# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocols involved in the security incident are DNS and HTTP. The DNS protocol was used for resolving the IP addresses of the website while the HTTP protocol was used for communication between the web browser and the websites. | |
|

| **Section 2: Document the incident** |
| --- |
| A security incident occurred at yummyrecipesforme.com, a website that sells recipes and cookbooks. The incident was a result of a brute force attack executed by a disgruntled baker. The attacker repeatedly attempted to log in to the administrative account using known default passwords until the correct password was guessed. Once access was gained, the attacker modified the website's source code.  As a consequence of the source code modification, visitors to the website were prompted to download and run an executable file. This file contained a script that redirected the visitors browsers to a fake version of the website. The fake website resembled the original website but provided the seller's recipes for free. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To prevent brute force attacks and enhance the security of the organization it is recommended to enforce Two Factor Authentication. Two Factor Authentication adds an extra layer of security by requiring users to provide two forms of authentication before gaining access to the system or account. |