

# Scripting Languages G22.3033-002 Summer 2008, hw08

Assigned Wednesday 7/16/2008, due Friday 7/25 at 9pm. 50 points.

<http://www.cs.nyu.edu/courses/summer08/G22.3033-002/>

## Homework instructions

Homeworks are due on Fridays at 9pm. This deadline will be strictly enforced.

Email your answers to Robert Soulé, [robert.soule@gmail.com](mailto:robert.soule@gmail.com).

### Problem 1 (3 + 3 + 3 + 3 + 3 + 3 + 3 = 21 points)

Consider the following table. Assume that a JavaScript program was loaded from `http://www.nyu.edu/dir/page.html`. For each row in the following table, both *indicate* and *motivate* the result of the JavaScript Same Origin Check.

*Example:* Under “Result”, you can indicate either *succeed* or *fail*. Under “Motivation”, you can say, respectively, *same domain, port, and protocol* or, for example, *different protocol*.

	URL of Target Window	Result	Motivation
1	<code>http://www.nyu.edu/index.html</code>		
2	<code>http://www.nyu.edu/~hirzel/index.html</code>		
3	<code>ftp://www.nyu.edu</code>		
4	<code>http://www.columbia.edu/index.html</code>		
5	<code>http://www.nyu.edu:80/index.html</code>		
6	<code>http://www.nyu.edu:8080/index.html</code>		
7	<code>http://www2.nyu.edu/dir/page.html</code>		

### Problem 2. (5 + 10 = 15 points)

Consider the following PHP program instruction:

```
$query = "SELECT * FROM accounts WHERE name='$name' AND password='$password'";
```

This code generates a query intended to be used to authenticate a user who tries to login to a Web site.

1. Show how an attacker can embed a name and password that could cause a table in the database to be erased (5 points).
2. Write a simple sanitization function in PHP that sanitizes name and password before they are used (10 points).

### Problem 3. (14 points)

Consider the Cross-Site Scripting (XSS) vulnerability described in Slide 70 of the lecture, which allows a malicious user to embed JavaScript code into what is supposed to be a parameter value.

For example, an attacker could cause the parameter value to be

```
John<script>alert('Uh oh');</script>
```

Describe how that vulnerability could be prevented.