1. (40 + 10 bonus pts) In this assignment, you will be using a “Secure Photo Sharing” website at

http://ec2-54-201-8-162.us-west-2.compute.amazonaws.com/

This website allows you to upload pictures to share with other people. When a picture is uploaded, an associated copyright key is generated. If someone would like to use your picture for his/her own purpose, he/she has to purchase the picture to get the copyright key. This website has built with several vulnerabilities. Your assignment in this homework is to identify these vulnerabilities and hack this website. There are three tasks:

(a) Reflected Cross-Site Scripting (XSS) attack (15 pts):

- What is the cookie associated with your current session of this website? Record your session ID as part of the answer to this question. (5 pts)
- Now please get our TA’s session ID. You might consider using email to launch your attack. Please send to our TA (vandycs285ta@gmail.com) an email with a crafted URL link. When our TA receives your email and clicks the link, you will receive his session information. We will regard your email to the TA as part of the answer to this question. (10 pts)

**Hint:** There are a couple of ways to deliver the session information back to you. Here are two options you may consider.

Option 1: Use email. You can assume that our TA has a default mail client on his machine and he will “accidentally” click “send”, if a new message pops up.

Option 2: Setup a web application to receive the information. A sample PHP script file is provided in badguy.tar.gz, which is available at our course website. We also host this script at http://ec2-54-201-8-162.us-west-2.compute.amazonaws.com/badguy.php for your convenience.

(b) Stored XSS attack (10 pts):

Please explore the website and see where you can launch a stored XSS to steal the website administrator’s session cookie. **Hint:** The website administrator will login and check your comments to his website every day. As the solution to this question, please 1) put your script that steals the session cookie to the location you’ve identified; 2) write down the location of the website (URL), where you’ve launched a stored XSS.

(c) SQL injection attack (10 pts):

“cs285web” is a user of this website. The goal of this question is to bypass the authentication mechanism of the website and hack into this account. Once you hack into the account, you can view the following information shown on his home page: 1) his date
of birth and 2) SSN. (Please don’t make changes with this account). As the answer to this question, please provide 1) the date of birth and SSN of “cs285web”; 2) the SQL injection script; 3) the location (URL) where you’ve launched the SQL injection attack.

**Hint:** The authentication check is performed by sending query to the database using your input username and password. The password is hashed to avoid eavesdropping. The query has the following format:

```
SELECT * FROM `users` WHERE login = `username` AND password = SHA1(`password`);
```

(d) Forceful browsing (5 pts):

The copyright key of a picture will only be revealed to the users who purchased it. In this question, you will try to get the copyright key of a picture called “monkey” with picid 69. This picture costs 1000 tradebux, which is higher than the balance of your account. Please try to get the copyright key without purchasing it. As the answer to this question, please provide 1) the copyright key for this picture; 2) how you get this information.

(e) Bonus questions (10 pts): There are much more vulnerabilities on this website than the above three. Feel free to explore them. For each additional vulnerability identified on this website, you will be credited with 5 additional points as a bonus (up to 10 pts). Register on the website and start hack! You can register with any username but provide your username in your homework submission.

2. (30 + 10 bonus pts) In this assignment, you will practice a well-known denial-of-service attack, called TCP SYN flood. You will create a real attack using DETERlab, and to observe its effect on legitimate traffic. Afterwards, you will be asked to apply a known defense against SYN flood known as SYN cookies, repeat the attack and observe the protection.

(Acknowledgement: this homework question is based on an exercise prepared by Jelena Mirkovic, USC/ISI)

(a) **Read the following information** and make sure that you understand how TCP SYN flood attack works, which resource it ties up, and how syncookies help mitigate this attack.

- SYN cookie overview ([http://cr.yp.to/syncookies.html](http://cr.yp.to/syncookies.html))

In your homework submission, explanation 1) how the TCP SYN flood attack works; 2) how SYN cookies work to prevent denial-of-service effect from SYN flood attack. (5 pts)

(b) **Start a new experiment**. You should load the supplied topology file synf.ns into the DETERlab to create a new experiment. Do not modify the topology file but read it through and identify what each directive does. Especially important are the lines in the NS file that add support for traffic generation and visualization via SEER.

```
#Add SEER support to each node
tb-set-node-startcmd $node "sudo python /share/seer/v160/experiment-setup.py Basic"
#complete Ba with Basic in the command above
```
(c) **Attach the experiment to SEER.** Once the experiment has been swapped in, use SEER GUI by clicking at ”Launch SEER now” option from [http://seer.deterlab.net/trac](http://seer.deterlab.net/trac). (You should have Java installed first). Once SEER starts, (1) choose the ”Emulab” interface in the first dialog; (2) choose Emulab Interface – > Attach to Experiment and input Project and Experiment Name. (Note: capitalization matters here.) (3) Next, you will need to input your username on DETERlab and the same password you use to log on to DETER. If don’t have the SSH public key set up, delete the information in the SSH Key File input field.

Once the experiment is attached to SEER, the topology is visible in the Topology tab. Right clicking on nodes should open a menu that allows users to open graphs in the Graph tab. Once traffic starts flowing, legitimate traffic will show as green and attack traffic will show as red on these graphs. Notice that you can change the counters to show packets or bytes (selection option on top of a graph). The rest of this assignment assumes that you have opened the graph that shows traffic reaching and leaving the server node.

(d) **Generating legitimate traffic.** Create a Web traffic stream between the client and the server nodes by following these steps from Controls tab in SEER:

Click on Traffic item on the left sidebar
Click on Web
Click on New Web group
Choose some name for the group
Choose client node as a client, server node as a server.
Choose exponential distribution of Thinking Time (arrival time) with lambda 5, scale 1 and max 5.
Choose minmax distribution of file sizes with min 1,000 and max 10,000.
Click Start.
You should be able to see some green traffic now on your graph include it in your homework submission. (5 pts)

(e) **Turning off/on SYN cookies.** SYN cookies are often on by default in Linux and FreeBSD. To check if they are on do the following:

```
ssh yourusername@users.deterlab.net
ssh server.YourExperiment.YourProject
sudo sysctl net.ipv4.tcp_syncookies
```

If you see 1 as the result, it means SYN cookie is on. Type the following on the server machine to turn off SYN cookie.

```
sudo sysctl -w net.ipv4.tcp_syncookies=0
```

If you want to turn SYN cookie on, use the same command, but change 0 to 1.

(f) **Generating attack traffic.** Create a SYN flood between the attacker and the server nodes.

Click on the Attack item on the left sidebar
Click on Packet Flooder
Click on New Packet Flooder
Choose some name for the group
Choose attacker node as the Attack Source Nodes. Input 1.1.2.0 and 255.255.255.0 in the IP source field to ensure subnet spoofing. Choose server node as the Target node in the Basics and set the protocol type to TCP. Leave the Target Mask, Length Min and Length Max unspecified. Choose Flood Type to be flat and set the high rate to 1,000 packets per second (this is the unit of measure for rate fields in SEER). Set the destination ports to min 80 (Dport Min) and max 80 (Dport Max) and the TCP flags field to SYN. Leave all the other default values as they are.
Click Start. You should be able to see some red traffic now on your graph. Make sure you are looking at a graph of pps not bps (selection option on top of the graph). Include two graphs in your homework submission with no SYN-cookies and with SYN-cookies. (10 pts)

(g) Collecting statistics. You will now collect tcpdump statistics on client machine with and without SYN cookies, calculate connection duration and draw graphs of connection duration on y-axis and connection start time on x-axis. Perform the following steps:
Stop all traffic using Stop button for each traffic group in SEER
Start tcpdump on the client

```
ssh yourusername@users.deterlab.net
ssh client.YourExperiment.YourProject
ip route get 5.6.7.8
```
You should see something like this as a result:

```
5.6.7.8 via 1.1.2.2 dev eth2 src 1.1.2.3 cache mtu 1500 advmss 1460 metric 10
```
Thus, you can discover the interface name leading to the client IP 5.6.7.8 is eth2. Note here this could be different in your experiment. Change it to the interface you see. To see the traffic flowing, type

```
sudo tcpdump -nn -i eth2
```
You will need to discover proper tcpdump options to see only IP traffic and to save recorded traffic into a file. Start tcpdump with these options. You can also download the dump files to your local computer and view it using wireshark.
Using a stopwatch to perform the following scenario:
Start legitimate traffic
After 30 seconds start the attack
After 120 seconds stop the attack
After 30 seconds stop the legitimate traffic
Stop the tcpdump on the client and save the file
Turn the SYN cookies on and repeat the above steps.

Using the recorded traffic files and tcpdump to read them, process the output and calculate connection duration for each TCP connection seen in the files. Connection duration is the difference between the time of the first SYN and of the ACK following a FIN-ACK (or between the first SYN and the first RESET) on a connection. Remind yourself what
uniquely identifies a TCP connection, i.e. how to detect packets that belong to the same connection? If a connection did not end with an ACK following a FIN-ACK assign to it the duration of 200 s. Include two graphs in your submission, showing connection duration vs connection start time for the case without and with SYN cookies. Label the graphs so they can be distinguished and indicate on each graph using vertical lines or arrows the start and the end of the attack. Explain what happens in each case. Is the attack effective? How can you tell this from the graphs? (10 pts)

(h) **Bonus Question** 10 pts. This is an open ended question. Your goal is to generate attack traffic in the network to disrupt the legitimate web traffic without using TCP SYN flooding. As the solution to this question, you need to show 1) how you generate the attack traffic, 2) illustrate the effect of your attack (e.g., in terms of prolonged connection time or lost packets, etc). Credits will only be given, if you’ve launched effective attacks.

**FAQ:**

- **Q: Experiment cannot be swapped in.** First, check the error message you will receive in the email. One possible reason for this is that the NS file was changed from the one listed above. Verify that the file looks exactly like supplied with this exercise. Another reason may be that there is a lack of available nodes in DETER and the error message will say so. This happens occasionally and usually resources become available in a few hours.

- **Q: SEER GUI does not run.** The GUI usually requires the latest version of Java so if it does not run this means you need to upgrade your Java version.

- **Q: SEER GUI cannot attach the experiment.** Very likely reason for this is that you are not typing the correct username and password. Try to SSH into users.deterlab.net with the same username and password you are using to attach the experiment.

- **Q: There is no legitimate (attack) traffic on graphs.** First verify that the options are set exactly as shown in the pictures that go along with steps 2.4 and 4.4. If this is all fine, SSH to one of your experimental machines and try to ping another two (e.g., ping server and attacker from client). Use short names (e.g., ping server and NOT ping server.YourExperiment.YourProject) in ping commands. If you notice any connectivity problems click on Modify Experiment on your DETER Web page and then click on Submit. The experiment will reset to its original state - this may take several minutes and you will receive an email when it’s done. If connectivity problems persist email your TA. Finally, if everything else seems fine it may be that SEER backend has died for some reason (perhaps you rebooted one of the machines without going through Modify Experiment?) To fix this click on Modify Experiment on your DETER Web page and then click on Submit. The experiment will reset to its original state - this may take several minutes and you will receive an email when it’s done. Another reason for missing traffic is if your experiment is not swapped in.