# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocol involved in this incident is Hypertext transfer protocol(HTTP) at the application layer. By analyzing the traffic log using tcpdump , we observed that the malicious file is being transported to the user’s computer by redirecting the user to a different URL: greatrecipesforme,com using HTTP protocol. | |
|

| **Section 2: Document the incident** |
| --- |
| Multiple customers emailed yummyrecipesforme’s helpdesk to complained that the company’s website had prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.The website owner attempted to log into the web server but failed as he/she was locked out of his/her account.  The cybersecurity analyst used a sandbox environment to test the website and check their network and protocol traffic packets by using tcpdump.During the interaction with URL:yummyrecipesforme.com website , the analyst was prompted to download a file claiming it would update the user’s browser. Once the analyst accepted the download , the browser is then redirected to a fake website URL:greatrecipesforme.com.By inspecting the tcpdump log , it can be observed that the log showed a sudden change in network traffic as the browser requested a new IP resolution for the URL:greatrecipesforme.com through DNS request.  After analyzing the source code for the websites and the downloaded file , the analyst discovered that an attacker had manipulated the website by adding a code that prompts user to download a malicious file disguised as a browser update.Since the website owner stated that he/she had been locked out of their administrator account, the team hypothesized that the attacker used a brute force attack to access the account and change the admin password. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| The security measure the team plants to implement to protect against brute force attack is by enforcing two-factor authentication (2FA) as it is an effective security measure to prevent brute force attacks because it adds an extra layer of security beyond just username and password authentication. 2FA requires users to provide two forms of identification before gaining access to an account or system. Typically, these factors fall into three categories: something you know (e.g., password), something you have (e.g., a mobile device), and something you are (e.g., biometric data).Even if an attacker manages to obtain a user's password through methods like phishing or social engineering, they would still need the second factor to complete the authentication process. This reduces the risk of account compromise in the event of password theft. |