1 Background

Nowadays, most of the famous websites have deployed HTTPS, but for different reasons (primarily performance reason), some pages on these websites are still served over HTTP. This mixed-content serving model is insecure, as users’ privacy might be exposed over HTTP traffic. This is what we have seen in previous lab session, when one of google.com’s urls was accessible over HTTP, users’ email account and real name could be leaked to attackers. To enforce HTTPS, web servers need to use the HSTS header.

2 Preparation

1. Create an account on starbucks.com if you don’t have one; DO NOT LOGIN right now, or make sure you are logged out before you start the following experiments.

2. Make sure you have Burp Suite installed, with its certificate installed as well; proxy setting in your browser is correct so that Burp Suite will serve as your proxy.

3 Instructions

1. HSTS was covered in Jidong’s lectures, if you think his lecture sucks and therefore you didn’t listen to him, search and go to HSTS’s wikipedia page and figure out what HSTS stands for and its purpose.

2. Open Burp Suite, make sure you are on the 'Proxy'-"Intercept" page. Turn 'Intercept' on. Type www.starbucks.com in your browser. Go back to Burp Suite, click "Forward" several time, like 10 to 20 times. Then turn "Intercept" off, and turn it on. Then click the 'HTTP history' tab, you should see requests sent to starbucks.com, facebook.com, doubleclick.com, google-analytics.com, yahoo.com, bing.com, and many many many many other websites. (Yes, the trackers gonna track, track, track, track; baby, you’re just gonna shake, shake, shake, shake, shake.) Let’s shake it off and just focus on the above 6 websites. Select "Response" (at the bottom half of the Burp Suite), examine the responses from these 6 websites, see which of them have that HSTS header set, which do not.
3. So starbucks.com does not set HSTS, right? Now make sure 'Intercept' is still on, or if not, turn it on. Click "Sign in" on that starbucks.com homepage, and go back to Burp Suite, click "Action"->"Do Intercept"->'Response to this request"; and then click "Forward", you should see a response from starbucks.com. Did you see the HSTS header? If yes, explain why you didn’t see this in Step-2, but see this in Step-3.

4. Type-in your username and password to sign in. On that starbucks.com home page, there are buttons such as "COFFEE", "TEA", "MENU", "BLOG", "SHOP", etc. Click on one or two of these buttons, and go to Burp Suite, see if the requests were sent over HTTP or HTTPS.

5. When HSTS deployed properly, every request will be sent over HTTPS. However, this is not the case in practice. Go to the bottom of that starbucks.com home page, click on "Investor Relations". Go to Burp Suite, turn "Intercept" off. Click the "HTTP history" tab, examine how many requests are sent to investor.starbucks.com. You should notice this time the requests were sent over HTTP, rather than HTTPS. Figure out why. (Hints: Go to HSTS’s wikipedia page, and read the "Deployment best practices").

6. Not every company cares about best practices. Go to starbucks' bug bounty program page on hackerone.com, see if they care about this mixed-content issue or HTTPS/SSL/TLS best practices issue.