# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| * **DNS**: Resolved domain names (yummyrecipesforme.com and greatrecipesforme.com) to IP addresses. * **HTTP**: Loaded web pages from the server. * **TCP**: Established reliable connections between the browser and server. | |
|

| **Section 2: Document the incident** |
| --- |
| * A former employee executed a **brute force attack**, guessed the default admin password, and accessed the admin panel. * Malicious JavaScript was added to the website, prompting visitors to download an executable file. * The file redirected users to greatrecipesforme.com, infecting their systems with malware. * Customers reported slow computer performance(possible malware infection) and browser redirection.   **Root Cause**:   * The admin account used a **default password** with no brute force protection. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Implement **account lockout mechanisms**:   * Lock accounts after a set number of failed login attempts (e.g., 5 attempts). * Add **multi-factor authentication (MFA)** for admin accounts to enhance security.   This will prevent brute force attacks and protect against unauthorized access. |