# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocol involved in this event was the HTTP or HyperText Transfer Protocol. This is an application layer protocol and by analyzing the logs using tcpdump they were able to observe a HTTP GET request likely used to deliver the malicious file to the user. | |
|

| **Section 2: Document the incident** |
| --- |
| Multiple customers emailed the yummyrecipesforme.com help desk to complain about being prompted to download a file to update their browsers. This resulted in the users being redirected to a different URL and noticing network performance issues. The website owner then proceeded to try accessing the admin panel unsuccessfully leading them to contact the cybersecurity team to investigate.  The analyst used a sandbox environment to access the website and run a network analyzer, tcpdump. They were immediately prompted to download the malicious file which they did and were redirected to a different URL with a similar looking website.  Analyzing the DNS & HTTP traffic log showed the browser made a DNS request for the website and later a HTTP GET request was made where the website initiates the malicious file download. There is then another DNS request which returns a new IP address for the compromised website.  A senior analyst confirmed these findings and after looking through the source code for the site found a Javascript function to prompt the download of an executable file. Analysis of the downloaded file shows a script to redirect the user from yummyrecipesforme.com to greatrecipesforme.com. It was determined by the team that a disgruntled baker had used a brute force attack to gain access to the admin panel using a default password. There were no controls in place to prevent this attack. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To avoid this type of incident in the future the team should implement more stringent password guidelines as well and two factor (2FA) or multifactor authentication (MFA). These extra steps to login credentials would ensure brute force attacks could not occur. |