# ISEC 325 Homework 09

Answer the following questions based on your reading of the text books, the module key points, and the instructor’s presentation this week.

1. [3 points] What is SMTP used for? What are some common attacks against SMTP servers?

SMTP is used for sending mail across the internet. Common attacks include open relay and mail bombing.

1. [3 points] What is LDAP used for? What are the common attacks against LDAP servers?

LDAP is used for communication with centralized directories. The most common attacks are like the SQL injection attacks.

1. [2 points] What are the common types of attacks against DNS servers?

Common attacks against DNS servers are DNS open resolver, DNS poisoning, and DNS denial-of-service attack.

1. [3 points] What is SQL injection and how does it work? What are some recommended methods to combat SQL injection?

SQL injection is when an attack will inject data into the SQL. Some methods to combat this would be to limit access to the web within the database, scrub input, and use some prebuilt statements that cannot take user input.

1. [3 points] What is an XSS attack and how does it work? What are ways to prevent XSS attacks?

XSS attacks are when servers send out unverified data to clients and the vulnerabilities are found on the legitimate web sites. Ways to prevent this is to scrub accepted input, remove special URL characters, and ensure that untrusted data can not be inserted into HTML.

1. [2 points] What are some ways to prevent authentication or session vulnerabilities.

Some ways to prevent this is to use strong passwords, use verification methods like texting or emailing a code, and lock accounts when too many wrong passwords are tried in a go.

1. [3 points] What are some ways to harden a web server?

Some ways to harden a web server would be to make sure the software is up to date, enforce strong password policies, monitor user activity, and limit access to sensitive information.

1. [6 points] Watch this video on BeEF (the Browser Exploitation Framework) for remotely attacking a web browser via XSS: <http://www.youtube.com/watch?v=utPBQOZS_TU>. Also, do some research into BeEF (<http://beefproject.com/>).
   1. What are your observations about how this process works and the tools used to carry out the attack?

The attacker can inject a JavaScript shell so that it will keep connecting to the attacker’s server while it waits for the next command. This way the attacker can just write the code on their server and then send it to the victim. The attacker uses a cross-site shell to be able to manage this. BeEF has a nice UI that helps with the process.

* 1. Who must take steps to prevent a browser from being exploited by XSS?

The who must take steps to prevent a browser from being exploited are the ones who run the browser as they need to make sure that they do not have vulnerabilities that can reach their clients. There is also the clients who need to make sure to scrub their inputs afterwards to make sure they are safe.

* 1. Since BeEF hooks to Metasploit, is there any safe way to use the web today? Explain.

The safest way to use the web today is to keep up with antivirus technology, use firewalls, and check inputs from websites.

1. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize, and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about.  In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

This week we looked at the security of web applications and the vulnerability involved with the web. There are a lot of ways that we go about with trying to protect ourselves from these attacks. The video above showed how to connect to another’s computer similar to the lab from last week. I do find it fun to learn just how these attacks can be carried out, but it also makes me think of just how many steps ahead are we from these attacks? We can use a lot of these methods to deter people from attacking us as they are more likely to move on to a newer less secure target than trying to spend the time taking apart our protection. As a person, these methods are good at making sure we are secure with our personal systems as the average person becomes a target because of lack of protection or wrong place, wrong time. If we worked for a big important company that holds very sensitive materials, then we would need to focus on the attacks more as if a person is attacking, they are not likely to be deterred because of the steps in security.