Problem 1 [15 pt]

- **1 pt** for each part
- **0 pt** if you gave more than one term

Problem 2 [20 pt]

2a: stack layout [12 pt]

- Contents and order [6 pt]
  - error in arg entry [–2 pt]
  - error in any other entry [–1 pt]
- Addresses [6 pt]
  - addresses in decimal but otherwise correct [–2 pt]
  - addresses in increasing order but otherwise correct [–2 pt]
  - j2: treating an int as 1 byte [–2 pt]
  - one wrong offset [–2 pt]
  - addresses missing (or wildly off) but sizes ok [–4 pt]
  - buf: treating a char as 4 bytes [–4 pt]

2b: badfile for g() [3 pt]

badfile: N nonzero bytes [2 pt] + 4-byte Z1 [1 pt]

- N is 36 for exam-1-01; N is 28 for exam-1-02
- N off by 4 bytes [–1 pt]
- N off by more [–2 pt]

2c: badfile for g(4) [3 pt]

- Answer 1 (wrong but full marks):
  - badfile: N nonzero bytes [1 pt] + 4-byte Z1 [1 pt] + 4-byte 4 [1 pt]
  - –1 pt for incorrect N (regardless of 2b)
- Answer 2 (correct)
  - badfile: N nonzero bytes [1 pt] + 4-byte Z1 [1 pt] + 4-byte nonzero + 4-byte 4 [1 pt]
  - Bonus +2 pt

2d: Canary [2 pt]

- correct location (below saved ebp) [1 pt]
- correct size (4 bytes) [1 pt]
- absurdly wrong size or location [0 pt]

Problem 3 (exam-1-01) [10 pt]

- 3a: injection [6 pt]
  - `414’); UPDATE Grades SET (Grade = ’A’) WHERE (Course = ’414’ AND Name = ’Bob’);`
    [2 pt] **[4 pts]** →
  - Missing “)” [–1 pt]
- 3b: prepare [4 pt]

  `getcourseinfo.php:`
  `$stmt = $db->prepare("SELECT * FROM Courses WHERE (CourseName = ?);");` **[2 pt]**
  `$stmt->bind_param("s", $csname);` **[2 pt]**
  `$stmt->execute();` **[0 pt]**

Problem 3 (exam-1-02) [10 pt]

- 3a: injection [6 pt]
  - `a1=Bob’); --&a2=whocares&a3=fqr123`
    [2 pt] **[2 pt]** **[2 pt]**
  - `a1=Bob’); UPDATE Users SSET Pwd=’fqr123’ WHERE Name = ’Bob’;)`
  - Missing “)” [–1 pt]
- 3b: prepare [4 pt]

  `chpw.php(name, opwd, npwd):`
  `$stmt = $db->prepare("UPDATE Users SET Pwd=’?’ WHERE (Name=?’ AND Pwd=’?’);");` **[2 pt]**
  `$stmt->bind_param("sss", $npwd, $name, $opwd);` **[2 pt]**
  `$stmt->execute();` **[0 pt]**

Problem 4 (exam-1-01) [5 pt]

- Vulnerability exploit [3 pt]
  `filename` a symbolic link. Change where it points to between first `fopen` and second `fopen`.
- Fix [2 pt]
  Replace last two statements by: `return temporary`.

Problem 4 (exam-1-02) [5 pt]

- Yes.
  `y` is in heap, not stack, so canary doesn’t help **[3 pts]**
- 16 nonzero bytes **[1 pt]** + 4-byte `0xababab` **[1 pt]**

Problem 5 [5 pt]

- Yes **[2 pt]**
  No: **0 pt** for the entire problem
- Fix **[3 pt]**

Problem 6 (exam-1-01)

- protocol **[2 pt]**
- hostname **[2 pt]**
- port **[1 pt]**

Problem 6 (exam-1-02)

- **hostname =** `www.cs.umd.edu` **[1 pt]**
- **path =** `projects/tss/index.html` **[2 pt]**
- **protocol =** `https` **[2 pt]**

Problem 7 (exam-1-01)

- `x`: number of chars [2 pt]
- `y`: size of memory block [3 pt]

Problem 7 (exam-1-02)

- 1 pt for each part

Problem 8

- **8a**: `seteuid(uid)` **OR** `seteuid(uid)` **[3 pt]**
- **8b**: `setuid(uid)` **[2 pt]**

Problem 9

- All or nothing