Security incident report

Section 1: Identify the network protocol involved in the incident
The incident occured in the afternoon [14:28] and the network protocol involved is the HTTP (Hypertext transfer Protocol) which is a Applucaton layer protocol in TCP/IP model

Section 2: Document the incident
The attacker gained the credential information (username, password) by using the brute force method. After gaining the login credentials, the attacker added a malicious javascript code that sends the customer to a different website (greatrecipesforme.com) from where the users can download the recipes of the owner(yummyrecipesforme.com) for free. The website owner tried logging into the web server but noticed they were locked out of their account. The users informed that they received a link to download before redirecting to the malicious website thus making their computers slow. By using the sandbox method, we determined that the password was still set to default. The attacker could guess the password and gained access to the website.

Section 3: Recommend one remediation for brute force attacks
To prevent the brute force attacks from happening in the future we can take the following measure: ● Frequently changing passwords ● Set a password policy that include a capital letter, a symbol, a number & must be 8 letters long

- 2FA
- Limit login attempts

These all measure can allow the organisation to maintain extra security to protect their business operation and protect their valuable assets

One security measure the team plans to implement to protect against brute force attacks is two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identification by confirming a one-time password (OTP) sent to either their email or phone. Once the user confirms their identity through their login credentials and the OTP, they will gain access to the system. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authorization.