# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Network protocol DNS and HTTP are both involved in an incident involving an unsecured admin account, brute force login, malicious code injection, and a redirection attack. | |
|

| **Section 2: Document the incident** |
| --- |
| After receiving several customer complaints about our website (yummyrecipesforme.com) asking them to download a file and redirect them to a website that was accessed via a sandbox/VM where tcpdump was run while accessing our website. It prompted the analyst to download a file and upon doing so the machine started running slower and we were redirected to another website (greatrecipesforme.com). Where our cookbooks were being listed for free and including a download link for them.  It appears the threat actor has managed to brute force login to an unsecured admin account in the admin panel as the password was left as the default password and no policy or security control was in place to prevent access from which they then injected malicious java code that prompted visitors to download a file. This file then redirects them to a new website (greatrecipesforme.com). |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Recommended steps to take are as follows: We are still using the unsecure HTTP protocol and should instead move over to using HTTPS as it is more secure.  We shall implement and enforce new password security controls and policies such as 2FA, password requirements, and limited login attempts.   Our 2FA plan will require users to associate their phone number to their accounts and upon correctly entering their credentials they will receive an OTP on their phone via a text message to be given access to their account. Further we will implement a time out for incorrect logins and after 3 failed attempts within 5 minutes the account will be locked for 30 minutes and an email will be sent to the user associated with the username that was used to inform them.  Malicious code to be removed and security scan of the website and its remaining code to ensure no other changes have been made. |