# Security Incident Report

| Section 1: Identify the network protocol involved in the incident |
| --- |
| The impacted protocol in the incident is HTTP (Hypertext Transfer Protocol). The team ran a tcpdump in a sandbox environment then accessed the yummyrecipesforme.com website to detect the problem, isolate/capture the protocol. The traffic activity in a DNS and HTTP traffic log file provided the evidence needed.<br>The malicious file is observed being transported to the users' computers using the HTTP protocol in the application layer of the TCP/IP model. |

| Section 2: Document the incident |
| --- |
| We received multiple emails from customers at the yummyrecipeforme.com's helpdesk stating that when they visited the website, they were asked to download to file to update their browsers. This file compromised their personal devices and has caused them to run slowly ever since. The website owner attempted to login to the admin panel but is unable to do so.<br><br>The cybersecurity analyst setup a sandbox environment that allowed them to test the website and investigate the issue without impacting the network. A tcpdump was then ran to capture the network and protocol traffic packets. The analyst had the same issue as the customers. They were prompte to download a file to update their browser, and the updated browser then redirected the analyst to a fake website - greatrecipesforme.com - that was identical to the original website, except it had yummyrecipesforme.com's best-selling recipes displayed for free.<br><br>Upon further inspection of the tcpdump log, it was found that the browser initially requested the IP address for the original website and once the connection was established over the HTTP protocol, the analyst downloaded and executed the file. |

The logs showed a change in the network traffic as the analyst was redirected to the new IP address for the fake website - greatrecipesforme.com

After analysing the website source code, it was discovered that an attacker had brute-forced to guess the password to the admin panel and added code to promt the users to download the malicious file. We believe it is a brute-force attack as the website owner is locked out of their account. Lastly, the execution of the malicious file compromised the end users' computers.

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| One remediation for brute force attacks would be for the website owner to implement a multi-factor authentication system (MFA). This plan will require 3 ways for the website owner to validate their identity by answering questions related to; something they know, something they have and something unique about them.<br><br>With these heavily personalised questions, it would be harder for brute-force attacks to work as the attacker would need to be extremely close to the victim and be knowledgeable about the website owner's personal life to gain access to the system. |