

# Security incident report

## Section 1: Identify the network protocol involved in the incident

DNS Resolution: The browser requested DNS resolution for YummyRecipesForMe.com and later for GreatRecipesForMe.com.  
HTTP Requests: The browser initiated HTTP requests for webpage access, as well as for the download of the malware.

## Section 2: Document the incident

YummyRecipesForMe.com experienced a security breach orchestrated by a disgruntled baker who executed a brute force attack to gain unauthorized access to the website's admin panel. The attacker successfully guessed the default administrative password, allowing them to infiltrate the system. Subsequently, they manipulated the website's source code, embedding a malicious JavaScript function. This function prompted visitors to download and execute a file that redirected them to a fraudulent website, GreatRecipesForMe.com, where the company's premium recipes were made available for free.

## Section 3: Recommend one remediation for brute force attacks

The security incident at YummyRecipesForMe.com resulted from a successful brute force attack, leading to unauthorized access and the compromise of the website's integrity. To prevent such incidents in the future, we suggest the following:

1. Enforce complex password requirements, ensuring that default passwords are changed immediately upon deployment.
2. Deploy security mechanisms, such as account lockouts or rate limiting, to mitigate the risk of brute force attacks.
3. Conduct regular security audits to identify and address vulnerabilities before they can be exploited.

