Security incident report

Section 1: Identify the network protocol involved in the incident
HyperText Transfer Protocol (HTTP)

Section 2: Document the incident
Multiple customers reported that the address of the website (yummyrecipesforme.com) changed and their personal computers began running more slowly. After many reports, the website owner tried to log in to the admin panel but was unsuccessful and reached to the website hosting provider. After investigating this with other security analysts, we found that there was a prompt to download a file that redirects to a different URL that contains malware and it was later confirmed that the website was compromised. We examined the tcpdump log to determine what had happened. It was reported that the admin panel was accessed by brute force. And It what appears to be by a disgruntled employee who guessed the password correctly because the admin passwords were still set to default. By investigating further, there were no security controls in place to stop this brute force attack.

Section 3: Recommend one remediation for brute force attacks
Implement stronger password requirement policies. Example: Use at least 25 characters that include letters, numbers, and symbols. It is very effective because the longer and complex the password is, the longer it will take for brute force attack to happen.