Lab 08 - Attacking Session Management

16 points

In this lab, we’ll be looking at ways to attack session management and token generation. As with the last couple of labs, these can be challenging - start early and let me know if you run into any issues!

Complete the following tasks in **Lab 5. Attacking Session Management** on Pablo:

1. **[ 5 points]** Complete tasks **a - e.** You can attempt **g - i** but they are not required.
2. **[ 6 points]** Complete tasks **a - f.**
3. **[ 5 points]** Complete tasks **a - e.**

As with other labs, hints are provided on page 2.

**Deliverable:**

Turn in a Word Document or PDF that contains screenshots for each task as well as an explanation of what you are doing. If there are any additional questions, provide answers for those as well.

**Selected Hints**

1. Session Generation
   1. Easy

<https://gyazo.com/d11c6c739b523dc157532114a0cac539>

* 1. Look for a pattern

The sessions still need to be active for these attacks to work. I’m noticing that theme. If the person is logged out you can’t hop on a dead session.

<https://gyazo.com/287395c71852657dbffafffaa1452e57>

<https://gyazo.com/0b9e826cd2a12c17d1de905b1149b46d>

* 1. This one uses encoding, what you can you decode? Further hint, cookies…

<https://gyazo.com/963e1dad9f6b0a08cf706523db2c95b7>  
<https://gyazo.com/963e1dad9f6b0a08cf706523db2c95b7>

* 1. Similar to 1b, uses encoding and a larger offset though.

<https://gyazo.com/2352ff8ed21c651d23bc1618b5dc0d87>

* 1. The session ID is generated from a specific date/time

<https://gyazo.com/1dcf1ee1a30d251039205c4a12cbb761>

* 1. Look at the pattern, similar to the previous (look for a difference)

I ran packets through the comparer, to spot differences between part e. and part f.  
the only differences were:

the session ID itself

the date/time on the packets (by a matter of seconds)

and anywhere the number 55 showed up – cookie Id, url strings, etc. was replaced by 56…  
 the session ID also appeared to have an offset, or other encoding scheme, as the session ID appeared vastly different. It still tracked time similarly, but it was 4e64xxx…instead of d208xxx…

1. Session Handling
   1. Is the secure flag set? Think cookies

The secure flag is not set, http only is set though, which means that anyone can pick up their cookie throughout the session. I don’t think a demonstration of hopping into a session is necessary, since it is the same process as all those above.

* 1. Is it secure? HTTP vs HTTPS  
     Better in that we don’t use http the entire time, but still exposed at time of login, before the transition to https (when you get sent the home page)
  2. Are there any unsecure requests?
  3. Where is the session id?
  4. Concurrent logins are bad!
  5. What is your cookie value?
  6. When are you given your token?

1. Terminating Sessions
   1. logout
   2. but does it work?
   3. Is it still alive?
   4. Client side logic is not enough.