command injection (review?)

```
name = UNTRUSTED_INPUT
subprocess.check_call(
    "write_report_for '" + name + "' output.pdf"
)
```

```
name = '; malicious_command; /bin/true '
```

command injection (review?)

```
name = UNTRUSTED_INPUT
result = db_connection.execute(
    "SELECT a, b, c FROM items WHERE name = '" + name + "'"
)
```

```
name = '; SELECT password FROM users WHERE
name = 'foo
```

input as wrong thing pattern

with command injection: input interpreted for wrong purpose

supposed to be label/string to match/etc.

actually interpreted as part of command

input as wrong thing pattern

with command injection: input interpreted for wrong purpose

supposed to be label/string to match/etc.

actually interpreted as part of command

same pattern for a bunch of memory vulnerabilities we'll look at

- input supposed be part of buffer
- overflow or similar makes part of it interpreted as something else

backup slides