Security incident report

Section 1: Identify the network protocol involved in the incident
The DNS and HTTP protocols were used to establish a connection between the user and the website. The user's machine sent a DNS resolution request to the DNS server to obtain the IP address of the website. The DNS server replied with the correct IP address. Then the user's machine sent the HTTP connection request sent an HTTP connection request to the website's server to initiate the connection.

Section 2: Document the incident
A disgruntled baker executed a brute force attack to gain access to the web host of the yummyrecipesforme.com website. After obtaining the login credentials, the attacker was able to access the admin panel and modify the website's source code. They embedded a JavaScript function that prompted visitors to download and run a file. After running the downloaded file, the customers were redirected to a fake version of the website where the seller's recipes are now available for free. Several customers reported that the company's website prompted them to download a file to update their browsers. The customers complained that after running the file, the website's address changed, and their personal computers began to run more slowly. The website owner was unable to log in to the admin panel and reached out to the hosting provider. The cybersecurity team confirmed the website was compromised, and the web server was impacted by a brute force attack.

Section 3: Recommend one remediation for brute force attacks

I suggest using strong /unique passwords to reduce brute force attempts. The admin password was set to the default password, which made it easier for the hacker to get into your system. Stronger and more unique passwords can help significantly reduce this.