PROJECT 3 – WEB SECURITY

CS 6324: Information Security

What is it about?

- You are provided with code to an online bulletin board – “hackme”
  - Users can register accounts
  - Users can login, post blogs, or read posts
- Perform a series of attacks on the website
- Fix the website’s code to prevent such attacks

hackme

- Hosted at fiona.utdallas.edu
- php-based:
  - Beginner guide to PHP is available at the course website.
- Files:
  - index.php: login interface
  - members.php: login check, and global thread view
  - show.php: view one thread
  - post.php: post a new thread
  - register.php: register a new user
  - connect.php: db connection utilities
  - others: header.php, footer.php, style.css

Password Management

- Explore how passwords are “managed”
- Identify 2 vulnerabilities:
  - Should be something other than “weak passwords” and should not involve cookies
- Fix the vulnerabilities

Session Management

- Cookies!
- Describe how they are used
- Identify 3 vulnerabilities
  - HINT: look at what the cookies store, how they store it, how checks are performed
- Fix the vulnerabilities

Cross Site Scripting (XSS)

- Users are allowed to post new threads
  - Posts are *allowed* to contain HTML
- Craft a new post that conducts a XSS attack to steal users' cookies
  - If a user views your posting, his/her cookies should be stored in a file at the attacker's server.
  - Explain what, how and why?
- Provide any extra webpages, files, scripts that the attacker needs
  - I should be able to replicate your attack!
- Fix the vulnerability that caused this
  - The code fix should make your attack impossible.

Cross-Site Request Forgery (XSRF)

- Post a new thread **without** the user's consent
- Attack:
  - Lure a user to your malicious website while he is logged in to hackme
  - Post an advertisement to hackme
    - "You won the lottery!"
  - Should be completely (100%) stealthy (no redirection, etc.)
- Describe the vulnerability
- Explain three methods to prevent this attack

SQL Injection Attack

- Private version at [http://fiona.utdallas.edu/hackme]:
  - But you need a secret key to register a user account.
- Use an SQL-injection attack to register a new user and post something on the bulletin board
- Explain your attack:
  - Where, how + exact input.
  - I should be able to replicate it.
- Fix the vulnerability.

Weak Password attacks

- hackme does not check password strength
- A group of 100 users registered user accounts with weak passwords
- You need to recover their passwords by running a brute-force dictionary attack
- Get a corpus of weak passwords
  - Many are available online
- If you recover all 100 passwords, you get bonus points!

Weak Password attacks

- Usernames available in users.txt
- Your results should be in a separate file. Each username should be on a separate line

  username <tab> password
- The order of usernames should be the same as the order in users.txt
- If you do not recover a password for a user, write the username on the line
  - I want to be able to run diff to grade this.

Logistics

- Your website is on fiona.utdallas.edu
  - Your home directory will contain a web directory called “public_html”
  - You can access anything you put there on

  http://fiona.utdallas.edu/~username/

Logistics

- You will all be using the same database backend
  - Username: cs6324spring21
  - Database name: cs6324spring21
  - Schema: cs6324spring21_schema.sql
  - Play Nice!

- Another database is used for SQL injection attacks and weak passwords

Fixes

- Your code should run with no errors
- Fix the vulnerabilities without introducing new ones!
- Point clearly to the files you changed and what you changed and why?

What to submit:

- The complete modified source code for the webpage
- Supplemental files, scripts and webpages needed for the attack
- pass.txt: list of recovered passwords
- Complete running final version of your website at: fiona.utdallas.edu/~username
- Written portion of the project
  - PDF only.
- If you want to use extra days in this project, please notify me before the due time.

Questions?