CS6003: Web Security

Course Overview & Logistics

Kameswari Chebrolu
Room 302, Kresit
Department of CSE, IIT Bombay

(Course website: robin.bodhi.cse.iitb.ac.in)

CS6003 Course Content

- Module-1: Web Background
  - Motivation, brief history
  - What constitutes a web page
  - Browser internals
  - Web protocols
  - Session management
  - Server internals
  - Web security landscape.

- Module 2: Server side attacks and defense
  - SQL (Structured Query language) injection
  - Server Side Request Forgery (SSRF)
  - Information disclosure
  - Command injection
  - File Upload Vulnerabilities
  - Authentication Vulnerabilities
  - Authorization Vulnerabilities
  - Path traversal
  - DOS attacks
  - Firewalls and Web Application Firewalls

- Module3: Client side attacks and defense
  - Cross Site Request Forgery (CSRF)
  - Cross Origin Resource Sharing (CORS)
  - Cross Site Scripting (XSS)
  - Web sockets
  - Clickjacking
- Miscellaneous: (Time Permitting)
  - Server Side Template Injection
  - Third Party Code
  - Web LLM attacks
  - HTTP Parameter Pollution
  - Subdomain Takeover

Hands-on Labs

- Hand-in-hand with theory, we will also have periodic lab sessions
  - Firefox/chrome browser developer tools
  - OWASP ZAP, a versatile tool for web application security testing
  - A subset of server side attacks
  - A subset of client side attacks

(Lab sessions during regular class on select days)

References

- “Computer Security: A hands-on Approach”, Third edition, 2022 by Wenliang Du (only part-II on web security)
- Web Security for Developers: Real Threats, Practical Defense by Malcolm McDonald, No Starch Press, 19 Jun 2020
- Real-World Bug Hunting: A Field Guide to Web Hacking by Peter Yaworski, No Starch Press, 9 Jul 2019

- https://portswigger.net/web-security/all-materials
- https://owasp.org/www-community/attacks/
- https://developer.mozilla.org/en-US/docs/Web
- https://www.zaproxy.org/docs/

Pre-Reqs

- Knowledge of unix command line
- Python
- HTML, CSS, Javascript
- SQL
- Exposure to PHP or other dynamic web frameworks is useful but not necessary.

Evaluation

Safe Quizzes -2	20%
Regular Labs (attendance + submission)	10%
Midsem + Lab exam	15 + 15 = 30%
Final + Lab Exam	25 + 15 = 40 %

Next Action Item

- You will be enrolled on Bodhitree
  - Material will be shared there
- cLab app needs to be installed
  - Instructions will be shared closer to the first lab (8th Aug)

Enrollment

- Course open only to CS students
  - Only 2 TAs, hands-on labs → 80 capacity (really stretching it here)
  - No exceptions will be made!
- Highly competitive!
  - 350+ applied in pre-registration; 45 shortlisted based on CPI
    - Not serious please drop -> waitlisted will get chance!

Questions ???