# Security incident report

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

The network protocols involved in this incident were DNS and HTTP. DNS was used to resolve the IP addresses for the domain names yummyrecipesforme.com and greatrecipesforme.com. HTTP was the protocol used to transmit web page data, including the download of a malicious executable file and the redirection to the fake website.

## Section 2: Document the incident

The incident occurred on the website yummyrecipesforme.com and was discovered after multiple customers contacted the helpdesk. They reported being prompted to download a file claiming to offer free recipes, which, after execution, redirected them to a different website (greatrecipesforme.com) and resulted in slower system performance.  
  
Upon investigation, tcpdump logs revealed that the attacker had modified the source code of the legitimate website by injecting JavaScript. This code triggered an automatic download of a malicious file once a user accessed the main page. The DNS request for yummyrecipesforme.com returned the correct IP, and an HTTP GET request was initiated. Following this, another DNS query was issued for greatrecipesforme.com, and a subsequent HTTP request was made to that new IP, confirming the redirection behavior.  
  
A senior analyst confirmed the site’s code had been changed, and the executable file contained redirection scripts. It was also discovered that a former employee gained unauthorized access via a brute force attack on the admin panel, exploiting weak credentials that had not been changed from their default values. The attacker then changed the password after gaining access, locking out legitimate administrators.

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

To prevent future brute force attacks, it is recommended that the organization implement two-factor authentication (2FA) for all administrative accounts. This adds an additional layer of security by requiring a second form of verification beyond just a username and password. Even if an attacker guesses the password, they would be unable to log in without the secondary authentication factor. This significantly reduces the risk of unauthorized access through brute force methods.