Q1: Consider a website site.com that includes a third-party script, e.g.:

```
<script src="http://otherdomain.com/library.js"></script>
```

From what origin can this script read cookies?

If this script sets a cookie, under what origin will that cookie be set?

Do you see any security concerns with this?

Q2: **State in Hidden Forms Fields.** How would you fix the vulnerable shopping cart application?

Q3. **XSS.** What are the key elements of an XSS attack?

Q4. **Login CSRF.** Why would an attacker want to force a victim to log in under an account the attacker controls?

Q5: **CSRF Defenses.** How might a web application defend itself against CSRF attacks?