Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in this incident is HTTP(Hypertext Markup Language). Since, the issue was with accessing the web server for yummyrecipesforme.com. The customers would be redirected to another website using HTTP protocol where malicious file was present.

Section 2: Document the incident
Several customers contacted the website's helpdesk stating that when they visited the website they were prompted to download and run a file that contained access to new recipes. Since then, the operating system of their computers have been slow. In response to the incident , the website owner's tries to log into the admin panel but is unable to do so. The cybersecurity analyst inspected the tcpdump log and observed that the logs showed a sudden change in network traffic as they tried to open the website the same as the customers. The network traffic was routed to a new IP address for the greatrecipesforme.com where the malicious file had been. After analysis, it occurred that the source code for the websites had been altered to download malicious files disguised as a browser update by redirecting the customers to another website. Since the website owner had not been able to log into their administrator account, the team believes that the attacker used brute force attack to access the account and change the source code in the admin panel.

Section 3: Recommend one remediation for brute force attacks
One security measure the team plans to implement to protect against brute

force attacks is to disallow previous passwords being used and strengthen the password by using MFA(Multi factor authentication). Since the vulnerability that led to this attack was the attacker's ability to use a default password to log in, it is important that we prevent any old passwords from being used frequently as reset passwords. Also, adding another layer of security by confirming a one time passcode (OTP) as 2FA would strengthen the security. 2FA requires authentication via password and OTP is sent to either email or phone for another authentication. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authentication.