

Security incident report

Scenario Summary: A former employee gained unauthorized access to the website's admin panel through a brute force attack on the default password. They modified the site's source code to deliver malware that redirected users to a fraudulent domain. Customer complaints and tcpdump analysis confirmed the compromise. The incident highlights weak authentication controls and the need for stronger brute force protections.

Prepared By: Dhyanam

Role: Cyber Security Student (Training)

Year: 2025

Section 1: Identify the network protocol involved in the incident

The network protocol involved in this incident is HTTP (Hyper Text Transfer Protocol) using which the user established connection with yummyrecipesforme.com. The problem occurred when the HTTP Get request was made using the HTTP 1.1 version when the website had prompted the user to download the file to access free recipes.

Section 2: Document the incident

This incident was reported by the customers when they tried to access the website, and they were asked to download a file which took them to a fake website called greatrecipesforme.com. This website contained malware which affected the customer's devices and made them slow. The website owner tries to login to the admin panel but is unable to, so they reach out to the website hosting provider.

Later upon investigating the incident in a sandbox environment, the security team came to know that there was a brute force attack carried on the website which allowed the hacker to get access to the admin panel and embed a javascript code into the source code of the website. This took the visitors to the fake website (greatrecipesforme.com) where the malware was downloaded in the user's system.

Section 3: Recommend one remediation for brute force attacks

The whole problem occurred due to a weak password which was easily guessed by the hacker which gave the hacker access to the website's source code.

We need to have strong password policies in place for the organization. Policies can include guidelines on how complex a password should be, how often users need to update passwords, whether passwords can be reused or not, and if there are limits to how many times a user can attempt to log in before their account is suspended. CAPTCHA and reCAPTCHA should also be used to tell computers and humans apart. This reduces the chances of brute force attack carried out by a machine. Multi Factor Authentication (MFA) is a security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password (OTP) sent to a phone number or email. 2FA is similar to MFA, except it uses only two forms of verification. By this way hackers would not get access to the system just on the basis of password there will be extra steps to be carried out in addition to password to get the access.