

Web Application Incident Handling Toolkit

Listed below are certain tools that can be used by the incident handler to handle web application security incidents.

Category	Tools
Web Application Firewalls	<ul style="list-style-type: none">▪ dotDefender (http://www.applicure.com)▪ AppTrana WAF (https://www.indusface.com)▪ FortiWeb (https://www.fortinet.com)▪ SP//WAF (https://www.stackpath.com)▪ F5 Advanced WAF (https://www.f5.com)▪ Barracuda Web Application Firewall (https://www.barracuda.com)
SIEM Tools	<ul style="list-style-type: none">▪ ArcSight Enterprise Security Manager (ESM) (https://www.microfocus.com)▪ AlienVault OSSIM (https://cybersecurity.att.com)▪ IBM Security Qradar SIEM (https://www.ibm.com)▪ Logpoint SIEM (https://www.logpoint.com)▪ FortiSIEM (https://www.fortinet.com)▪ Exabeam Fusion SIEM (https://www.exabeam.com)
Tools for Detecting Web Application Security Incidents	<ul style="list-style-type: none">▪ IllusionBLACK (https://www.smokescreen.io)▪ Alert Logic MDR (https://www.alertlogic.com)
Application Whitelisting/Blacklisting Tools	<ul style="list-style-type: none">▪ ManageEngine Application Control Plus (https://www.manageengine.com)▪ ShadowNet (https://riskanalytics.com)▪ Cisco Umbrella (https://umbrella.cisco.com)▪ Delinea Server Suite (https://delinea.com)▪ McAfee Application Control (https://www.mcafee.com)▪ NordVPN (https://nordvpn.com)
Web Content Filtering Tools	<ul style="list-style-type: none">▪ BrowseControl (https://www.currentware.com)▪ OpenDNS (https://www.opendns.com)▪ inCompass (https://incompass.netstar-inc.com)▪ WebTitan (https://www.webtitan.com)▪ Smoothwall (https://www.smoothwall.com)▪ NetSentron (https://www.netsentron.com)
Web Proxy Tools	<ul style="list-style-type: none">▪ Proxy Switcher (https://www.proxyswitcher.com)▪ IPRoyal (https://iproyal.com)

	<ul style="list-style-type: none"> ▪ CyberGhost VPN (https://www.cyberghostvpn.com) ▪ Tor (https://www.torproject.org) ▪ Burp Suite (https://www.portswigger.net) ▪ Proxifier (https://www.proxifier.com)
Web Server Content Analyzers	<ul style="list-style-type: none"> ▪ ClamAV (https://www.clamav.net) ▪ HTTP Debugger (https://www.httpdebugger.com)
Web Server Content Analysis Tools	<ul style="list-style-type: none"> ▪ ClamAV (https://www.clamav.net)
Log Analysis Tools	<ul style="list-style-type: none"> ▪ http Logs Viewer (https://www.apacheviewer.com) ▪ Atomic OSSEC (https://atomicorp.com) ▪ http Logs Viewer (https://www.apacheviewer.com) ▪ SolarWinds Loggly (https://www.loggly.com) ▪ Logentries (https://logentries.com) ▪ Stackify (https://stackify.com) ▪ Logz.io (https://www.logz.io) ▪ Graylog (https://www.graylog.org)
Tools for Recovery after Web Application Incidents	<ul style="list-style-type: none"> ▪ ApexSQL Log (https://www.apexsql.com) ▪ CrowdStrike Falcon™ Orchestrator (https://www.crowdstrike.com) ▪ SysTools SQL Recovery (https://www.systoolsgroup.com)
Web Application Fuzz Testing Tools	<ul style="list-style-type: none"> ▪ WSFuzzer (https://sourceforge.net) ▪ WebScarab (https://github.com) ▪ Burp Suite (https://www.portswigger.net) ▪ HCL AppScan® Standard (https://www.hcltechsw.com) ▪ Peach Fuzzer (https://peachtech.gitlab.io)
Web Application Security Testing Tools	<ul style="list-style-type: none"> ▪ Acunetix Web Vulnerability Scanner (https://www.acunetix.com) ▪ N-Stalker Web Application Security Scanner (https://www.nstalker.com) ▪ Browser Exploitation Framework (BeEF) (https://beefproject.com) ▪ Metasploit (https://www.metasploit.com) ▪ PowerSploit (https://github.com) ▪ Watcher (https://www.casaba.com) ▪ Invicti (https://www.invicti.com) ▪ Arachni (http://arachni-scanner.com)