Introduction to Application Security

Hello!

I am James Alt

I am an Enterprise Application Architect at the State of Louisiana. I also run a small consulting company on the side.

You can find me at @jimmyalt

Photo by Tarpit Grover on Unsplash

Information Security

A bunch of seagulls?

Why does InfoSec hate me?

You're actively trying to get them fired...

Have you ever thought about what would happen if there is a security breach because of your app? Who is to blame? You, or the information security team?

They hate everyone...

It's not that big of a stretch now is it?

Security Fundamentals

Confidentiality

Integrity

Availability

Additions

Authentication

Confirming the identity of the entity that wants to interact with a secure system.

Authorization

Specifying access rights to secure resources. These rights describe the privileges or access levels to the resource in question.

Auditing

Keeping track of implementation-level events, as well as domain-level events taking place in a system.

Multi Factor Authentication

Something you know

PIN

Password

Answers to “secret” questions

Keystroke pattern

Something you have

Credit card

Smart phone

Hardware token

Something you are

Fingerprint

Face scan

Iris Scan

Voice print

OWASP

The Open Web Application Security Project

1 Injection

SQL, NoSQL, OS, LDAP

```
namespace do.not.do.this
{
   public class InjectionDemo
   {
       public void InsertUser(string id, string name)
       {
           using(var client = new SqlClient())
           {
               var sql = $"INSERT INTO Users (id, name) VALUES ('{id}', '{name}')";
               client.ExecuteSql(sql);
           }
       }
   }
}
```

2

Broken Authentication

Incorrect implementations

3

Sensitive Data Exposure

Weakly protected data

XML External Entities (XXE)

Entity references within XML documents

5

Broken Access Control

Authorization & Permissions

6

Security Misconfiguration

Incomplete and insecure configurations

7

Cross-Site Scripting

Trusting untrustworthy code

8

Insecure Deserialization

Gateway to other attacks

9

Using Components with Known Vulnerabilities

Dependencies all the way down

10

Insufficient Logging & Monitoring

Do you even know what’s going on?

Does my code have vulnerabilities?

Don’t just think about it, find out!

- Vulnerability Scanning
- Code Review
- Penetration Testing
- Static Analysis

Based on those results, take action and make an informed decision.

Vulnerability Scanning

Detects when systems could be compromised

- Searching for known vulnerabilities
- Can and should be automated
- Should be done regularly

Code Review

Security Code Reviews

Penetration Testing

Identifies and reduces weaknesses

- Attempts to identify
  - Insecure business processes
  - Weak security settings
- Doesn't need to happen as often but should be done on a regular basis.
- Should be conducted by a third-party

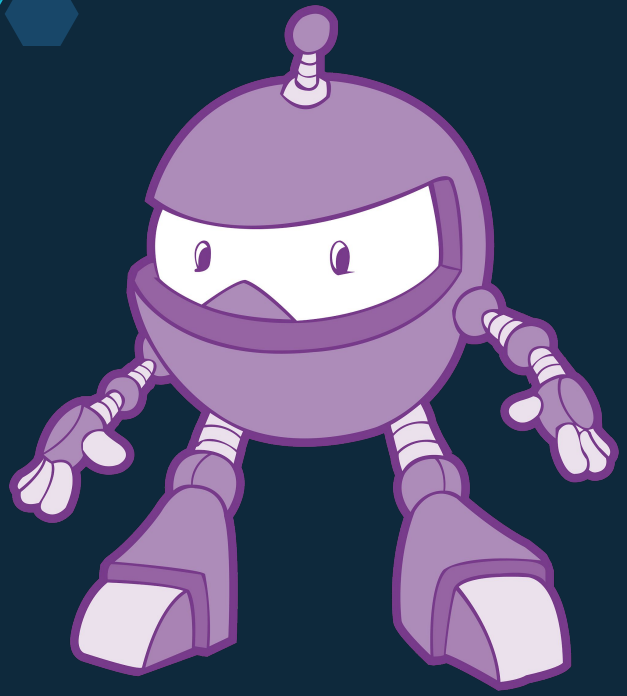
Static Analysis

- Scales well
- Useful for things that can be automatically found with high confidence
- Good for developers

Not a silver bullet, has a potential for a high number of false positives.

DEMO

Static Analysis for ASP.NET Core



.NET & SQL Server User Groups

- Second Wednesday of every month
- Free food
- Learn new things
- Network with great people
- https://bit.ly/brusergroups

Thanks!

Any questions?

You can find me at:

- @jimmyalt
- james.alt@la.gov
- http://bit.ly/appsecsqlsat2018

Appendix

OWASP Top 10 - 2017

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Code Review Guide - V2

https://www.owasp.org/images/5/53/OWASP_Code_Review_Guide_v2.pdf

Reddit Security Incident

https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

Security Code Scan - Static code analyzer for .NET

https://security-code-scan.github.io/

';--Have I Been Pwned?

https://haveibeenpwned.com

.NET & SQL Server User Groups

https://www.meetup.com/Baton-Rouge-NET-and-SQL-Server-User-Groups/