# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The connection between the user and the website was established using the DNS and HTTP protocols. First, the user's machine sent a DNS resolution request to the DNS server to get the website's IP address. After receiving the correct IP address from the DNS server, the user's machine sent an HTTP connection request to the website's server to initiate the connection. | |
|

| **Section 2: Document the incident** |
| --- |
| An unhappy baker launched a brute force attack on the web host of the yummyrecipesforme.com site. After breaching the login credentials, the attacker accessed the admin panel and altered the website's source code, embedding a JavaScript function that prompted visitors to download and run a file. Upon executing this file, customers were redirected to a fraudulent version of the site where the recipes were freely available. Several customers reported receiving a prompt to download a file for a browser update from the company's website. After running the file, they noticed the website's address changed, and their computers began to slow down. The website owner couldn't log in to the admin panel and contacted the hosting provider. The cybersecurity team confirmed that the site had been compromised by a brute force attack. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Ensure that passwords are both strong and unique. The admin password was left at its default setting, making it easy for the attacker to guess. Utilizing complex and unique passwords can prevent such breaches. |