Uma das formas para bloquear este ataque é por meio de ferramentas de inteligência de ameaça, normalmente é usado o *Web Application Firewall* (WAF), segundo a OWASP (2016), um WAF funciona como um firewall para aplicativos HTTP, ele aplica um conjunto de regras na comunicação com o site, ou seja, é realizado uma análise nas solicitações de GET e POST enviados por HTTP ou HTTPS e aplica regras configuradas para detectar e filtrar o tráfego malicioso da Web, e assim bloqueando a comunicação caso seja detectado que o pacote é malicioso.

Também é possível utilizar biblioteca de *footprint*, seria um modo de combinação de dados que não podem ser duplicados em outro lugar. Usando essas bibliotecas é possível verificar as semelhanças entre um usuário e grande fatias de tráfego, podendo criar padrões para que seja bloqueado caso tenha suspeita que não seja o usuário.