# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| IP = INternet Protocol and HTTP | |
|

| **Section 2: Document the incident** |
| --- |
| Um ataque de força bruta resultou na obtenção da senha do administrador e no comprometimento do site. O atacante obteve acesso ao servidor e alterou a senha do administrador. Além disso, ele inseriu um código malicioso em javascript que direciona os usuários ao site greatrecipesforme.com onde compitador do usuário é infectado por um outro código malicioso, tornando as máquinas dos usuários lentas. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| * Alteração do nome do usuário do Admnistrador por um mais forte; * Desabilitar uso de senhas padrões de administradores; * Habilitar troca periódica de senhas dos usuários e inclusive administradores; * Criação de senhas mais fortes de usuários administradores; * Usar autenticação 2FA (OTP) para acesso a área administrativa; * Backup regular do site a fim de impedir situações assim. |