CSci 5271
Introduction to Computer Security
Day 27: Student Project Presentations #3

Stephen McCamant
University of Minnesota, Computer Science & Engineering

Outline

Password managers (D D S) 2:30

JIT spraying 2:43

Persistent data-only malware 2:55

SVG vulnerabilities 3:08

Announcements, evaluations 3:20

Outline

Password managers (D D S) 2:30

JIT spraying 2:43

Persistent data-only malware 2:55

SVG vulnerabilities 3:08

Announcements, evaluations 3:20

Outline

Password managers (D D S) 2:30

JIT spraying 2:43

Persistent data-only malware 2:55

SVG vulnerabilities 3:08

Announcements, evaluations 3:20

Outline

Password managers (D D S) 2:30

JIT spraying 2:43

Persistent data-only malware 2:55

SVG vulnerabilities 3:08

Announcements, evaluations 3:20

Outline

Password managers (D D S) 2:30

JIT spraying 2:43

Persistent data-only malware 2:55

SVG vulnerabilities 3:08

Announcements, evaluations 3:20

Final exam Thursday 12/18

- Same room (ME 108), 10:30am-12:30pm
- Similar to midterm:
  - Open-book, open-notes
  - Multiple-choice and exercise-like questions
- Slightly longer than midterm
- Comprehensive, but weighted on second half of course

Optional review session

- Thursday 6:30pm in 3-125 Keller
  - (Sorry, no UNITE coverage)
- Similar to office hours: bring questions
- N.B., not a "get Yang to reveal the exam questions" session

Reflected XSS

```
String username = req.getParameter("username");
if (username == null)
     username = "";
String digest_hex = ...;
resp.setStatus(HttpServletResponse.SC_OK);
resp.setContentType("text/html;charset=utf-8");
resp.getWriter().print("User \"");
resp.getWriter().print(username);
resp.getWriter().print("\" is id'd with the MAC ");
resp.getWriter().print(digest_hex);
resp.getWriter().println("\".");
```

DOM-based XSS dangers

- XSLT
- XHR
- JSON
- CSS

ViruSniff

- "100% effective"?
- Possible without solving the halting problem?
- Mimicry attack against ViruSniff
- Countermeasures

DoS protection: Sly's scheme

- Requests get delayed bit if not first in queue from their IP
- Delayed requests re-queued until a second has passed
- Can an attacker still deny service?

DoS protection: Carl's scheme

- When overloaded, redirect traffic to previous clients
- Can attackers still deny service?
- What else can go wrong?