

Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocols involved in the incident are the Domain Name System (DNS), which resolves domain names to IP addresses, and the Hypertext Transfer Protocol (HTTP), which facilitates communication between web clients and servers.

Section 2: Document the incident

Yummyrecipesforme.com experienced a security breach where a former employee executed a brute force attack to access the admin panel. The attacker injected malicious JavaScript into the website's source code, prompting visitors to download a file that redirected them to a fake website containing malware. Multiple customers reported slow performance on their personal computers after downloading the file.

Section 3: Recommend one remediation for brute force attacks

Implement robust password policies, including complex passwords and regular changes, to deter brute force attacks. Enable account lockout mechanisms after several failed login attempts and consider implementing multi-factor authentication (MFA) for enhanced security.