# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Communication between the host client and the web server was happening using the HTTP protocol. This is an unencrypted protocol which runs on port 80. | |
|

| **Section 2: Document the incident** |
| --- |
| From the log details, it is clear that the host host client “your.machine.33086” establishes a successful connection [Flag S] with the web server “yummyrecipesforme.com” through the DNS server. However log line 20 shows “your machine” making another DNS request for “greatrecipesforme.com” This indicates that the website source code must have been changed by a threat actor. This prompts another request to the DNS server to resolve to a different server on a different port containing possible malware [log line 22]. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| The following is recommended to prevent future brute force attacks.   1. Stronger password policies must be set up. These must ensure that user passwords are not shorter than 8 characters, must contain at least one numeric character, one special character and symbol. Maximum password attempts should be set to 5 after which access to the account is locked. |