# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocol involved in the incident is HTTP, included in the application layer, of the TCP/IP model. | |
|

| **Section 2: Document the incident** |
| --- |
| The incident occurred today at 14:18.  The IT team became aware of the incident through multiple customer reports, signaling that the website prompted them to download a file. We created a sandbox environment to analyze network traffic using tcpdump. The logs revealed that the browser used the DNS protocol to receive the IP address of yummyrecipesforme.com. After the standard HTTP request for the webpage, the logs indicate that a data push was acknowledged, meaning the download of the malware, followed by a lot of traffic on port 80, the port destined for HTTP.  After checking the source code of the website, we found out that JavaScript code has been added. The website owner was also unable to access the admin panel. We think a brute force attack took place, with the malicious actor gaining control to admin permissions because the admin password was still set to default. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| One recommendation for mitigating future brute force attacks is to require strong passwords, by updating password policies, so that attackers won’t be able to access sensitive data so easily. Nevertheless, the more security resolutions applied, the better for the safety of the employees and customers. |