# Security incident report: yummyrecipesforme.com Brute force incident

| **Section 1: Network protocol involved in the incident** | |
| --- | --- |
| The attacker utilized TCP, DNS and HTTP protocols in order to execute this attack. When the sandbox environment attempts to reach the yummyrecipesforme.com website, the malicious code instead causes the device to redirect the computer to the greatrecipesforme.com website, which is malicious. | |
|

| **Section 2: Document the incident** |
| --- |
| At 2:18 PM an attacker gained access to the dashboard of the yummyrecipesforme.com website by repeatedly guessing default passwords that they were familiar with due to their previous employment at the organization. Upon accessing the website, the attacker inserted malicious code which contained a download to malware that would modify a computer to cause it to access greatrecipesforme.com instead, a malicious website. After inserting the malicious code, the attacker then changed the admin password for the dashboard, preventing the website owner from accessing the dashboard. |

| **Section 3: Remediation for brute force attacks** |
| --- |
| Implementation of a strong password policy and multi-factor authentication is recommended to prevent this type of attack in the future. A strong password policy will help prevent attackers from guessing commonly used or default passwords, and ensure that passwords are changed regularly so previous employees are less likely to be able to use passwords that they are familiar with to gain access. Multi-Factor authentication would also help prevent this type of attack because even if the attacker correctly guessed the password, they would still require additional authentication before being able to access the system. |