activereach®

WAF TESTING SERVICES

activereach's Web Application Firewall (WAF) testing service challenges your security resilience to the OWASP Top 10 - the Open Web Application Security Project's most critical application security risks – and more.

WHY TEST YOUR WEB APPLICATION FIREWALL?

Web applications, including consumer-facing applications and enterprise apps, play a vital role in day-to-day business operations. Web apps have grown from just a few business applications to a multitude of backend web apps, SaaS apps and other cloud-delivered solutions.

Many web apps process sensitive data such as user, PII and financial information, which means they are frequently targeted by cybercriminals. As web apps become increasingly complex, the range of exploitable vulnerabilities is rising. Furthermore, the number and diversity of threats continues to increase, from advanced malware to web-specific application-layer attacks, as well as distributed denial of service (DDoS) attacks.

Organizations rely on WAF technology for protecting their web apps. These days, it is very easy for cybercriminals to locate all manner of automated application attack tools online. A notorious example is the infamous Equifax breach that was caused by an application vulnerability (Apache Struts) in one of its websites - affecting the PII of over 140 million consumers.

WEB APPLICATION VULNERABILITIES

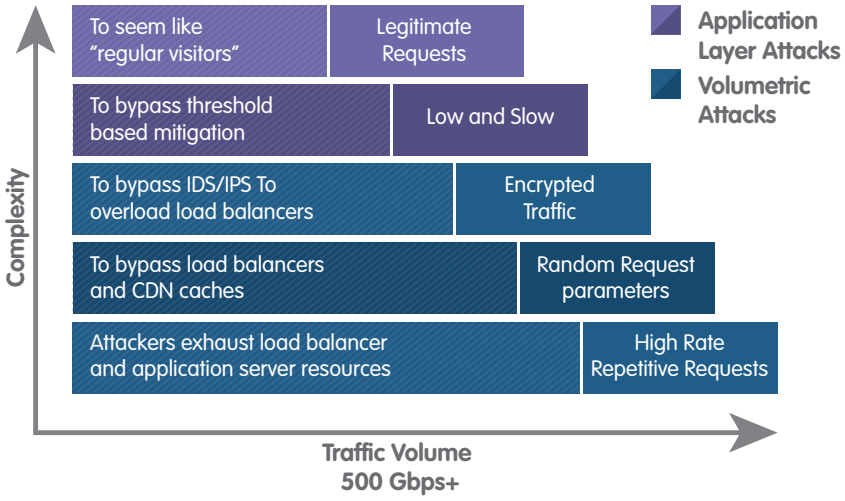
By using the same techniques utilised by genuine attackers, our WAF testing services help to identify vulnerabilities including:

- Injection flaws
- Authentication weaknesses
- Poor session management
- Broken access controls
- Security misconfigurations
- Database interaction errors
- Input validation problems
- Flaws in application logic

ACTIVEDEFENCE WAF TESTING METHODOLOGY

The activeDEFENCE WAF Testing platform utilises a globally managed legitimate botnet that is capable of generating an extensive range of attack types. These can range from Layer 7 application attacks to large multi-gigabit DDoS attacks that can scale up to in excess of 500Gbps. The Botnet does not use anonymous infected computers, but instead a global testing network using dedicated co-located and cloud-based servers to generate the traffic.

These tests mimic user behaviour and often take advantage of web-based encryption (i.e. SSL), which can hide the attack from mitigation systems and services. The difficulty here is ensuring that WAF/mitigation systems can distinguish illegitimate traffic from legitimate traffic and minimise or eliminate false-positives. Aggressive mitigation can impact legitimate users and a test can help enumerate the risks or poor customer experience.



Please access our online DDoS attack dictionary: www.activereach.net/support/ddos-dict

With activereach's WAF attack test, you can check if your WAF configuration, implementation and features are able to block payloads (e.g. XSS or SQL Injection) before they get anywhere near your web applications.

ATTACK VECTOR SIMULATIONS

Layer 7 (Lower volume, higher connections, low and slow, application attacks) that activereach can simulate include:

- BroBot
- DNS ANY Query
- DNS Reflection Attack
- Dynamic HTTP Flood
- Extreme Bot Attack
- HTTP/s Flood with Browser Enumeration
- HTTP GET Flood/HTTP Flooders
- HTTPS Flood
- PHP Hash Collision
- Pyloris
- RefRef
- RUDY
- SlowLoris
- Slow Post
- Tor's Hammer

At the end of each WAF attack simulation, or other simulation vector, a Risk Score is provided, indicating the organization's exposure, along with other KPI metrics and actionable guidelines to fine-tune controls and close security gaps.

THE THREAT OF APPLICATION ATTACKS

An application attack directly targets a service or application at layer 7, the end user level. Huge problems can be caused with just one dedicated attack machine, and because attackers can get away with using low traffic rates, they can be difficult to detect and neutralise. Over the last couple of years this form of attack has become more and more commonplace.

HTTP GET attacks. The classic attack of this type is the HTTP (Hypertext Transfer Protocol) GET attack. A web server receives an HTTP GET command from a browser to request some kind of information – perhaps an image, some text, or the result of a database query.

An attacker simply uses a sufficient volume of HTTP GET requests – usually asking for resource-heavy information such as database queries. Like a protocol attack, the volume of inbound (request) traffic is low, but the target server can be overwhelmed very quickly. Unlike a protocol attack, the traffic looks legitimate and sophisticated techniques are required to distinguish between a user browsing the site, and a bot making spurious and damaging requests.

OWASP API SECURITY TOP 10

Our WAF attack simulation service helps defend against the most critical application security risks.

API1:2019	Broken Object Level Authorization	APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object level authorization checks should be considered in every function that accesses a data source using an input from the user.
API2:2019	Broken Authentication	Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising system's ability to identify the client/user, compromises API security overall.
API3:2019	Excessive Data Exposure	Looking forward to generic implementations, developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user.
API4:2019	Lack of Resources & Rate Limiting	Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force.
API5:2019	Broken Function Level Authorization	Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers gain access to other users' resources and/or administrative functions.
API6:2019	Mass Assignment	Binding client provided data (e.g., JSON) to data models, without proper properties filtering based on a whitelist, usually lead to Mass Assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads, allows attackers to modify object properties they are not supposed to.
API7:2019	Security Misconfiguration	Security misconfiguration is commonly a result of unsecure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information.
API8:2019	Injection	Injection flaws, such as SQL, NoSQL, Command Injection, etc. occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
API9:2019	Improper Assets Management	APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints.
API10:2019	Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems to tamper with, extract, or destroy data. Most breach studies demonstrate the time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Let Us Help You Get Ready - Call: 0845 625 9025 or Email: contactus@activereach.net

About activereach

activereach® is a leading technology integrator providing bespoke IT solutions and professional services to customers in the areas of Security and Connectivity. Our independent consultative approach helps organizations maximise business value from their technology investments, providing a platform for businesses to grow, reinvent and transform.

Working in partnership with many of the world's leading technology vendors and software providers, we offer the most innovative hosted, on-premise and cloud based services. Our consultancy, technology and services have transformed hundreds of businesses across the UK, Europe & Middle East – ranging from FTSE 500 enterprises to corporates and SMEs. Operating across our activeNETWORKS™ and activeDEFENCE™ technology divisions, activereach is headquartered near London, UK.

activereach Ltd.
4 Cliveden Office Village, Lancaster Road, High Wycombe, Bucks HP12 3YZ
Tel: 0845 625 9025 | Email: contactus@activereach.net | Web: www. activereach.net

Ref:WTO2019.V1