

Containment of Web Application Security Incidents Checklist

Note: Prior to starting the containment of web application incidents checklist, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, if Applicable, Extension:			
<i>Additional Details (If Any):</i>			

Section 3: Checklist of Containing Web Application Security Incidents	
Actions	Completed
Whether a black hole feature on the web application is enabled so that it drops all requests from the same source after a limit	<input type="checkbox"/>
Whether the capacity of the servers is increased in terms of handling the connections	<input type="checkbox"/>
Whether the administrators blacklisted the IP or blocked it, so that no further traffic emerges from that IP in case the attack seems to originate from a single IP	<input type="checkbox"/>
Whether the organization selected the services of anti-DDoS service providers, such as Cloudflare to effectively fight back against web attacks	<input type="checkbox"/>
Whether a load level is defined that the authenticated users can place on the web application (terminate the previous request and raise a new request to process their request further if there is more requirement)	<input type="checkbox"/>
Check whether unnecessary access to any resource for unauthorized users is denied	<input type="checkbox"/>
Whether you clarified the queries and did not lose their trust to guide the users	<input type="checkbox"/>
Whether specially designed routers are used that can consume all incoming traffic and filter out the legitimate ones by identifying their protocols, patterns, and standard samples of incoming packets to mitigate DDoS attacks	<input type="checkbox"/>
Whether the entry points are identified, and the server and applications are restored to a normal situation	<input type="checkbox"/>
Whether the traffic flow is restricted from one network to another, typically from a compromised system	<input type="checkbox"/>
Check whether a WAF is used to monitor and block potential threats	<input type="checkbox"/>
Whether the attacker's operation on the network is isolated by removing suspicious user credentials from the network and web application	<input type="checkbox"/>

Whether egress filtering is enabled to restrict the flow of traffic from one network to another, typically from a compromised system	<input type="checkbox"/>
Whether a dedicated hardware or software firewall is installed to block the user datagram protocol (UDP) or TCP flood attack	<input type="checkbox"/>
Whether a content delivery network (CDN) is established that can automatically hosts website codes, images, and dependencies	<input type="checkbox"/>
Whether Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is implemented to ensure that only humans are able to submit any requests or forms in the web application	<input type="checkbox"/>
Whether it is ensured that the web application does not displays debugging information to the users	<input type="checkbox"/>
Whether a backup Internet connection is maintained with a pool of IP addresses for crucial users	<input type="checkbox"/>
Whether malware and virus scans are performed	<input type="checkbox"/>
Whether manual and automatic intercepting proxies such as Burp Suite, IBM AppScan, and Skipfish are used to scan for the presence of potential threats	<input type="checkbox"/>
Whether web applications are scanned for injection, session-based, and other vulnerabilities using vulnerability scanning tools and patched	<input type="checkbox"/>
Whether the design and coding errors are eliminated in a web application	<input type="checkbox"/>
Whether the data is whitelisted, blacklisted, or inputs are sanitized according to the requirement if all the input data is untrusted	<input type="checkbox"/>
Whether the user input is validated based on the length, type, format, characters, and range of the input	<input type="checkbox"/>
Whether characters that improve the security of the web applications to the best possible level are used	<input type="checkbox"/>
Whether the HTML and JavaScript code is sanitized to handle untrusted inputs	<input type="checkbox"/>

Whether the web server is scanned to identify common ports and vulnerabilities using tools such as Nmap, Sandcat Browser, WebInspect, and NetScanTools Pro	<input type="checkbox"/>
Whether awareness about the security implications and training is provided to the developers for creating secure code	<input type="checkbox"/>
Whether similar indicators of compromise are checked across other servers and web applications	<input type="checkbox"/>
Whether the vulnerabilities found in the web application are reported to the service providers and web application developers	<input type="checkbox"/>
Whether the web application administration and management accounts passwords are reset	<input type="checkbox"/>
Whether two-factor authentication for the affected accounts are implemented	<input type="checkbox"/>
Whether alternate authentication methods like certificates are disabled	<input type="checkbox"/>
Whether authentication tokens of admin and management accounts are revoked	<input type="checkbox"/>
Whether malware sample for forensic investigation is preserved if the system is infected with malware	<input type="checkbox"/>
Whether the compromised system is not shut down unless necessary	<input type="checkbox"/>
Whether the associated indicators such as URLs, domains, IP addresses, and file hashes in security controls are blocked	<input type="checkbox"/>
Whether a complete backup (bit-by-bit) of the disk containing the web server for forensic investigation is taken	<input type="checkbox"/>
Whether the system and its services are examined on which the web server is running	<input type="checkbox"/>
Whether a temporary web server is deployed in place of the compromised server with the same level of data	<input type="checkbox"/>