CSCI 1320
Creating Modern Web Applications
Lecture 29-30: Security Challenge
Mechanics

• We are going to take 2 classes to let you experiment with web site security.

• PRELAB (should be done already)
  • Split into teams
  • Install the insecure server on a public site
  • Each team makes a list of vulnerabilities
  • Each team gets to choose defend or attack
  • Each team should have done some preliminary work
Web Site

• We have provided you with a simple web site
  • Using HTML, CSS, Node.js, MySQL
  • You have access to source code, tables, etc.

• There is certain private information
  • Passwords, Bank account information, social security numbers, ...
Attacker’s Goal

• Access the private information
• Alternatively, disable or break the web site
Defenders’ Goal

• Protect the private information
• Keep the web site up
• Keep the web site functional
Constraints

• Only minimal changes to database tables
  • Can add fields, nothing else
  • Basic functionality and URLs should remain the same
• Source code needs to be available
• Can’t use more than 3 computers simultaneously to attack
  • (No distributed denial of service attacks)
• Otherwise, anything goes...
Schedule: Class I

• Defenders:
  • Upload your safer server to host
  • Post the URL of your web site – on the white board
  • Monitor the logs

• Attackers:
  • Run your scripts/tests against as many servers as you want
  • See what works and what doesn’t
  • You can use curl or selenium if desired

• Both:
  • Make plans for better defenses, improved attacks
  • Edit your servers/attacks as needed
Schedule: Homework I

• Create improved server, improved attacks
Schedule: Class II

• Defenders:
  • Upload your safer server to host
  • Post the URL of your web site on the whiteboard
  • Update your site as needed during class

• Attackers:
  • Provide scripts
  • Modify scripts as needed
Homework II

• For class on Monday
  • Written hand-in
  • Be prepared to present

• List the security flaws
  • Defenders
    • That you missed in the initial implementation and fixed
    • That still exist in your implementation
  • Attackers
    • That you successfully exploited
Next Time

• Project presentations
  • For those not handing in a report
  • Make the presentations interesting and informative
    • Teach the class how things are done in practice
  • Make the presentations entertaining

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

• Privacy

• Pre-Class Work:
  • Sign up at aboutthedata.com and check that data that Acxiom has on you personally. Is it accurate? Are you comfortable with them having this data? Is any of the data surprising?
  • Come prepared to discuss (without revealing private information)