# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocols involved in this incident were DNS and HTTP for executing malicious scripts on the client slide. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A former employee successfully executed a brute-force attack to gain administrative access to the website and has changed the source code and change the password to the administrative account as well as redirecting the customers to a fake website that contains malware. In the traffic log, it shows the HTTP GET requests to the legitimate site later changing to the fake site showing the redirection to the malicious site. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To prevent future brute force attacks, the organization can enforce stronger password policies with more complex requirements or can implement multi-factor authentication to verify if it is the authorized user trying to gain access by providing two or more verification factors to gain access making it harder for attackers to access even if they have compromised passwords. |