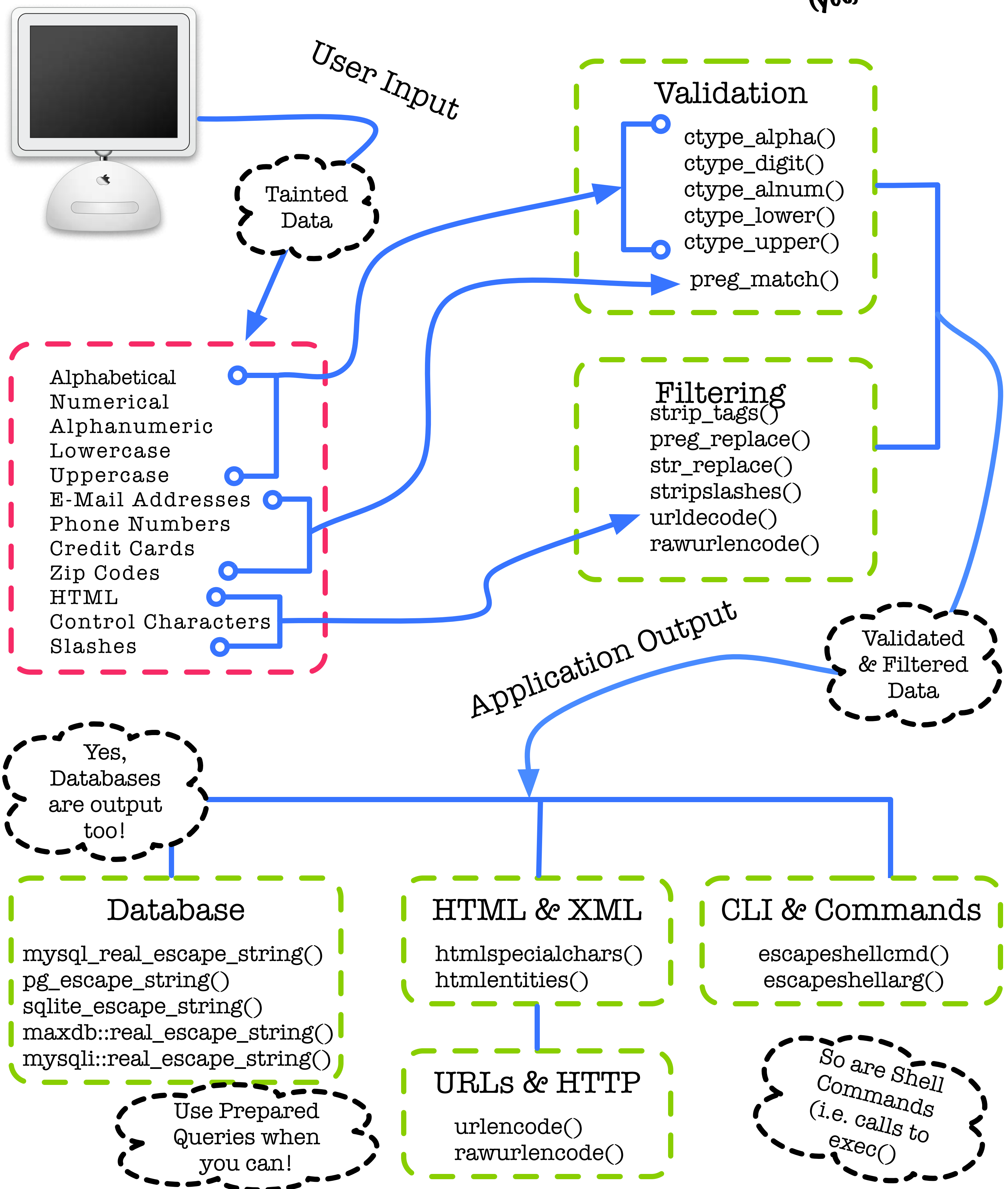
Filtering & Escaping

(yes, it's a mantra)



User Input

Tainted Data

Alphabetical
Numerical
Alphanumeric
Lowercase
Uppercase
E-Mail Addresses
Phone Numbers
Credit Cards
Zip Codes
HTML
Control Characters
Slashes

Validation

ctype_alpha()
ctype_digit()
ctype_alnum()
ctype_lower()
ctype_upper()
preg_match()

Filtering

strip_tags()
preg_replace()
str_replace()
stripslashes()
urldecode()
rawurlencode()

Validated & Filtered Data

Application Output

Yes, Databases are output too!

Database

mysql_real_escape_string()
pg_escape_string()
sqlite_escape_string()
maxdb::real_escape_string()
mysqli::real_escape_string()

Use Prepared Queries when you can!

HTML & XML

htmlspecialchars()
htmlentities()

URLs & HTTP

urlencode()
rawurlencode()

CLI & Commands

escapeshellcmd()
escapeshellarg()

So are Shell Commands (i.e. calls to exec()

cheatsheet © Davey Shafik [http://pixelated-dreams.com]