Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol used is HTTP protocol which is relatively unsafe and the tcpdump logs proves it.

Section 2: Document the incident
The attacker was able to crack the password of the administrator . After he gained access to the source code of the website, he changed it so it prompts the user to download malicious code and redirecting to another illegitimate website.

Section 3: Recommend one remediation for brute force attacks
A strong password and tight firewall rules. The use of MFA or 2FA. Strictly pushing the users to change the default passwords.