

Content Security Policy (CSP)

Presentation Slides

Training Kit



CyberEco

معا لدعم السلامة الرقمية
Together to support digital safety



High School



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property rights

The National Agency for Cyber Security in the State of Qatar owns the work, and copyright, publishing, printing rights, and all other intellectual property rights are protected by the National Agency for Cyber Security in the State of Qatar.

As a result, the Agency retains all rights to these materials, and it is prohibited to republish, quote, copy, or transfer them in whole or in part in any form or by any means whether electronic or mechanical, including photographic reproduction, recording, or the use of any information storage and retrieval system, whether existing or invented in the future, unless the agency has given written permission.

Anyone who breaks this could face legal consequences.

December, 2023

Doha, Qatar

This content is produced by the team of

National Cybersecurity Excellence Management, National Cyber Security Agency.

For inquiries about the initiative or program, you can contact us through the following websites or phone numbers:



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

🌐 <https://www.ncsa.gov.qa/>

✉ cyberexcellence@ncsa.gov.qa

☎ 00974 404 663 78

☎ 00974 404 663 62

Workshop Time Table

Content	Allocated Time
General Introduction	5 minutes
The theoretical aspect	25 minutes
Educational Videos	25 minutes
Short Break	20 minutes
Training games	25 minutes
Dialogue and Discussion with Students	15 minutes
Graduation Project	5 minutes
Total training time	2 hours

Scientific Content Index

Chapter 1

Concept of Content Security Policy (CSP) and its Operation Mechanism

Firstly: Concept of Content Security Policy (CSP).....4

Secondly: Operation Mechanism of Content Security Policy (CSP)14

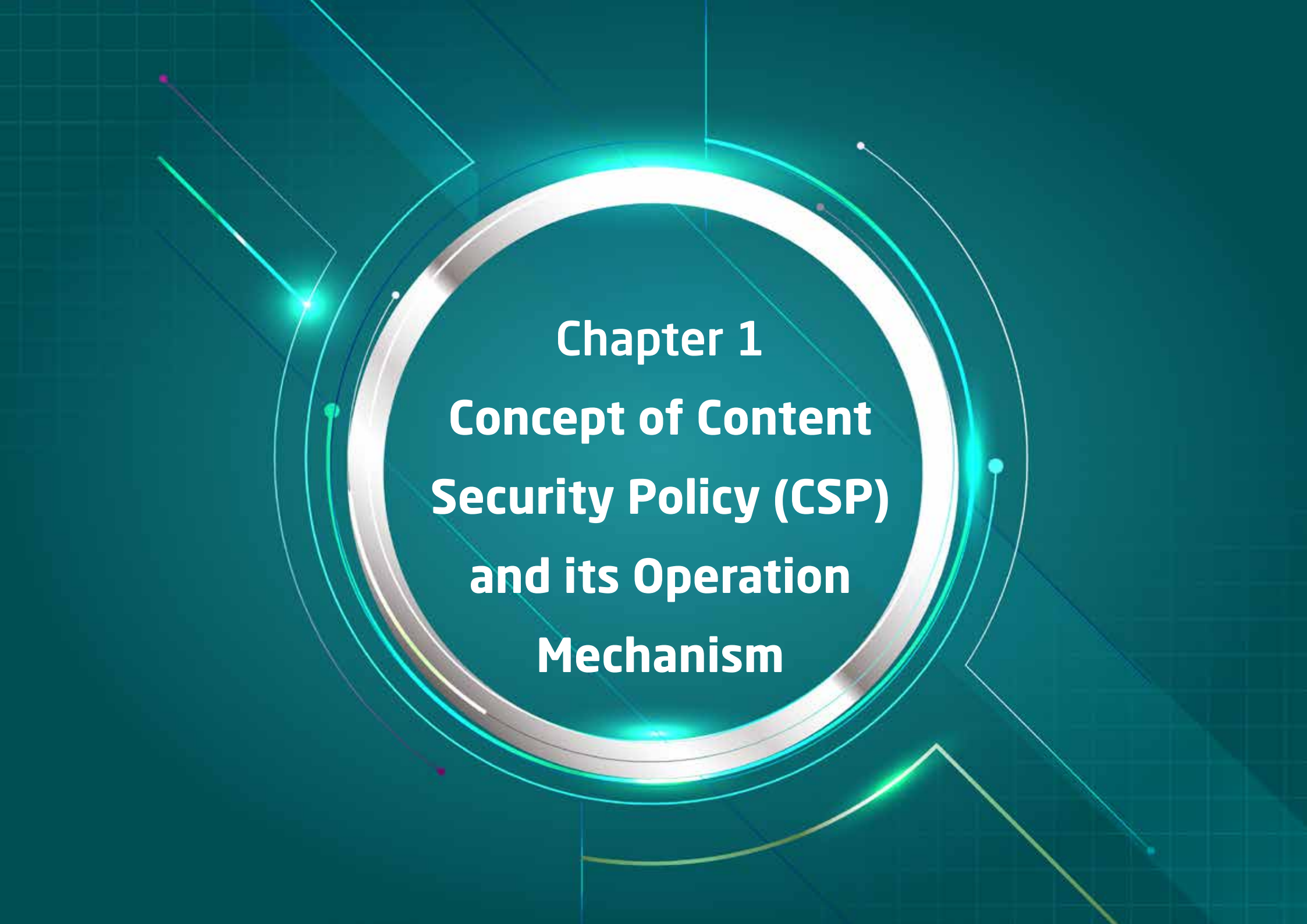
Chapter 2

Activating Content Security Policy (CSP) and Digital Risks Mitigated by It

Firstly: Activating Content Security Policy (CSP)..... 24

Secondly: Digital Risks Mitigated by Content Security Policy (CSP).....29

Exercises and trainings.....38



Chapter 1
Concept of Content
Security Policy (CSP)
and its Operation
Mechanism

Concept of Content Security Policy (CSP)

Content Security Policy (CSP) is an additional layer of security that helps detect and mitigate certain types of cyberattacks, including Cross-Site Scripting (XSS) attacks, data injection attacks that steal data, manipulate websites, and distribute Malware.

CSP enables server administrators to mitigate the potential damage caused by XSS attacks by specifying valid script sources to the browser, which executes only the received scripts from allowed domains, as defined by the CSP.



The term “policy” refers to

a set of policy directives that describe the user’s content security policy on the web. Each type of content has its own policy directives, including fonts, images, audio and video media, and scripts.

Content Security Policy directives are defined in HTTP response headers called CSP headers, which guide the browser to trusted content sources and include a list of sources that should be blocked.



There are several categories of CSP directives that vary based on usage and content attributes, including:



Fetch directives, which include:

Child-source



This directive specifies the valid script sources included in the browsing context's whitelist for iframes and web workers.

Connect-source



This directive specifies the URLs that can be loaded using scripts.

default-source



The fallback directive for all fetch directives, defining the default list of allowed sources for other fetch directives.

Object-source



Specifies the allowed sources for `<applet>`, `<embed>`, and `<object>` elements.

Style-source

Provides a list of valid sources for inline style sheets, which are responsible for the look and design of web pages.

Document directives, which help control the work environment properties (document), including:

01

Sandbox: Protects a specific resource similar to inline script elements.

02

Base-uri: Specifies the allowed URLs in the document's base element.

Navigation directives, which control document traversal (navigation) locations, including:

01

Form-Action: Defines the URL addresses to which form submission is allowed.

02

Frame-ancestors: Restricts the assets that can be included in a web page.

Reporting directives, which are responsible for documenting and reporting violations of the content security policy, including:

01

Initiates the process of reporting CSP violations.

02

Report-URI: Directs the user agent to report any attempts to violate CSP specifications.

Here are other directives report violations of the Content Security Policy (CSP):

require-sri-for

This directive enforces the use of Subresource Integrity (SRI) for the style attribute and script sources on the page.



trusted-types

This directive specifies a list of trusted values that cannot be bypassed by cyber attackers, thus mitigating XSS attacks.



require-trusted-types-for

This directive guides the enforcement of trusted types policy on script sources.



upgrade-insecure-requests

Some websites may include insecure, old-fashioned URLs. This directive instructs the browser to handle those addresses and replace them with more secure HTTPS URLs.

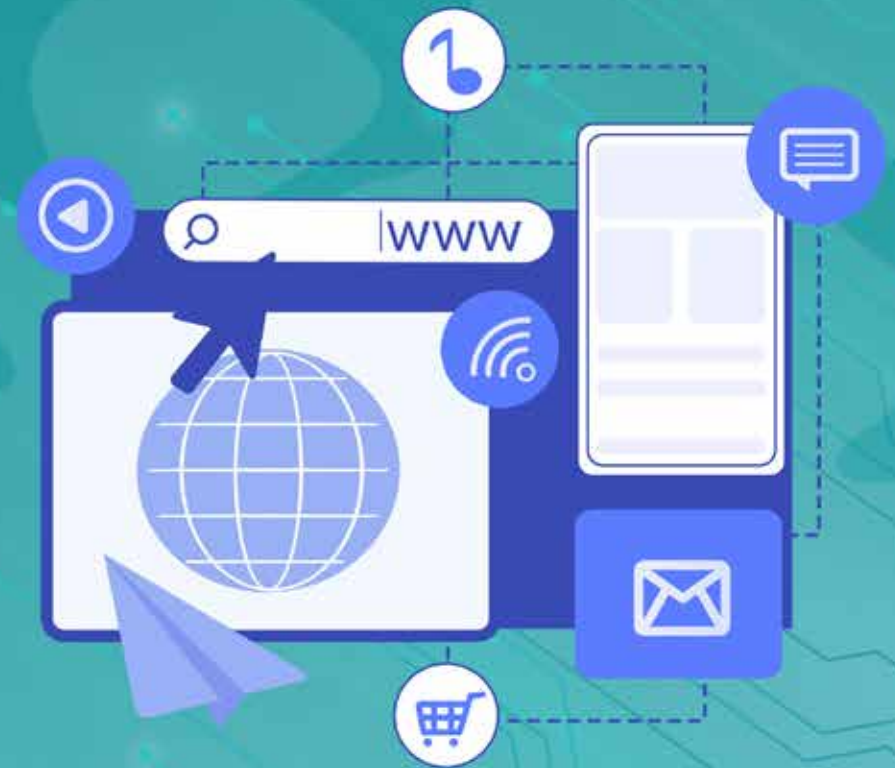
Operation Mechanism of Content Security Policy (CSP)

The Content Security Policy (CSP) works by specifying a completely empty whitelist, blocking everything. Initially, the policies should be run in report-only mode, allowing the browser to evaluate the rules before blocking content. Users can review and classify errors in an allowed or disallowed list.



When a browser loads a page with a Content Security Policy,

it verifies the CSP to ensure that the content is authorized. If it is not authorized, the browser blocks the content and displays an error message. This helps prevent attackers from injecting malicious code into the page, protecting web users from malicious attacks.



The Content Security Policy also helps protect the user's website

from being flagged by search engines like Google for hosting Malware. This can affect the number of visits, customers, brand reputation, and profits.



**To implement the Content Security Policy
(CSP), follow these steps:**



Choose a service provider for your website.

It is preferable to customize the policy to fit the needs of each user on their website or application. For that purpose, you should create a list of directives policies to specify the resources that are allowed or not allowed on your website.



Common CSP directives from service providers specializing in web security include:

1

Use `frame-src` to block the loading of iframes on the website.

2

Use `script-src` to prevent the loading of JavaScript on the website.

3

Use `img-src` to restrict content other than images on user-specific web pages.

4

Use `default-src` to allow content only from the same source, the user's website, and its subdomains.

5

Allow only executable media or other scripts from the same source.

Users can receive notification alerts if their policy is violated, without content being blocked, by configuring the HTTP response header to report only the Content Security Policy.

Adding a Content Security Policy (CSP) to the HTTP response header of a website

Most of changes is done by making modifications to the HTTP response header. First, it is necessary to identify the server hosting the user's website before setting up the HTTP response header.

To determine the server hosting each user's website, you can log in to their cPanel and check the server information interface. cPanel provides a reliable system for managing servers and websites.

In summary, there are several options to do this:



Setting up CSP using Internet Information Services (IIS Manager):

IIS (Internet Information Services) is a web server from Microsoft that runs on the Windows operating system. It is used for serving static and dynamic web content to internet users and can also be used for hosting, deploying and managing web applications.



Setting up CSP using Apache:



Apache is a web server responsible for accepting Hypertext Transfer Protocol (HTTP) requests from internet users and sending them the requested information in the form of web files and pages.


Implementing Content Security Policy:

Content Security Policies are enforced through a special HTTP header sent with the response from the server, which includes rules that are later enforced by the browser.

There are two ways to do this:

- Adding Content Security Policies for the website via meta tags that work across all browsers.
- Setting up those policies for the user's site using the HTTP response header. This method is supported by most browsers, except Internet Explorer and some older browser versions.





Chapter 2
How to Enable
Content Security
Policy (CSP) and
the Digital Risks it
Mitigates

Enabling Content Security Policy (CSP)



To find the Content Security Policy in the response headers, you can follow the following steps:

01

Using the browser, open the Developer Tools (using DevTools in Chrome), then navigate to the website you choose and open the "Network" tab.

02

Look for the file that creates the page, which has the same domain as the website you are browsing. It is usually the first item in the "Network" tab.

03

When clicking on the file, more information will be displayed, and here you start searching for the 200 OK response code.

04

At the bottom, it will show whether Content Security Policies are being used or not.

The second place to find the Content Security Policy (CSP) is in the “meta” tag:

1. Navigate to the page source and open the browser and select the website.
2. Right-click on an empty area and select “View Page Source.”
3. Once the page source is displayed, search for the term “Content Security Policy” using the system’s search function (Ctrl-F in Windows).



Free Tools to Help Create, Evaluate, and Monitor

Content Security Policy:



w3af Audit Tools: It includes an additional component for automatically auditing web applications to ensure the activation of Content Security Policies (CSP).



CSP Tester (Browser Extension): It allows building and testing the CSP for the user's website application.



CSP Generator (Chrome/Firefox Extension): It automatically generates Content Security Policies.



CSP Evaluator: It evaluates the current Content Security Policies.



Csper Reporting Tool: It monitors the Content Security Policy using the URI reporting feature.

Digital Risks Mitigated by Content Security Policy (CSP)



Cross-Site Scripting (XSS) Attacks

Cross-Site Scripting (XSS) attacks are a type of injection attack where a cyber attacker injects malicious scripts into trusted websites. The attack occurs when the attacker uses a web application to send harmful script instructions from the browser side to the user.

In this attack, the malicious script appears to come from a trusted source, allowing it to access any stored cookies or sensitive information that the browser retains and uses with the website. These scripts can also rewrite the content of an HTML page.



XSS attacks can be categorized as follows:

Reflected XSS Attacks:

In this category, the injected malicious script is reflected by the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request. Reflected XSS attacks are delivered to victims through another means, such as an email or on other compromised websites. When the user clicks on the malicious links or browses the affected website, the injected script is transferred to the vulnerable web server, reflecting the attack back to the user's browser. The browser then starts executing the script because it came from a "trusted" server, leading to a deceptive process.

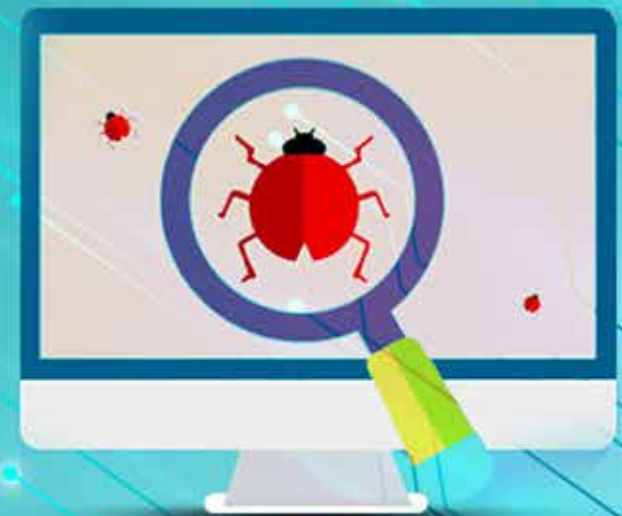


Stored XSS Attacks:

Stored XSS attacks involve permanently storing a script payload on targeted servers, such as in a database, visitor log, or comment field. The victim user then retrieves the malicious script from the server when requesting the stored text.

Blind XSS:

Blind XSS is a form of persistent XSS attack that occurs when an attacker stores and retrieves malicious scripts from the server, such as in "data forms." The attacker sends the malware, and as soon as the user opens the form, execution begins.



The damages caused by XSS attacks include:

Complete account breach.

01

Installation of Trojan horses.

02

User redirection to another page or website.

03

Modification of content display.

04

Alteration of press releases or news about a company's stock price, leading to a loss of consumer trust.

05

Packet Sniffing Attack

A packet sniffing attack is a hacking technique that involves collecting data packets transmitted over an unencrypted computer network. Cyber attackers monitor network traffic, intercepting sensitive information such as financial details or login credentials to sell or use in other attacks.

This attack falls under the category of espionage attacks and is particularly effective on unencrypted networks. This requires caution while using a public Wi-Fi network to encrypt connections and prevent users and their data from being tracked.



Types of Packet Sniffing Attacks:

Active Packet Sniffing:

This type of attack is used on larger networks. As more devices connect to a single network, a network switch is required to direct internet traffic to its intended destination, preventing traffic congestion. Active packet sniffing attacks are more detectable because they need to announce themselves to initiate the sniffing process.

Passive Packet Sniffing

Passive packet sniffing attacks are executed on smaller networks where all devices are connected to a single network hub. In this case, the attack doesn't rely on network switches to direct traffic, and don't need to announce themselves making it harder to detect.

When to Use Content Security Policy (CSP) Policies?

It is recommended to use CSP policies for applications that handle sensitive data, such as administrative user interfaces, device management control units, or products that host user-generated documents, messages, or media files.

However, for static applications without any login functions or cookie-based sessions, it is not necessary to use CSP policies. Similarly, for large applications with a history of XSS attacks, CSP policies can provide an additional layer of security, but the primary focus should be on secure coding practices to protect against such cyber attacks.





Exercises and trainings



First: In-Class Exercises

Did you know that

It is recommended to use **Content Security Policy (CSP)** for applications that handle sensitive data, such as administrative user interfaces, device management control units, or products that host user-generated documents, messages, or media files.





Exercise 1

Complete the following sentences:

1. Content is a for securing computer systems and was developed to prevent or harmful software through websites.
2. attacks are a type of malicious and harmful code in trusted, often used to attack sites.
3. The security policy (CSP) can be specified in the HTTP response header when requested by the web client.
4. CSP stands for "....." in English.
5. Content policy is very important for owners of websites.



Pay Attention!

Content Security Policy (CSP) Concept

Content Security Policy (CSP) is an additional layer of security that helps detect and mitigate certain types of cyber attacks, including Cross-Site Scripting (XSS) attacks and data injection attacks that steal data, manipulate websites, and distribute malware.

Exercise 2

Mark (✓) or (✗) for the following statements:



1

CSP is a program similar to antivirus software.



2

Content security policy only helps in detecting web attacks.



3

Content security policy cannot help prevent data theft.



4

There is no relationship between content security policy and defacement attacks on websites.



5

Content security policy provides a comprehensive set of policy directives that help control the resources allowed to be loaded by a webpage.





6

Enabling content security policy for a website has a negative impact on communications, scripts, and fonts.



7

Content security policy continues to work by default all the time.



8

Content security policy is an insignificant addition to websites.



9

Content security policy is an additional layer of security that helps detect web attacks.



10

A large number of websites need content security policy to increase site speed.



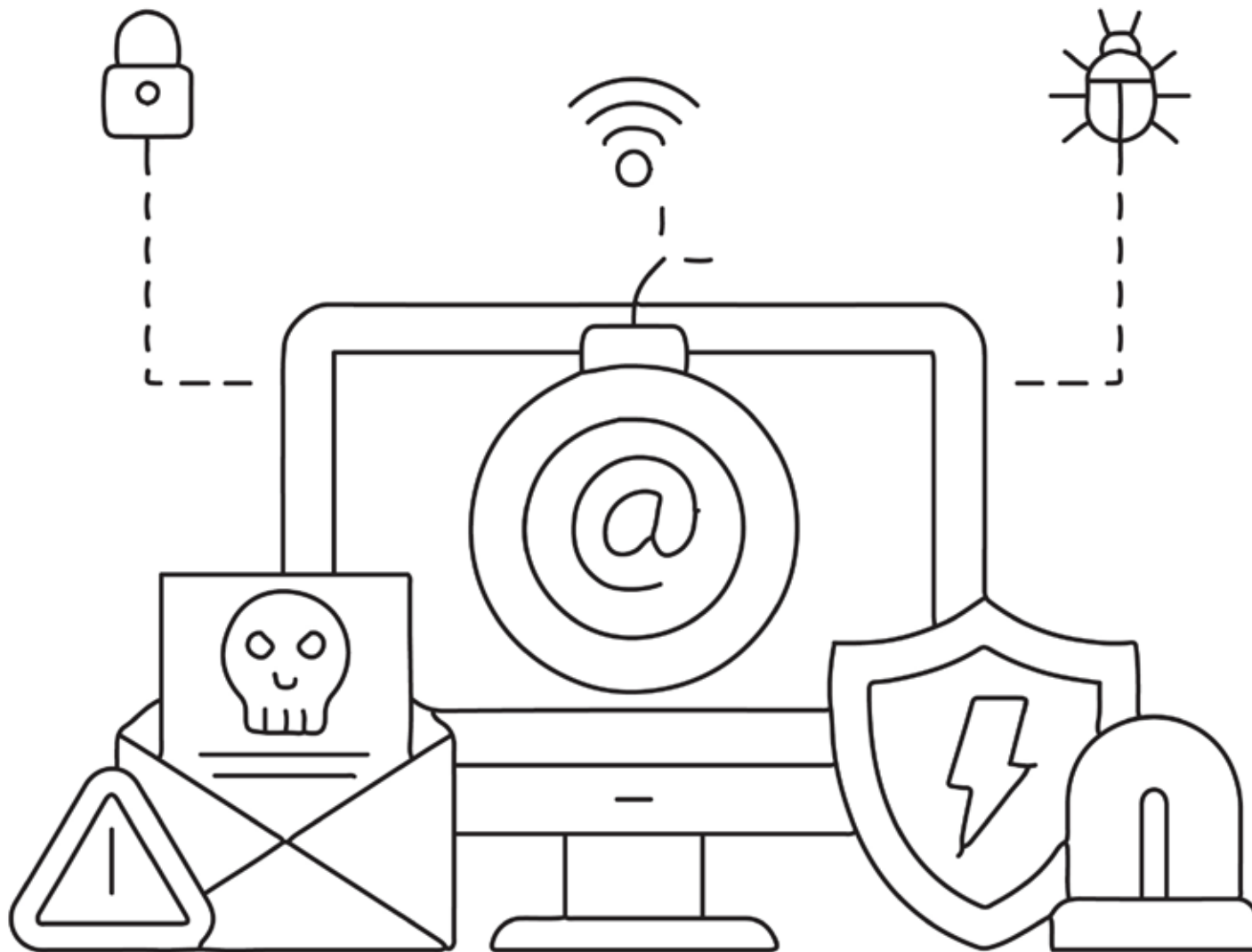
Pay Attention!

The best way to add Content Security Policy (CSP) with retroactive effect to an entire website

to define an empty whitelist to block everything. The desired approach is to initially enable these policies in report-only mode, allowing the browser to evaluate the rules first before blocking the content. From there, the user can review and classify errors, categorizing each item as either allowed or disallowed.







Pay Attention!

Functions performed by Content Security Policy

include limiting packet sniffing attacks, which are cyber attacks carried out by intruders to intercept and monitor network traffic, targeting unencrypted email messages, login credentials, and financial information. These policies work by restricting the domains from which content can be loaded by specifying the server for allowed protocols.



Did you know that

Content Security Policy (CSP) allows server administrators to mitigate the damages that can be caused by XSS attacks by displaying valid and executable script sources to the browser.





Pay Attention!

Cross-Site Scripting (XSS) Attacks

XSS attacks are a type of injection attack in which a cyber attacker injects malicious scripts into trusted websites. The attack occurs when the attacker uses a web application to send malicious script instructions from the browser's side to the user.

Exercise 1

Mark (✓) or (✗)

To the following sentences



The Content Security Policy (CSP) can be found in the website's definition tag.



Enabling a development/testing environment is necessary due to the risks of Content Security Policy.

You should enable Content Security Policy immediately without testing.

Content Security Policy takes at least 48 hours to work.

Content Security Policy service cannot provide reporting or identify issues or vulnerabilities.

Cross-Site Scripting (XSS) attacks on shared websites can lead to account compromise.

Active package sniffing attacks are used on small networks.

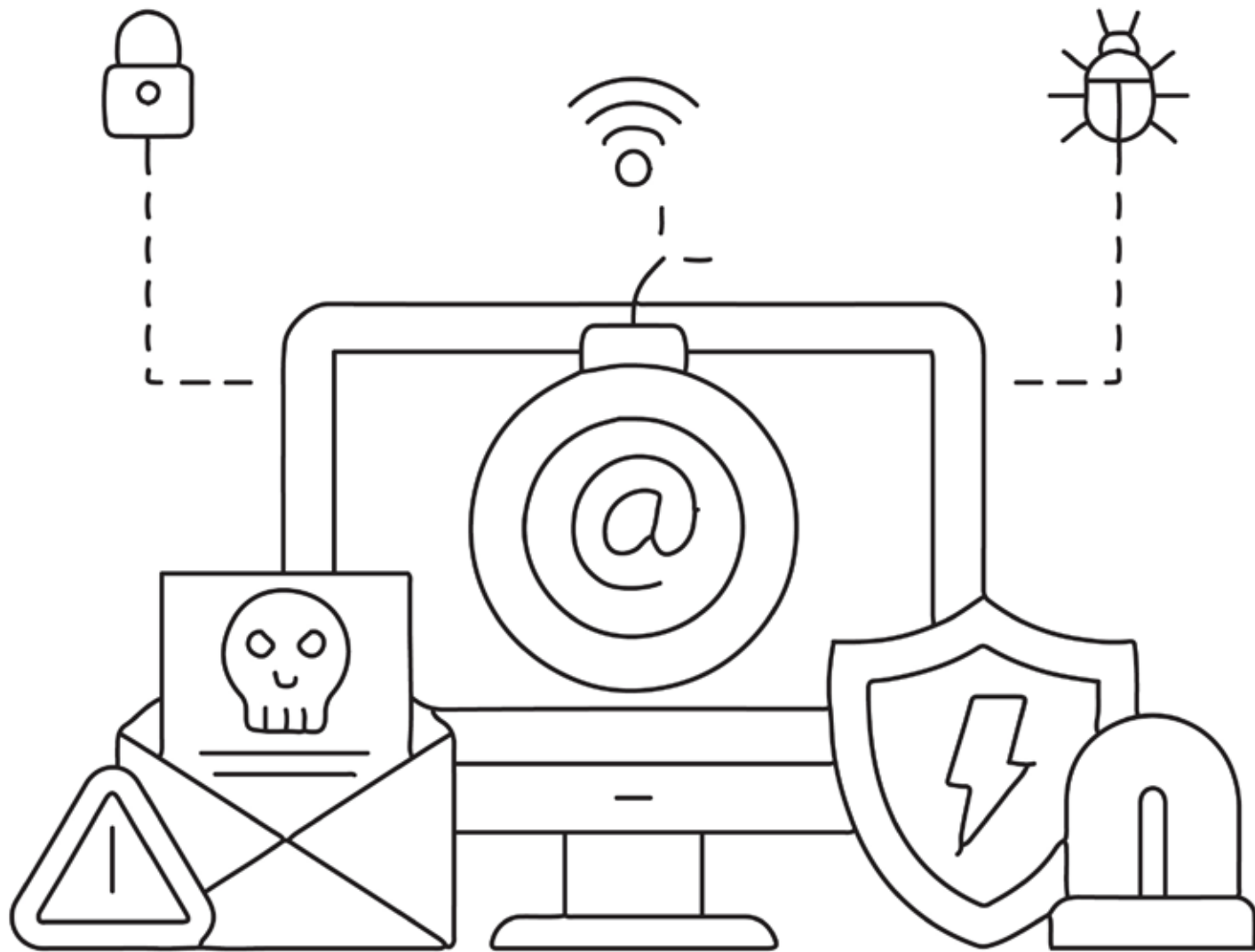
You can never control individual directives within the policy.



Pay Attention!

Stored XSS Attacks:

Stored XSS attacks involve permanently storing a script payload on targeted servers, such as in a database, visitor log, or comment field. The victim user then retrieves the malicious script from the server when requesting the stored text.



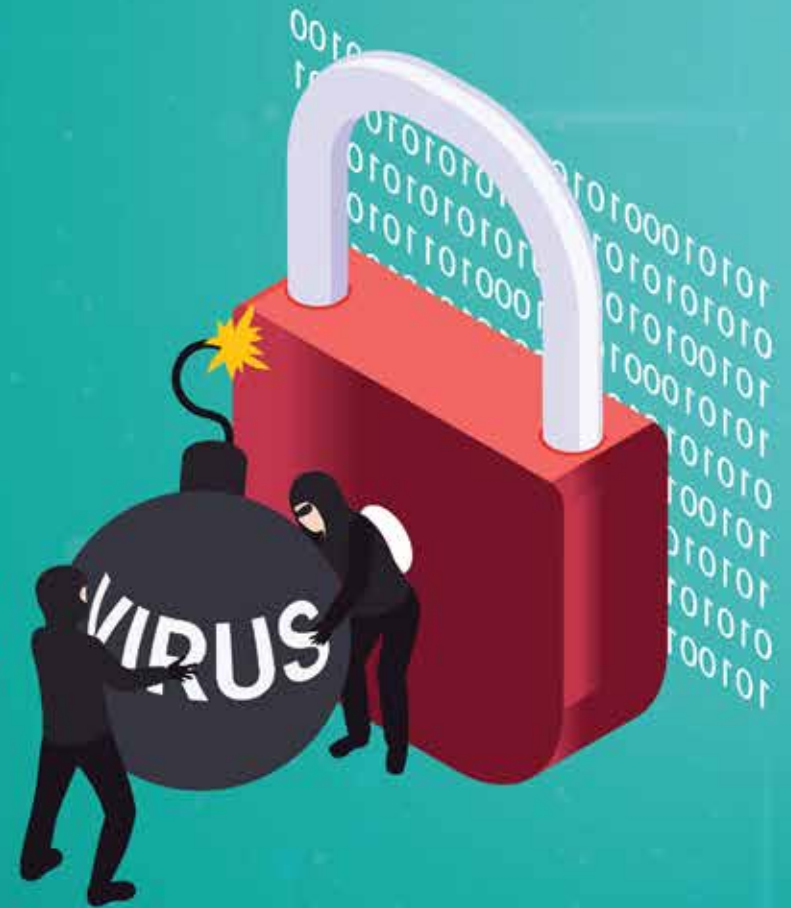
Did you know that

Internet users can receive notification alerts if **their policy is violated**, without content blocking, by setting the HTTP response header to report-only for Content Security Policy.



Risks of Cross-Site Scripting (XSS) Attacks:

- Modification of content display.
- Complete account compromise.
- Installation of Trojan horses.
- User redirection to another page or website.
- Alteration of a press release or news about a company's stock price, leading to a decrease in consumer trust.





Exercise 2

Extract the following words from the table

Guide

Read the words below carefully and search the table for consecutive letters that form these words. Below is an example of the word **"Application"** and how to find its letters in the table:

S	E	N	C	R	Y	P	T	I	O	N	S	P	Q	T	R
E	R	E	S	P	O	N	S	E	M	T	O	O	L	S	E
C	F	I	X	T	C	O	N	T	E	N	T	U	R	V	P
U	A	Z	Y	A	T	T	A	C	K	S	R	E	O	Z	O
R	B	F	X	M	O	C	L	O	U	D	Y	N	F	K	R
L	D	E	M	L	R	S	N	X	O	W	P	Z	Q	S	T
I	C	O	N	F	I	D	E	N	T	I	A	L	I	T	Y
T	J	I	P	O	L	I	C	Y	W	E	B	S	I	T	E
Y	K	S	T	R	U	C	T	U	R	E	V	N	T	A	F
A	P	P	L	I	C	A	T	I	O	N	U	W	R	L	K

~~Application~~ - Security - Cloud - Encryption - Fix - Response - Structure - Vulnerabilities
Policy - Content - Website - Confidentiality - Attacks - Reports - Tools

Pay Attention!

Content Security Policy helps protect the user's website from being flagged as malicious by search engines like Google when they detect any malware on it. This can impact the number of visits and customers, as well as the reputation of the brand and profits.



Did you know that

Content Security Policy (CSP) enables website owners to define their own rules that suit their website's needs while preventing unauthorized access to crucial information.

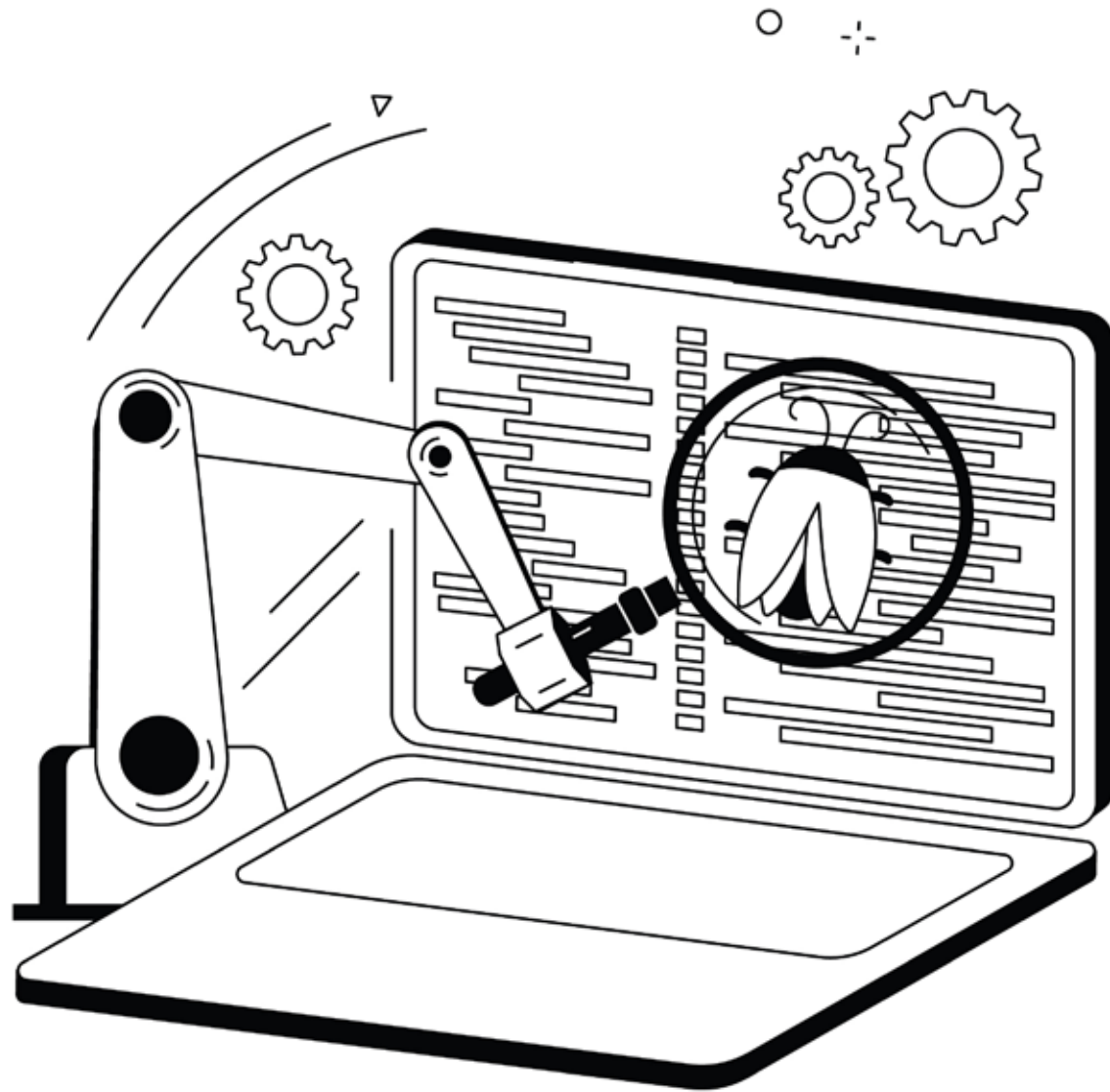


Pay Attention!

Blind XSS

Blind XSS is a form of persistent XSS attacks. It occurs when the attacker stores malicious scripts on the server and serves them to the victim. For example, in "data forms," the attacker sends malicious scripts, and as soon as the user opens the form, the execution begins.



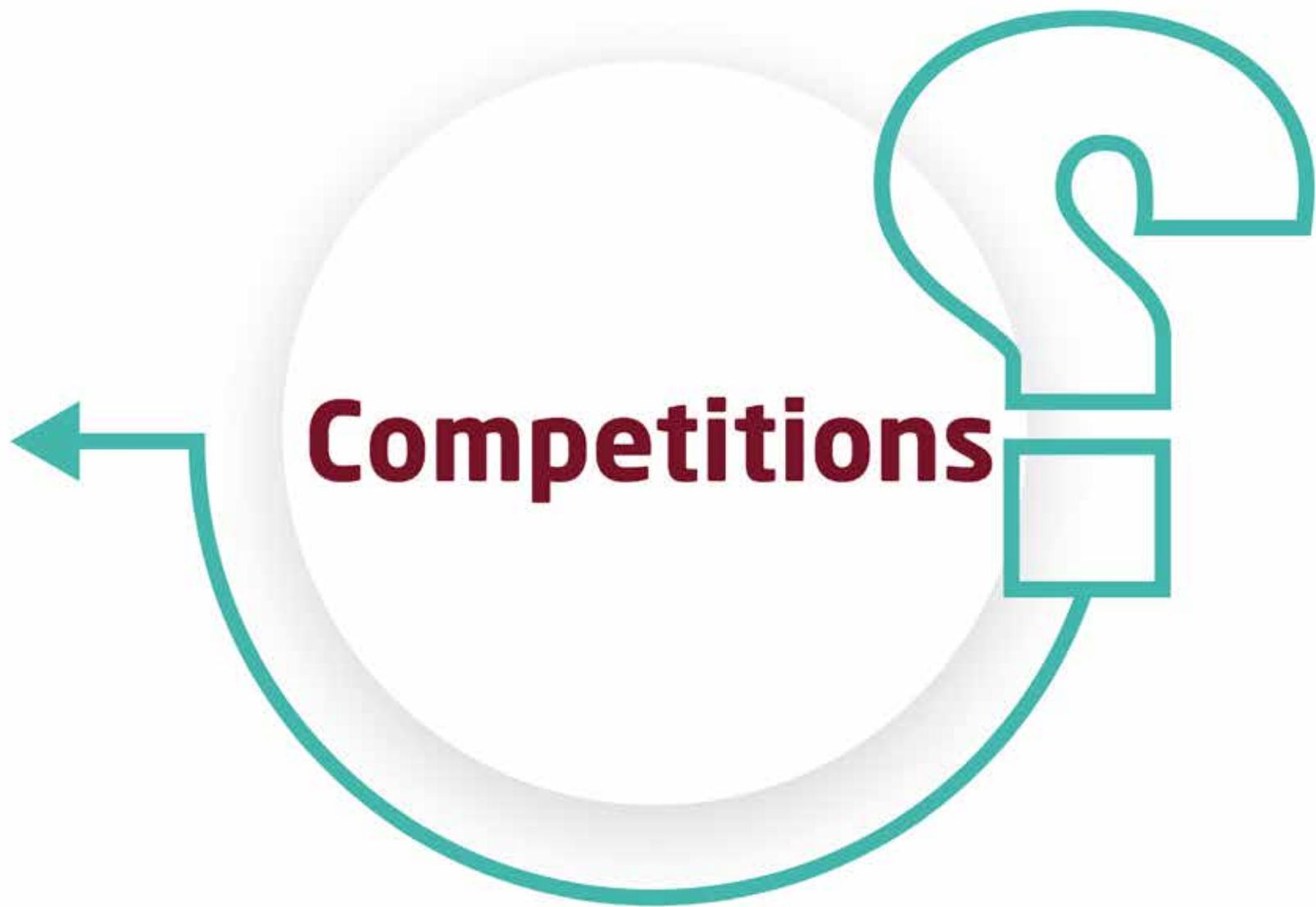


Pay Attention!

Internet Information Services (IIS)

IIS Manager is a web server from Microsoft that runs on the Windows operating system. It is used to exchange static and dynamic web content with internet users and can also be used to host, publish, and manage web applications.





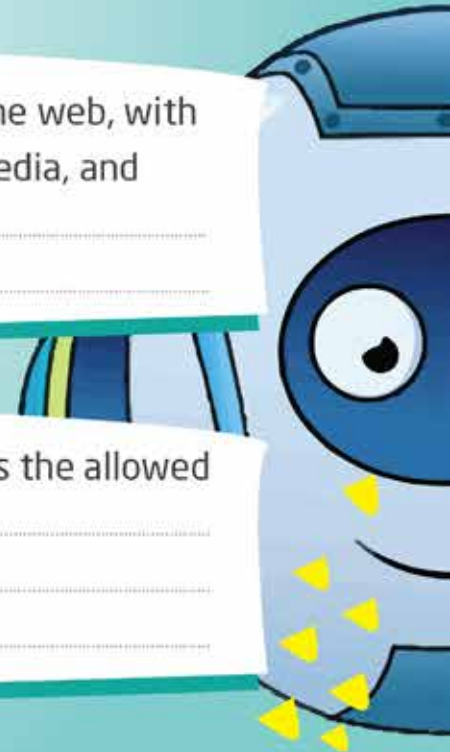
What is this?

Content Security Policy (CSP) is an additional layer of security that helps detect and mitigate certain types of cyber attacks, including

Cyber attacks executed by intruders to intercept and monitor network traffic, targeting unencrypted email messages and financial information

A set of directives that describe the user's content security policy on the web, with each type having its own policy, including fonts, images, audiovisual media, and scripts.

One of the categories of Content Security Policy directives that specifies the allowed locations from which specific types of content can be loaded.



What is this?

One of the categories of Content Security Policy directives that helps control the working environment settings.



A web server from Microsoft that runs on the Windows operating system, used to exchange static and dynamic web content with internet users, and can also host, publish, and manage web applications.

A web server responsible for accepting Hypertext Transfer Protocol (HTTP) requests from internet users and sending them the requested information in the form of web files and pages.

Two places where you can find providers that have implemented content security policy.




What is this?



It refers to the storage of a script that is loaded onto target servers, such as in a database, visitor log, or comment field, and so on. The victim user then retrieves the malicious script from the server when requesting the stored text.

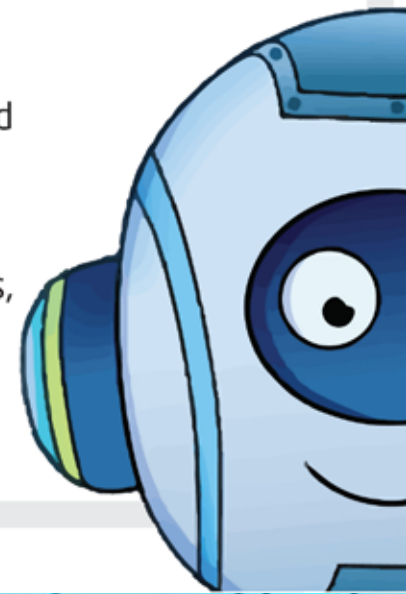
It is a form of persistent XSS attacks, occurring when the attacker stores malicious scripts on the server and serves them to the victim. For example, in "data forms," the attacker sends malicious scripts, and as soon as the user opens the form, the execution begins.

It is defined as a hacking method that works by collecting data packets that are transferred over an unencrypted computer network. Cybercriminals monitor data packets in network traffic in order to intercept sensitive information such as financial details or login data, to sell it or use it in other attacks.



Complete the following sentences:

- The additional security layer provided by Content Security Policy (CSP) aims to.....
- Content Security Policy (CSP) allows server administrators to mitigate the damage that can be caused by an XSS attack by.....
- One of the functions that Content Security Policy also performs is to limit attacks, which are cyberattacks carried out by attackers to intercept and monitor network traffic.
- Content Security Policy directives are defined in, which are called CSP headers. Their purpose is to instruct the browser to trusted content sources, and they also include a list of sources that should be blocked.
- Document directives help to control the properties of the working environment (document), and they include:, and.....
- Reporting directives are responsible for documenting and reporting violations of CSP policies, and they include:, and.....



- Some websites may contain old, insecure URLs, so the-requests directive instructs the browser to treat those URLs and replace it with a safer one as HTTPS.
- The best way to add CSP retroactively to an entire website is to specify, to block everything.
- CSP helps to protect a user's site from being placed in, which is a list of websites like Google identifies as having malware.
- Internet users can receive warning notifications if their policy is violated, but without blocking content, by setting to CSP report-only.



Choose the correct answer:



In this category of cross-site scripting attacks, the cyber attacker permanently stores a malicious script on the targeted servers, as is the case in the database, or visitor log, or comment field, and so on.

- Stored XSS attacks.
- Reflected XSS attacks.
- Blind XSS.
- Packet sniffing attacks.

Cross-site scripting (XSS) attacks cause:

- Partial account hacking.
- Ransomware installation.
- Failure to redirect the user to another page or site.
- Modify content display.

3. This type of attack is used on larger networks; as more devices connect to a single network, there is a need for a network switch.

- Blind XSS.
- Active packet sniffing.
- Reflected XSS attacks.



4. In the event that password sniffing attacks fail, attackers resort to using attacks, which are a type of network hijacking attack to collect password data.

- Transmission Control Protocol (TCP) session hijacking.
- JavaScript sniffing.
- Man-in-the-middle.



5. Cyber attacks in which the attacker enters malicious instructions at the point of purchase on e-commerce sites

- Transmission Control Protocol (TCP) session hijacking.
- JavaScript sniffing.
- Man-in-the-middle.

6. Once a connection is established between the sender and the receiver, the attacker hacks in and transfers the trusted data, sniffing the network traffic

- Address Resolution Protocol (ARP) spoofing.
- Transmission Control Protocol (TCP) session hijacking.
- JavaScript sniffing.

Graduation Project

The graduation project is an assignment that you undertake individually or in collaboration with one or two classmates, supervised by a trainer. Through this project, you are required to:

- Write a short story, article, or report explaining the content security policy.
- Assume the role of the trainer and write general instructions for your classmates or family, explaining the procedures required to benefit from the content security policy and its importance what Content Security Policy is.





CyberEco



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency