7 Security (fms27)

As an Elite Pentester, you must demonstrate the flaws of Megacorp's obsolete website, which was developed without any of the modern countermeasures against well-known attacks. The website includes a web bulletin board that allows users to post arbitrary text or HTML content, without any pre-filtering. Technically, a logged-in user posts a message by sending a `GET` request to `http://www.megacorp.com/bb/post.php`, with appropriate values for the parameters `Subject` and `Body`. Let *PAYLOAD* stand for a malicious piece of Javascript source code.

(*a*) Write a message (somehow including *PAYLOAD*) that, if posted on the bulletin board from an unprivileged guest account, would cause *PAYLOAD* to be executed on your victim's browser. Explain clearly how this would happen and who the victim would be. [4 marks]

(*b*) Briefly explain what cookies are and why an attacker might wish to steal them. Then, within *PAYLOAD*, write Javascript code to copy the victim's cookies into the `stolenCookies` variable. [4 marks]

(*c*) Within *PAYLOAD*, write Javascript code to exfiltrate the victim's cookies to you, the attacker, and explain clearly how your technique works. [4 marks]

(*d*) Using the techniques in parts (*a*)–(*c*), you have obtained the cookies of the CEO of Megacorp. As a demonstration of the vulnerability of Megacorp's website, write a raw HTTP request that will post the message "My account has been hacked", purporting to be from the CEO. Write also the command you would type to send the request to the server with `netcat`. [4 marks]

(*e*) You test your attack in part (*d*) and it works. Great. You delete the fake message immediately. You test it again successfully, and again delete the message. Then you tell your boss that you are ready for the big demo. You two have a meeting with the Megacorp CEO. You run your attack again but... it fails miserably. You are supremely embarrassed. Why did your attack work the first and second time but not the third? [4 marks]