# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocols used in this attack include the DNS, and the HTTP. The user used a DNS protocol to probe for the IP add of the desired URL. The use also used a http protocol to connect to both legitimate and spoofed URLs. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Users legitimately used accessed the DNS server to probe for the IP address of the yummyreipesforme.com. the DNS server correctly returned the proper IP add for the desired URL. The connection successfully connected to the URL judging from the completed 3-way handshake. While connecting to the URL however, users were prompted to download a file which I think introduced a script to their browser. The script introduction initiated a new http request to a spoofed URL/website (greatrecipesforme .com) that was not the desired destination of the users. The script equally changed the http port of the host computer.  Since the website owner revealed that they were locked out of their admin account, it is suspected that the attackers might have gained access to the backend through brute force password compromise of any of the admins. Through this, I suspect they were able to introduce a file download and spoof script to manipulation traffic routing. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To prevent this incident from re-occurring, it is recommended that admins establish security procedures that overcome brute force attacks. This include Requiring strong passwords, enforcing two-factor authentication (2FA), monitoring login attempts, and limiting the number of login attempts.  Establishing a limited login attempts would effectively deter use of automated and persistent password compromise from attackers. It will also alert security analysts to failed or even possibly ongoing brute force attempts. |