# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol involved in the incident was the hypertext transfer protocol (https) since the problem was accessing |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Customers contacted the help desk about an issue that when they visited the website yummyrecipesforme.com it prompted them to download a file that contained access to new recipes and at that there computers been running slower ever since. So first a sandbox environment was used to open the website without compromising the companies network. After the tcp dump was ran to capture network traffic packets produced by interacting with the network it was prompted to download a file claiming it would provide access to more free recipes. After downloaded the browser redirected me to a fake website 9 greatrecipesforme.com). The initial request from the browser was the IP address of yummyrecipesforme.com but once connection was established through the http protocol and the file was downloaded the logs showed a sudden change in the network traffic as the browser requested a new IP address for greatrecipesforme.com. The network traffic was then rerouted to the new IP address for greatrecipesforme.com. As the source code was analyzed its seen that the attacker may have used a brute force attack to manipulate the website to add code that prompted the users to download the malicious file disguised as a browser update. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| One recommendation for this brute force attack is to use is to use a disallow previous passwords used and to also add some OS hardening practices like updating the password policy and making them more demanding in terms of requirements. Another things is adding a two step authentication. |