

Preparation to Handle Web Application Security Incidents

Objectives:

At the end of this episode, I will be able to:

Understand how web applications work.

Explain what the architecture of a web application is.

Identify what the steps to handle Web Application Security Incidents are.

Define what advantages proactively deploying Web Application Firewalls (WAFs) and Security Information Event Management (SIEM) systems provide for IH&R team members.

External Resources:

Preparation to Handle Web Application Security Incidents

How do Web Applications work? -

The main function of web applications is to fetch user-requested data from a database. When a user clicks or enters a URL in a browser, the web application displays the requested website content in the browser.

This mechanism involves the following step-by-step process:

- The user enters the website name or URL in the browser; the request is sent to the web server.
- The web server checks the file extension:
 - o If the user requests a simple web page with an HTM or HTML extension, the web server processes the request and sends the file to the user's browser.
 - o If the user requests a web page with extensions that needs to be processed at server side such as (php, asp, cfm, etc...), then the web application server must process the request.
- The web server passes the user's request to the web application server, which processes the user's request.
- The web application server accesses the database to perform the requested task by updating or retrieving the information stored on it.
- After processing the request, the web application server sends the results to the web server, which in turn sends the results to the user's browser.

What is the Web Application Architecture? -

The web application architecture is comprised of three layers:

1. Client or presentation layer
2. Business logic layer
3. Database Layer

The client or presentation layer includes all physical devices present on the client side, such as laptops, smartphones, and computers. These devices feature operating systems and compatible browsers, which enable users to send requests for required web applications.

The "business logic" layer itself is comprised of two layers:

- The web-server logic layer
- The business logic layer

The web-server logic layer has a firewall that offers security to the content, an HTTP request parser to handle requests coming from clients and forward responses to them, as well as a resource handler capable of handling multiple requests simultaneously. The web-server logic layer holds all coding that reads data from the browser and returns the results (for example, IIS Web Server, Apache Web Server).

The business logic layer includes the functional logic of the web application, which is implemented using technologies such as .NET, Java, and "middleware" technologies. It defines how the data flows, according to which the developer builds the application using programming languages. The business logic layer stores the application data and integrates legacy applications with the latest

functionality of the application. The server needs a specific protocol to access user-requested data from its database; this layer also contains the software and defines the steps to search and fetch the data.

The database layer is comprised of cloud services, a B2B layer that holds all the commercial transactions, and a database server that supplies an organization's production data in structured form (for example, MS SQL Server, MySQL server).

What are the causes of web incidents? -

- Insecure Coding
- Configuration Errors
- Platform Vulnerabilities
- Logic Errors

What are the steps to handle Web Application Security Incidents? -

1. Develop incident handling plan for most common web incidents
2. Maintain and keep ready a backup website
3. Plan to maintain continuity of internet services
4. Maintain a comprehensive contact list
5. Create a whitelist of all critical IP addresses and protocols
6. Maintain an inventory of organizational IT Infrastructure
7. Maintain a Disaster Recovery Plan
8. Deploy monitoring tools to detect abnormal activities
9. Design and maintain good network infrastructure
10. Customize TTL settings for critical systems
11. Review and audit web server logs and settings

What about Deploying a WAF? -

A WAF captures, filters, and analyzes all the incoming traffic to detect, block, and thwart various application layer attacks. A WAF filters the content based on a certain set of rules or instructions and blocks application layer attack attempts that match the rules.

A WAF includes built-in behavioral and reputational analysis that can also assist in protecting the applications against zero-day threats. Most WAFs allow the security personnel to customize security policies and design them according to the access privileges and user inputs.

Some of the common factors that WAF policies or rules are designed to address include:

- IP address and geolocation data
- Request methods such as POST or GET
- URL parameters
- HTTP/S header values
- Access rate

What about Deploying SIEM Solutions? -

The incident handling team must also deploy Security Incident and Event Management (SIEM) solutions to efficiently log, analyze, and alert on security incidents. It assists in threat detection and security incident response activities. SIEM provides security by tracking suspicious end-user behavior activities within a real-time IT environment.

SIEM offers security management services combining Security Information Management (SIM) and Security Event Management (SEM). SIM supports permanent storage, analysis, and reporting of log data. SEM deals with real-time monitoring, correlation of events, notifications, and console views.