# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The HTTP protocol is involved when communicating with both yummyrecipesforme.com and greatrecipesforme.com in this incident |
|

|  |
| --- |
| **Section 2: Document the incident** |
| After receiving complaints from from customers that when they visiting the yummyrecipesforme.com website they are being prompted to update their browsers after which they are redirected to another website where the yummy recipes are displayed for free and their browsers subsequently become slow the IT department investigated incident, using a packet sniffing tool to capture the network traffic.  At 2:18p.m a security analyst attempts to reach yummyrecipiesforme.com, a DNS request successfully returns the IP address for the website’s server, and they are able to connect to the server. However, as soon as connection is established a lengthy communication occurs between client and the server, using HTTP. This is when we suspect that a malicious script on the server is downloaded on client machine.  At 2:20p.m the security analyst’s client makes another DNS request, this time the request is for IP address greatrecipesforme.com, the IP address is returned and the client is directed to the greatrecipesformewebsite.com  At 2:25p.m the security analyst’s client establishes a connection with the greatrecipesforme.com server and is served multiple web-pages over HTTP. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| In order to prevent future brute force attack, multi-factor authentication should be implemented when authorizing access to the web-server. This will ensure that only an authorized user with the correct login credentials can access the server. |