# Security incident report

| Section 1: Identify the network protocol involved in the incident |
| --- |
| The protocol involved with the incident was the HTTP protocol since the issue was with accessing the web server. When running tcpdump, the corresponding log file showed the usage of the HTTP protocol used for establishing a connection with the site. The malicious file is observed being transported to the users' computers using the HTTP protocol. |

| Section 2: Document the incident |
| --- |
| A brute force attack was used to gain access to the web host. Several hours after the attack, multiple customers emailed helpdesk about the company's website prompting them to download a file to access free recipes. The website owner tried to log in to the admin panel but was unable to.<br><br>To address this incident, the security team created a sandbox environment to observe the suspicious website behavior using network protocol analyser tcpdump. They downloaded the executable file that was prompted and ran it to observe the effect.<br><br>The log shows that at first, a DNS resolution request was sent to the DNS server using port 52444 to get the IP for yummyrecipesforme.com. The DNS server responded with the IP address of the destination URL (203.0.113.22). A HTTP request is then made using TCP from the machine to the acquired IP address for the webpage in which the server responded normally. The log with the code HTTP: GET / HTTP/1.1 shows the browser was requesting data from the website with HTTP: GET which could be the download request for the malicious file. After this the traffic was routed from the source computer to the DNS server to another DNS resolution request, this time for the domain greatrecipesforme.com. The machine sent a HTTP request to the spoof website (192.0.2.172) in which the website acknowledged the request and established a connection with the machine. |

A senior analyst confirms that the website was compromised. They checked the source code for the website and noticed that javascript coffee had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatreicpesforme.com.

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To prevent future brute force attack, a stronger password policy should be in place. The policy will require stronger passwords and enforce 2FA. The login attempts will also be monitored so it is harder to keep guessing the password. It will require the passwords to be changed often and disallow previous passwords from being used. CAPTCHA could also be used to prevent machine automation of password guessing. |