

Recovery 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 Recovery from Web Application Security Incidents	
Actions	Completed
Check whether the vulnerabilities that attackers have exploited are identified and patched.	<input type="checkbox"/>
Scan all of the web application resources, such as servers and databases, for malware and traces of the attack and check whether they are removed or not.	<input type="checkbox"/>
Elevate logging and monitoring levels of the web application to gather realistic information about the latest events	<input type="checkbox"/>
Check whether the log storage limit and disk space are increased	<input type="checkbox"/>
Check the web application backups for traces of the attack and clean them	<input type="checkbox"/>
Check whether the malware from the affected applications and its resources are removed	<input type="checkbox"/>
Check whether the administrative passwords for all devices and resources are changed	<input type="checkbox"/>
Check whether all resources are properly working before restarting the application	<input type="checkbox"/>
Check whether the firewall, IDS, and other security solutions are configured to detect the identified attack using signatures and behavior analysis	<input type="checkbox"/>
Check whether the security of the network perimeter is improved by implementing strict WAF, IDS, and ACLs policies and rules	<input type="checkbox"/>
Check whether the compromised user accounts from the web server are identified and removed after informing the users	<input type="checkbox"/>
Check whether a cleaned, verified, and patched backup version of the web application is used to restore the services	<input type="checkbox"/>
Check whether the web servers and databases are restored from clean and trusted backups	<input type="checkbox"/>
Rebuild the entire system if the backup is not available for the damaged systems	<input type="checkbox"/>
Check if the application has recovered completely along with the user accounts, privileges, and configurations	<input type="checkbox"/>
Restart any services that were terminated as part of the containment process	<input type="checkbox"/>

Use an access control matrix and define the access control rules with a list of accessible and authorized requests	<input type="checkbox"/>
Reconfigure the incident detection system to identify similar types of incidents quickly in the future	<input type="checkbox"/>