# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The HTTP protocol has been involved in the incident. From the tcpdump logs, it can be concluded that a malware is being transported to the customer’s devices using the HTTP protocol when they’re trying to access the yummyrecipesforme.com website. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several users contacted the helpdesk regarding that the website was prompting them to update their browsers by downloading a file and their systems have been working slower since then.  The cyber analysts used a sandbox environment to test the website. When the analyst tried to access the website, he was asked to download a file to update the browser and then the website was being redirected from yummyrecipesforme.com to greatrecipesforme.com  The analyst then observed the source code and found out that a malicious file was being downloaded into the devices of the customers who tried to access the website and were being redirected because of the malicious code. The analysts think that the attacker had used simple brute force method to compromise the website and changed the source code. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| In order to tackle simple brute force attacks, one can use MFA i.e multi factor authentication which involves using several proofs like OTP’s, fingerprints, other passwords etc.. to make sure that any account can’t be breached easily and the verification ensures right people are able to access through the gateway. |