



MIS|TI™ PRESENTS

# InfoSecWorld

Conference & Expo 2018

## ARE YOU A SECURE CODE WARRIOR?

*Stephen Allor*

*Director, Americas*

*Secure Code Warrior*

# WHAT WE BELIEVE...

... that developers can become the first line of defense against cyber attacks.

# INTRODUCTION



# Coding failure costs money

Ariane 5 rocket

- \$7 billion
- 10 years of work

Technical:

- Velocity: 64-bit float
- Convert to 16-bit int
- Overflow
- Error handling suppressed (performance)



# Coding failure brand damage



# C-Level people get fired



# APPSEC



# Code Sample: Ariana 5 rocket

## Why visibility matters—the Ariane 5 crash

- Velocity was represented as a 64-bit float
- A conversion into a 16-bit signed integer caused an overflow
- The current velocity of Ariane 5 was too high to be represented as a 16-bit integer
- Error handling was suppressed for performance reasons

```
-- Vertical velocity bias as measured by sensor
L_M_BV_32 :=  
    TBD.T_ENTIER_32S ((1.0/C_M_LSB_BV) *  
        G_M_INFO_DERIVE(T_ALG.E_BV));  
-- Check, if measured vertical velocity bias can be  
-- converted to a 16 bit int. If so, then convert  
if L_M_BV_32 > 32767 then  
    P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;  
elsif L_M_BV_32 < -32768 then  
    P_M_DERIVE(T_ALG.E_BV) := 16#8000#;  
else  
    P_M_DERIVE(T_ALG.E_BV) :=  
        UC_16S_EN_16NS(TDB.T_ENTIER_16S(L_M_BV_32));  
end if;  
-- Horizontal velocity bias as measured by sensor  
-- is converted to a 16 bit int without checking
P_M_DERIVE(T_ALG.E_BH) :=  
    UC_16S_EN_16NS (TDB.T_ENTIER_16S ((1.0/C_M_LSB_BH) *  
        G_M_INFO_DERIVE(T_ALG.E_BH)));
```

\*Source: <http://moscova.inria.fr/~levy/talks/10enslongo/enslongo.pdf>

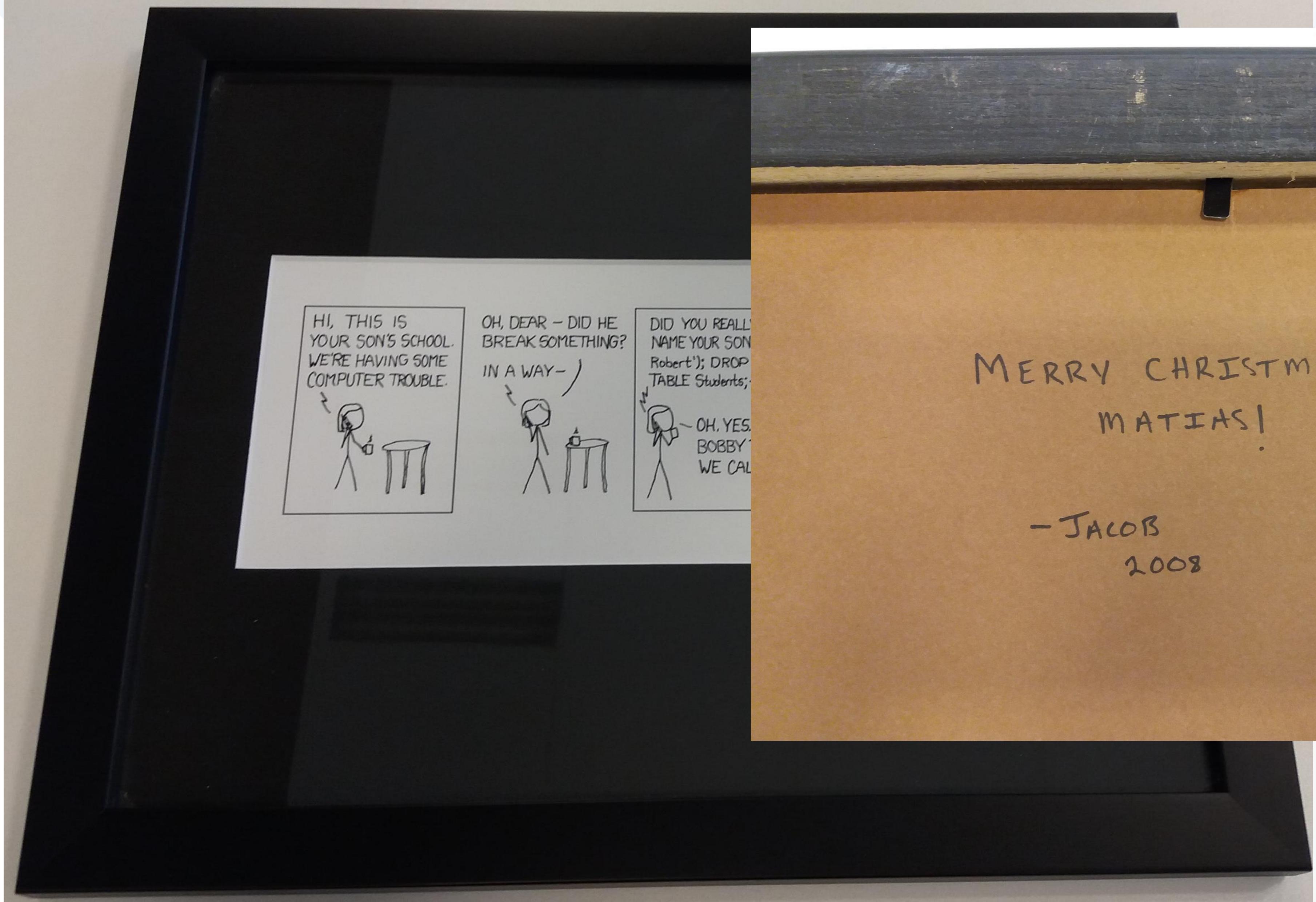


# Typical SQL Injection sample

PaymentController.java  
⚠ > PaymentDAOImpl.java

```
20  /**
21  * Method will save the payment details into the database.
22  */
23
24  public boolean savePaymentDetails(PaymentDetails paymentDetails) {
25      //Session session = HibernateUtil.getCurrruntSession();
26      Session session=null;
27      Transaction tx=null;
28      boolean isSuccess=true;
29      try{
30          session = sessionFactory.getCurrentSession();
31          tx = session.beginTransaction();
32          String dml = "insert into paymentDetails (orderId, cardNumber, cardOwner, totalAmount) va
33          dml = dml.replace(":orderId", String.valueOf(paymentDetails.getOrderId()));
34          dml = dml.replace(":cardNumber", paymentDetails.getCardNumber());
35          dml = dml.replace(":cardOwner", paymentDetails.getCardOwner());
36          dml = dml.replace(":totalAmount", String.valueOf(paymentDetails.getTotalAmount()));
37          jdbcTemplate.update(dml);
38
39          tx.commit();
40      }catch (Exception e) {
41          logger.error("Error at saving Payment Details information ", e);
42          if (tx != null) {
43              tx.rollback();
44              throw new ApplicationException(1111,"Database Exception.");
45          }
46          isSuccess=false;
```

# Frame



# Why is this not resolved yet?

Security knows about issues in code

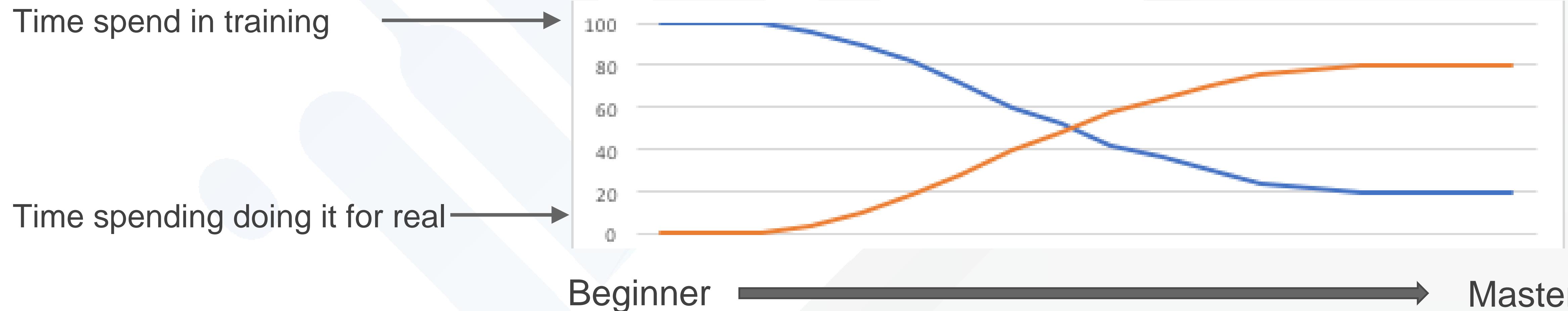


- 1) Fix known security issues → Scale of AppSec team?  
Ton of overhead!
- 2) Do not introduce new issues → 700+ categories of problems!



Never ending story...

# Flying a plane: simulator vs flying for real



# TRAINING



# Provide language specific training

If you want to be better at English, will you take a course in Polish?

What language do you want to learn?

German

English

French

Spanish

Turkish

Italian

Portuguese

Swedish

Danish

Norwegian

Indonesian

Dutch

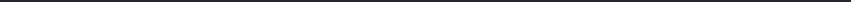
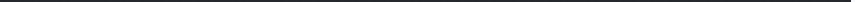
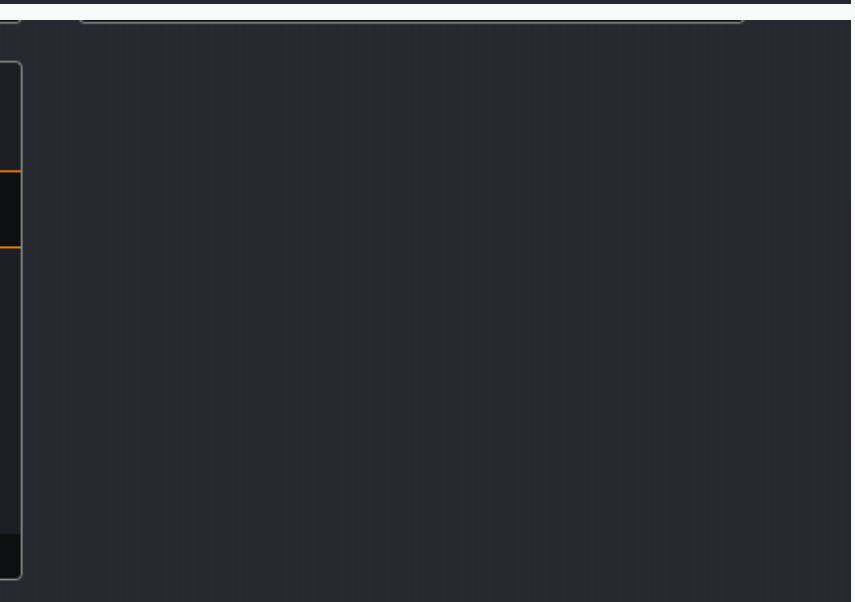
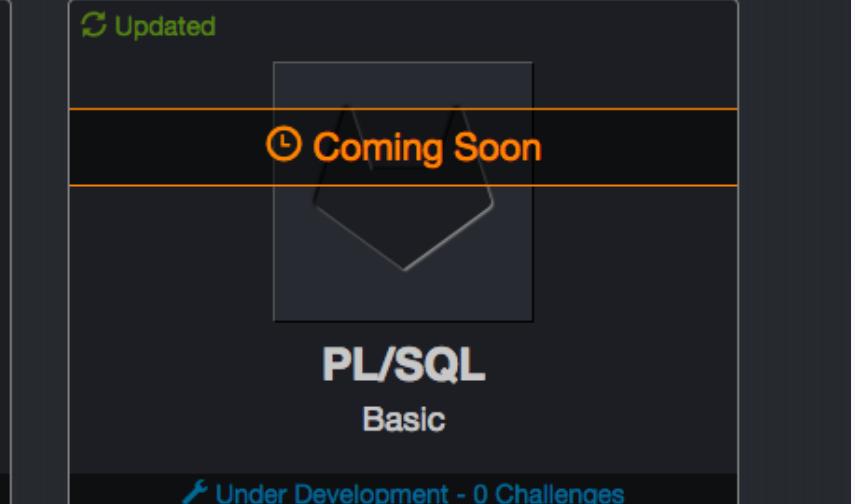
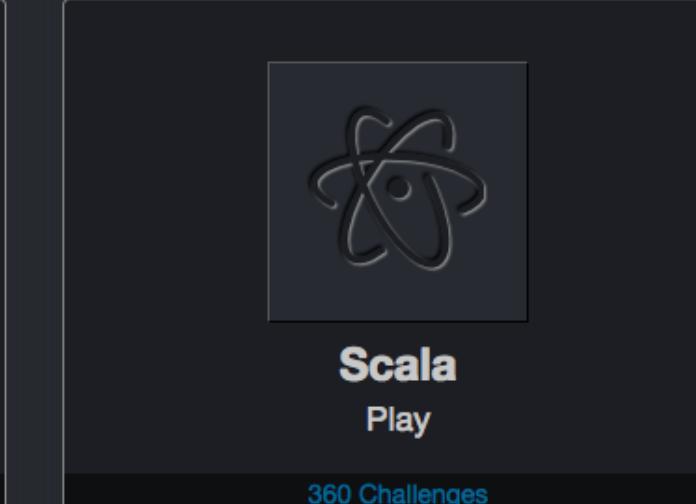
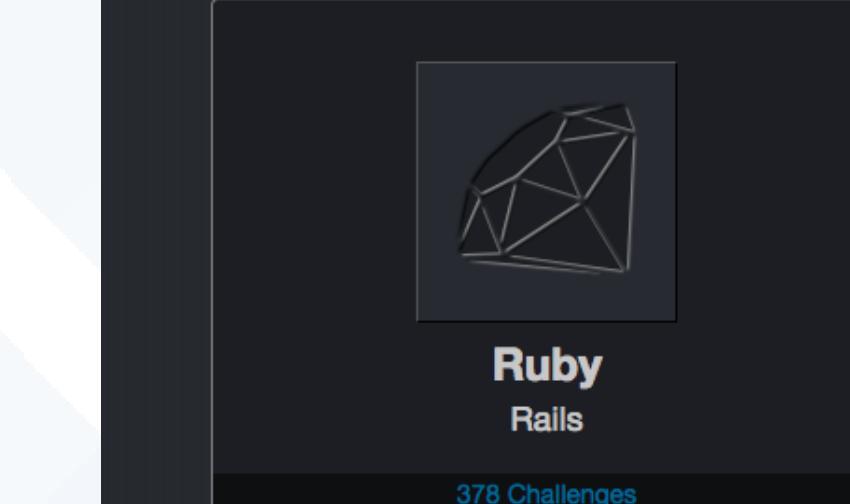
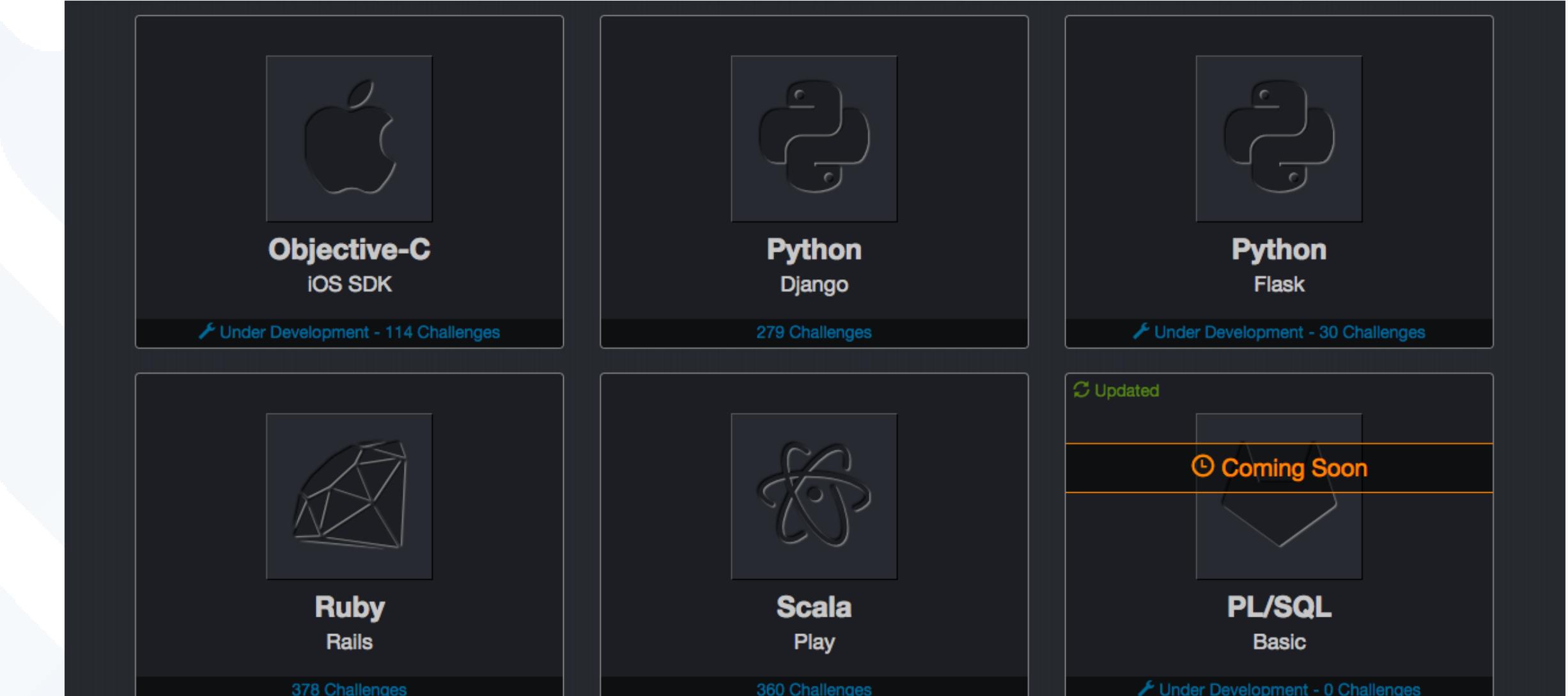
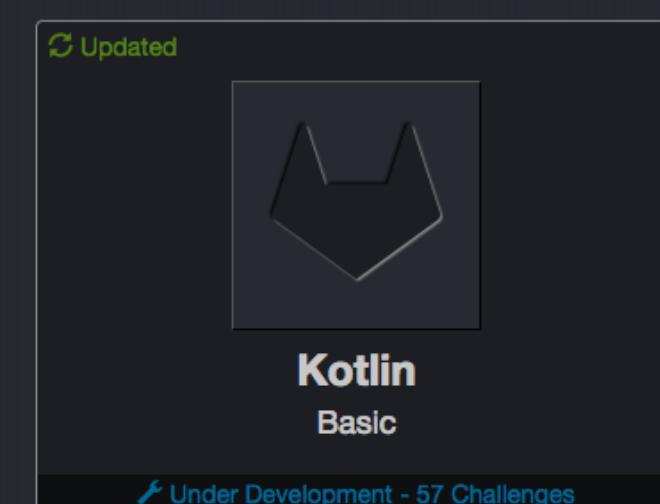
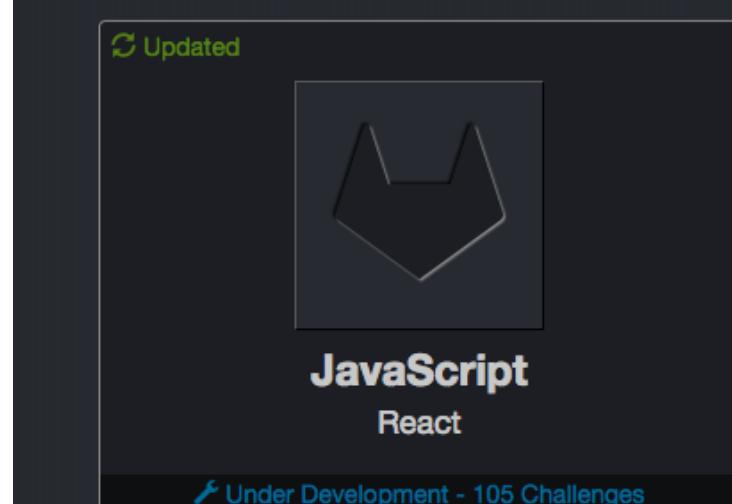
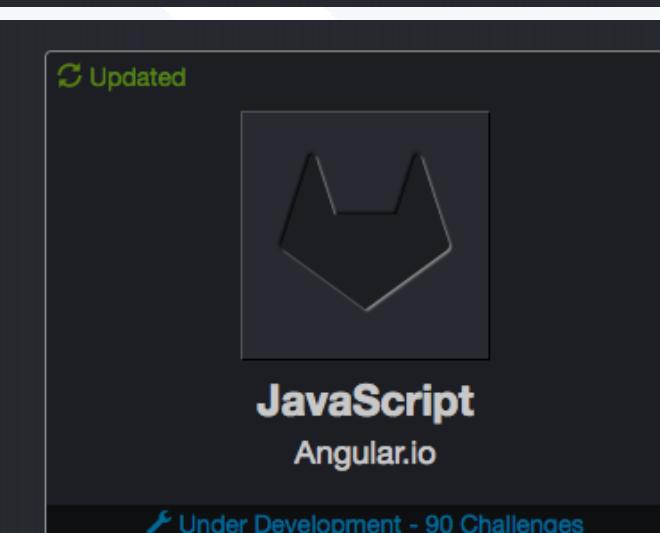
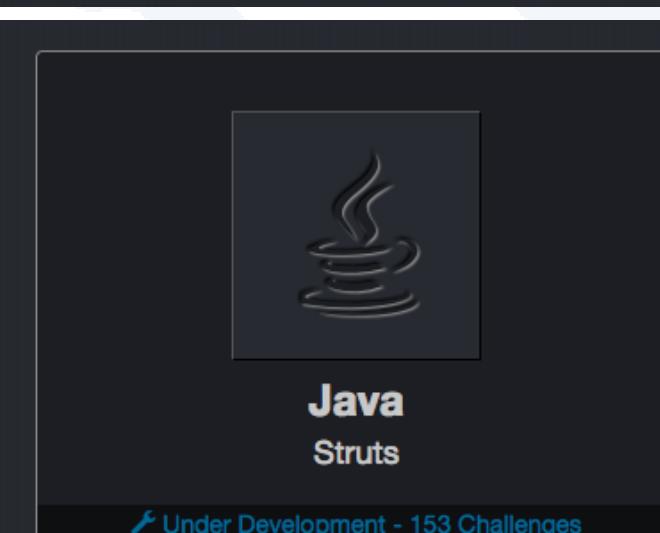
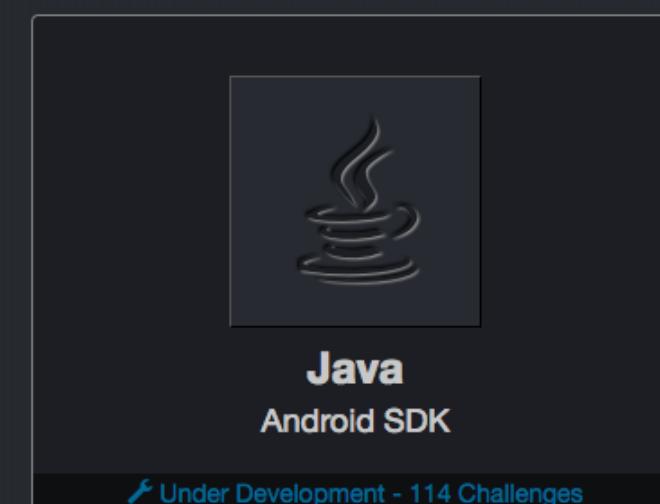
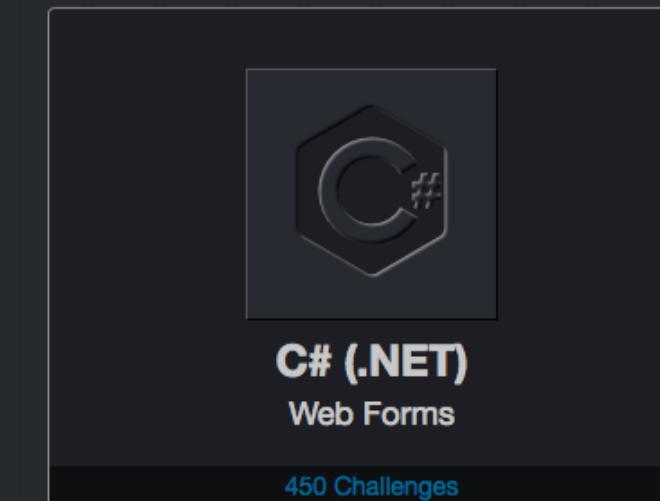
Polish

Russian

# Language/Framework Specific

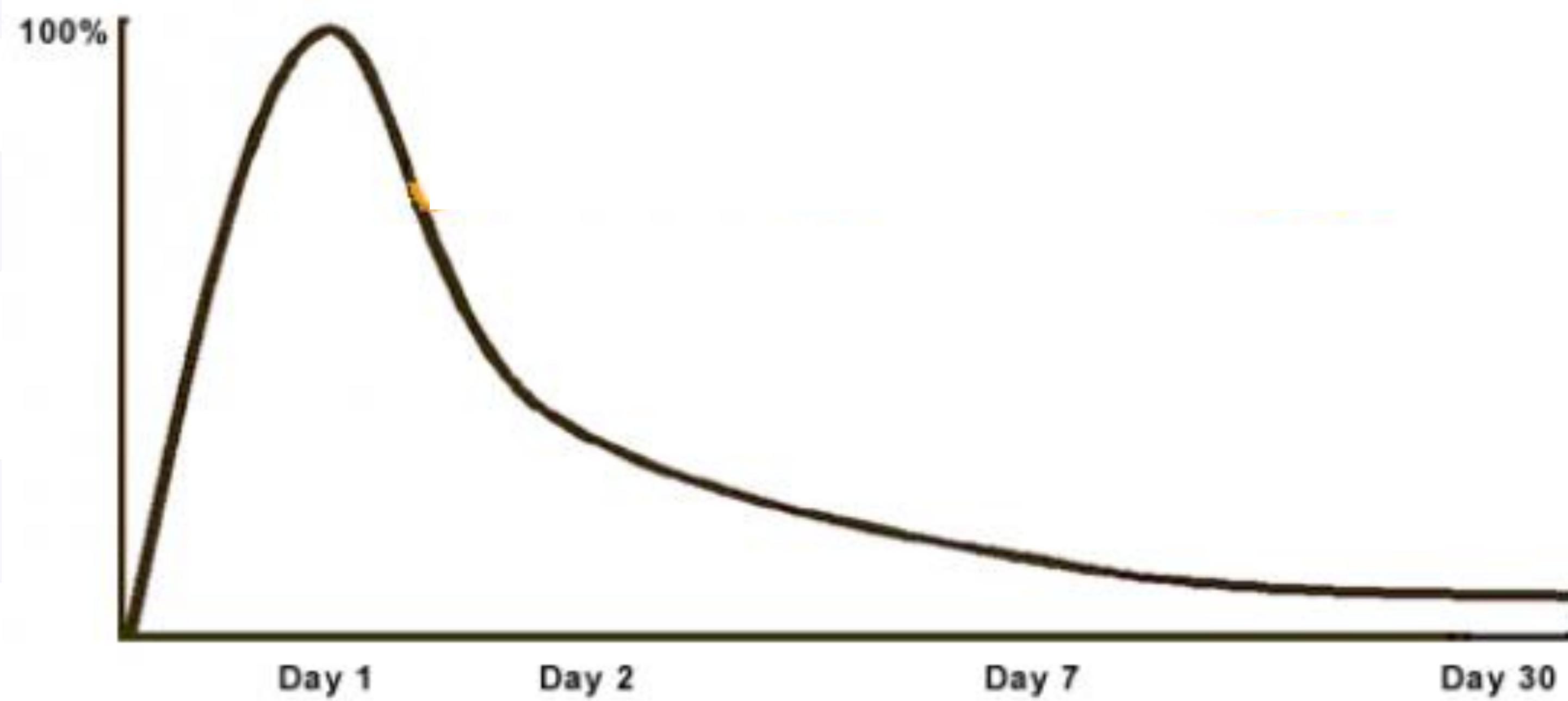
## Available Languages and Frameworks

Pick your preferred coding language and framework

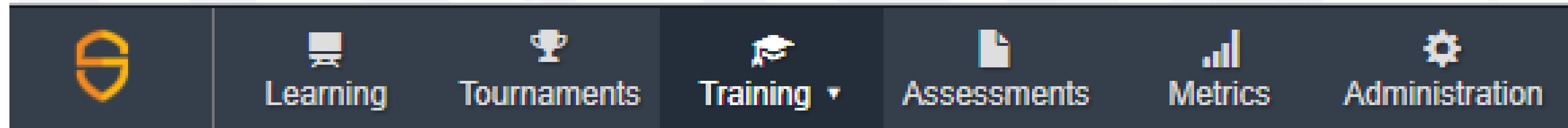


## The forgetting curve

How fast do you forget a new word?



# Hands-on and Self-paced



1                    2                    3

Locate Vulnerability      Identify Solution      Challenge Complete

**Locate Vulnerability**

- Identify and select the code hunks that cause the vulnerability listed below by clicking the ▲ next to the line numbers in the code viewer.
- Files containing selectable code hunks have been marked with ▲.

**Vulnerability Category**

- Injection Flaws - SQL Injection

**Submit Your Answer**

- There is 1 vulnerable hunk in the source code that you need to locate.
- You have selected 0 code hunks.

Hint Next

▲ LoginController.java  
▲ > UsersRepositoryImpl.java  
▲ UsersService.java  
▲ login.jsp

```
9 import java.util.Date;
10
11 import com.securecodewarrior.challenges.banking.model.User;
12 import com.securecodewarrior.challenges.banking.util.ApplicationException;
13 import com.securecodewarrior.challenges.banking.util.ConnectionFactory;
14 import com.securecodewarrior.challenges.banking.util.Constants;
15 import com.securecodewarrior.challenges.banking.util.Log;
16
17 /**
18 * The <code>UsersRepositoryImpl</code> interface provides methods for managing User related information in
19 * <b>OnlineBankingSystem</b> application.
20 *
21 * @author kushal shah
22 */
23 public class UsersRepositoryImpl implements UsersRepository{
24
25     String sqlQuery = null;
26
27     /* (non-Javadoc)
28      * @see
29      *      com.securecodewarrior.challenges.banking.repository.UsersRepository#checkUserNameExistsOrNot(java.lang.String)
30      */
31
32     public User checkUserNameExistsOrNot(final String user) {
33
34         Log.info(this.getClass().getName()+" ==> Method : checkUserNameExistsOrNot ==> Enter");
35
36         sqlQuery = "SELECT
37             ID,SECURITYQUESTION,LOCKEDUNTIL,FIRST_NAME,LAST_NAME,PASSWORD,USERNAME,ROLE_ID,API_PARTNER FROM USER
38             WHERE USERNAME=':USERNAME'";
39
40         sqlQuery.replaceAll(":USERNAME", user);
41
42         Statement statement = null;
43         Connection connection=null;
44         User returnUser = null;
45         ResultSet resultSet = null;
46         try {
47             //Getting connection object
48             connection = ConnectionFactory.getConnection();
49             statement = connection.createStatement();
50             resultSet = statement.executeQuery(sqlQuery);
51
52             if (resultSet.next()) {
53
54                 returnUser = new User();
55                 returnUser.setUsername(resultSet.getString("USERNAME"));
56                 returnUser.setFirstName(resultSet.getString("FIRST_NAME"));
57                 returnUser.setLastName(resultSet.getString("LAST_NAME"));
58                 returnUser.setPassword(resultSet.getString("PASSWORD"));
59                 returnUser.setRole_id(resultSet.getInt("ROLE_ID"));
60                 returnUser.setId(resultSet.getLong("ID"));
61                 returnUser.setSecurityQuestion(resultSet.getString("SECURITYQUESTION"));
62                 returnUser.setApi_partner(resultSet.getBoolean("APT_PARTNER"));
63             }
64         } catch (SQLException e) {
65             e.printStackTrace();
66         }
67     }
68 }
```

What style would you prefer?



duoLingo

VS.



# Gamified platform

The screenshot displays a gamified platform interface with a dark-themed header and sidebar.

**Header:** Includes navigation links for Learning, Tournaments, Training (with a dropdown), Assessments, Metrics, Administration, and a user profile icon labeled "C++ Basic".

**Left Sidebar:** Features icons for zooming in and out, a refresh button, a home button, and a speaker icon.

**World Map:** Shows the outlines of continents with several circular markers indicating flagged locations. These markers include icons such as a power plant, a flag, a person, and a mask, with some showing small national flags like Germany and Spain.

**Level Progress Bar:** Located in the top right corner, it shows "Level 1" with "0 points" earned. It lists "Most Critical Weaknesses" including Accuracy and Security Maturity, each accompanied by a small icon.

**A-Team Leaderboard:** A section titled "A-Team Leaderboard" with the note "Developer names have been anonymised by your company administrator". The table lists developer ranks, names, and points.

Rank	Name	Points
33	Firebreathing Wireworm	0
34	Next Zebraswallowtailbutterfly	0
35	Crazy Hamadryas	0
36	Noncollinear Bighornedsheep	0
37	Smartalecky Malamute	0
38	Uncongestive Marbledmurrelet	0
39	Bilingual Germanspaniel	0
40	Shiny Squamata	0
41	Angeli Castro	0
42	Germless Whitebeakeddolphin	0

**Active Missions:** A section at the bottom left lists "Proof of Concept Challenges" and "Proof of Concept Challenges II", each with a "View" button.

This map is based on public domain map data available from jVectorMap and Natural Earth.

© Secure Code Warrior 2017

# TOURNAMENT



# Prizes



## AND YOU CAN TRY IT OUT...

- ① GO TO: <https://portal.securecodewarrior.com/#/register>
- ② CLICK ‘REGISTER’, FILL IN YOUR EMAIL AND USE THE FOLLOWING TOKEN KEY: **745 661 143 686**
- ③ Click on the **Tournaments** Tab, and then click “Join”

THE TOURNAMENT WILL GO LIVE AT **10.10AM** and stop at **11:40AM**

→ Follow us on Twitter and be in with a chance to win some more cool prizes

@Seccodewarrior #securecodewarrior



# DEMO





MIS|TI™ PRESENTS

# InfoSecWorld

Conference & Expo 2018

**THANK YOU  
PLEASE FILL OUT YOUR EVALUATIONS!**

*Matias Madou, Ph.D.,  
CTO and co-founder  
Secure Code Warrior*