# Security incident report

Made By: NIDA AZAM

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| ->DNS (UPD port 53): Used to resolve domain names into ip addresses.  ->HTTP (TCP port 80): Used for transferring website content and malicious files. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A former employee carried out a brute force attack on the website’s administrative account. Because the password was weak and still set to the default, the attacker was able to gain access. After logging in as an administrator, the attacker modified the website’s source code and embedded a malicious JavaScript file.  When users visited **yummyrecipesforme.com**, the script prompted them to download an executable file. Once downloaded and executed, the malware redirected the users’ browsers to a fake site, **greatrecipesforme.com**, which contained additional malicious content.  This incident was confirmed through tcpdump logs, customer reports to the helpdesk, and analysis of the modified website source code. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| So my one remediation for brute force attack is to use a strong password with combination of uppercase letters, lowercase letters, special characters , numbers etc. Additionally implementing a two factor authentication (MFA) will secure administrative accounts. |