# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| HTTP communication on port 80, the application layer protocol used for web traffic, was compromised in this incident. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers reported that when going to our website, they were prompted to download a file. Upon installing the file, they were redirected to a different website and their computers became slow.  A malicious actor, likely a disgruntled employee gained access to the web server using a brute force attack that used login credentials for an administrator account. They were able to retrieve intellectual property (recipes) as well as modify the source code. Visitors to the website are prompted to click to on a link to download a file. This file is malware and contains a script that would redirect the user’s browser to a spoofed website that looks like yummyrecipesforme.com. The recipes are available for free on this site.  We were able to recreate the issue in a sandbox environment. Upon navigating to yummyrecipesforme.com we received a prompt to download the file containing malware. Installing the file triggered the browser to query DNS for another domain name: greatrecipesforme.com. The browser navigated to this site which is a spoofed copy of yummyrecipesforme.com but with all recipes available for free. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| One recommendation to help prevent brute force attacks is to update the login policy to limit the number of login attempts. The team can discuss an appropriate number of failed login attempts before blocking access to the account. We can also determine an appropriate policy for time to wait before re-enabling the account. |