# Security incident report

| Section 1: Identify the network protocol involved in the incident |
| --- |
| The network protocol involved in the incident is DNS and HTTP. The malicious file was transferred by the HTTP protocol. |

| Section 2: Document the incident |
| --- |
| At 14:18 the user request access to yummyrecipiesforme. A request is sent to the DNS server. The DNS server responds with the IP address. The user machine sends a SYN to the server. The recipes server sends back SYN ACK immediately. The user machine send an ACK to confirming to stablish connection. A data push starts from the user machine. The recipes server sends an ACK to the user machine. After 2 minutes the user machine requests a DNS request for a different domain greatrecipiesforme. This request is returned back with the IP address of the new source. After 5 minutes the new source website greatrecipiesforme starts the handshake and establishes connection with the user machine. |

| Section 3: Recommend one remediation for brute force attacks |
| --- |
| This incident could have occurred due to vulnerabilities in the password policy. The employees must be made aware of the impact of these type of incidents and make changes to password policies by making it stronger by not allowing previous password characters, having a min limit of characters, adding symbols and mandating uppercase and symbol characters to make brute force attack tougher. Also an added layer of security can be stablished by implementing MFA. The user can be authenticated by asking them to enter a |

code send to their email or phone which will be difficult to obtain by the threat actors.