# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The protocol impacted in the incident is Hypertext Transfer Protocol (HTTP). I used tcpdump to capture the network traffic while accessing the yummyrecipesforme.com website and saved it in a DNS & HTTP traffic log file. This file showed that the malicious file was transferred to the users’ computers using the HTTP protocol at the application layer. | |
|

| **Section 2: Document the incident** |
| --- |
| Several customers reported that they were asked to download and run a file that claimed to update their browsers when they visited the yummyrecipesforme.com website. Their computers became slow after that. The website owner could not log in to the web server because their account was locked. I tested the website in a sandbox environment to avoid affecting the company network. I also used tcpdump to capture the network traffic while interacting with the website. I downloaded and ran the file as instructed. The browser then redirected me to a fake website (greatrecipesforme.com) that looked like the original one. I analyzed the tcpdump log and found that the browser first requested the IP address for the yummyrecipesforme.com website. After the connection was established over the HTTP protocol, the browser requested a new IP address for the greatrecipesforme.com website and switched to it. The senior cybersecurity professional examined the source code for the websites and the downloaded file. They found that an attacker had added code to the website that tricked the users into downloading a malicious file disguised as a browser update. The team suspected that the attacker used a brute force attack to access the website owner’s account and change the password. The malicious file compromised the users’ computers. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| * One security measure the team recommends to prevent brute force attacks is two-factor authentication (2FA). This 2FA method will require users to verify their identity by entering a one-time password (OTP) sent to their email or phone, in addition to their login credentials. This way, only authorized users can access the system. A brute force attacker will not be able to access the system without the OTP. |