# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The malicious file is observed being transported to the users’ computers using the HTTP protocol at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The incident took place for the website yummyrecipeforme.com. A former employee (baker) lured users to a fake website with malware. Several hours after the attack, multiple customers emailed to complain claiming the company website had prompted them to download a file to access free recipes and on running the file the website address changed and their personal computers began running more slowly.  The baker executed a brute force attack and gained access to the administrative account and was able to embed a malicious code in the source code of the website which prompts customers to download and run a file upon visiting the website. when customers downloaded the file they were redirected to a fake version of the website that contains the malware. The baker also changed the password of the administrative account because of which the website owner was unable to log in to the admin panel of the website. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Using long Alphanumeric passwords – Using long and strong password limits the ability of the brute force attack to be able to guess the password. |