Security Challenge Review

• How did your team to
• What vulnerabilities were easiest to exploit
• What vulnerabilities were hardest to defend
• What did you overlook
Pre-Class Review

• You looked at aboutthedata.com
  • What did you find?
  • How accurate was the data?
  • What surprises did you find?
  • Are you comfortable with outsiders having this data?
Privacy and Web Applications

• What is privacy?
• How important is privacy?
• What data do you want to keep private?
Privacy Policies

• Statement saying what the web site does with any information it collects
  • Or otherwise obtains from the user
  • And why the web site needs this information
• Generally considered legally binding
  • Must obey the laws of the land
  • Different lands have different laws
• Users may or may not pay attention
  • Google privacy policy
  • itunes store policy
Sensitive Information

- Personal information
  - Name, address, phone, email
  - Age, sex, race, ...
  - Past contributions, purchases, rentals, friends, ...
  - Why is this sensitive?

- Financial information
  - Credit cards
  - Bank accounts

- Legally sensitive
  - Health information (HIPA)
  - Student information (FERPA)
  - Information from children
Using the Data

- Amazon
- Google
- Facebook
- Microsoft
- Apple
Using the Data

• Data might be required for the application
  • Credit card numbers
  • Order information

• Data might be helpful to the application
  • Past buying history in making recommendation
  • Past credit cards used
  • Past shipping history

• Data might be helpful in the future of the application
  • Data might be needed to assist application sponsors
  • Targeting ads, emails, etc.
Why Care About The Data

• The data might be worth more than the application
  • Selling personal information is lucrative
  • Providing contacts is lucrative
  • Ads are worth more if targeted correctly
  • Ads pay for the application

• The data can be misused if it gets in wrong hands
  • Unauthorized use of credit cards
  • Release of health information
  • Who looks at pornography
  • Who cheats on their spouse

• Laws make your application responsible
  • For specialized data
  • For general privacy (EU)
Securing the Data

• Your application is responsible for its data
  • If it is stolen, given out, etc.

• You should make sure the data is secure
  • Encrypting the data
  • Limiting access to the data

• You should make sure the data is safe
  • Backup, recovery plans, ...
The Role of a Privacy Policy

• Delineate what types of information are collected
  • Whether that information is used immediately or saved
  • If saved, for how long it is kept
  • If saved, can the user request it be deleted

• Specify why the information is needed
  • Not always done
  • Useful if the application is not obvious

• Specify who owns the information
  • If user owns the information, company can’t use it freely
  • If company owns the information things are more flexible
The Role of a Privacy Policy

• Specify what the application can do with the information
  • Use in the application only
  • Use in the application and the owning company
  • Use in the application, owning company, affiliates
  • Share (sell to) with related businesses
  • Share (sell to) with anyone

• Specify what controls you have over the information
  • Can you stop it from being collected
  • Can you request any collected information be discarded
  • Do you obey requests not to track?
Legal and Ethical Issues

• Privacy has ethical and legal implications
  • Already covered by laws in many places
  • Already covered by laws in many domains
  • European policy is generally much stricter than US

• You are responsible for breaches of your policy
  • You need to use “best efforts” to avoid them
  • Implications can be large
    • Fines, imprisonment
    • Cost to protect the consumer
    • Costs related to the breach
    • Costs to your company's reputation
Other Legal and Ethical Issues

• If your web site sells something
  • That doesn’t get sent
  • That isn’t valid (i.e. airline ticket)
  • That is defective

• If your web site performs a critical purpose
  • Analyzing data to determine if you are sick or not
  • Monitoring a nuclear plant
  • Creates lethal X-rays
  • Crashes an airplane

• Click-Through Licenses
Other Legal and Ethical Issues

• What if your web site gives out bad advice
  • Bad medical advice
  • Bad legal advice

• What if your web site gives out fake product ratings

• What if your web site disguises ads as fact
  • Fake news

• What if your web site freely distributes private material
  • Copyright violations

• What if your web site becomes compromised
Your Responsibilities

• You are the creator/maintainer of the web site
  • You should understand your responsibilities
  • Both legally and morally

• How much attention should you pay to these issues
  • As you design the site
  • As you code the site
  • As you develop a privacy policy

• Is it more important to get a working application fast
  • Or to have a secure one?
  • Is this really a trade-off?
Privacy and Your Projects

• We expect your web application to have a privacy policy
  • As long as there is any data being used
  • Readable, accessible
  • Privacy policy generators exist

• Client projects
  • Work with client on this (or use existing policy)

• Student projects
  • Develop a policy as part of the web site
Testing

• When looking at security and privacy
  • We keep asking “what can go wrong”
  • What happens if a user does <x> when <y>
• You want to do this in general for your application
  • To make sure it will work
  • To make sure it will keep working
You’ve Built a Web Application

- What do you know about it
  - Does it work?
  - Does it work correctly?
  - Does it work correctly under all circumstances?
  - Will users like it?
  - Did you build the right application?
  - Will it scale?

- How do you answer such questions?
  - Testing
What is Testing?

• The process of running software in order to find bugs
  • Not to show that bugs are not there
  • What is the difference?

• **A successful test case is one that finds a bug**

• Good testers are people who
  • Can sit in front of software and break it
  • Are in the frame of mind where you want to break things
  • Are TAs grading homework assignments

• Testing won’t show what’s right, just what isn’t wrong
Software Testing

- Introduced in 15/16/17/18/32
  - Agile programming: write the test cases first
  - Incremental development: continuous testing
- You’ve possibly seen tools to help with testing
  - JUnit for java testing
    - Test cases are methods annotated with @Test
    - Automatically find and run all tests for a system
  - Supports repeated testing
Regression Testing

• Testing software once is not very useful
  • You might make it work for some case then
  • But what if the software changes
  • Did you test the right case?

• Regression tests
  • Tests that are run each time the system changes
  • Rerun after each change to ensure no regression

• Test cases are permanent, not throw-away
  • How to do this for web tests?
Next Time

• Project presentations
  • For those not handing in a report

• Testing
  • We will look at different testing technologies
  • And then give you a chance to try them on your projects
Different Kinds of Testing

• Functional testing
  • Test an individual function
  • Extend to handle scenarios or use cases

• Continuous testing
  • Emphasizes integration and system testing
  • Make sure the system as a whole works correctly

• User testing
  • Determine what users like and dislike, errors made, etc.

• Stress testing
  • Test with large problems or lots of users
  • Finding the limits of a system
Testing Web Applications

• Is software testing relevant to web applications?
  • Individual functions are event-triggered
    • Not easily tested
  • The app is all user interface
    • Hard to create test cases
  • The back end is inside a server framework
    • Difficult to test it by itself
  • The database is live
  • Actions to test might have real-world consequences
Testing Web Applications

• You still should test your web applications
  • Lots of tools and techniques exist
    • No real standards or stand outs
• Testing should be done at all levels
• Testing should be considered from the start
  • Plan a test database, etc. to facilitate
  • Design the application to facilitate testing
What Can Be Tested

• Usability
• Front end: HTML, CSS, Links
• Back end: unit test the node.js/php/python/...
• Application testing (front + back end)
• Compatibility testing
• Performance testing
• Stress testing
• Security testing
• Accessibility testing