# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| **Network Protocols Involved**   * **DNS (Domain Name System):** Used to resolve the domain name *yummyrecipesforme.com* to its corresponding IP address. * **TCP (Transmission Control Protocol):** Established a reliable connection between the client and the web server through the three-way handshake. * **HTTP (Hypertext Transfer Protocol):** Used to deliver the website content. In this case, it was exploited for redirection and malware delivery. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| This incident started with a user sending a DNS request for the website yummyrecipesforme.com over HTTP. After DNS resolution, the TCP three-way handshake was completed, and the web server began delivering the page content. However, investigation revealed that the source code of the website had been modified by an attacker. The injected code caused the site to redirect users from yummyrecipesforme.com to greatrecipesforme.com.  When redirected, a new TCP session was established with greatrecipesforme.com, and the site immediately pushed a malware download to the user’s device. Once the redirection completed, the malicious payload executed, and the user’s system was infected. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Brute force attacks often succeed when weak or default passwords are used, like in this incident. To reduce this risk, administrators should always change default credentials and use strong, complex passwords. It’s also recommended to enable multi-factor authentication (MFA) and set account lockout policies after several failed login attempts. |