Imperial College London

446H – Applied Network Security

1. Web application security

Dr Sergio Maffeis
Department of Computing
Course web page: https://446h.cybersec.fun

Project 1

Imperial College London

- **Web application security auditing tool**
- Goal: passive security auditing of websites
  - to be used on non-malicious websites, currently not under attack or compromised
  - report security misconfigurations, or failure to use best security practices.
- Build a Chrome extension
  - user navigates and interacts with interesting websites
  - extension reports warnings relevant to visited pages, observed events
  - this should be a passive scanner
    - the extension does not tamper with parameters or issues new requests by itself

Budget your effort

Imperial College London

- Each group member should aim to spend about 6 hours on the project
- It will not be possible to address more than one or a few concerns.
- Strike a balance between depth and breadth of the audit.
- Take usability in consideration, and in particular avoid reporting false positives.
- Make sure to evaluate the effectiveness of your extension by running appropriate experiments.

Requirements (1)

Imperial College London

- Deployment
  - Work on reasonably recent versions of Chrome
    - on reasonably modern desktop operating systems.
  - Work out-of-the-box when using the "load unpacked extension" functionality of Chrome.
- Quality of service
  - Extension should stay active (and not crash) also on large, reactive websites
  - The extension should not interfere with the functioning of the visited website.
  - Ok if it slows down a site or occasionally cause an error

Requirements (2)

Imperial College London

- Output
  - Incrementally generate a report
    - in a separate window
    - in a panel of the development console of Chrome
  - Each entry should detail the issue identified and useful context
    - what is the top level website being visited?
    - what element on the page or iframe the issue refers to?
    - what page or iframe issued the request being reported?
  - Each entry should have a numeric severity score

Report

Imperial College London

- 2-3 pages long, please write clearly and concisely
  - what you are detecting
    - why that is relevant, what attacks could be possible?
  - how to use the extension and interpret its output
  - what the key technical ideas and/or challenges in your implementation are
  - how you have evaluated your extension
  - describe specific examples of your extension findings, and your assessment wrt to the security of the visited website(s)
- The goal of the report is to help me assess your project weeks after you have presented it

Discussion

Imperial College London

- What can we capture from an extension?
- Some examples
  - lack of use of security-relevant headers were most appropriate
  - misconfigured CSP or Sandbox policies
  - state-changing requests that are open to cross-site forgery
  - direct inclusion of scripts from third-party websites
  - DOM-based XSS