# Security incident report

| Section 1: Identify the network protocol involved in the incident |
| --- |
| Protocol involved is the HTTP Protocol. Shown in the tcpdump when accessing the yummyrecipesforme.com website an HTTP gets requested by HTTP: GET / HTTP/1.1. Meaning that the request HTTP is probably the malicious file downloading. So most likely being transported by this HTTP GET. The malicious file is a redirection to a spoof site called greatrecipesforme.com |

| Section 2: Document the incident |
| --- |
| Customers contacted us and said visitors of the website yummyrecipesforme.com experienced a security issue when loading the main webpage. Reading the tcpdump it showed that HTTP protocol GET request was issued, and it lead to a spoof website. A previous employee decided to lure users to a fake website with malware called greatrecipesforme.com. The way the malicious user infected the users by embedding a javascript function in the source code that prompted visitors to download and run a file upon visiting yummyrecipesforme.com and the file would redirect users to the spoof website. Also from this file the users reported that their computers became slower. Couldn't log into the admin panel so they changed the password for that to. Cybersecurity team reported that the web server was breached by a brute force attack. The admin password was set to the default password so the malicious actor was able to access it easily, and 0 controls to prevent a brute force attack. |

| Section 3: Recommend one remediation for brute force attacks |
| --- |
| There's multiple ways to prevent a bruce force attack and one way is limiting the number of login attempts. This will cause the brute force attack to be minimized to 4 attempts instead of unlimited so it becomes near impossible to brute your way to acquiring the password. |