Security incident report

Section 1: Identify the network protocol involved in the incident
We believe that the protocol used was HTTP in the application layer. This is because the incident involved accessing the web server for yummyrecipesforme.com.

Section 2: Document the incident
When visiting the website, several customers contacted yummyrecipesforme.com's help desk stating that they were prompted to download a file to access all free recipes. After downloading the contents, their computers have been running noticeably slow. Additionally, the website owner tried to log into the website and noticed that he was locked out. We have used a sandbox environment to investigate this issue w/o impacting the company network. Upon following through the steps to replicate the issue, we can confirm that the website prompted users (customers) to download a file claiming it would provide access to contents within the website. After running the file, we were redirected to a fake website greatrecipesforme.com. In continuation of our investigation we used the tcpdump tool to analyze network traffic produced by the website. The log indicated that the browser initially requested access to yummyrecipesforme.com however was later redirected to fake website greatrecipesforme.com after successful connection and file download. We believe that the attacker implemented an additional code embedded within websites code that prompted users to download a malicious file masked as a browser update. Additionally, we believe that the malicious actor used a brute force attack to initiate all changes including website owners lock out.

Section 3: Recommend one remediation for brute force attacks
We would like to recommend multiple security measures that would harden

security and benefit both the website owner and customers. One of which being: disallowing the use of default and old passwords. The assumption that the malicious attacker used a brute force attack indicates that old passwords or easy to guess passwords would have been used. Preventing this use would greatly improve security posture for possible future attacks. Another way to improve security from brute force attacks is to use OTP or other Multi-Factor Authentication. This would prompt the website owner to verify that an admin is trying to access the website preventing lock out.