TRAINING KIT – CODE2

Secure Coding Labs

EXCELLIUM

Your first call when it comes to IT and Security!

March 16, 2017

TLP: WHITE

Agenda

EXCELLIUM
Your first call when it comes to IT and Security!

- Objective
- Secure coding pillars
- Let’s code
- Links
- Q&R

Objective

This labs have to objective to help you to learn how to code taking in account the secure coding pillar. The point viewed here can be applied to any technology like Java/.Net / PHP / Ruby…

No special framework will be used in order to teach you how to handle secure coding in every situation because you can be in a case in which the web framework that you (must) use do not provide security features or miss some one.

We will implements a set of REST services performing Create, Read, Update, Delete operation and using authentication/authorization in a context of posting message like a tweet.

Objective

REST stands for Representational State Transfer. (It is sometimes spelled "ReST".) It relies on a stateless, client-server, cacheable communications protocol and in virtually all cases, the HTTP protocol is used.

REST is an architecture style for designing networked applications. The idea is that, rather than using complex mechanisms such as CORBA, RPC or SOAP to connect between machines, simple HTTP is used to make calls between machines.

Objective

EXCELLIUM
Your first call when it comes to IT and Security!

CURL is an open source command line tool and library for transferring data with URL syntax, supporting DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMTP, SMTPS, Telnet and TFTP.

```
::::/bin/bash
# send login data with POST request
curl --request POST 'http://www.somedomain.com/login/' \
--data 'username=myusername&password=mypassword'

# send search data to with get request
curl --request GET 'http://www.youtube.com/results?search_query=my_keyword'

# send PUT request with data
curl --request PUT 'http://www.somedomain.com/rest-api/user/12345/'\
--data 'email=myemail@gmail.com'

# same thing but this one get data from a file named data.txt
curl --request PUT 'http://www.somedomain.com/rest-api/user/12345/'\
--data @data.txt
```

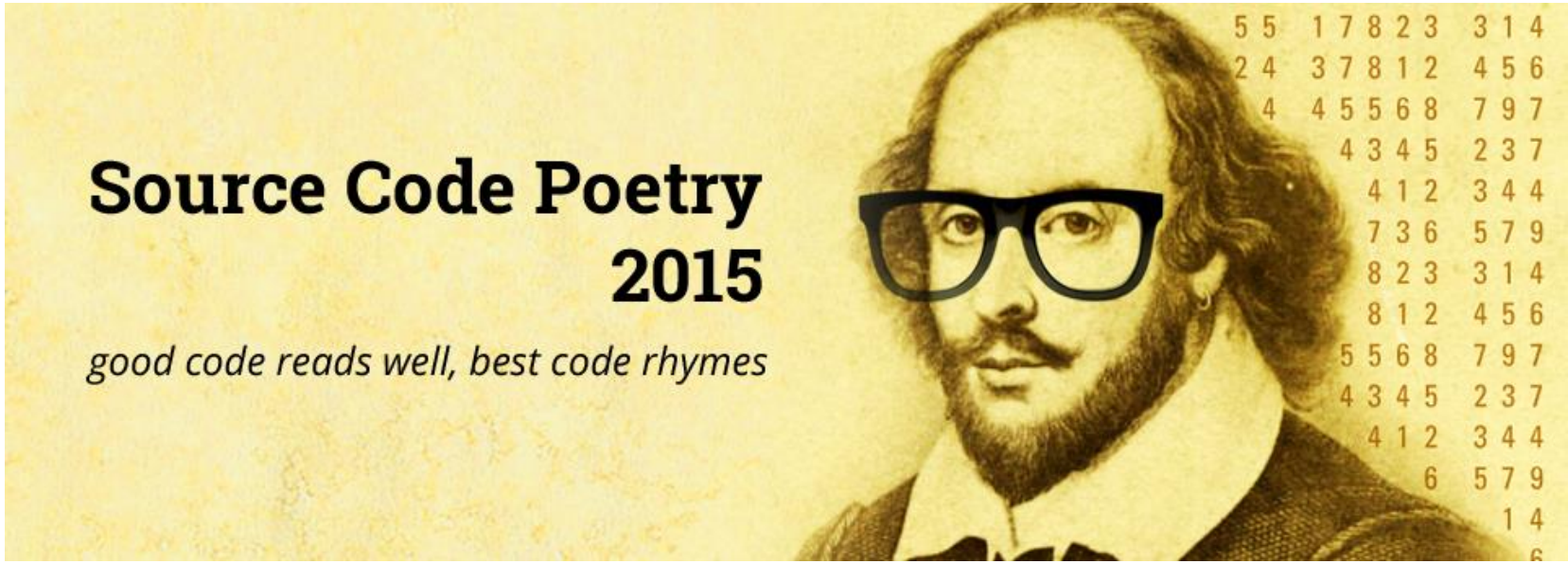
Secure coding pillars

EXCELLIUM
Your first call when it comes to IT and Security!

- Authentication
- Session management
- Authorization
- Input validation and Output encoding
- Error handling and Logging
- Audit Trail
- Trusted network channel/storage:
  - Data protection
  - File system access
  - Cryptography
- Enable defensive feature in modern browsers

Let's code ☺

EXCELLIUM
Your first call when it comes to IT and Security!



Let's code – Setup

EXCELLIUM
Your first call when it comes to IT and Security!

1. Connect via Remote Desktop (mstsc.exe) to remote machine ending with IP ".5" according to your LAN configuration:
   - **User:** `Administrator`
   - **Password:** `Given by the instructor during this step`
2. On remote station:
   a) Open the IDE (Eclipse or Visual Studio), project is already imported.
   b) Open, using WordPad, the file named "labs-tasks.docx" in the sub folder of the technology that you have choose to perform the labs.
   c) Read the section about Info for **student** and follow the labs instruction…

Let's code – Part 1

EXCELLIUM
Your first call when it comes to IT and Security!

- Authentication ←
- Session management ←
- Authorization
- Input validation and Output encoding
- Error handling and Logging
- Audit Trail
- Trusted network channel/storage:
  - Data protection
  - File system access
  - Cryptography
- Enable defensive feature in modern browsers

Let's code – Part 2

EXCELLIUM
Your first call when it comes to IT and Security!

- Authentication
- Session management
- Authorization ←
- Input validation and Output encoding ←
- Error handling and Logging ←
- Audit Trail ←
- Trusted network channel/storage:
  - Data protection
  - File system access
  - Cryptography
- Enable defensive feature in modern browsers

Let's code – Part 3

EXCELLIUM
Your first call when it comes to IT and Security!

- Authentication
- Session management
- Authorization
- Input validation and Output encoding
- Error handling and Logging
- Audit Trail
- Trusted network channel/storage:
  - Data protection ←
  - File system access
  - Cryptography ←
- Enable defensive feature in modern browsers ←

Let's code – Done ☺

EXCELLIUM
Your first call when it comes to IT and Security!

- Authentication
- Session management
- Authorization
- Input validation and Output encoding
- Error handling and Logging
- Audit Trail
- Trusted network channel/storage:
  - Data protection
  - File system access
  - Cryptography
- Enable defensive feature in modern browsers

Links

EXCELLIUM
Your first call when it comes to IT and Security!

- Useful HTTP header
  - https://www.owasp.org/index.php/List_of_useful_HTTP_headers
- Introduction to Cache header
  - http://www.mobify.com/blog/beginners-guide-to-http-cache-headers/
- REST
  - http://rest.elkstein.org/
- CURL
  - http://curl.haxx.se/
  - http://curl.haxx.se/docs/httpscripting.html

Q&R

EXCELLIUM
Your first call when it comes to IT and Security!