WEBPSEC – Exercise 3: Session Management

|  |  |
| --- | --- |
| Date |  |
| Leader |  |
| Members |  |
|  |
|  |
|  |

*(Do not include members who are absent)*

INSTRUCTIONS DOCUMENT

# Objective/s

* To be able to analyze determine different types of session management.
* To learn some vulnerabilities on poorly developed session management features.

Expected Output

Soft copy version of this lab exercise with answers to the theoretical and application parts.

# Prerequisite/s

* Burpsuite
* PC running Windows
* Internet  MS Office

# Instructions

* For the theoretical part, you may research the answers as long as you can defend it in class.

Don’t forget to cite sources. Explain your answers in your own words.

* For the application part, use the actual tool when doing the tasks and show it to your teacher.

Screenshot the answers afterwards as evidence in your report.

* Two groups will present in class: one group will present the theoretical part answers and the other one will present the application answers.
* Save your work in a PDF format: <Subject>\_<Topic>.pdf.
* Send your outline to: justindavidpineda@gmail.com with a subject: <SUBJECT> - Exercise <number> - <topic> - <Last Names of Members> at the end of class time.

# Tasks

## Part 1: Theoretical (50 points)

(You may answer the Application part first to help you answer the theoretical part.)

1. In a security perspective, which is the most preferred session management type? Why?
2. In a security perspective, which should developers create, a client-side session or a server side session?
3. In what instance can HTTPS traffic be sniffed in clear text? Explain the process.
4. If you force HTTPS to an HTTP session, will the traffic be encrypted? If yes, why and how? If no, why not?
5. If the certificate is not found by the browser in a corresponding website you visit, will you be able to visit the site? If yes, why and how? If no, why not?

## Part 2: Application (50 points)

Observing data sent in a website.

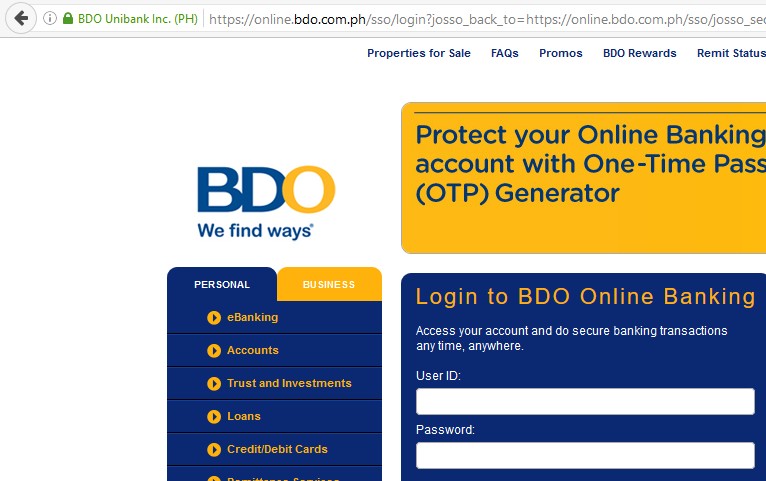
1. Using Burp, go to the following websites, create a dummy account and login:
   1. [http://gmx.com](http://gmx.com/)
   2. [http://pinoyexchange.com](http://pinoyexchange.com/)
   3. [https://tipidpc.com](https://tipidpc.com/)
2. Determine for each website how data is stored and sent to the server. What type of session management do these website use?
3. What are the session ID’s for each website?
4. Now, for each website, logout from your profile then login again. Do the session ID’s for the websites change? List them down.

Forcing HTTPS to an HTTP website.

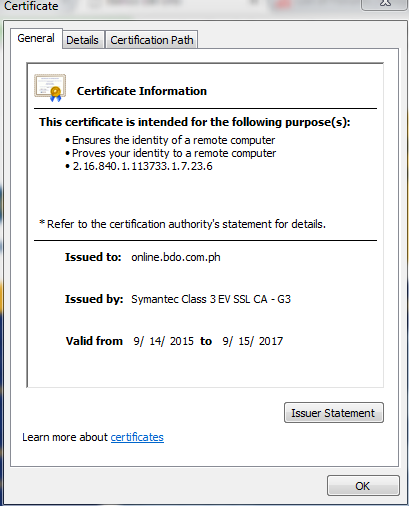
1. Go to [http://www.gmx.com/.](http://www.gmx.com/)
2. Force the website to run securely- [https://www.gmx.com.](https://www.gmx.com/)
3. Is the connection secured? How so?
4. Screenshot results.

Evaluating Certificates

1. Go to [https://www.online.bdo.com.ph](https://www.online.bdo.com.ph/)

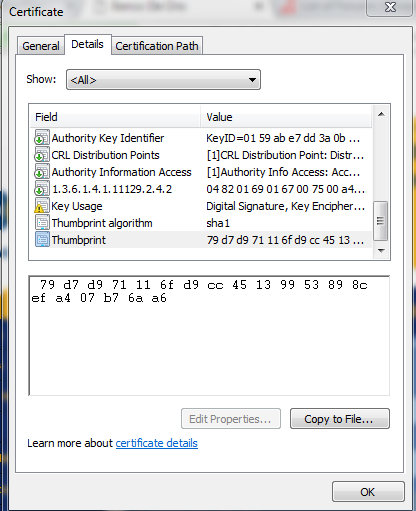


1. Click the green lock and browse over the information in there.
2. What is the website’s Certificate Authority?



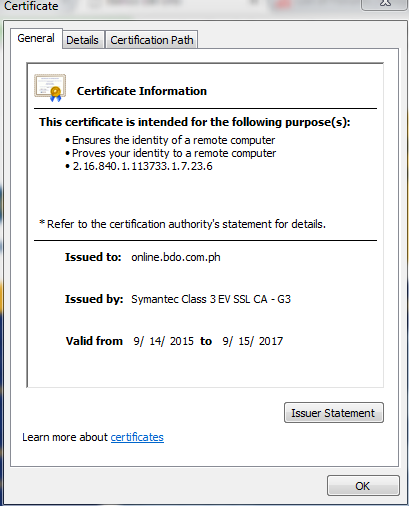
1. What is the website certificate’s hash value?

* ‎79 d7 d9 71 11 6f d9 cc 45 13 99 53 89 8c ef a4 07 b7 6a a6



1. Until when is the certificate available?

* Valid from 9/14/2015 to 9/15/2017

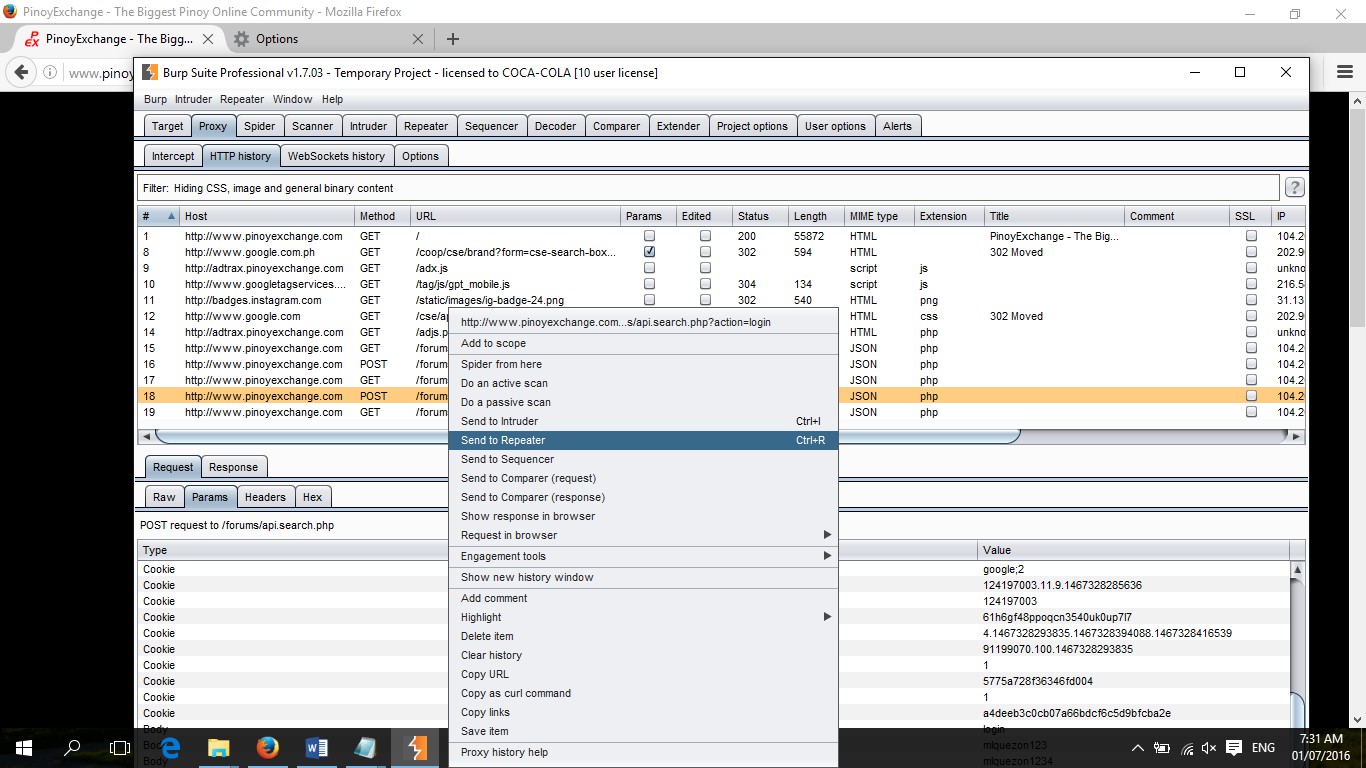


1. Screenshot the necessary details.

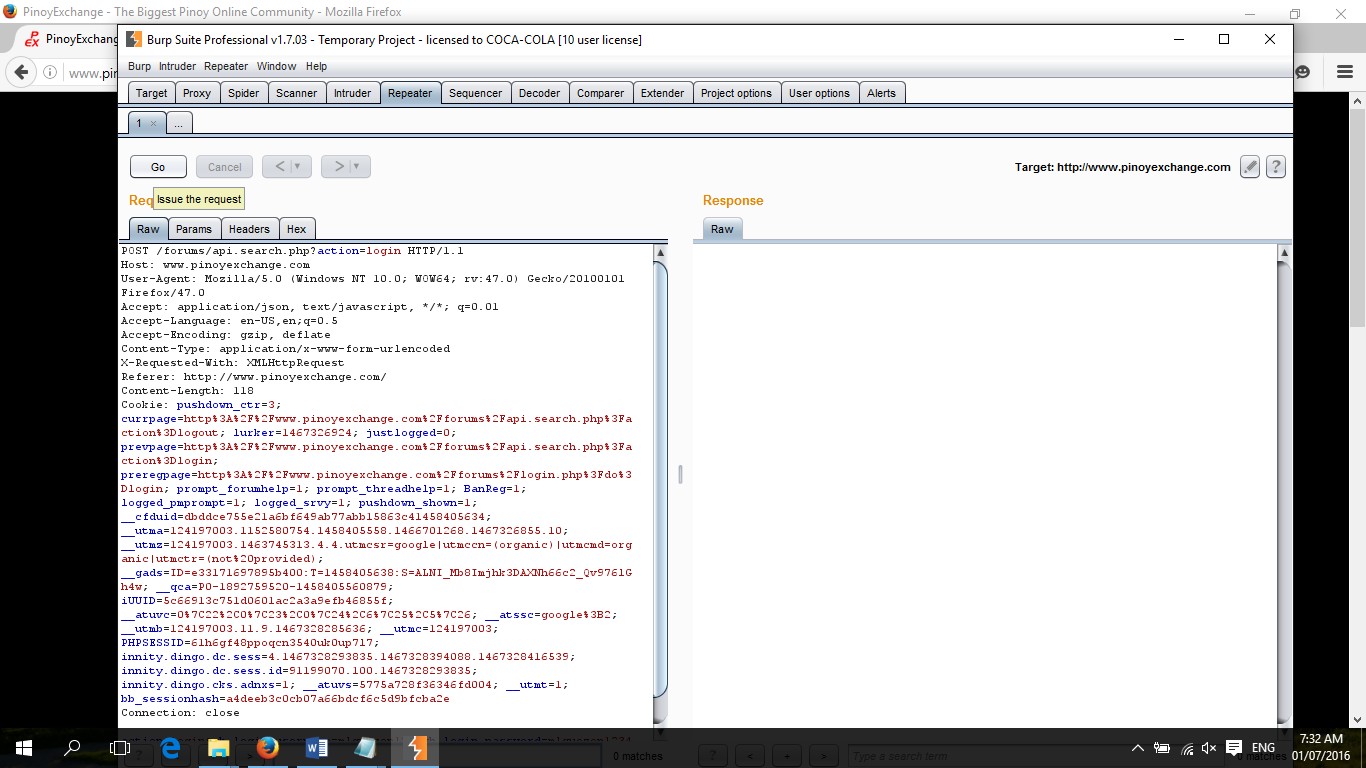
Request Replay Vulnerability

1. Open Burp and login to your dummy account in pinoyexchange.com 2. After logging it, note the session ID.

1. Logout of the account. Then login again the second time.
2. After logging it, note the session ID.
3. Logout of the account.
4. Did the session ID change?
5. Look for the POST method, right click on it and send to the repeater.



1. Repeat the request.



1. What was the result?

### ----- NOTHING FOLLOWS -----