# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The incident revolved around a convergence of critical network protocols, including DNS (Domain Name System), IP addressing, and HTTP (Hypertext Transfer Protocol). |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A disgruntled baker executed a brute force attack on yummyrecipesforme.com, a recipe-selling website. After successfully guessing the admin password, they gained access to the site's admin panel and manipulated the source code. Within the code, they embedded a script that coerced site visitors into downloading a file, subsequently redirecting them to a counterfeit version of the site featuring free recipes. Multiple customers who fell victim to this ploy reported sluggish performance on their personal computers following the download. Unable to access the admin panel, the website owner sought assistance from the hosting provider, prompting a cybersecurity team, including the analyst, to establish a sandbox environment for investigation. Utilizing a network protocol analyzer, the team observed the website initiating file downloads, ultimately leading visitors to the counterfeit site offering complimentary recipes. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To enhance security and deter brute force attacks, implementing salting and hashing techniques is recommended. These measures bolster defense by making it significantly more challenging for threat actors to breach the admin panel. The complexity introduced by hashing and salting processes renders brute force attempts considerably more time-consuming and resource-intensive, acting as a formidable deterrent against unauthorized access. |