Mitigating OWASP Automated Threats

COMBAT CREDENTIAL STUFFING WITH WAF AND THREAT INTELLIGENCE

Account takeovers are a financial burden and reputation risk!

63%
of data breaches involve stolen or weak credentials[1]

$8B
annual loss from account takeover by 2018[2]

95%
of breaches are financially motivated[3]

CREDENTIAL STUFFING
Attack Kill Chain

Capabilities Required to Combat Credential Stuffing

Threat Intelligence: Bad Bots, CAPTCHA, Bad IPs, Anonymous Proxies, TOR networks

Web App Firewall: Application Profiles, Correlated Attack Validation, Velocity Checks

With millions of stolen credentials circulating on the dark net, a 1% success rate can mean tens of thousands of compromised accounts. Fight back.

Learn More | Mitigating OWASP Top-20 Automated Threats

IMPERVA®

1. 2016 Verizon DBIR
2. Javelin Data Breach Fraud Impact Report
3. 2016 Verizon DBIR
4. World's Largest Data Breaches