

# CS 461 / ECE 422

## Midterm Review Jeopardy

University of Illinois

ECE 422/CS 461

# Midterm

- Quiz 7 due tomorrow
- March 13<sup>th</sup> in class (12:30-1:45, 1404 Siebel)
- Multiple choice and short answer questions
  - Will use Scantron, bring pencil (and eraser)
- Open note (no restriction)
- Closed device
- Testable content: all lectures, discussions, MPs
- Sample midterm available on Canvas

# This Lecture

- A Jeopardy-inspired review game!
- Some questions are NOT good sample exam questions
- Instructions
  - After I read a question, anyone can raise hand. The first person to raise hand will be called on.
  - If you get the answer right, you can pick the next question!
  - Correct answers rewarded with ... bragging rights!

**Software  
Security**

\$100

\$200

\$300

\$400

\$500

\$600

**Web  
Security**

\$100

\$200

\$300

\$400

\$500

\$600

**OS  
Security**

\$100

\$200

\$300

\$400

\$500

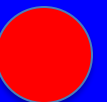
\$600

## Software Security \$100

Consider the following function in x86

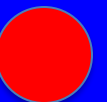
```
void add(int x, int y, int z);
```

Where is parameter x located on the stack immediately after the call to add?



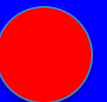
## Software Security \$200

**What attack makes use of functions that already exist in memory to defeat Data Execution Prevention (DEP)?**



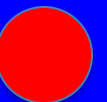
## Software Security \$300

What type of virus modifies itself semantically every time it propagates to a new host?



## Software Security \$400

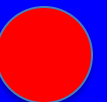
Name a type of memory corruption vulnerability that is guaranteed to happen on the heap.





## Software Security \$500

Which register(s) is/are modified  
by the x86 “ret” instruction?



# Software Security \$600

How would you set up the stack when using ROP with the following gadget in order to set %eax to 2?

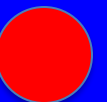
L1: xor %eax, %eax

L2: pop %edx

L3: inc %eax

L4: pop %ebx

L5: ret



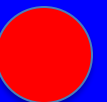
## Web Security \$100

In this type of web attack, a malicious server takes advantage of a client's logged-in session on another website to send web requests that perform actions not intended by the client.



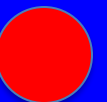
## Web Security \$200

This technique uses a library function to sanitize inputs and insert them into a templated SQL query to prevent SQL injections.



## Web Security \$300

This HTTP header can tell the browser to not execute inline `<script>` tags. It also can specify trusted origins to fetch scripts from.



## Web Security \$400

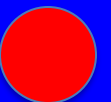
What is the difference between Stored and Reflected XSS? Which of these did you create in MP2?



# Web Security \$500

Explain the rules for when cross-origin requests can send cookies for each of the 3 SameSite options:

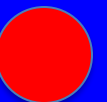
1. None
2. Lax
3. Strict



## Web Security \$600

Write a SQL injection that returns just one row corresponding to the user with username 'victim'.

```
SELECT * FROM users  
WHERE username = 'not_victim'  
AND pw = '{INPUT_HERE}'
```





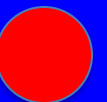
## OS Security \$100

**This component of the Linux Audit framework is responsible for writing events to disk and generating reports.**



## OS Security \$200

**Spoofing attacks are most likely to be a problem with this authentication method.**



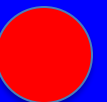
## OS Security \$300

Linux Security Module is most closely related to this pillar of Lampson's “Gold Standard” of Operating System Security.



## OS Security \$400

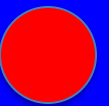
**This technique prevents the attacker from pre-computing a lookup table to aim cracking of password hashes.**



## OS Security \$500

What does the following command do?

```
chmod 754 ./grading.sh
```



## OS Security \$600

Consider a program “ $A[x] += 1$ ” runs on a processor with a 1KB direct-mapped cache with 64B cachelines.

How many bits of information might an attacker learn about the variable  $x$  using the prime+probe attack?

