efter vissa kolumner.

```
SELECT CustomerName, City from Customers
WHERE OrderID='1045';
```

Detta visar enbart CustomerName och City

Jokertecknet (wildcard) * låter dig välja alla.

DROP och UNION

SQL-språket innehåller fler direktiv

Till exempel DROP DATABASE users; som raderar en databas vid namn users.

Ledtråd inför labben: Det finns ett SQL-kommando som heter UNION ALL som kan kombinera flera SELECT-kommandon

```
SELECT City FROM Customers
UNION ALL
SELECT City FROM Suppliers
ORDER BY City;
```

Databasangrepp

SQL-injektion

Antag att en webtillämpning använder en SQL-databas för att visa ordrar

Användaren anger objektnummer i ett formulär

Webtillämpningen tar detta ID och bygger följande SQL-query:

```
SELECT * FROM orders WHERE itemID='ID';
```

Detta returnerar alla rader med detta ID.

SQL-injektion

Nu lägger angriparen in följande ID:

```
1' OR 'a'='a
```

Detta resulterar i följande SQL-query:

```
SELECT * FROM orders WHERE itemID='1' OR 'a'='a';
```

Observera OR-uttrycket. Eftersom 'a'='a' alltid är sann, detta returnerar *alla* rader!

SQL-injektion: Avancerade attacker

En angripare kan använda SQL-kommentarer för mer avancerade attacker.

Två bindestreck är en kommentar: --

Antag att detta är normalt:

```
SELECT MyRecord FROM MyTable WHERE
MyEmail='$email' AND MyPassword='foo';
```

SQL-injektion: Avancerade attacker

Antag att detta är normalt:

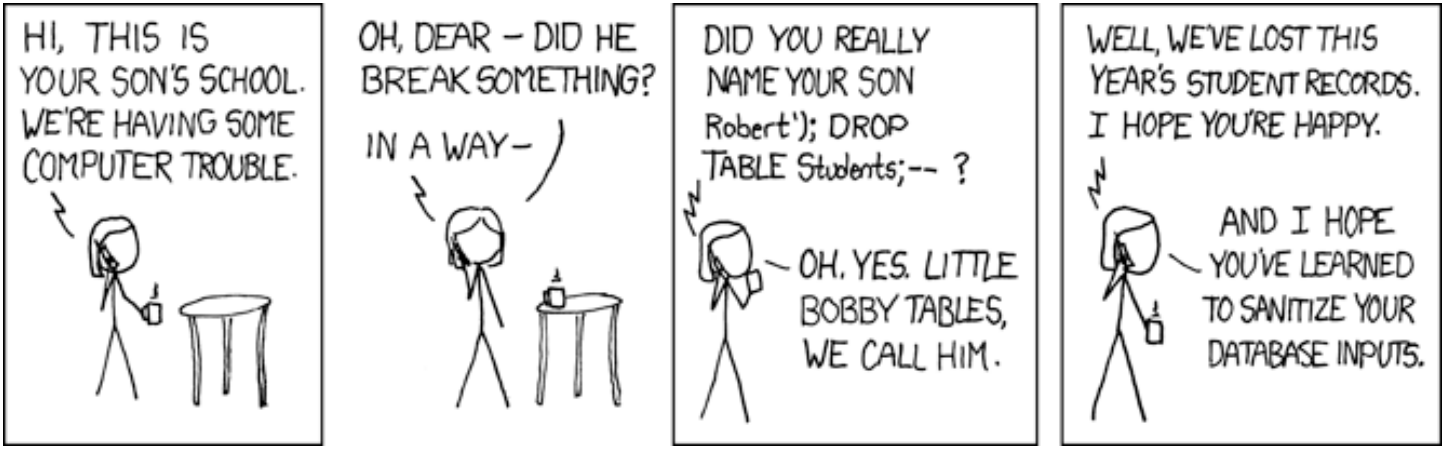
```
SELECT MyRecord FROM MyTable WHERE
MyEmail='$email' AND MyPassword='foo';
```

Med en falsk E-postadress:

```
SELECT MyRecord FROM MyTable WHERE MyEmail='';
DROP TABLE MyTable; --' AND MyPassword='foo';
```

All data efter de två bindestrecken ignoreras!

Håll dina parametrar rena



Inte ett vanligt problem idag eftersom alla har sett denna!