Session Hijacking

Question: What kind of session identifier does the application employ? Answer options (without quotation marks): "URL parameter", "URL argument", "body argument", "cookie" or "proprietary solution"

Answer: cookie

After adding the vHosts to the /etc/hosts by putting the IP and xss.htb.net, then you can look at the developer tools and in storage you can see that the only session identifier is cookie.

Session Fixation

Question: If the HttpOnly flag was set, would the application still be vulnerable to session fixation? Answer Format: Yes or No

Answer: Yes

Obtaining Session Identifiers without User Interaction

Question: If xss.htb.net was an intranet application, would an attacker still be able to capture cookies via sniffing traffic if he/she got access to the company's VPN? Suppose that any user connected to the VPN can interact with xss.htb.net. Answer format: Yes or No

Answer: Yes