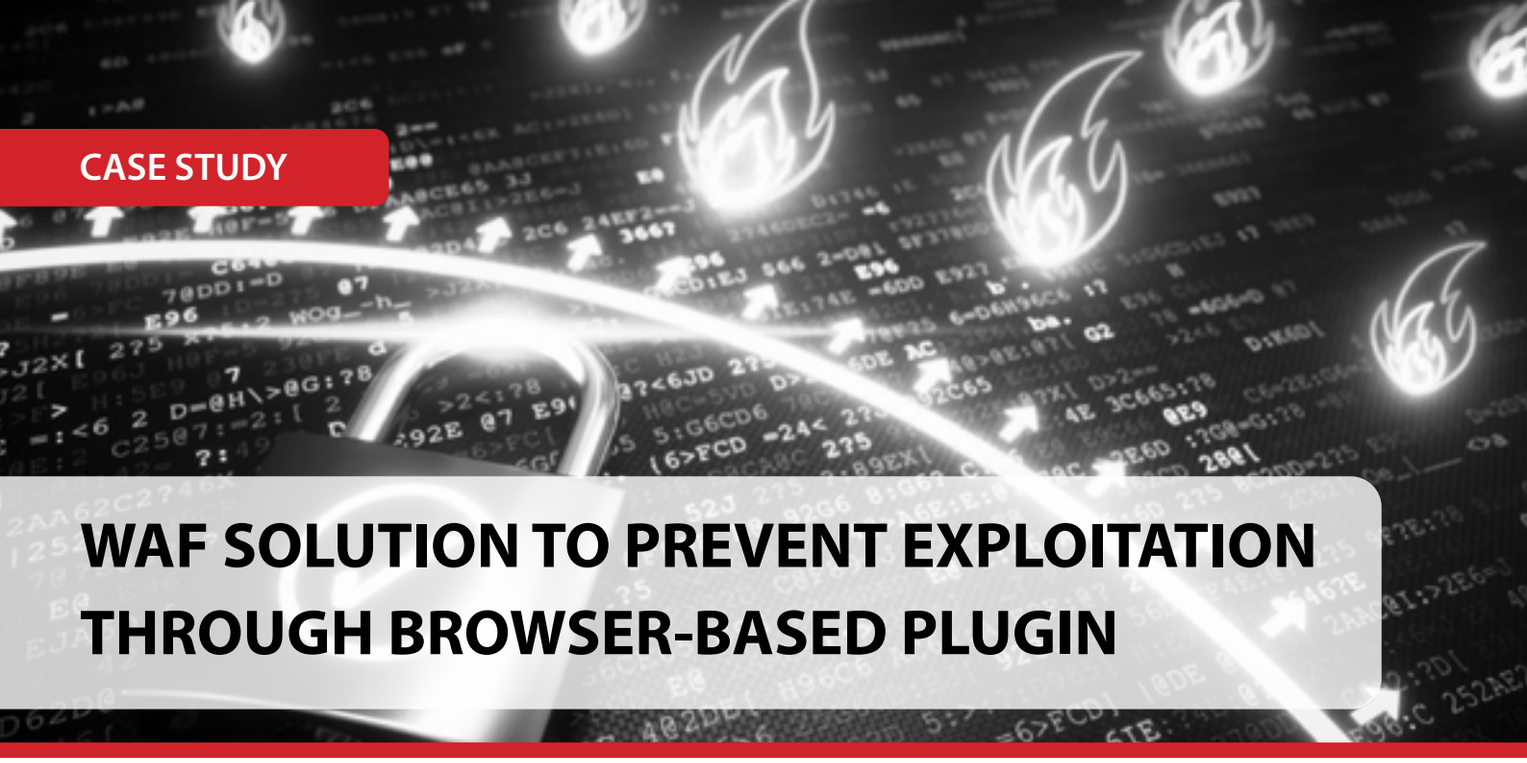

CASE STUDY

WAF SOLUTION TO PREVENT EXPLOITATION THROUGH BROWSER-BASED PLUGIN

ABSTRACT

- It is one of the organizations which has web-based forms on their website for users to input the data for registration and sign up. Application is designed to enrol the users and provides an appointment scheduling platform wherein the Applicant logs in to their web portal and book an appointment for specific use case.

KEY CHALLENGES

- The problem statement reported by the customer illustrates that some malicious users were performing dummy registrations and booking dummy appointments constantly which is impacting the business use case as genuine users are not able to get the online benefit.
  - Initially, we started recording such IP addresses from Application database and getting them immediately blocked at WAF level, but then malicious users started using different IP address for every such dummy registration.
  - Further we restricted the Application access to specific countries but again the malicious users started initiating the traffic from allowed countries for dummy registration.
  - As a next step, we implemented rate limiting rules to block an IP address if more than X number of requests comes in Y minutes then block it for Z minutes or throw a captcha page. But then the malicious users started to change the IP so frequently that it never breached the set threshold.
  - As this issue was impacting the organization as it as a brand, revenue, and financial damage, it required a robust solution which can defend against such exploitation attempts at the perimeter level before reaching the Application server. With this it also required a solution which is scalable and highly available all the time.

STRATEGY & RECOMMENDED SOLUTION

- To get a success, we strategize to enable Advance logging at WAF level and understand the malicious traffic pattern. With this, we were successfully able to capture below details.
  - Here, attacker was using a Tamper Monkey script which was a chrome browser-based plugin. This is an automation tool which uses random user details and fill up the web forms continuously. With the help of this tool, attacker was performing dummy registrations and booking dummy appointments.
  - We have analysed that it was using xyz.html file in multiple POST request and all the malicious request were performed using HTTP POST Method.
  - Further analysis illustrated that the POST request was using a different content-type as “text/plain;charset=UTF-8” compared to standard content-type “application/x-www-form-urlencoded”
  - To defend this attack, we built a robust custom WAF policy in reference to above captured statistics and initially deployed in learning mode for analysis and then finally moved it to block mode to start blocking such malicious patterns.

RESULTS

- The custom WAF policy was built, simulated by our Security experts, and was activated in the production. It was concluded that all such bad traffic was blocked successfully, and genuine users were able to signup and book the appointments. This helped the customer to retain the brand reputation with online business.

INDUSFACE™