# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocols involved in this incident are HTTP and DNS. Through DNS, the attacker was able to redirect users to a malicious website, and through HTTP, malicious files were downloaded along with the access request and redirected to a fake website. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The first discovery came after several customers contacted the website help desk. Customers were prompted to download and run a file when they visited the website. After that the computer runs slowly. Therefore, cybersecurity analysts use a sandbox environment and tcpdump to analyze websites. The Traffic-log attachment is an analysis of traffic confirmed through tcpdump. Additionally, the fact that the administrator account was locked tells us that the website suffered a security breach due to a brute force attack. This allows the attacker to manipulate the website's source code and inject malicious JavaScript. This incident exposed sensitive customer data and compromised the integrity of the website. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Website may needs to use one of a variety of security measures to mitigate the risk of future brute force attacks. The first is to use an account lockout mechanism. This temporarily locks the user account after a specified number of consecutive login failures. Second is to implement 2FA authentication. This allows authentication through one-time confirmation. They are usually sent via email, phone, or app. By adopting these security measures, website can strengthen its defenses against attacks without inconveniencing legitimate users. |