# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| In this incident user used http request that works on application layer, which is used for web page requests to web servers. When accessing the website, tcpdump logs confirmed the usage of the HTTP protocol. Furthermore, the malicious file was transported to users' computers via HTTP at the application layer, highlighting the role of HTTP in the incident. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Because of the disgrutled employee the organization faced this consequence and few mistakes was made by the organization as well. The bakers tried to brute force the webpage of yummyrecipe.com and it got the success because of the weak password policies and once he got the admin panel he changed the password so that the real administrator can’t get in and then the threat actor also did the changes in the web source page that leads the customers in downloading malicious software on the other websites that is greatrecipes.com. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Brute force attacks can be prevented by a lot of measures one of them could be the strong password policies. Strong password policies include different rules like length should be 8 characters must include speacial characters and numbers. Moreover, password policies does include the regular password changing that can prevent these type of attacks. |