# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The incident involves the HTTP (Hypertext Transfer Protocol) network protocol. When attempting to access the webpage, the traffic was routed through the HTTP protocol, resulting in the file being downloaded. Subsequently, the webpage was redirected to another destination. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers reported to the website’s helpdesk that they were prompted to download a file claiming to provide access to new recipes. After running the file, their computers began operating sluggishly. The website owner attempted to log into the server but discovered they were locked out of the administrator account.  A cybersecurity analyst investigated the issue in a sandbox environment to avoid impacting the company network. Using **tcpdump**, the analyst captured network traffic generated by interacting with the website. During the test, the analyst was prompted to download a file disguised as a recipe tool. After executing the file, the browser redirected to a fraudulent website, *greatrecipesforme.com*.  The **tcpdump** logs revealed the browser initially requested the IP address for *yummyrecipesforme.com*. Once connected over the HTTP protocol, the download and execution of the file triggered a sudden shift in network traffic, redirecting it to a new IP associated with *greatrecipesforme.com*.  Further analysis by a senior cybersecurity professional uncovered that attackers had inserted malicious code into the website. This code tricked users into downloading a fake browser update, compromising their systems upon execution. It was also determined that the attackers likely used a brute-force attack to gain unauthorized access to the administrator account and change the password, locking out the legitimate owner. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| **Adopt a Strong Password Policy**: Follow the guidelines outlined by NIST, requiring users to create strong, unique passwords that are resistant to brute-force attempts.  **Eliminate Default and Reused Passwords**: Enforce policies that prevent the use of default credentials and previously used passwords, reducing vulnerabilities from recycled passwords.  **Enable Multi-Factor Authentication (MFA)**: Add an extra layer of security by requiring users to verify their identity through additional factors (e.g., biometrics, one-time passwords), ensuring that compromised credentials alone cannot grant access.  **Frequent Password Changes**: Enforcing a regular password change policy can be highly effective in situations where the default password is not updated during deployment. This ensures that such default credentials are only active for a limited time, minimizing the risk of unauthorized access due to their prolonged use. |