

Question 1 Warmup: SOP

(15 min)

The Same Origin Policy (SOP) helps browsers maintain a sandboxed model by preventing certain webpages from accessing others. Two resources (can be images, scripts, HTML, etc.) have the same origin if they have the same protocol, port, and host. As an example, the URL `http://inst.berkeley.edu/eecs` has the protocol HTTP, its port is implicitly 80, the default for HTTP, and the host is `inst.berkeley.edu`.

Fill in the table below indicating whether the webpages shown can be accessed by `http://amazon.com/store/item/83`.

Origin	Can Access?	Reason if not
<code>http://store.amazon.com/item/83</code>		
<code>http://amazon.com/user/56</code>		
<code>https://amazon.com/store/item/345</code>		
<code>http://amazon.com:2000/store</code>		
<code>http://amazin.com/store</code>		

Question 2 *SQL Injection*

(15 min)

- (a) Explain the bug in this PHP code. How would you exploit it? Write what you would need to do to delete all of the tables in the database.

```
$query = "SELECT name FROM users WHERE uid = $UID";  
// Then execute the query.
```

(Here, \$UID represents a URL parameter named UID supplied in the HTTP request. The actual representation of such a value in PHP is a bit messier than we've shown here. We leave out the syntactic details so we can focus on the functionality.)

- (b) How does blacklisting work as a defense? What are some difficulties with blacklisting?
- (c) What is the best way to fix this bug?

Question 3 *Clickjacking***(10 min)**

In this question we'll investigate some of the click-jacking methods that have been used to target smartphone users.

- (a) In many smartphone browsers, the address bar containing the page's URL can be hidden when the user scrolls. What types of problems can this cause?

- (b) Smartphone users are used to notifications popping up over their browsers as texts and calls arrive. How can attackers use this to their advantage?

- (c) QR codes haven't taken off and become ubiquitous like some thought they would. Can you think of any security reasons why this might be the case? (If you aren't familiar with QR codes, ask another group!)