

# Exercises – Basics of Web Security

## Experiential Learning Workshop

### 1 General Guidelines

1. Make a team of two unless stated otherwise.
2. For each exercise, use wireshark capture to verify contents
3. Ensure to use proper capture filter and don't capture irrelevant traffic
4. Where appropriate or applicable, use **wget** or **nc** to access the web server.
5. The default client for accessing web server is assumed to be browser, preferably **firefox**. You can use Chrome or any other browser as well.
6. The webserver in the example below is taken as 'myweb.com'. Please use your hostname or corresponding IP address instead in your exercise.
7. To kill any program in the **Linux** terminal, please press **Ctrl-C** and not **Ctrl-Z**. The latter will suspend the program and not stop it.

### 2 Hands-on 1: Installing SSL Certificate

Note: It is assumed that Apache web server has been installed on one of the machine and let us call it web server. In case, it is not, please install it by invoking the command `sudo apt install apache2`.

#### 2.1 Invalid SSL certificate.

In the exercises below, we will work with SSL Certificate that are not compatible with browser expectation.

##### 2.1.1 Accessing websites with invalid certificate.

1. Find the IP address of [www.google.com](http://www.google.com), (e.g. `ping -c2 www.google.com`). Let this IP address be `a.b.c.d`
2. Open Firefox (or chrome) browser and access <https://a.b.c.d>.
3. The browser should display a warning rather than displaying the google search page.
4. Analyze the warning. Click thru this warning and browser should display google search page.
5. Make an entry for this IP address `a.b.c.d` in your `/etc/hosts` file like below. Use editor of your choice to make an entry (e.g. nano, edit, gedit, vi etc.)
  - a. `a.b.c.d mygoogle.com`
6. In the browser type the URL, <https://mygoogle.com>
7. Analyze the web page response.

##### 2.1.2 Running your own web site with HTTPS

1. Generate and deploy a web site SSL certificate e.g. for (`mywww.com`) on Apache web server. The steps are given in Appendix.
2. Create an entry in the `/etc/hosts` file of the client machine (creating this entry on the web server doesn't really matter). The entry should be something like as below where `10.1.1.101` is server's IP Address
  - a. `10.1.1.101 mywww.com`

3. Verify that Apache web server is running. In browser of client machine, first enter <http://mywww.com>. It should display Apache welcome page.
4. Now, in the browser, enter the URL <https://mywww.com>.
5. Analyze the web page response. It should be warning again, but this warning should have different indicator compared to when accessed Google search page with <https://mygoogle.com>.
6. Analyze the warning web page thrown by the browser. The warning should correspond to unknown certificate authority rather than website name (as was the case earlier when accessing Google with its IP address or any other locally defined name).
7. Import the certificate of into browser repository as Exception. Click thru and then browser should display the Apache welcome page. Import
8. Close the browser, reopen it again and access again the web page <https://mywww.com>. This time no warning should be displayed since browser knows the certificate authority.
9. Access the website, <https://mtechthesis.vtu.ac.in>. Analyze the error thrown by the browser.

### 2.1.3 Exercise Expectations

1. Understand SSL certificate errors in case of any mismatch of information (unrecognized certificate authority, website name mismatch, improper certificate validity period).

## 3 Mixed Content.

In the exercises below, we will work with web pages that has embedded objects with both HTTP and HTTPS.

### 3.1 Pure content.

1. Create a web pages, e.g. pure.html as below in your directory /var/www/html.

```
<html>
<head>
<title>Pure Content </title>
<body>
<h1>Pure Content Demonstration</h2>
<h2>Image 01 with inherited security access.</h2>
<h2>Image 02 with inherited security access.</h2>


</body>
</html>
```

2. Create the directory /var/www/html/img and copy some images with the name img-01.jpg and img-02.jpg in the images directory.
3. The web page has two embedded objects for which web protocol is not defined explicitly. The browser will inherit the protocol (HTTP or HTTPS) used to access the parent page i.e., pure.html
4. Access this web page using HTTP and HTTPS in the browser i.e. <http://mywww.com/pure.html> and <https://mywww.com/pure.html>.

Alternatively, you can access these web pages at [rprustagi.com/accs/pure.html](http://rprustagi.com/accs/pure.html) with HTTP and HTTPS.

5. Browser should show the content properly without any warning. With HTTPS access, it should show Green Lock icon.

### 3.2 Mixed content.

1. Create a web page like below (mixed.html) in the directory /var/www/html.

```
<html>
<head>
<title>Mixed Content </title>
<body>
<h1>Mixed Content Demonstration</h1>
<h2>Image 01 with inherited security access.</h2>
<h2>Image 02 with insecure access.</h2>


</body>
</html>
```

2. This web page specified the second embedded object explicitly with HTTP protocol. Thus, even if the parent page (mixed.html) is accessed with HTTPS, the second object will be accessed using HTTP. This web page represents a lot web content on the internet as developers have hard coded the HTTP protocol in the web content by means storing these in Database, java beans, images etc. Possibly, because some of the websites serving these contents support only HTTP and not HTTPS.
3. In Firefox browser, access this web page with HTTP and HTTPS protocol i.e. <http://mywww.com/mixed.html>, and <https://mywww.com/mixed.html>. Alternatively, access these web pages at [rprustagi.com/accs/mixed.html](http://rprustagi.com/accs/mixed.html).
4. The first access will show content properly. The 2<sup>nd</sup> access with HTTP will show the gray lock icon with a warning sign.

### 3.3 Mixed content.

1. Create a web page like below (mixed-active.html) in the directory /var/www/html.

```
<html>
<head>
<title>Mixed Active Content </title>
</head>
<body>
<script src="http://rprustagi.com/js/mywww.js">
</script>
<h1>Mixed Content Demonstration</h1>
  <button type="button" onclick="hello()"> insecure
  access
  </button>
<h2>Image 02 with insecure security access.</h2>

```

```
</body>
</html>
```

2. Create a javascript file mywww.js with following content in the directory like below (mixed-active.html) in the directory /var/www/html/js on the web server.

```
<script>
??
</script>
```

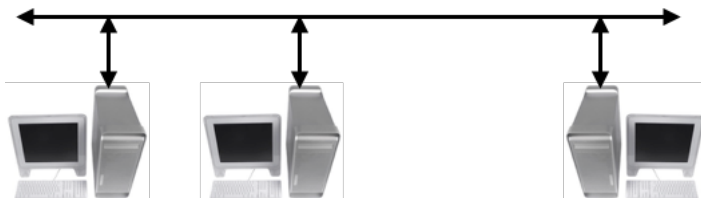
3. In the Firefox browser, access the web page <https://mywww.com/mixed-active.html> (alternately <https://rprustagi.com/accs/mixed-active.html>).
4. Browser should show gray lock icon with a cross indicating danger. Click on the button "Insecure Access". It should pop up "Hello" text.
5. The java script has been obtained explicitly using HTTP and this causes a serious vulnerability to an intruder/attacker.
6. Click on the gray lock/information icon and enable the security protection in the browser. Refresh the web page. This time, browser would show Green lock icon indicating the safe access to the web page.
7. Click on the button "Insecure Access", and no pop-up occurs. This is because browser has disabled the insecure access of javascript.
8. It is recommended to always use enable security protection in the browser to ensure that your web access is not compromised.

### 3.4 Exercise Expectations

1. Understand lock icons display when web page has insecure references i.e. mixed contents.
2. Understand what kind of contents are secure and insecure and how to disable insecure access.
3. Differentiate between passive mixed content with active mixed content, the latter being lot more dangerous in nature.

## 4 Hands-on 4: Understanding ARP

### 4.1 Study ARP table maintenance



1. Setup three machines A, B, and C as shown in ( 5.1 ICMP Redirect). In this exercise we do not need 2<sup>nd</sup> and 3<sup>rd</sup> network i.e., 10.x.2.0/24 and 10.x.3.0/24 and thus these addresses need not be assigned. Use of separate small switch is not recommended for this exercise
2. Study the existing ARP table and identify which machines are these.

- a. `arp -an`
3. Ping one live machine (i.e. machine which is reachable) and one unreachable machine. Study the ARP table. What does the entry show for unreachable machine.
4. Ping the broadcast address of your network. This requires sudo privilege.
  - a. `sudo ping -b -c2 10.x.1.255`
5. Analyze in wireshark on number of ICMP response received as well as number of entries added in ARP Table.

#### 4.2 Study Gratuitous ARP

1. Use the same setup as above. Note down MAC Address of 3 machines (A, B & C).
2. Install arping on the machine A (and may be others)
  - a. `sudo apt install arping`
3. On A, add the IP address of A to that of C (replace eth0 with applicable interface name)
  - a. `sudo ip addr add 10.x.1.201/24 dev eth0`
4. Issue arping with this new address to B
  - a. `sudo arping -s 10.x.1.201 -c 2 10.x.1.101`
5. Study the ARP table at B. It should show updated MAC address of A for IP Address of C.

#### 4.3 Exercise Expectations

1. Able to understand the use of ARP and Gratuitous ARP.

#### 4.4 Proxy ARP

1. Connect 3 m/cs in a network as shown in diagram below. Assign the address manually to these systems Use the mask of /22 to ensure that both Ha and Hc are in same network.
2. Define the subnet mask for router interface to be /24 to ensure that Ha is network-1 and Hb is in network-2.
3. Enable proxy ARP on Hb (router)
  - a. `sudo sysctl -w net.ipv4.conf.all.proxy_arp=1`
  - b. `sudo sysctl -w net.ipv4.ip_forward=1`
4. No need to define routing entries at A and C since they are part of same network. Clear up their ARP table (`sudo arp -d <IP address>`) for each IP Address.
5. Check reachability and check ARP table. Analyze the ARP Response in wireshark. ARP Reply should come from Hb for both Ha and Hc though both Ha and Hc do not know about this router.

#### 4.5 Exercise Expectations

1. Able to understand proxy ARP, Routing, and ICMP errors and source address of packet corresponding to ICMP errors.

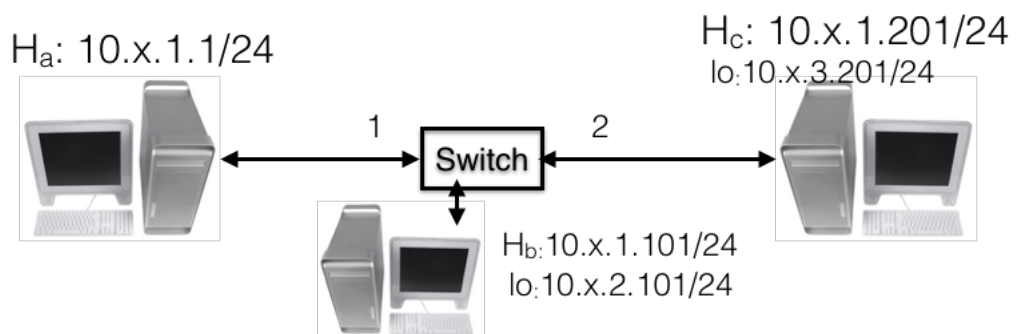
## 5 Hands-on 3: ICMP Errors

### Note:

- The IP addresses specified in the below example are for illustrative purposes only. Use the IP Address assigned to your machines in the network.
- For this exercise you need to make a group of 3.

### 5.1 ICMP Redirect

1. Connect 3 m/cs in a network as shown in diagram. Assign the address manually to these systems Use the appropriate mask. Use value of x as per your team number e.g. 1 for team 1, 2 for team 2 and so on. The exercise can work without the use of small 4/8 port switch separately i.e. this exercise can be carried out in regular lab network.

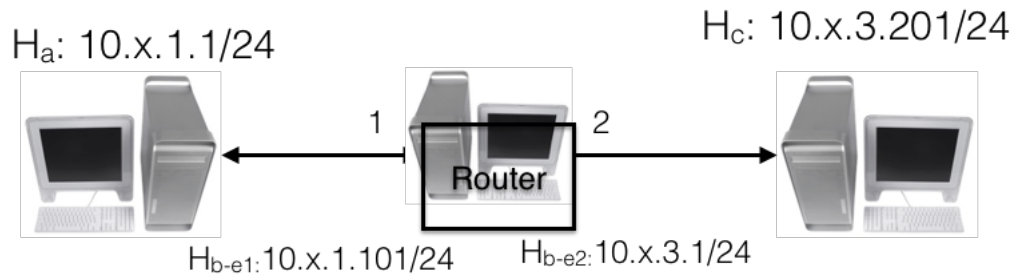


2. On B and C, assign addresses from a different network on the loopback (lo) interface?
  - a. `sudo ip addr add 10.x.2.101/24 dev lo on B`
  - b. `sudo ip addr add 10.x.3.201/24 dev lo on C`
3. Disable acceptance of ICMP redirect on A to ensure that its routing table is not updated as per ICMP redirect. It is assumed that ethernet interface on the machine is eth0 in the examples below. Replace it with appropriate values.
  - a. `sudo sysctl -w net.ipv4.conf.all.accept_redirects=0`
  - b. `sudo sysctl -w net.ipv4.conf.default.accept_redirects=0`
  - c. `sudo sysctl -w net.ipv4.conf.eth0.accept_redirects=0`
4. Add mis-redirected (incorrect) routing entries on A.
  - a. `sudo ip route add 10.x.2.0/24 via 10.x.1.201`
  - b. `sudo ip route add 10.x.3.0/24 via 10.x.1.101`
5. Ping from A to addresses  $10.x.2.101$  and  $10.x.3.201$
6. Analyze in wireshark the icmp redirect packets. Use the capture filter `icmp`.

### 5.2 PMTU Discovery

1. Connect 3 m/cs in a network as shown in diagram. Assign the address manually to these systems Use the appropriate mask. Use value of x as per your team

number e.g. 1 for team 1, 2 for team 2 and so on. To get a second interface on B, use the USB to ethernet adaptor on B.



2. Convert machine B into a router as well as change the MTU value of the link between B and C.
  - a. `sudo ip link set dev eth1 mtu 1000`
  - b. `sudo sysctl -w net.ipv4.ip_forward=1`
3. Define appropriate routing on A to reach C
  - a. `sudo ip route add 10.x.3.0/24 via 10.x.1.101`
4. Define appropriate routing on C to reach back A
  - a. `sudo ip route add 10.x.1.0/24 via 10.x.3.1`
5. Send a ping packet bigger than 1000 bytes from A to C. Run following on A
  - a. `ping -c1 -s 1200 -p 50515253 10.x.3.201`
6. Analyze wireshark capture to study ICMP error (fragmentation needed) and subsequent packet fragmentation (This will be studied later). How many packets are finally generated from A. Analyze the ping response. Are there two responses?

### 5.3 Exercise Expectations

1. Able to understand ICMP errors and source address of packet corresponding to ICMP errors.
2. Able to understand ICMP Redirect, PMTU Discovery and TTL expired.

## 6 Hands-on 2: ARP Spoofing and MITM

This exercise requires setup of 3 machines.

### 6.1 Silent snooping

1. Identify the attacker machine, say X. Identify the IP address of A and B.
2. Install **dsniff** on attacker machine (`sudo apt install dsniff`)
3. On A, ping  $IP_B$  and on B, ping  $IP_A$  and note down their MAC address in ARP Table (`arp -an`). Verify that ARP table has correct MAC addresses.
4. Run the ARP Spoof attack, i.e. issue following commands on attacker machine X. The first command will send gratuitous APR message and send will enable routing on X.
  - a. `sudo arpspoof -I enp1s0 -t  $IP_A$  -r  $IP_B$`
  - b. `sudo sysctl -w net.ipv4.ip_forward=1`
5. Look at the ARP table of A and B. On A, for  $IP_B$ , it should show MAC address of X. Similarly, on B, for  $IP_A$ , it should show MAC address of B.

6. Run wireshark capture on X with capture filter as host IP<sub>A</sub> and host IP<sub>B</sub>.
7. Do the chat using nc between A and B. Identify chat contents of A and B on X in wireshark

## 6.2 Dealing with ARP spoofing

1. In the above setup, issue make the static ARP entry for B on A and vice versa e.g.
  - a. (On A) `sudo arp -s IPB MACB`
  - b. (On B) `sudo arp -s IPA MACA`
2. Explore if silent snooping by attacker can still work.

## 6.3 Exercise Expectations

1. Able to understand working of ARP spoofing and simplicity with which it can be done.
2. Able to understand working ARP and how to avoid silent ARP spoofing and snooping attacks.

# 7 Hands-on 4: Exploration work

## 7.1 Implement Content Security Policies

### 7.1.1 CSP for images

Define a web page with embedded images having reference from other machine. Define CSP for image for self and then explore if the images are displayed. Ensure that when access the image directly in the browser, then image display works.

### 7.1.2 CSP for scripts

Define a web page with scripts linked a javascript file from a different machine. Define CSP to include image only from that URL. Load the web page and ensure the web page works.

## 7.2 Implement sslstrip

Install **sslstrip**, explore how sslstrip works. Using sslstrip and arpspoof, become the MITM attacker and capture the traffic of your neighbour. Run the arpspoof for your neighbour and default router, and run sslstrip. Let your neighbour access flipkart.com and then capture the credentials of your neighbour.

## 7.3 Implement Secure HTTP headers

Read the article on web security in <https://acc.digial>, and implement other HTTP headers to enable secure web.

## 7.4 Exercise Expectations

1. Able to understand working of MITM attack.
2. Understand use of Content Security Policy.



## Appendix: Generating and installing SSL certificate

1. Follow the steps below to create a self-signed certificate with a private key for the website mywww.com (or choose your own website name) with validity period of 10 year (3650 days).

```
2. sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048
   -keyout /etc/ssl/private/self.key -out
   /etc/ssl/certs/self.crt
```

It will prompt to provide following information items:

- i. Country Name
- ii. State or Province Name
- iii. Locality Name
- iv. Organization Name
- v. Organizational Unit Name
- vi. Common Name
- vii. Email Address.

Use the value mywww.com for Common name. This is the website name that will be used in the browser to access the website using HTTPS. The above command creates the required files in the directory **/etc/ssl** but can be kept anywhere as per your preference.

3. Edit the apache web server configuration file `/etc/apache2/site-available/default-ssl.conf` and make/update the following entries.

```
ServerName mywww.com
SSLEngine on
SSLCertificateFile /etc/ssl/certs/self.crt
SSLCertificateKeyFile /etc/ssl/private/self.key
```

4. Enable the SSL changes in Apache web server.

```
sudo a2enmod ssl
sudo a2ensite default-ssl
```

5. Restart Apache web server.

```
sudo systemctl restart apache2
```

← end of exercises →