Security incident report

Section 1: Identify the network protocol involved in the incident
Hypertext Transfer Protocol (HTTP). We have determined that the issue was accessing the web server from yummyrecipesforme.com. It is known that requests to web servers for web pages involve using HTTP traffic. Furthermore, the tcpdump log file showed the usage of the HTTP protocol. In conclusion, the malicious file is observed being transported to the user's computer using the HTTP protocol in the application layer.

Section 2: Document the incident
An individual obtained the login credentials of the company's admin panel and changed the website's source code. The attacker embedded a malicious JavaScript that prompted individuals to download a malicious file upon visiting the website. When customers downloaded the file, they were taken to a fake website. Customers later contacted yummyrecipesforme's helpdesk several hours later, complaining that their computers ran more slowly after the installation of the malicious file. In response to this incident, the website owner tried to log in to the admin panel but was unable to. The website owner later reached out to cybersecurity analysts to investigate this event. The cybersecurity analysts created a sandbox environment to observe the suspicious website. Tcpdump was used to analyze the network, and it was shown that the original website, yummyrecipesforme, was compromised.

Section 3: Recommend one remediation for brute force attacks
To combat a brute force attack, the company could have set a security measure in place that disallows previous passwords from being used repeatedly. Since the attack started with the attacker being able to easily guess

the login credentials due to the admin passwords being set to default, it's important to disallow the use of old passwords. Furthermore, 2MFA could have also been set as a security measure. 2MFA would have required 2 or more verification methods to access the admin panel.