CS 331: Computer Security and Information Assurance
Lab Session-1: Using Burp Suite to Understand HTTP Traffic and Cookies

1 Prepraration

Install Burp Suite, install its certificate; setup proxy in your browser so that Burp Suite will serve as your proxy.

2 Trackers Used By boisestate.edu

1. Open Burp Suite, make sure you are on the "Proxy"-"Intercept" page. Turn "Intercept" on. Type www.boisestate.edu in your browser. Go back to Burp Suite, click "Action"-"Do Intercept"-"Response to this request". Before moving forward, answer the question: What type of request are you going to send to the server, "Get" or "Post"?

2. Click "Forward", you should then see a response from www.boisestate.edu. Your should see a status code 302, and a HTTP header named 'Location'. A 302 status code redirects your browser to a different page, the HTTP Location header tells your browser which page it should visit next. Before moving forward, answer the question: What page your browser is instructed to visit next?

3. Keep clicking "forward" until you see a web tracker in the 'Http history' tab. What’s the name of the tracker? (The website you intend to access is called a first-party website, every other website is called a third-party website. Every third-party website is a tracker.)

4. The reason you see trackers is because the first-party website - the website you are accessing, embedded some HTML tags in its source code, typically these are <script>, <img>, <iframe> tags. Let’s find out the related tag to the above tracker. Go to the web page displayed in your browser (i.e., www.boisestate.edu), right click and select "view source" or "view page source". Search the tracker’s name (such as Google) in the source code, you should be able to find out the tag related to the tracker. So what HTML tag is used?

5. When you send a request to a tracker for the first time, the tracker should respond to you. The response might also contain HTML elements or Javascript code that subsequently initialize other requests. Go to 'Proxy'->'HTTP history', find out the response, see if it contains a Javascript.

3 Trackers Used By espn.com

6. Turn off "Intercept", close that boisestate.edu page, and turn "Intercept" on, and then type www.espn.com in your browser. Go back to Burp Suite, keep clicking "Forward" until you see a tracker named optimizely.com in the 'Http history' tab. Go to the espn.com page and view
source code, search "optimizely" and you will find out why your browser is sending a request to this
optimizely tracker.

7. Turn 'Intercept' off. In the 'Http history' tab, go to your next tracker. Investigate why your
browser sent a request to this tracker. (Hints: there are mainly two reasons, either it’s defined
in the source code of the web page you are visiting, i.e., the home page of www.espn.com; or it’s
dynamically initiated as a result of a Javascript. If it’s the latter, find out which Javascript initiated
this request (to the tracker).)

4  Cookies Used by CNN.com and starbucks.com

8. Clear cookies in your browser. Turn 'Intercept' on, and access www.CNN.com, go to Burp
Suite and examine the suspended request, see whether or not your browser is sending cookies to
the server;

9. Click "Action"->"Do Intercept"->"Response to this request"; and then click "Forward". You
should see the response from CNN.com; examine the response, see if CNN.com is sending you some
cookies, if so, what HTTP header is used in the response (to send the cookies)? Also, do any of
these cookies have a secure flag set?

10. Turn "Intercept" off, and then turn "Intercept" on. Refresh your web browser page, and go to
Burp Suite and examine the suspended request. See whether or not your browser is sending some
cookies to the server, if so, what HTTP header is used in the request (to send the cookies)?

11. Turn "Intercept" off, and then turn "Intercept" on. Type https://www.starbucks.com in your
address bar, go to Burp Suite, click "Action"->'Do Intercept'->"Response to this request"; and
then click "Forward". You should see a response from starbucks.com. Examine the response, see if
the server is sending you cookies, if so, do any of these cookies have a secure flag set?

12. Also, it is a good practice for website admin to conceal the web server version information
to web clients. From the above response, do you see the version of the starbucks.com web server
program? (web server program: such as Apache, Microsoft IIS, nginx).