CMSC 433
Programming Language Paradigms and Technologies
William Pugh
Feb 23rd, 2010
Project 2 grading

• In progress
• Leave your deployments up
• Don't change them; they should match your source code
• In several cases, submissions didn't include source code, or deployment descriptors weren't provided
  • students have been contacted
Project 3

- You really, really, *really* should have already accomplished the following:
  - Installed ANTLR and ANTLR plugin
  - Updated Course project manager plugin
  - Checked project out of CVS
  - Tried submitting project, check that it compiles on submit server
- Due Thursday, 11:59pm
Project 4 - Concurrency

• Concurrent graph explorer
• Due Wednesday, March 3rd
  • only one release token
• Posted to web, cvs and submit server
Project 5 - Concurrency

- Another concurrency project, TBA
- Due Tuesday, March 9th
Midterm

- Thursday, March 11th, in class
Web security exercise

• Craft a URL that, when opened, will make a signed in user add your linuxlab account to my guestbook on appengine

• I'll remove my CSRF forgery protection for GET requests

• Feel free to add more than just your name: e.g., cs433050 rocks

• Add URL to form for web security exercise

• Due Monday, March 1st
Open source contribution project

- Due March 12th
- Post a link to a web page describing your idea
- Can be a google doc, a web page hosted somewhere, whatever
- If anyone wants to do a group effort, needs to be submitted by March 12th
- For solo projects, you need to submit an idea but you can change your mind
Cookies with the professor

- Can delayed/postponed due to snow
- Restarting
  - tomorrow, Wednesday Feb 24th, 1:30pm
  - Friday, Feb 26th, 11:00am
  - Tuesday, March 2nd, 11:00am
Cross site request forgery

• Want to only act on requests from webpages that our website generated

• XSS: bad code on web pages generated by our web server

• CSRF: trick our web server into acting on requests from other web pages as though we generated the page/request
Initiating CSRF

- Get user to click on link or view web page
- Users click on anonymous links all the time
- View a web page (or email?)
- Embedded 1 pixel images or forms in hidden frames auto-submitted via JavaScript
CRSF

- Sometimes, you want to allow other sites to generate requests to your web site
  - for example, "show tickets for Black Eyed Peas"
- But requests to change password or transfer funds…
  - only we should generate such requests and perform them for signed in users
Can check referrer field

- From good users, if referrer header present, generally trusted
- but vulnerabilities exist
- If you get a POST request and the referrer field doesn't match, reject the request
- What to do if no referrer present?
Support for referrer field

Figure 2: Requests with a Missing or Incorrect Referer Header (283,945 observations). The “x” and “y” represent the domain names of the primary and secondary web servers, respectively.
Removing referrer field

- Attackers can force the removal of referrer field
- e.g., bounce user off of ftp: page
- lenient referrer checking blocks requests with a bad referrer, but allows requests with no referrer
- do not depend upon lenient referrer checking
Spoofing referred field

- Flash had a vulnerability that allowed referrer field to be arbitrarily set
- Internet explorer XmlHttpRequest vulnerabilities allowed referrer field to be arbitrarily set
- No current vulnerabilities?
- Prize if you are able to demonstrate http referrer spoofing with standard software
What if referrer field not present?

- If you want to handle this situation, then you need to include a secret in every link/form.
  - can use a hidden form field, or encode it directly in the URL.
- Must not be guessable value.
  - can be same as session id sent in cookie.
Real CSRF vulnerabilities (now fixed)

- [http://citp.princeton.edu/csrf/](http://citp.princeton.edu/csrf/)
- Generate email from NYTimes using logged in user's email
- On YouTube, mark videos as favorites, add people to user's "Friends" or "Family" lists, mark videos as inappropriate, pretty much anything
- ING DIRECT: transfer funds to another account
Good resources

- http://citp.princeton.edu/csrf/
- http://portal.acm.org/citation.cfm?id=1455782
- http://seclab.stanford.edu/websec/csrf/csrf.ppt
With great power comes great responsibility

• Trying out a web site to see if it is vulnerable can get you in big, big trouble
Project 4 - parallel graph exploration

• You have a graph with nodes and directed edges

• Want to find the set of nodes reachable from a start node, and perform a computation at each node

• both the determination of the set of edges from a node, and the computation at that node, may take time

• Want to use a certain amount of parallelism to do that

• not much more, not much less
Implementation

- Don't use locks, synchronization, or thread creation
- Instead, use:
  - ExecutorService
  - Future
  - other classes from java.util.concurrent