# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| This report applies the TCP/IP model describing which protocols were used during the transmission, at the Internet layer IP data packets was used from the browser to access the website yummyrecipesform.com, during this process at the application layer DNS was used to resolve the ip address to the corresponding domain name on the internet. Once this was fulfilled in HTTP at the application layer was used to serve the web client with traffic to return the output of the URL. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| It was reported that customers complained to the helpdesk when executing th URL yummyrecipesform.com from their web browser that it prompts them to download the file. Once users opened the file it ran malicious javascript code causing what is suspected to be DNS spoofing where they impersonate and redirect data packets to greatrecipesforme.com. A disgruntld former employee managed to perform a brute force attack whom succeeded to authenticate and change the source code.  The incident was detected at line 13 of the Tcpdump log file indicating that the website was redirected to greatrecipesforme.com  **14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)** |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| If I was to recommend a security measure, I would advise to implement multi factor authentiation this would help in confirming and validating the identity of the users attempting to access the website. |