# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| * Domain Name System – resolves the domain names to their corresponding IP addresses * Hypertext Transfer Protocol – used for communication between the client and the web server to load the webpage and initiate the malicious file download |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The web server for yummyrecipesforme.com was compromised by a former employee by executing a dictionary brute force attack and guessing the administrative account’s password and gaining access to the admin panel. The attacker modified the source code by embedding a malicious JavaScript function that prompts users to download an executable file, they also changed the admin’s password to lock them out of the system.  Once the malicious file was downloaded, the browsers were directed to the fake website greatrecipesforme.com. The file would initiate a DNS query to resolve the IP address of greatrecipesforme.com and send a HTTP request to load that malicious website.  This attack has compromised the customers’ systems, with potential for data theft, it has locked the administrator out and has caused reputation damage for the organization. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| In this case it would be important to have strong password policies to standardize good password practices as that was the main reason the admin account was accessed. This should be enforced with a password management system. In addition, they should implement multi-factor authentication to add layers to the security. |