MIS|TI™ PRESENTS

InfoSec World

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

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

```
-- 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 ban 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)));
```

Typical SQL Injection sample

PaymentController.java

⚠ > PaymentDAOImpl.java

```
20
21      /**
22       * Method will save the payment details into the database.
23       */
24      public boolean savePaymentDetails(PaymentDetails paymentDetails) {
25          //Session session = HibernateUtil.getCurruntSession();
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

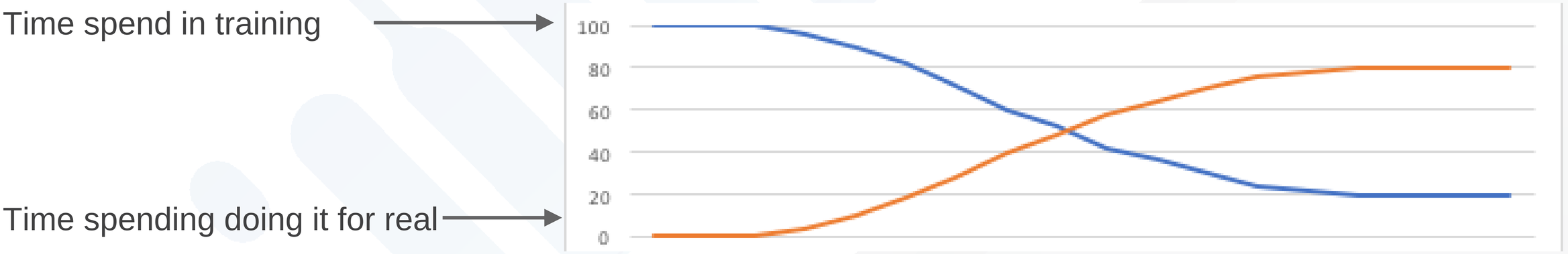
1) Fix known security issues → Scale of AppSec team?

→ 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

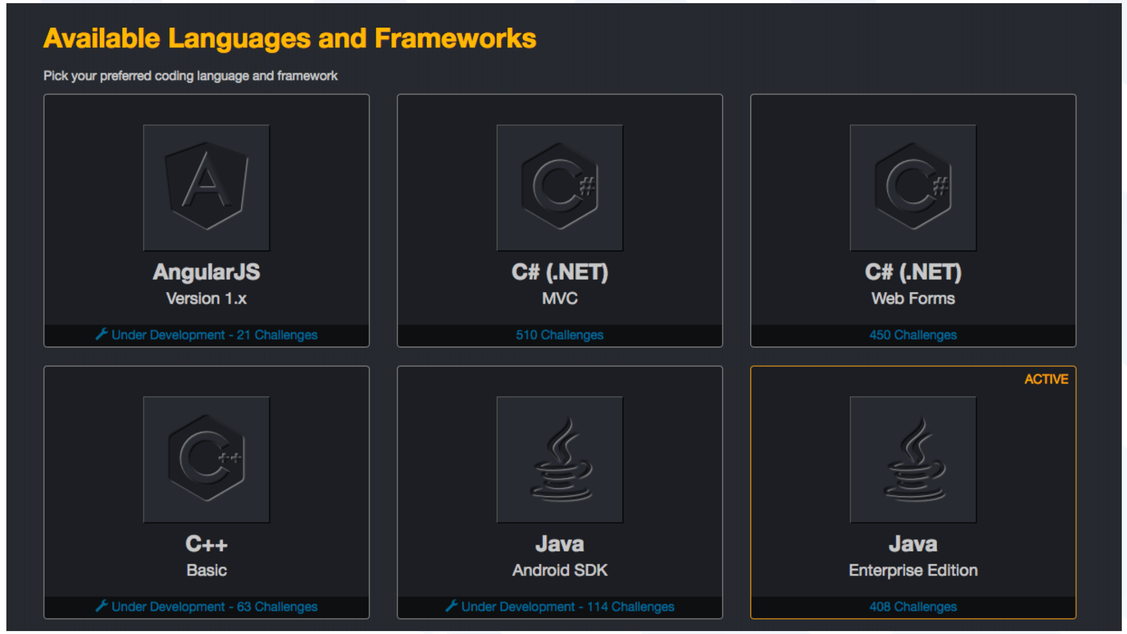
Provide language specific training

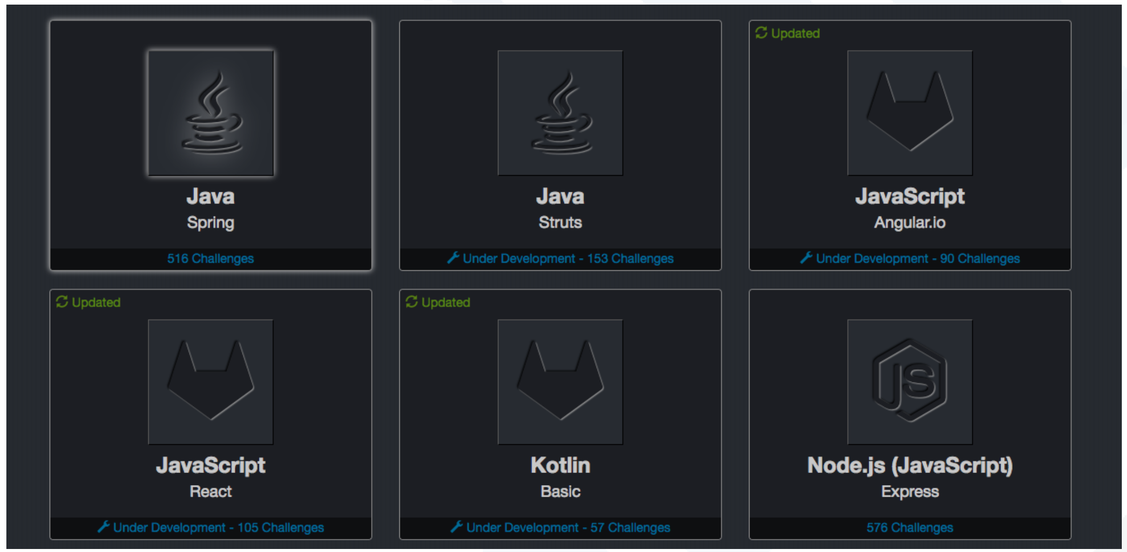
If you want to be better at English, will you take a course in Polish?

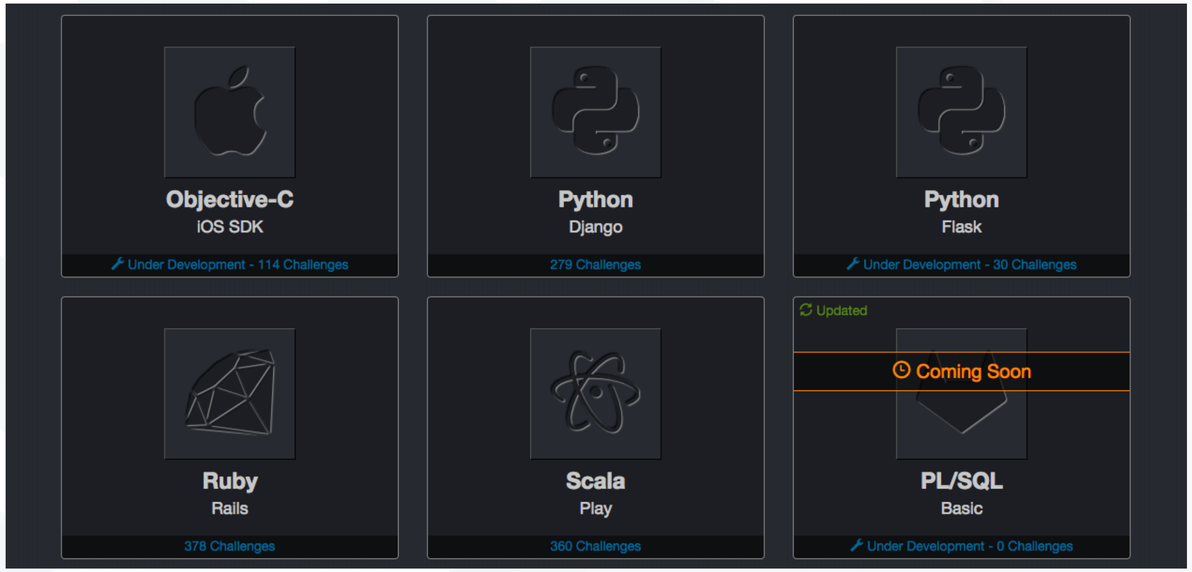
What language do you want to learn?

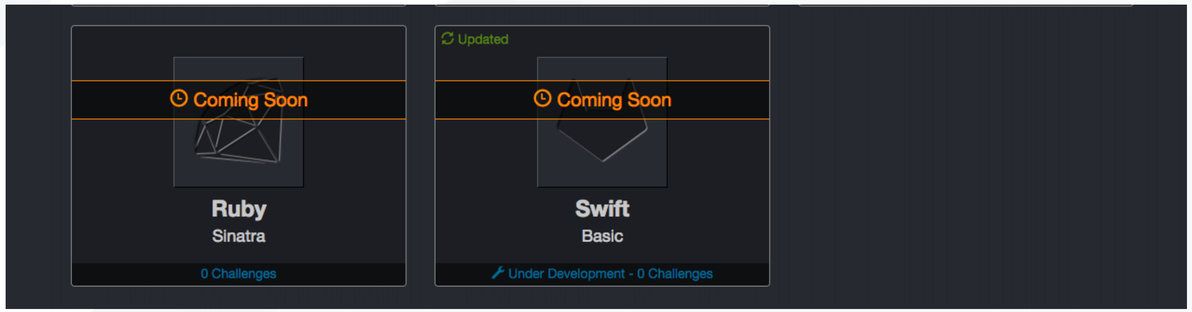
	German	English	French	Spanish	
Turkish	Italian	Portuguese	Swedish	Danish	Norwegian
	Indonesian	Dutch	Polish	Russian	

Language/Framework Specific



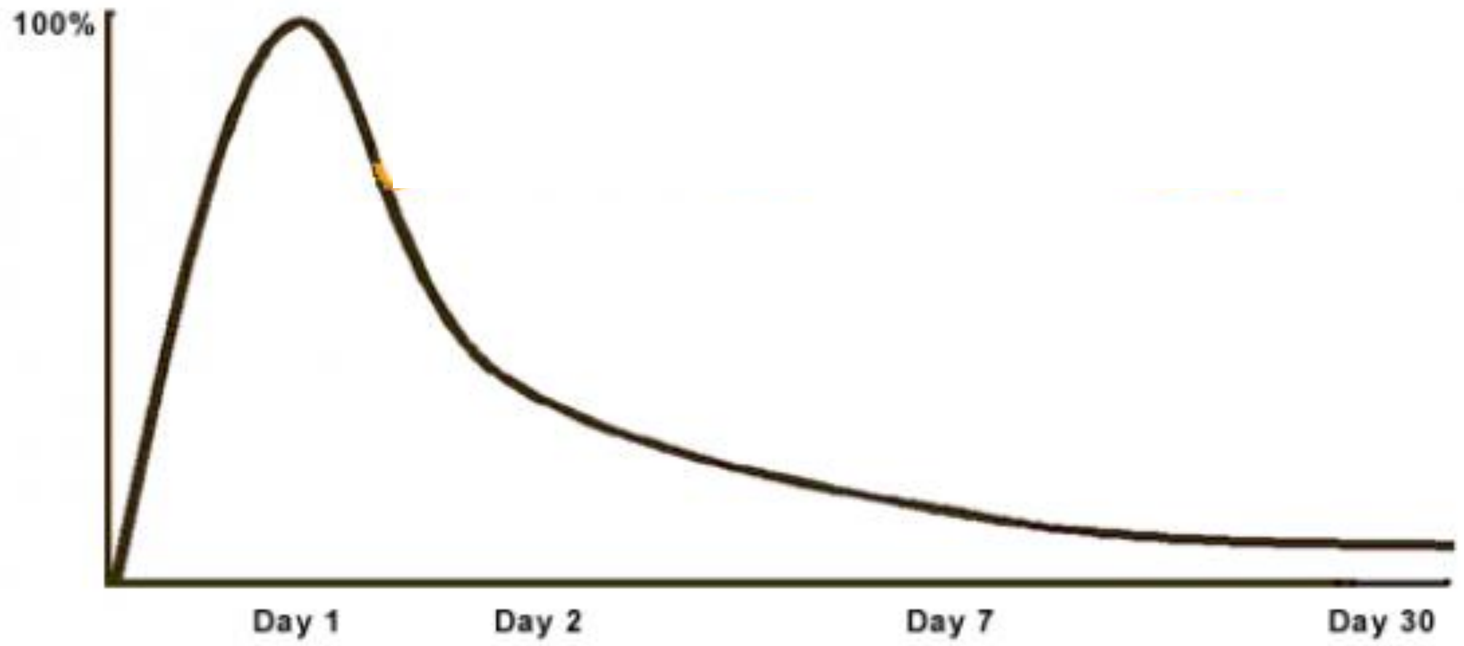






The forgetting curve

How fast do you forget a new word?



Hands-on and Self-paced

1 Locate Vulnerability — 2 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>UsersRepostitoryImpl</code> interface provides methods for managing User related information in
        <b>OnlineBankingSystem</b> application.
19  *
20  * @author kushal shah
21  *
22  */
23 public class UsersRepostitoryImpl implements UsersRepository{
24
25     String sqlQuery = null;
26
27     /* (non-Javadoc)
28      * @see
            com.securecodewarrior.challenges.banking.repository.UsersRepository#checkUserNameExistsOrNot(java.lang.Str
            ing)
29      */
30     public User checkUserNameExistsOrNot(final String user) {
31
32         Log.info(this.getClass().getName()+ "==> Method : checkUserNameExistsOrNot ==> Enter");
33
34         sqlQuery = "SELECT
               ID,SECURITYQUESTION,LOCKEDUNTIL,FIRST_NAME,LAST_NAME,PASSWORD,USERNAME,ROLE_ID,API_PARTNER FROM USER
               WHERE USERNAME=':USERNAME'";
35         sqlQuery.replaceAll(":USERNAME", user);
36
37         Statement statement = null;
38         Connection connection=null;
39         User returnUser = null;
40         ResultSet resultSet = null;
41         try {
42             //Getting connection object
43             connection = ConnectionFactory.getConnection();
44             statement = connection.createStatement();
45             resultSet = statement.executeQuery(sqlQuery);
46
47             if (resultSet.next()) {
48
49                 returnUser = new User();
50                 returnUser.setUsername(resultSet.getString("USERNAME"));
51                 returnUser.setFirstName(resultSet.getString("FIRST_NAME"));
52                 returnUser.setLastName(resultSet.getString("LAST_NAME"));
53                 returnUser.setPassword(resultSet.getString("PASSWORD"));
54                 returnUser.setRole_id(resultSet.getInt("ROLE_ID"));
55                 returnUser.setId(resultSet.getLong("ID"));
56                 returnUser.setSecurityQuestion(resultSet.getString("SECURITYQUESTION"));
57                 returnUser.setapi_partner(resultSet.getBoolean("API_PARTNER"));
```

What style would you prefer?

vs.

Gamified platform

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

InfoSecWorld
Conference & Expo 2018

DEMO

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Matias Madou, Ph.D.,

CTO and co-founder

Secure Code Warrior