# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The protocol involved in the incident is the Hypertext transfer protocol (HTTP). | |
|

| **Section 2: Document the incident** |
| --- |
| Several customers emailed yummyrecipesforme’s helpdesk. They complained that the company’s website had prompted them to download a file to access free recipes. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.In response to this incident, the website owner tried to log in to the admin panel but was unable to.  The Cybersecurity analyst created a sandbox environment outside of the network to observe the suspicious website behaviour. The analyst initiated tcpdump, entered the URL for the website, yummyrecipesforme.com. The analyst was prompted to download a file claiming it would provide access  to free recipes, accepted the download and ran it. The browser then redirected  the analyst to another website (greatrecipesforme.com).  Inspecting the tcpdump log, the analyst observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once connection was established, the browser initiated download of a file, There was a sudden change in the log as the browser requested a new IP address for greatrecipesforme.com and was rerouted.  A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. The analyst discovered that a hacker had manipulated the website to add code that prompted the users to download a malicious file disguised as a browser update.Analysis of the downloaded file found a script that redirects the visitors’ browsers from yummyrecipesforme.com to greatrecipesforme.com. The cybersecurity team reports that the web server was impacted by a brute force attack. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Enforcing 2FA: Two-factor authentication requires an additional authentication method beside passwords to allow access into a system. |