# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| * The protocol used in the incident are DNS (Domain Name System) and HTTP (Hyper Text Transfer Protocol). * Hypertext Transfer Protocol (HTTP). HTTP is an application layer communication protocol. This allows the browser and the web server to communicate with one another. It uses port 80 and its considered insecure. * Domain Name System (DNS). DNS is an application layer protocol that translates, or maps, host names to IP addresses. DNS normally used UDP on port 53. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The attacker used brute force to gain access to the web host. They accessed the admin portal and changed the websites source code. They embedded a JavaScript function in the source code that prompted visitors to download and run a file upon visiting the website. After running the downloaded file, the customers are redirected to a fake version of the website where the seller’s recipes are now available for free. After receiving the call of several customers that the website had prompted to download a file and after running the file, the website address changed from yummyrecipesforme.com to and their personal computer began running slowly. The website owner tries to login in the admin portal, but the owner has been locked out. After analyzing the website, the senior analyst confirmed that the website has been compromised. They notice that JavaScript code 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 greatrecipesforme.com. The cybersecurity team reports that the web server was impacted by a brute force attack. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| The most common remediation for brute force attacks is mentioned below:   1. Salting and Hashing – Hashing converts the information into unique value. It is not possible to decrypt the original text again. Salting adds random characters to hashed passwords. This increases the complexity of hash values and making them more secure. 2. Multi Factor Authentication (MFA): This security measure which requires a user to verify its identity in two or more ways to access the system or network. 3. CAPTCHA: This helps preventing software from trying to brute force a password 4. Password Policies: Password policies to standardize good password practices throughout. |