# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Protocols used - TCP/UDP, HTTP | |
|

| **Section 2: Document the incident** |
| --- |
| A customer shares an email regarding their experience with the company’s website stating that while accessing the website they were prompted with a download of a file. Upon download, the user is redirected to a fake website which is used to inject malware into the user's system.  The threat actor used Brute force attack to gain access to the web host of the original site. They guessed the password using several attempts and after successfully gaining the access, they modified the original javascript code such that a file containing an external script is downloaded on the user's machine which will be used to redirect them to the fake website. Additionally, the threat actor changed the credentials for the web host so that the authentic owner cannot gain access. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Secure password policies can be implemented to ensure safety against Brute force attacks. |