

# Security incident report

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

Going into the logs, we query the yummyrecipesforme.com and it involved HTTP protocol as we are accessing a website

## Section 2: Document the incident

Going to the site of yummyrecipesforme.com over port 80 we then get redirected to greatrecipesforme.com as stated by the customers and the owner of the site. Customers are being notified that they need to download an unknown file which causes them to be redirected to a malicious site. While the website owner has been locked out of his own account indicating that there has been an account compromise that happened. This may be the cause of a brute force attack.

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

For username and password brute force attacks, use a stronger password and implement strong password policies.