Security incident report

Section 1: Identify the network protocol involved in the incident
This incident involves HTTP protocol.

Section 2: Document the incident
Customers want to access the client's website (yummyrecipesforme.com), but are rerouted to another webpage after downloading a malicious script stored in the website's code. The IT team received emails from customers after the incident slowed down their devices. It was found that a former employee was able to gain access to the source code of the client's website using a dictionary attack, easily infiltrating the system. The attacker then injected malicious javascript into the source code. A sandbox environment was created to assess the situation. At 2:18 PM, we attempted to access the client's website. Browser sent a DNS request for the website and was successful. After acknowledging and establishing a connection to the client's website, an HTTP GET request was automatically executed and we presume this is the malicious file being installed on the customer's device. After two minutes at 2:20PM, traffic is rerouted to the DNS server again, which sends back a new IP address to the requesting web browser and redirects the customer to the non-legitimate website greatrecipesforme.com.

Section 3: Recommend one remediation for brute force attacks
It is highly recommended that the client implements stronger password policies for the employees and the system, and is advised they do not use repeated passwords or ones that are similar to old passwords to reduce the risk of brute force attacks.