UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

IS2109 Information Systems Security - Practical 2

Secure Web Browsing

Instructions:

- **Submit answers for all the following questions. Clearly mention the Question Numbers.**
- **You must submit your answers as a PDF document named as P2_GroupNumber (E.g. P2_Group 5)**
- **Only one document should be submitted from a group and make sure to mention the index numbers of the group members at the end of the document.**

1. Web browser

1. Identify where the browser stores the following information in a PC

   i. cookies
   ii. temporary internet files
   iii. Passwords
   iv. Form fields
   v. Bookmarks
   vi. Browser settings

2. Web site certificates

Certificates are used by secure web sites to prove the identity of their servers and protect the communication between their servers and your web browser.

1. How do digital certificates ensure secure communication?
2. What includes those certificates?
3. How does a browser verify the originality of the certificates?

4. How can you verify the originality of the certificates?
5. How to get a certificate for your website?
6. Problems related with web site certificates?

3. Private browsings

Your web browser keeps track of activities you perform in the web. In order to stop it from doing so, you can use the private browsing mode of your web browser.

1. What is the purpose of private browsing?
2. List some occasions where you can use private browsing?
3. Explain about private browsing in different browsers.
4. What is tracking protections in browsers?
5. What are the limitations and/or disadvantages of private browsing?

4. Using web proxies

When you browse the web, your packets that reach the web server can see your identity by looking at the IP address. In order to protect your identity, you can send your packets via a proxy server which will work as a middleman between your web browser and the web server.

1. How do proxies work?
2. What are the privacy and security concerns in proxies?
3. Types of proxies?

5. Cookies:

**** Include screenshots of each step you followed when answering the below questions.**

1. Open a new browser tab and visit https://cookie-2019.herokuapp.com/ and find the available cookies in your browser.

2. Initializing a cookie
   i. Use https://cookie-2019.herokuapp.com/init to make a new cookie.
   ii. What is the name and the value of the new cookie?

3. Alter the value of a cookie.
   i. Set a new value to the cookie using this route. https://cookie-2019.herokuapp.com/edit?value=test. You can change the “test” word with any text. (Ex:is2109) Take a screenshot of the developer tools cookie view with your edited cookie.

4. Destroying a cookie

    i. To destroy the above-mentioned cookie use https://cookie-2019.herokuapp.com/destroy endpoint.
    ii. Check the developer tools and verify the cookie is destroyed.

5. Hijacking a website using cookies

    - Assume that you are going to use https://cookie-2019.herokuapp.com/v1/test web site.
    - To use this site you have to log in. for that use https://cookie-2019.herokuapp.com/v1/login?id=lasith&key=YouCantGuessThis.
    - Reopen the https://cookie-2019.herokuapp.com/v1/test site.
    - Now check the available cookies.
    - Make required changes to cookies available and try to login to the site. (You should be able to view the "**Login Successful**" message on the screen). Include a screenshot of that message.

References

https://us-cert.cisa.gov/ncas/tips/ST05-010

https://www.hongkiat.com/blog/private-browsing/

https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history

https://support.google.com/chrome/answer/95464?hl=en