# Brute Force Attack: Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| This is an application layer attack focusing on abusing HTTP and DNS requests to download malicious updates to the user’s browser and redirect them to a fake copy of yummyrecipesforme.com. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A disgruntled user of yummyrecipesforme.com carried out a brute force attack to break into the web server’s admin account. After successfully guessing the password, the attacker accessed the admin panel and modified the website’s source code. They added a JavaScript function that made visitors download a file when they accessed the site. After downloading the file, users were redirected to a fake version of the website at greatrecipesforme.com. The attacker also uploaded a seller’s paid recipes for free on this fake site. Additionally, users reported their computers slowed down after running the downloaded file.  A cybersecurity analyst tested this scenario in a virtual machine and confirmed the following sequence of events when visiting yummyrecipesforme.com:  1. The browser requests the DNS resolution for yummyrecipesforme.com.  2. The DNS provides the correct IP address.  3. The browser makes an HTTP request for the site.  4. The browser begins downloading malware.  5. The browser requests a DNS resolution for greatrecipesforme.com.  6. The DNS replies with the new IP address.  7. The browser sends an HTTP request to the fake site’s IP address. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| It was later found that the admin account still had the default password, making it vulnerable to brute force attacks. To prevent this type of attack in the future, secure password policies should be enforced for both this account and the organization. Key policies include:  1. Blocking multiple failed login attempts (e.g., locking out specific IPs after too many attempts).  2. Setting stronger password requirements, like longer passwords with a mix of characters, not just letters.  3. Enforcing regular password changes.  4. Implementing 2-Factor or Multi-Factor Authentication (2FA or MFA).  One key focus is limiting failed login attempts. In a brute force attack, the attacker tries many passwords from a list until one works. Since the admin account didn't have protections in place to block repeated failed attempts, the attacker was able to guess the password without restrictions. |