# Security Incident Report

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

The network protocols involved in this security incident were DNS (Domain Name System) and HTTP (Hypertext Transfer Protocol).  
  
- DNS was used to resolve the domain names (yummyrecipesforme.com and later greatrecipesforme.com) into IP addresses.  
- HTTP was used to establish communication between the user's browser and the web server, including downloading the malicious file.

## Section 2: Document the incident

Incident Summary:

- Location: The web server hosting the site yummyrecipesforme.com  
  
- How It Happened:  
 - A disgruntled former employee performed a brute force attack by repeatedly guessing common default administrator passwords.  
 - After successfully logging in, they modified the website’s source code by injecting a malicious JavaScript script.  
 - This script prompted visitors to download and execute a malicious file under the pretext of a browser update.  
 - Upon execution, the script redirected users' browsers from yummyrecipesforme.com to a fake, malware-laden site greatrecipesforme.com.  
  
- Witnesses:  
 - Multiple customers reported to the help desk that they were asked to download a file when visiting the website.  
  
- Discovery:  
 - Customers' complaints led the site owner to attempt logging into the admin panel, which failed.  
 - The cybersecurity team investigated and analyzed tcpdump traffic logs confirming malicious activities.  
  
- Evidence:  
 - Tcpdump logs showed DNS queries and HTTP traffic involving yummyrecipesforme.com and greatrecipesforme.com.  
 - The downloaded executable file was analyzed and contained code redirecting users to the fake site.

Key Log Details:  
- DNS queries resolved domain names to IP addresses.  
- HTTP GET requests downloaded malicious content via port 80 traffic.

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

Recommendation:  
Implement Two-Factor Authentication (2FA) for administrator and privileged user accounts.  
  
Why it is effective:  
- 2FA requires users to provide not only a password but also a second factor (such as a mobile code, authentication app, or hardware token) to log in.  
- Even if a password is compromised, unauthorized access is prevented without the second authentication factor.  
- It significantly reduces the success rate of brute force attacks and strengthens the security posture.