# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The incident involved two primary network protocols: DNS (Domain Name System) and HTTP (Hypertext Transfer Protocol). DNS was utilized to resolve domain names to IP addresses, enabling the attacker to redirect users to a malicious website. HTTP was used to initiate requests for webpage access, download the malware, and redirect users to the fake website. These protocols were key in facilitating the unauthorized access, malware distribution, and content manipulation observed during the incident. | |
|

| **Section 2: Document the incident** |
| --- |
| The YummyRecipesForMe website experienced a security breach originating from a successful brute force attack on the administrative account, which still employed the default password. This granted the attacker unauthorized access to the admin panel, allowing them to manipulate the website's source code. A malicious JavaScript function was inserted, coercing visitors into downloading an executable file that altered their browser behavior. Subsequently, users were redirected to a counterfeit version of the website, where premium recipes were unlawfully made available for free. This event exposed sensitive customer data, compromised the website's integrity, and posed potential risks to users' devices. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To mitigate the risk of future brute force attacks, it is recommended to implement an account lockout mechanism. This preventive measure temporarily locks user accounts after a specified number of consecutive failed login attempts. Such an approach hampers attackers' ability to repeatedly guess passwords, significantly reducing the likelihood of a successful brute force attack. Alongside account lockout, automated alerts should be configured to notify administrators of lockout incidents, enabling timely investigation and appropriate response. By introducing this security measure, YummyRecipesForMe can bolster its defenses against brute force attacks without inconveniencing legitimate users, ultimately enhancing the overall security posture of the website. |