# Brute Force Attack: Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| This is an application layer attack focusing on abusing HTTP and DNS requests to download malicious updates to the user’s browser and redirect them to a fake copy of yummyrecipesforme.com. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A disgruntled user of yummyrecipesforme.com executed a brute force attack on the administrative account of the web server. After obtaining the correct password, the attacker accessed the admin panel to change the website’s source code. A JavaScript function was added to the source code that prompted visitors to download and run a file when they visited the site. After downloading the file, users were redirected to a spoofed version of the website with the domain name greatrecipesforme.com. The attacker uploaded all of a seller’s paid recipes for free to this site, and users also stated that after running the downloaded file their computers began running more slowly.  I have simulated the customer’s actions in a sandbox (Virtual Machine) and confirmed that when visiting yummyrecipesforme.com the following occurs:   1. The browser requests a DNS resolution of the yummyrecipesforme.com URL. 2. The DNS replies with the correct IP address. 3. The browser initiates an HTTP request for the webpage. 4. The browser initiates the download of the malware. 5. The browser requests another DNS resolution for greatrecipesforme.com. 6. The DNS server responds with the new IP address. 7. The browser initiates an HTTP request to the new IP address. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| It was later discovered that the password to the admin account was still set to the default password. The best solution to protect against future brute force attacks is to implement secure password policies for this account and the organization as a whole. Specific password policies to implement for this account include:   1. Implement techniques to block large amounts of failed password attempts (ex: blocking specific IPs after too many attempts) 2. Update the password requirements to be a certain length and include different types of characters instead of just letters 3. Require recurring password changes 4. Require 2-Factor or Multi-Factor Authentication (2FA or MFA) |