How to break into Application Security world?

Srikanth Ramu
27/October/2016

Disclaimer:

The views and opinions expressed in this presentation do not necessarily reflect the views and opinions of my employer.

This presentation is intended for education purposes only.

The presenter assumes no responsibility for the Validity, Accuracy or Completeness of the contents.

Some of the points are real world examples for educational purpose and not to endorse any entity.

Agenda

- ❏ What’s wrong with this code?
- ❏ What can go wrong in this code?
- ❏ Application Security
- ❏ Application Security Engineer
- ❏ How to break into Application Security world?

Before we start

October is CyberSecurity Awareness Month

Twitter: @GetCyberSafe managed by Public Safety Canada.

1. What’s wrong with this code? 1/3

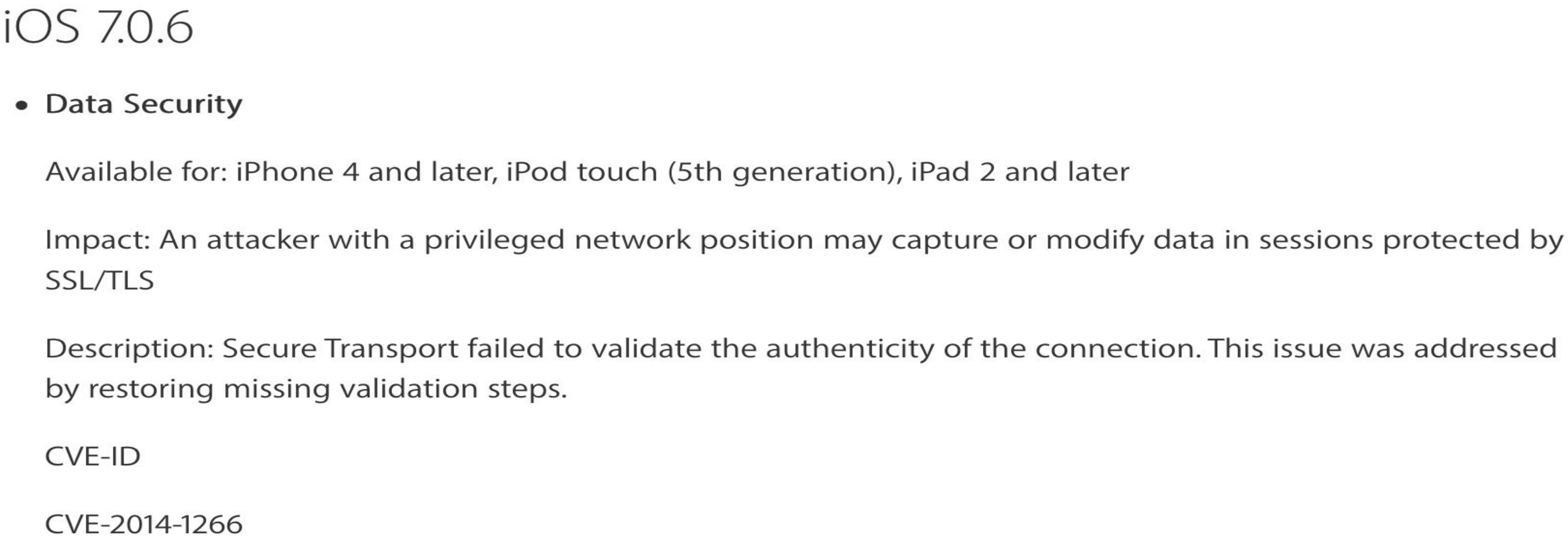
```
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
```

1. What’s wrong with this code? 2/3

```
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;  /* This line should not be here */
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
```

https://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/

1. What’s wrong with this code? 3/3



iOS 7.0.6

- **Data Security**

  Available for: iPhone 4 and later, iPod touch (5th generation), iPad 2 and later

  Impact: An attacker with a privileged network position may capture or modify data in sessions protected by SSL/TLS

  Description: Secure Transport failed to validate the authenticity of the connection. This issue was addressed by restoring missing validation steps.

  CVE-ID

  CVE-2014-1266

https://support.apple.com/en-ca/HT202934

2. What can go wrong in this code? 1/2

```
String user = request.getParameter (“user”);
String pwd = request.getParameter (“pwd”);
String sql = “SELECT * FROM User WHERE user = ‘“ + user + “‘ AND
pwd = ‘“ + pwd + “‘”;
Statement stmt = connection.createStatement ();
ResultSet result = stmt.executeQuery (s);
```

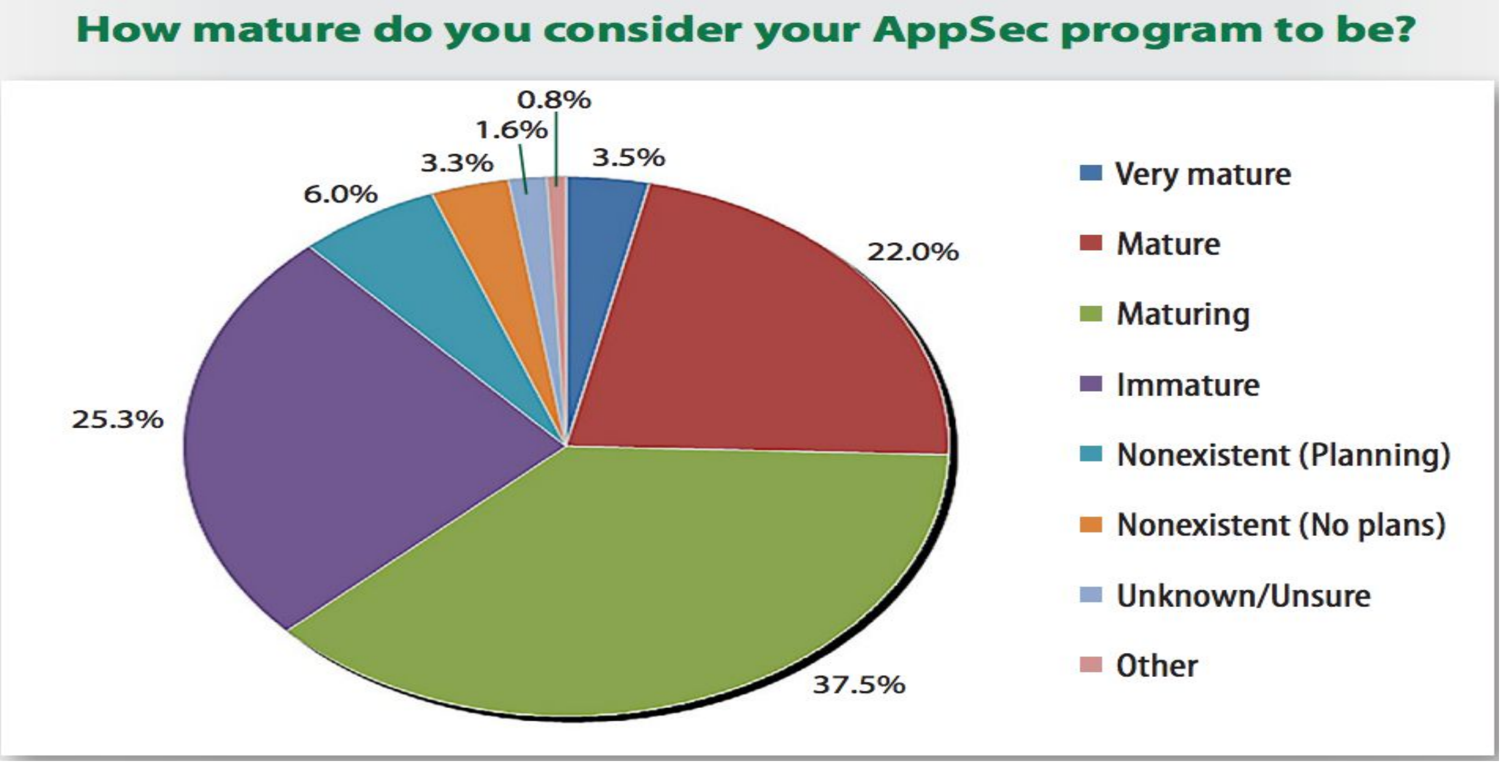
2. What can go wrong in this code? 2/2

```
String user = request.getParameter (“user”);
String pwd = request.getParameter (“pwd”);
String sql = “SELECT * FROM User WHERE user = ‘“ + user + “‘ AND
pwd = ‘“ + pwd + “‘”;
/*Query is constructed from request without any validation and …?*/
Statement stmt = connection.createStatement ();
ResultSet result = stmt.executeQuery (s);
```

National Vulnerability Database - https://nvd.nist.gov/

Application Security

SANS 2016 State of Application Security: Skills, Configurations and Components



How mature do you consider your AppSec program to be?

Application Security Engineer 1/2

Implement Secure Software Development Lifecycle (SSDLC) program

- ❑ Threat Modeling
- ❑ Risk Assessment
- ❑ Code Review
- ❑ Static and dynamic analysis
- ❑ Security testing

Application Security Engineer 2/2

Java Deserialization - AppSec Nightmare - WebLogic, WebSphere, JBoss, Jenkins, OpenNMS

- ❏ Remote Code Execution
- ❏ Denial of Service

https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/

How to break into Application Security world? 1/5

1) Learn and participate in open source projects such as OWASP (www.owasp.org) and http://www.webappsec.org/.
2) Useful tools -
   - HTTP Proxy - OWASP ZAP, Burp Suite etc
   - OWASP Dependency check
   - OWASP Top 10 and CWE Top 25
   - OWASP Application Security Verification Standard Project
   - https://www.ssllabs.com/
   - https://www.kali.org/
   - https://www.owasp.org/index.php/Web_Application_Firewall
   - Wireshark

How to break into Application Security world? 2/5

3) Bug bounty programs and responsible disclosures:

- ❑ $15,000 award! @ http://www.anandpraka.sh/2016/03/how-i-could-have-hacked-your-facebook.html
  - ❑ Password reset code brute force protection even for lesser known test services!

- ❑ Sometimes the bug bounty policies might not be clear.

How to break into Application Security world? 3/5

❑ Professional communication

How to break into Application Security world? 4/5

4) Daily dose of security news:

1. https://www.reddit.com/r/netsec
2. https://isc.sans.edu/podcast.html
3. Bugtraq mailing list
4. Bloggers - https://www.troyhunt.com/, https://krebsonsecurity.com/ etc.

5) Local Security groups - Vancouver

- https://vancitysec.org/
- http://infosecbc.org/
- BSidesVancouver 2017 - Volunteer

How to break into Application Security world? 5/5

6) Publish your research and views on Security - for example maintain a blog.

7) Certifications

8) Some good learning exercises

❏ https://cryptopals.com/ - Crypto Challenges
❏ OWASP WebGoat

References

https://www.sans.org/reading-room/whitepapers/analyst/2016-state-application-security-skills-configurations-components-36917

Q & A