SQL Injection, continued

SQL commands:

create table ...
insert into ...
select

select * from tablename
select ... where age < 20

update
comment-to-end-of-line using "--"
select * from tbl -- Hello world

SQL1-Demo.cgi

Guess: script does

update users set password = '⟨new password⟩'
where password = '⟨old password⟩'
and username = '⟨username⟩'

Debugging into: Sqli-demo.cgi ? show
Update users set password = '<new password>'
where password = '' or 1 = 1--
and username = '<username>'

Update users set password = 'new', admin = 1
where password = '
and username = '<username>'

Countermeasures:
 DB frameworks provide prepared queries
& placeholders executed many times, with different values
replaced by values each execution
Perl DBI example:

**Dumb way:**

```perl
$sq1 = "update set p=\$NEW where u=\$USER ... "
prepare ($sq1)
execute
```

**Placeholders:**

```perl
$sq1 = "update set p=? where u=? ... "
prepare ($sq1)
execute ($NEW, $USER, ...)
```