# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocol identified as the incident is at layer 4 which is the application layer to exact is the HTTP or hypertext transfer protocol of the TCP/IP model. From the log we could see that the incident involves the client web browser and the web server for the yummyrecipesforme.com and greatrecipesforme.com. The malicious file was transferred or being transported to the user’s computer using the HTTP protocol at the application layer. | |
|

| **Section 2: Document the incident** |
| --- |
| A security incident was observed at “yummyrecipesforme.com” , a website that sells recipes and cookbooks. The incident involved an unauthorized access and malicious threat to the web by making users being forced to download a file and after downloading the file, redirecting the website to the fake website (greatrecipesforme.com) that contains the malware.  The following details of the incident:   * Location of the incident : yummyrecipesforme.com website * Case : The baker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. * Impact : After Obtained the login credentials, threat actor was able to access the admin panel and change the website’s source code, then threat actor added / embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After embedding the malware, threat actor changed the password to the administrative account and made customers download the file, after that the were redirected to a fake website (greatrecipesforme.com) that contains the malware. * Discovery of the Incident : Multiple customers emailed yummyrecipesforme’s helpdesk. They complained that the company’s website had prompted them to download a file to access free recipes and claimed that, after running the file, the address of the website changed and their personal computers began running more slowly. * Source of incident : The password easily because the admin password was still set to the default password and there were no controls in place to prevent a brute force attack * Evidences : The evidence can be obtained from network protocol analyzer tcpdump log, which captures the DNS request HTTP request and response related to the incident. Also evidence can be obtained from reviewing the source JavaScript code that prompted downloads and browser redirection. * Incident Report Sources : multiple customers complaints via emails to the yummyrecipesforme’s helpdesk, network protocol analyzer tcpdump log, website source code |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| * Limit the number if login attempts to prevent the deters of brute force attack and limits to how many times a user can attempt to log in before their account is suspended. * Improve password policy by adding MFA, 2FA, OTP and guidelines on how complex a password should be, how often users need to update passwords, whether passwords can be reused or not. |