Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is (Hypertext Transfer Protocol)HTTP. Since the issue was with accessing the web server of yummyrecipesforme.com. HTTP operates at the application layer of the TCP/IP model and is primarily used for transmitting web content between a client and a server. The traffic captured in the tcpdump log indicates that the incident occurred over HTTP, the malicious file was observed being transport to user's computer using HTTP protocol at the application layer.

Section 2: Document the incident
An unauthorized breach occurred on the web server hosting yummyrecipesforme.com, where a former employee successfully executed a brute force attack using default administrative credentials. After gaining access, the attacker embedded a malicious JavaScript function into the website's source code. This script prompted visitors to download an executable file, which, once run, redirected their browsers to a spoofed domain (greatrecipesforme.com) containing malware. Customers began reporting unusual prompts to download files, followed by system slowdowns and website redirection. The website administrator was unable to log in, indicating a password change by the attacker. The cybersecurity team analyzed tcpdump log data, confirming DNS and HTTP traffic that supported the redirection behavior. The root cause was traced to the lack of password policy enforcement and absence of controls to prevent brute force attacks.

Section 3: Recommend one remediation for brute force attacks
To prevent future brute force attacks, implement **two-factor authentication (2FA)** for all admin accounts. This adds a second verification step, making it significantly harder for attackers to gain access even if they guess the correct password.