# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| 1. DNS (Domain Name System): The browser initiated a DNS request to resolve the IP address of the yummyrecipesforme.com URL from the DNS server. 2. HTTP (Hypertext Transfer Protocol): After obtaining the IP address from the DNS server, the browser initiated an HTTP request to access the yummyrecipesforme.com webpage. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Yummyrecipesforme.com, a website specializing in recipes and cookbooks, experienced a security breach orchestrated by a former disgruntled employee. The attacker utilized a brute force attack to gain unauthorized access to the website's admin panel. By repeatedly attempting known default passwords, the attacker successfully guessed the administrative account's password. Subsequently, they accessed the admin panel and tampered with the website's source code, embedding a malicious JavaScript function.  Upon embedding the malware, the attacker altered the administrative account's password, preventing legitimate access. Visitors to the compromised website were prompted to download a file purportedly containing free recipes. However, upon executing the file, users were redirected to a fraudulent website, greatrecipesforme.com, containing malware.  Multiple customer complaints regarding unexpected file downloads and decreased system performance prompted an investigation. Analysis revealed that upon accessing yummyrecipesforme.com, users were redirected to greatrecipesforme.com, facilitated by malicious JavaScript code embedded in the website's source.  Further investigation confirmed the compromise stemmed from a brute force attack due to the administrative account retaining the default password. Insufficient controls to prevent brute force attacks exacerbated the vulnerability. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Implement Account Lockout Policies: Enforce mechanisms that temporarily lockout user accounts after a specified number of unsuccessful login attempts. This proactive measure mitigates the effectiveness of brute force attacks by impeding attackers' ability to repeatedly guess passwords. Additionally, enforcing strong password policies and regular password rotation reduces the likelihood of successful brute force attacks. Regular security audits and updates to ensure default passwords are promptly changed further enhance the website's resilience against such attacks. |