#ret #hw

1 | User Input Validation

```
title: Assignment

For this assignment, show your understanding of at least one of these techniques by submitting:
-   code and notes demonstrating a successful break on a system meant for testing -- **_not on a produc
-   code and notes that demonstrate changes that would prevent your break
-   the name of a specific law you might be charged with if you were to do this on a system without per
```

1.1 | Python 2 script

Suppose someone had a very simple Python 2 script that they ran on their computer:

```
# original script
favorite = input('What is your favorite number? ') # vulnerability in input
print 'I like the number {}, too!'.format(favorite)
```

Show examples of input that would give you access to information that user had access to (e.g. the contents of a file on their machine).

```
> python2 bad_input.py
What is your favorite number? open("/Users/huxmarv/super_secret_secrets.txt").read()
I like the number password123, too!
```

Updated script:

```
# secure script
favorite = raw_input('What is your favorite number? ') # change input to raw input
print 'I like the number {}, too!'.format(favorite)
```

```
> python2 better_input.py
What is your favorite number? open("/Users/huxmarv/super_secret_secrets.txt").read()
I like the number open("/Users/huxmarv/super_secret_secrets.txt").read(), too!
```

Breaks: California Legislative Information > (502c) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network

1.2 | Cross-site scripting

Vulnerable site

Write a comment that will cause some JavaScript to run.

```
<img src="!exist" onerror="alert('XSS')">; // alerts XSS
```

Updated site:

```
var textDiv = document.createElement('div');
//textDiv.innerHTML = document.getElementById('commentText').value;
textDiv.innerText = document.getElementById('commentText').value; // change innerHTML to innerText
newDiv.appendChild(textDiv);
```

Breaks: California Legislative Information > (502c) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network

1.3 | Buffer overflow

Try to give a password that is not the correct one but does grant you access.

```
// from http://stackoverflow.com/questions/34247068/buffer-overflow-does-not-work-on-mac-osx-el-capitan
#include "stdio.h"
#include "string.h"

int check_authentication(char *password) {
    int auth_flag = 0;
    char password_buffer[20]; // vulnerability


    strcpy(password_buffer, password);

    if (strcmp(password_buffer, "password") == 0) { // correct password: password
auth_flag = 1;
    }

    return auth_flag;
}

int main(int argc, char* argv[]) {
    if (argc < 2) {
printf("Usage: %s <password>\n", argv[0]);
    }

    if (check_authentication(argv[1])) {
printf("Access Granted.\n");
    } else {
printf("Access Denied.\n");
    }
}

compile with  `gcc -fno-stack-protector -D_FORTIFY_SOURCE=0 buffer_overflow.c` !

> ./a.out 123456789abcdefghijkl
Access Granted.

> ipython
In [1]: x = "123456789abcdefghijkl"
In [2]: len(x) # overflow with len > 20
Out[2]: 21
```