# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocols involved in this incident were DNS and HTTP. DNS was used to resolve the IP addresses for both yummyrecipesforme.com and greatrecipesforme.com, while HTTP was used for web traffic between the browser and the web servers. The attacker manipulated the website's source code to redirect users from yummyrecipesforme.com to greatrecipesforme.com, which hosted the malicious content. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A disgruntled former employee executed a brute force attack on the administrative account of the website *yummyrecipesforme.com*. They repeatedly tried default passwords until gaining access to the admin panel. Once inside, they embedded a malicious JavaScript function that prompted visitors to download a malware-infected file. After downloading and running the file, users were redirected to a fake version of the website, *greatrecipesforme.com*, where the malware was hosted.  The attack occurred because the admin password was still set to the default, and there were no controls in place to prevent brute force attacks. The attack went unnoticed until several customers complained about unusual behavior, such as being asked to download files and experiencing slower computers.  Network logs confirmed the browser first made a DNS request for *yummyrecipesforme.com* and retrieved the correct IP address. After the website loaded, the malicious JavaScript triggered a second DNS request for *greatrecipesforme.com*, redirecting the user to the fake site, where the malware was further propagated. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To prevent future brute force attacks, the website should implement multi-factor authentication (MFA) for admin accounts.  Additionally, strong password policies should be enforced, including requiring non-default passwords and regular password updates.  Implementing account lockout mechanisms after several failed login attempts would also prevent brute force attacks from succeeding. |