

CSE 484 In-class Worksheet #3

Name: _____ UWNNetID: _____ Date: _____

Email address: _____

Partner names for this activity: _____

Q1: The goal of this code is to allow a program to open regular files, but not symlinks.

```
int openfile(char *path) {
    struct stat s;
    if (stat(path, &s) < 0)
        return -1;
    if (!S_ISREG(s.st_mode)) {
        error("only allowed to regular files!");
        return -1;
    }
    return open(path, O_RDONLY);
}
```

Can you spot any potential problems?

Q2: Consider this code:

```
char buf[80];
void vulnerable() {
    int len = read_int_from_network();
    char *p = read_string_from_network();
    if (len > sizeof buf) {
        error("length too large, nice try!");
        return;
    }
    memcpy(buf, p, len);
}
```

And note the following definitions:

```
void *memcpy(void *dst, const void * src, size_t n);
typedef unsigned int size_t;
```

Can you spot any potential problems?

Q3: Consider this code:

```
size_t len = read_int_from_network();
char *buf;
buf = malloc(len+5);
read(fd, buf, len);
```

Can you spot any potential problems?

Q4: What issues, if any, do you see with the following code for password comparisons?

```
// The following is the functional description of the code -- what it should do
```

```
PwdCheck(RealPwd, CandidatePwd) should:
```

```
    Return TRUE if RealPwd matches CandidatePwd
```

```
    Return FALSE otherwise
```

```
RealPwd and CandidatePwd are both 8 characters long
```

```
// The following is the implementation, like on the TENEX system
```

```
PwdCheck(RealPwd, CandidatePwd) // both 8 chars
```

```
    for i = 1 to 8 do
```

```
        if (RealPwd[i] != CandidatePwd[i]) then
```

```
            return FALSE
```

```
    return TRUE
```