Securing the code and waiting for skilled hackers
• >15 years information security

Age is not only a disadvantage!
  – Security engineer for Defense Intelligence
  – C(I)SO for Telco, Retail, Banking
  – Trainer (CompTIA Security+, CISSP)

• Security advisor / Technology Architect

• Secure the future:
  – Pushing my little girl toward black belt
Mick Fanning attacked by shark

ESPN’s Documentary On ‘Shark Attack’ Surfer Mick Fanning Is Brilliant [Video]

Source: http://www.2oceansvibe.com/2016/08/05/espn-documentary-on-shark-attack-surfer-mick-fanning-is-brilliant-video/
Limited to pen-testing team’s skills
Exploiting several vulnerabilities
Harmless and trusted
Good exercising
Time restricted
Localized

Swim and have fun!
This is what you know from previous breaches. Einstein was right: time & space are relative. Exploit everything Not a CTF! Harmful

Swim if you can!
• Some vulnerabilities exploited during the 7 days exercise:
  – SQL Injection
  – Remote OS Cmd Injection
• More than 95% of automated scan findings - not exploited
• All results should be reported
Small apps, small problems. / Big apps, big problems!
Fixing PT Findings

• Too many findings... before launch date
• What that finding means, actually?
• Are there other apps affected?
• Where in the code to fix it?
• Do we have experts?

Who says it’s a weakness?
### Security Standards

#### Benchmark

<table>
<thead>
<tr>
<th>OWASP Top 10</th>
<th>PCI DSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWASP Top 10 Mobile</td>
<td>Mitre CWE</td>
</tr>
<tr>
<td>SANS Top 25</td>
<td>FISMA</td>
</tr>
<tr>
<td>HIPAA</td>
<td>MISRA</td>
</tr>
<tr>
<td>BSIMM</td>
<td>NIST SP 800-53</td>
</tr>
<tr>
<td>DISA STIG 4.1</td>
<td>WASC 2.0</td>
</tr>
<tr>
<td>OWASP ASVS</td>
<td></td>
</tr>
</tbody>
</table>

- Many security standards
- Groups of experts do a great job for us
- Mandatory or not, we have to follow them
- Not easy to know details of all standards
- Static Application Security Testing (SAST) solutions use them for code review
February 23, 2017
Announcing the first SHA1 collision
https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

“Today, more than 20 years after of SHA-1 was first introduced, we are announcing the first practical technique for generating a collision.”

We are not all cryptologists!
What can SAST scanners identify?

- Vulnerabilities in the code (sample from Find Security Bugs):
  ```java
  MessageDigest sha1Digest = MessageDigest.getInstance("SHA1");
  ```

- How these vulnerabilities are propagated in the application:
  ```java
  sha1Digest.update(password.getBytes());
  byte[] hashValue = sha1Digest.digest();
  ```

- Which security standards are not fulfilled:
  ```java
  OWASP Top 10, SANS Top 25, ...
  ```
Not Simple Q: PBEWith... is OK?

Simple A: PBEWith... is not OK!

```java
public static synchronized String encryptString(String str, String pw) throws SecurityException {
    try {
        PBEParameterSpec ps = new javax.crypto.spec.PBEParameterSpec(salt, 20);
        SecretKeyFactory kf = SecretKeyFactory.getInstance("PBEWithMD5AndDES");
        Cipher passwordEncryptCipher = Cipher.getInstance("PBEWithMD5AndDES/CBC/PKCS5Padding");
        char[] pass = pw.toCharArray();
        SecretKey k = kf.generateSecret(new javax.crypto.spec.PBKEySpec(pass));
        passwordEncryptCipher.init(Cipher.ENCRYPT_MODE, k, ps);
        str = new String(passwordEncryptCipher.doFinal(str.getBytes("UTF-8")), "UTF-8");
    }
    return str;
}
```
StandardPBEStringEncryptor myFirstEncryptor = new StandardPBEStringEncryptor();
myFirstEncryptor.setProvider(new BouncyCastleProvider());
myFirstEncryptor.setAlgorithm("PBEWITHSHA256AND128BITAES-CBC-BC");

Bouncy Castle
is a powerful and complete cryptography package.

After several minutes of research...
• White-box Analysis with full access to source code

• Hard to exploit everything during PT exercises

• Results can be used by PT teams for white-box testing

• Compensate lack of application security skills
App Sec: Holistic view

OWASP
The Open Web Application Security Project
After fixing the code, there is a small attack surface left.

Can be input to white box /crowd security testing services.

Will challenge the skilled pen-testers.
• Provides full context of vulnerabilities
• Compensates lack of security skills
• Is developer-friendly
• Complements PT
• Still harmless
• Timely

Thank you!
Sergiu ZAHARIA
https://www.linkedin.com/in/sergiuzaharia/