Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol that was involved during the incident was Hypertext transfer protocol (HTTP) version 1.1. The malicious file is transported to the user's device using the HTTP: GET method at the application layer.

Section 2: Document the incident
Various customers reported to the site's helpdesk stating that the site prompted them to download a file to access the free recipes. Resulting in the site being redirected and making the user's machines run slower. After hearing this the site owner tried to log into the admin panel and discovered they were locked out. The cyber analysis team created a sandbox environment to observe what was reported. In the environment a network protocol analyzer tcpdump was used to capture the network packets while interacting witht the website and replicating what the users did. The analyst produced the same outcome when navigating the site the same way as the users. After inspecting the tcpdump logs the analyst observed the browser initiates a DNS request to the yummyrecipes.com URL and replies with the correct address. After successfully connecting over the HTTP protocol the analyst downloads the malicious file. This is were in the logs the network traffic changes and the browser initiates a request to a different URL greatrecipesforme.com. After analyzing this the security analyst discovered that the attacker had altered the source code and save the prompt for the malicious download was added to the javascript code. After the analysis the team reported the web-server was infected by a brute force attack.

Section 3: Recommend one remediation for brute force attacks
Enforcing two-factor authentication (2FA) is one remediation that can be implemented to prevent future brute-force attacks like this. 2FA requires a one-time passcode (OTP) that is either sent to an app, email, or phone. This confirms the identity of the user and verifies the request to gain access to the given system. This feature increases the overall security and will prevent malicious actors from likely gaining access to the system.