Security incident report

Section 1: Identify the network protocol involved in the incident
Transmission Control Protocol

Section 2: Document the incident
The attacker initiated a brute force attack to gain access to the web host. They repeatedly entered known default passwords for an admin account until they correctly guessed the right one. In doing so they were able to obtain the source code to the website. Then they embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website that would then redirect the customers to the fake website. This affected multiple customers. To investigate this a sandbox was used to observe the suspicious behavior of the website. Running the network protocol analyzer tcpdump I enter the url in to the website and am prompted to download and run the file, I then observe that the browser redirects me to a different url designed to look like the original site. The logs show that process.

Section 3: Recommend one remediation for brute force attacks
Require stronger more complex passwords; this will make it harder for brute force attacks to occur