Input Validation

MODIO
Secure & efficient energy information

Two levels

- Syntactic - Is it recognizable as a type, format e.t.c?
- Semantic - Does it make sense for it’s use-case?

Syntactic

Limited knowledge needed

NULL checks

atoi(), int(), DateTime()

MODIO
Secure & efficient energy information

Semantic

Requires knowledge of what it is

TimeStamp, User-ID, PIN

E.g. Date validation

DoB: 1986-02-29, 2015-02-29, 1802-02-29

Syntactic - Valid date string, mix/max length

Semantic - 1802? Huh?

Reminder: “Feb 30, 2015”

- Syntactical error, invalid date

Reminder: “Jan 1, 1919”

✔ Syntactically correct
- Semantically wrong, in the past

Reminder: “Jan 1, 2016”

✔ Syntactically correct
✔ Semantically correct date
- Semantically incorrect, Lacking TimeZone

MODIO
Secure & efficient energy information

E.g. PIN validation

```
int pin = 10056;
```
//Syntactically correct, semantically wrong

- ★ PIN must be **4 digits** (semantically wrong)
- ★ PIN cannot exceed **9999** (semantically wrong)
- ★ PIN cannot be a *negative number* (syntactically correct)
- ★ PIN must be a *number* (syntactically correct)

MODIO
Secure & efficient energy information

E.g.: PIN Validation

http://example.com/&pin=0x1235

http://example.com/&pin=-MAX_INT

MODIO
Secure & efficient energy information

Syntactic

Sanitize - Use language filters, language rules, regex, type-casting, logical errors, character encoding

https://simple.wikipedia.org/wiki/Mojibake

Syntactic

Length - Is min/max length valid, exact valid numeric length, etc.

Syntactic

Type - Boolean, IP Address, Alphanums, Date etc.

Syntactic

Typical example: Database Schema
(BIGINT, INT, VARCHAR, DateTime)

Semantic

Format - Casting, strip tags and unwanted characters

Semantic

Boolean comparisons, input verification

MODIO
Secure & efficient energy information

Things not to validate

Names

Addresses

email

Time

Names

http://www.kalzumeus.com/2010/06/17/falsehoods-programmers-believe-about-names/

Time

http://infiniteundo.com/post/25326999628/falsehoods-programmers-believe-about-time

MODIO
Secure & efficient energy information

Addresses

https://www.mjt.me.uk/posts/falsehoods-programmers-believe-about-addresses/

http://wiesmann.codiferes.net/wordpress/?p=15187&lang=en

Email

http://www.w3.org/Protocols/rfc822/

Script injection

```
Comment=”</BODY></HTML>”
```

```
Comment=”<script>for(;;){alert();}”
```


MODIO
Secure & efficient energy information

Script Injection

I will not trust user input

I will not trust user input

I will not trust user input

I will not trust user input

I will not trust user input

I will not trust user input

I will not trust user input

MODIO
Secure & efficient energy information

SQL Injection

```
user=’OR 1=1;DROP DATABASE;’
```


MODIO
Secure & efficient energy information

SQL Injection

- Constrain Input
- Use an ORM
- Parameters with stored procedures
- Parameters with dynamic SQL

URL parameters / XSS

- Convert URL vars to Session vars
- Escape special characters
- Don’t assume user-data is correct

Cross-site request forgery (XSRF)

- Secret Token
- Captcha
- Re-log in before important action

Resources

http://xkcd.com/327/

https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet,

https://msdn.microsoft.com/en-us/library/ms161953(SQL.105).aspx

http://cdn.oreillystatic.com/en/assets/1/event/36/SQL%20Injection%20Myths%20and%20Fallacies%20Presentation.pdf

MODIO
Secure & efficient energy information