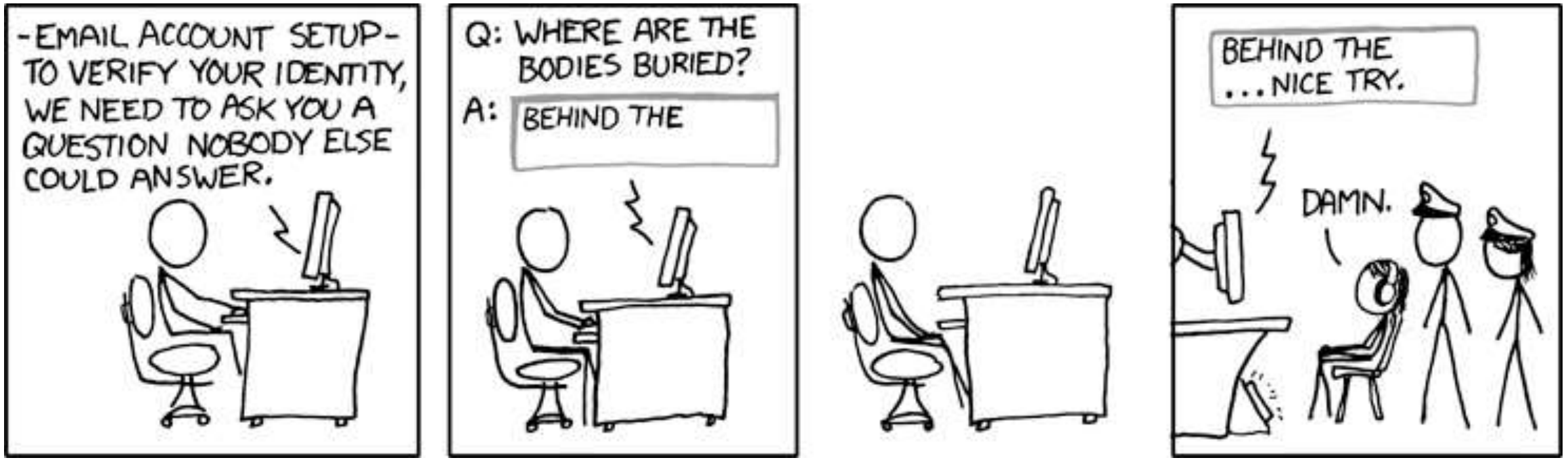
SQL Injection

COMP620


-EMAIL ACCOUNT SETUP-
TO VERIFY YOUR IDENTITY, WE NEED TO ASK YOU A QUESTION NOBODY ELSE COULD ANSWER.
Q: WHERE ARE THE BODIES BURIED?
A: BEHIND THE
BEHIND THE ...NICE TRY.
DAMN.

XKCD

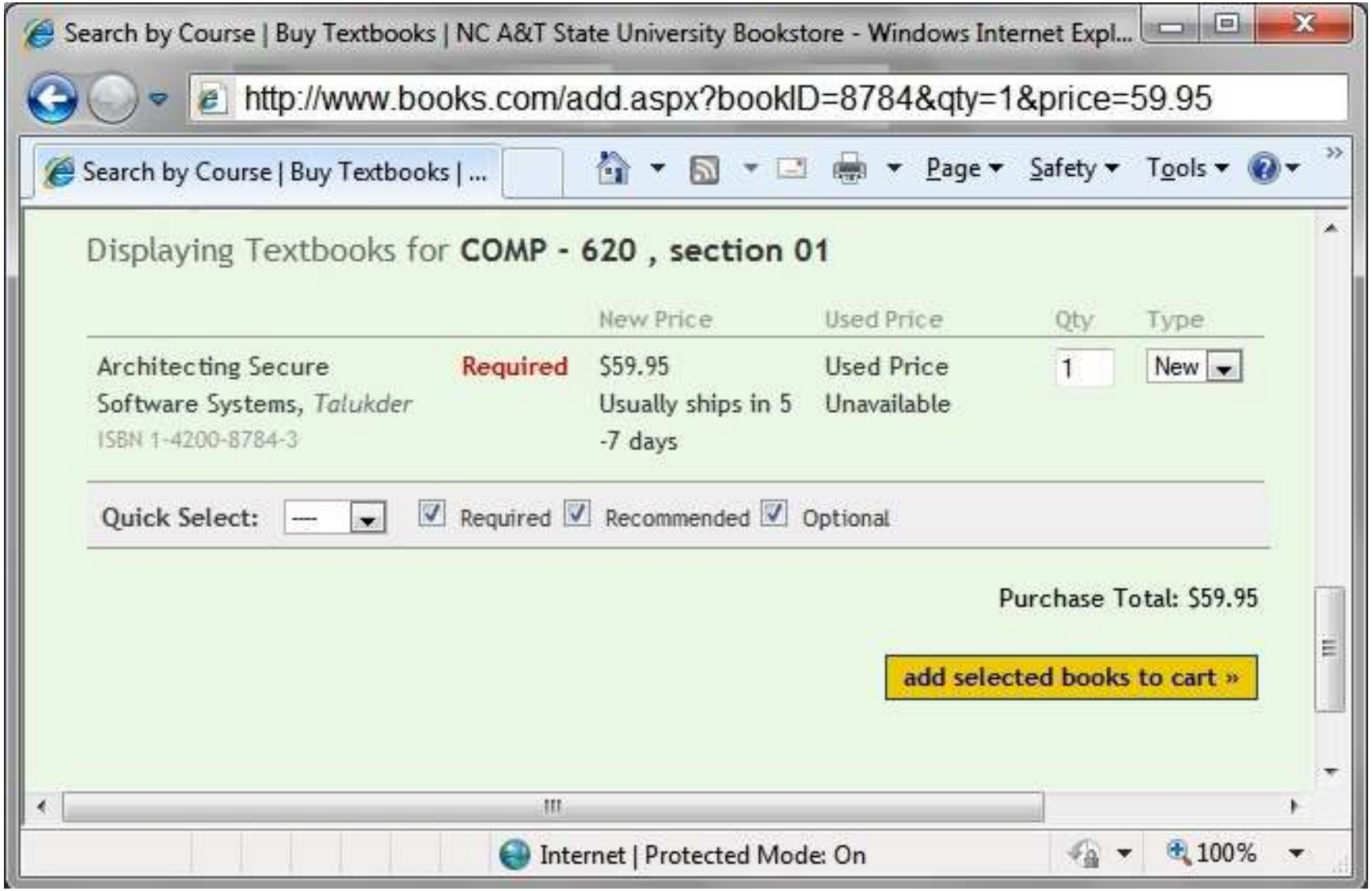
Second Exam

- The second exam in COMP620 will be on Friday, October 19
- It will cover all the material since the first exam

Parameter Tampering

- Some web applications transfer critical data between the browser and the server
- Changing that data can cause an exploit
- A proxy can be placed between the browser and the server to view and edit the HTTP requests
- The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools

Example Application



Modifying Parameters

- The URL sent to the server contains parameters specifying what is to be done

```
http://www.books.com/add.aspx?
bookID=8784&qty=1&price=59.95
```

- This information might be passed to the application to add the book to the cart
- A user could enter this URL with a different price and pay much less for the book

Avoiding the Problem

- Applications should not trust input from the user
- The application should get the price of the book from its database

Releasing Too Much Information

- Consider the bookstore site that might show your past orders as shown where you can click on an order number to get more detail

Order #	Date	Title
2456	2/14/2010	Karma Sutra
2457	2/14/2010	Ulysses
3801	3/2/2010	Computer Security

Changing the URL

- When you click on an order number, it might send the following to the server

`http://www.books.com/order.aspx?ordernum=2457`

- You can probably guess that there are other orders with similar numbers. You might be able to see another person's order if you sent the above URL changing the number.

Guessing Names

- Sometimes you can guess what the file name of a web page will be

  williams.comp.ncat.edu/comp620/HW3sol.pdf

- Even if there is no link to the file, you can enter the expected URL
- This can be avoided by using long random names

Hidden Parameters

- There can be more parameters sent in a web form than are visible on the page. There may be parameter values in the HTML text that are also sent.
- Since the HTML can be viewed by the users, this information is not secret or secure.

```
<input type="hidden" id="admin" />
```

- Users can change the URL to change this value

HTML Comments

- A good programmer includes comments in any code they write, including an HTML document
- Sometimes programmers will comment out a section of the HTML document that is not currently being used
- Comments might give information on how to test the system.

```
<! use id tester with password
    “badchoice” to test />
```

Viewing Directories

- If a default.html or index.html file exists, the system will send these when no filename is specified in a URL
- If you enter a URL without a file name, the web server might show you all of the files in the directory
- This is usually a configuration option in the web server. It is best turned off.

Second Exam

- The second exam in COMP620 will be on Friday, October 19
- It will cover all the material since the first exam