# Security incident report

## Section 1: Identify the network protocol involved in the incident

The network protocol involved in the incident is HTTP. Users are prompted to download  a file and run it on their devices. As soon as the file is ran on their devices the malicious files code runs and opens up the browser and directs them to the fake website where the content is posted for free.

## Section 2: Document the incident

Multiple Users contacted yummyrecipes.com’s help desk to inform that users are being prompted to download a malicious file for free recipes and after the users have downloaded the file and ran it the file redirects them to a new website where recipes are posted for free. On inspection using tcpdump logs and running the file on a sandbox environment it was found that as soon as users click on free recipes the website initiates a GET request which means it is requesting data from the server and receives the file. It was found that the admin panel was compromised and the source code was affected and it was modified to run a malicious script to prompt the user to download the file.

## Section 3: Recommend one remediation for brute force attacks

One remediation for brute force attacks is to maintain a password policy. For example

Passwords should be longer than 8 characters

Passwords should include 1 capital letter and 1 number

Passwords should have a special symbol.

Another good remediation would be to use 2FA (2 Factor Authentication) such as password and OTP(One Time Password) or MFA(Multi Factor Authentication) such as password, OTP and facial or fingerprint scan