Content Security Policy (CSP)

Student exercise and training | Training Kit

High School

CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Content Security Policy (CSP)

Student exercise and training

Intellectual Property rights

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

Dear Student,

This booklet is specifically for you, and you must have it with you when you attend training sessions. Your trainer will guide you on how to use it. This booklet contains a collection of fun and useful exercises, which you will answer either during class or at home.

The booklet also contains a set of educational competitions and cards, as well as general information in which you will find useful and enjoyable. Your trainer will guide you on how to deal with these competitions, and at the beginning of each exercise or competition, we will provide you with general instructions on how to answer.

Dear Student's Parents,

This booklet is specifically for the student and will accompany them during the training they will receive at school. It contains a collection of exercises, training activities, competitions, training games, and training cards, all of which revolve around concepts related to the content security policy and how to benefit from it.

The purpose of this booklet and and it's included mental exercises and activities is to reinforce and solidify the information that the student receives during the training session with the primary goal of enhancing the student›s ability to use the internet and technology effectively and safely.

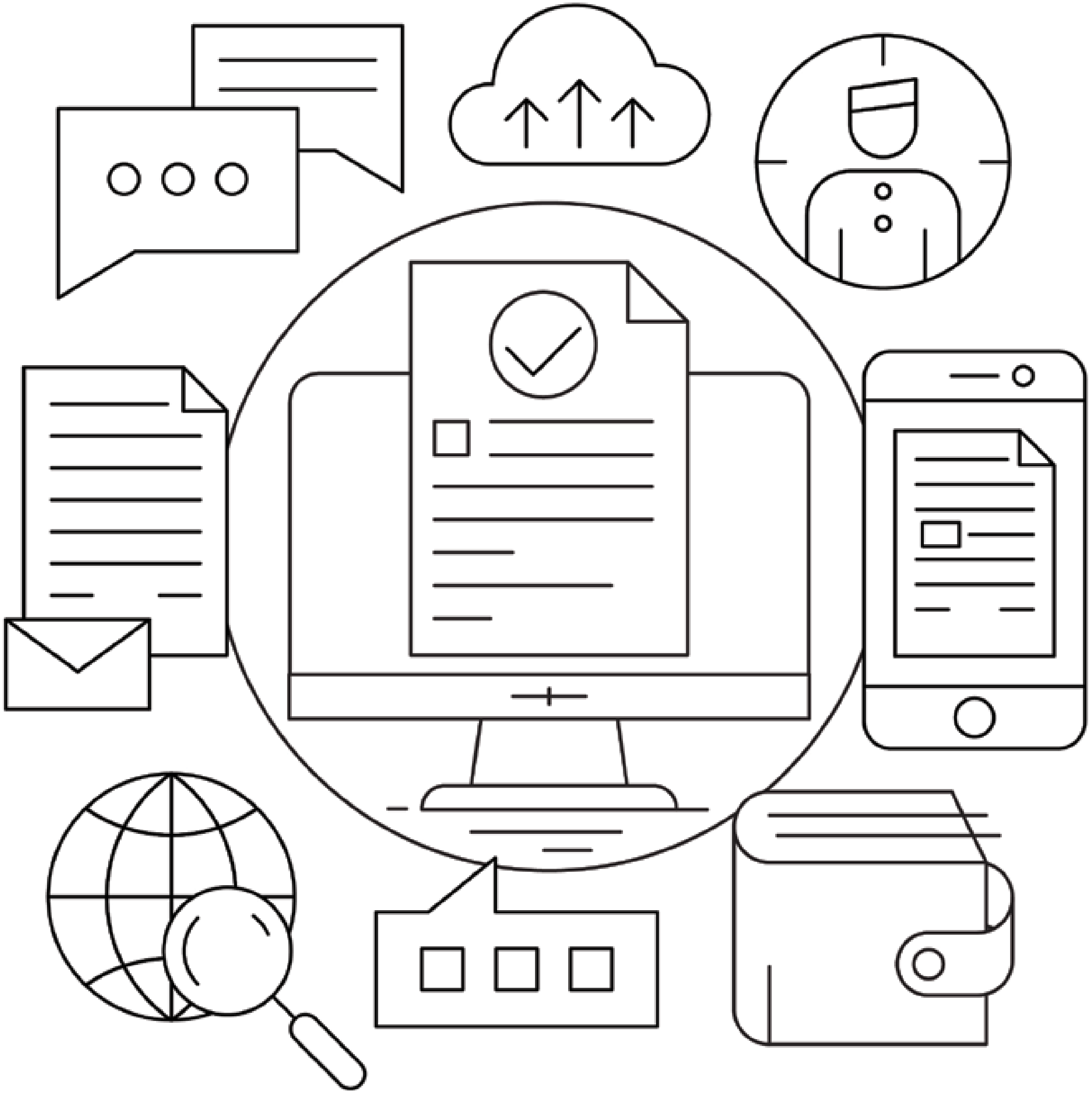
All the exercises and training in the booklet will be accompanied by general instructions on how to answer them. As for the training competitions, the trainer will provide guidance on how to solve them. The booklet also includes some non-classroom exercises, which the student will answer at home. These exercises will also be accompanied by trainer for the solving.

We kindly request your indirect supervision as the student interacts with this booklet. If the student has any question or inquiry about any of the exercises or training activities, please read the specific instructions for each exercise and provide assistance to student in light of these instructions.

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. The policy of content .... is a .... for securing computer systems and was developed to prevent .... or harmful software attacks 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 any content. From there, the user can review and classify errors, categorizing each item as either allowed or disallowed.

Exercise 3

Match each feature with its correct meaning:

Instruction

Read carefully the phrases in the first column of the table below, then match each phrase with its appropriate word from the second column.

Default-Source ○	●	Specifies the default list of sources for fetching other directives.
Child-Source ○	●	Defines the sources for nested browsing contexts, such as frames and workers, in the frame's whitelist.
Script-Source ○	●	Controls the loading of JavaScript on the website.
Object-Source ○	●	Specifies the allowed sources for <applet>, <embed>, and <object> elements.
Style-Source ○	●	Provides a list of valid sources for inline stylesheets, used for website layout and design.
Img-Source ○	●	Restricts content other than images on the website.
Frame-Source ○	●	Used to block frame loading on the website if desired.
Connect-Source ○	●	Specifies the allowed sources for <applet>, <embed>, and <object> elements.
Base-Url ○	●	Restricts the content other than images on the website.

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

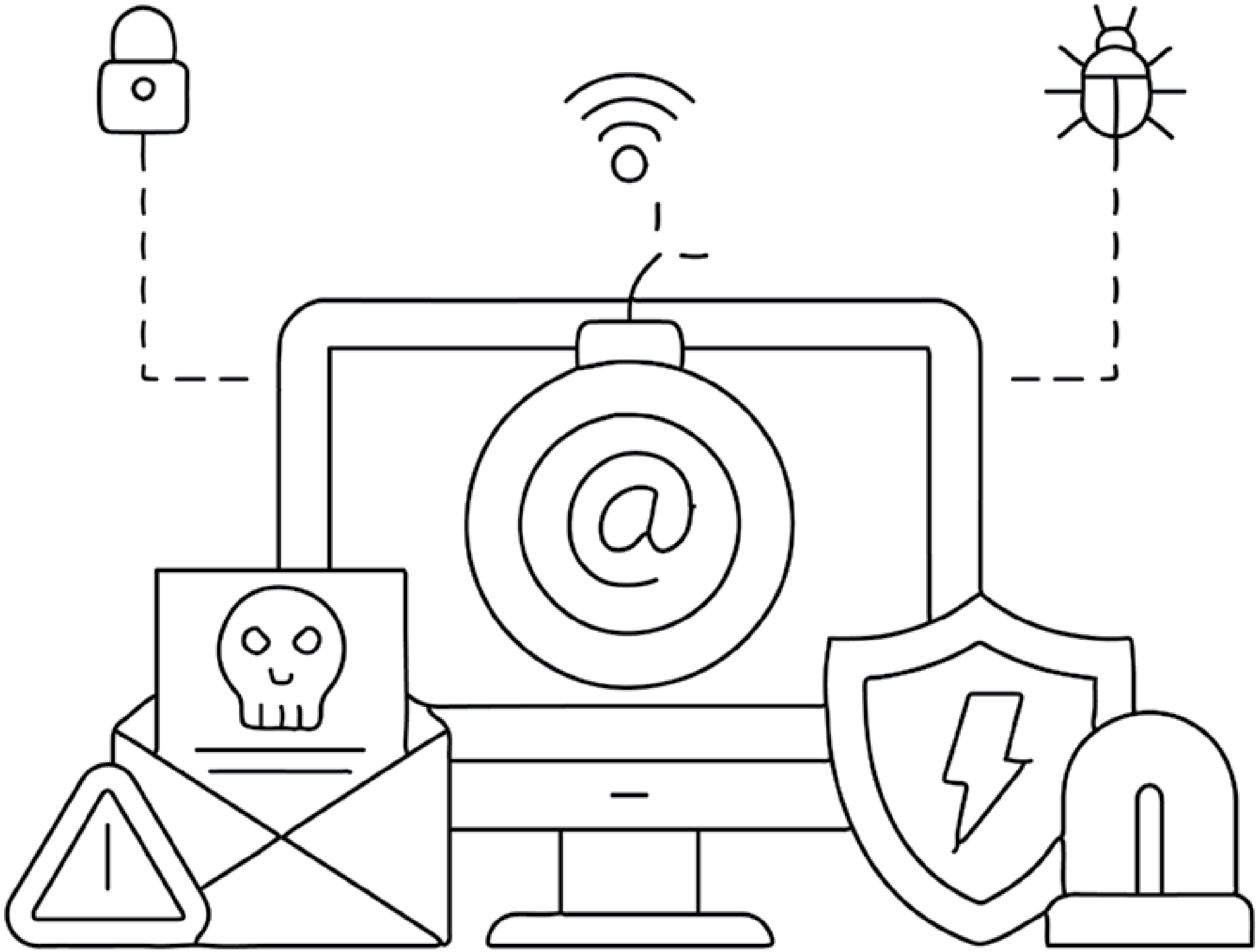
XSS attacks are a type of injection attack in which a cyber attacker injects malicious scripts into benign and trusted websites. The attack occurs when the attacker uses a web application to send malicious script instructions from the browser's side to the user.

Second: Non-classroom Exercises

Pay Attention!

Cross-Site Scripting (XSS) Attacks

XSS attacks are a type of injection attack in which a cyber attacker injects malicious scripts into benign and 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.



Risks of Cross-Site Scripting (XSS) Attacks:

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

Exercise 1

Mark (✓) or (✗)and correct the errors:

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!

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 .....?

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.

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.

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

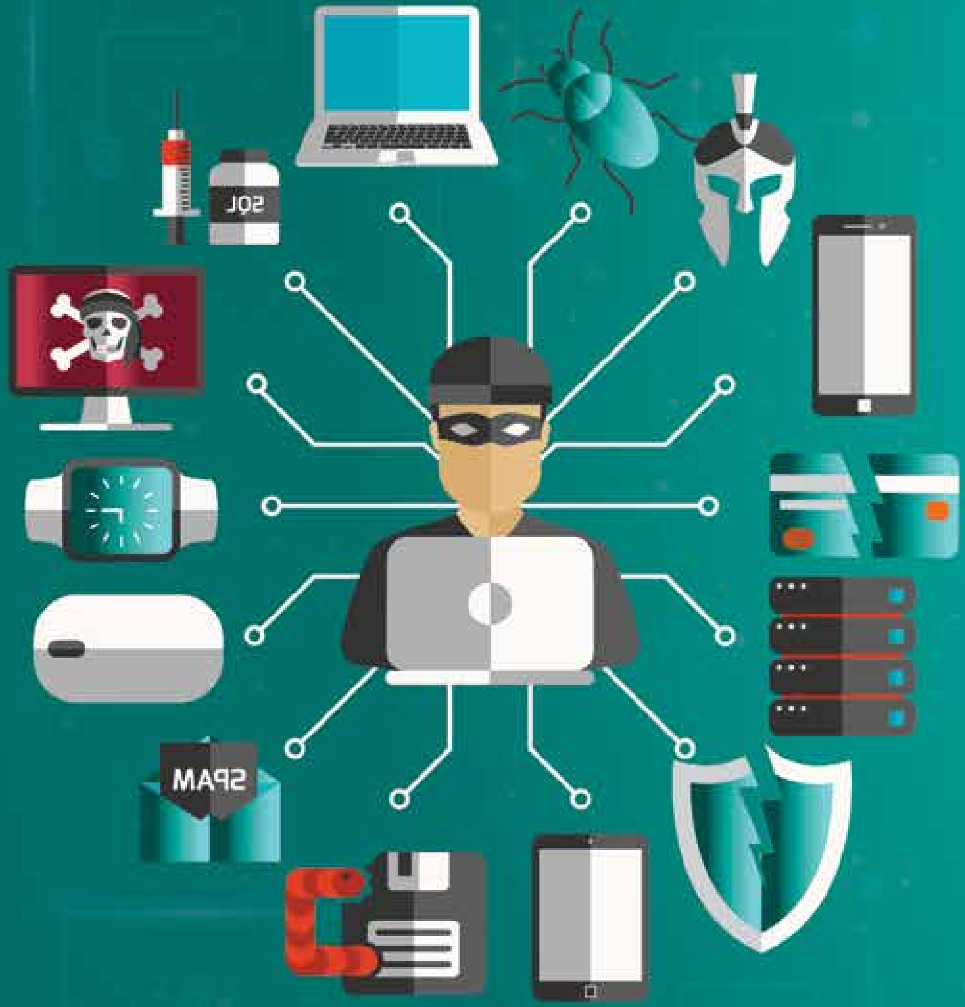
Pay Attention!

Internet Information Services (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.

Did you know that .....?

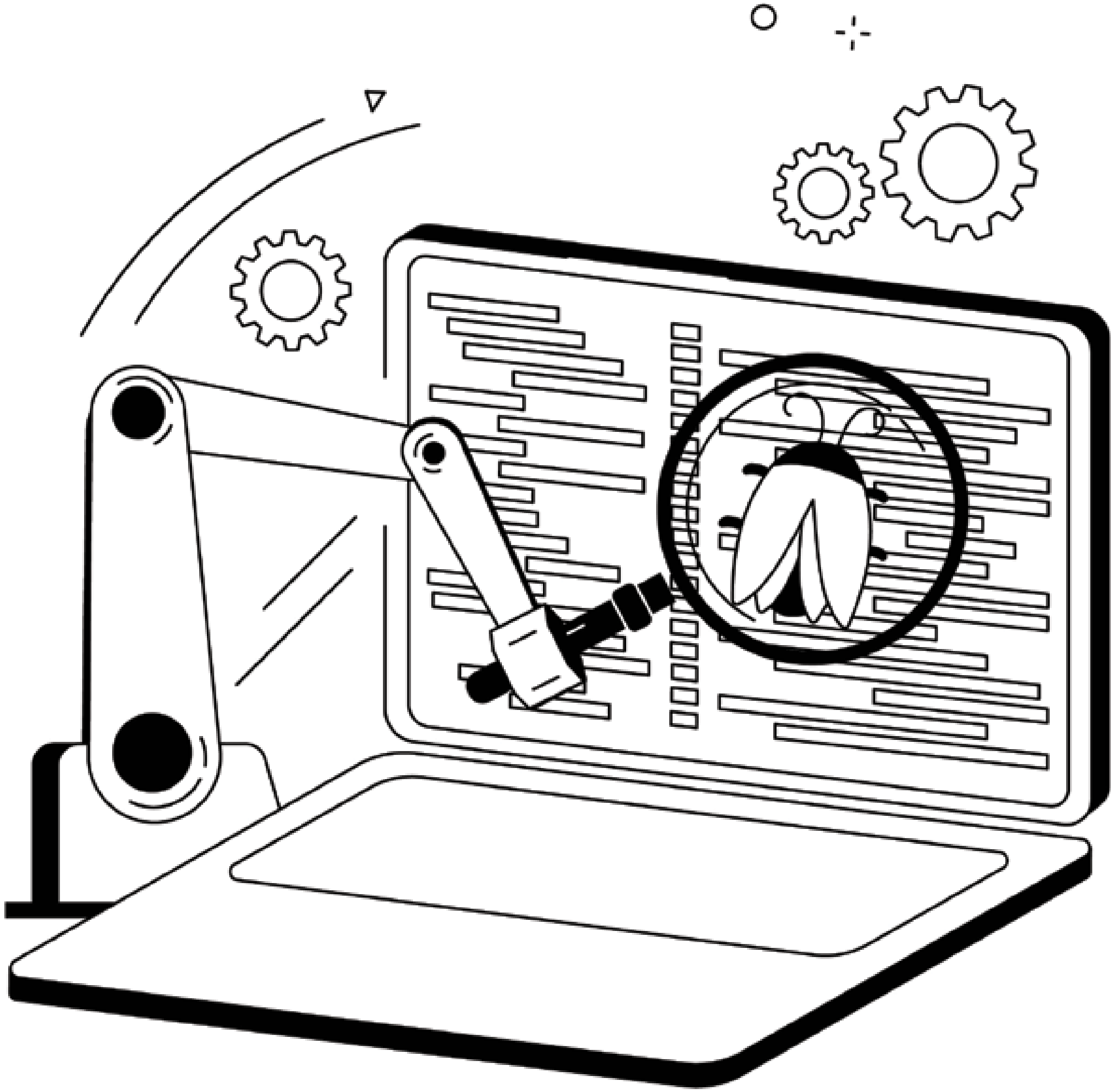
Content Security Policy (CSP) enables website owners to define their own rules that suit their website's needs while preventing unauthorized access to crucial information.



Pay Attention!

Packet Sniffing Attacks

Packet sniffing attacks involve intercepting unencrypted data packets transmitted over a computer network. Cyber attackers monitor network traffic with the aim of intercepting sensitive information such as financial details or login credentials to sell or use in further attacks.



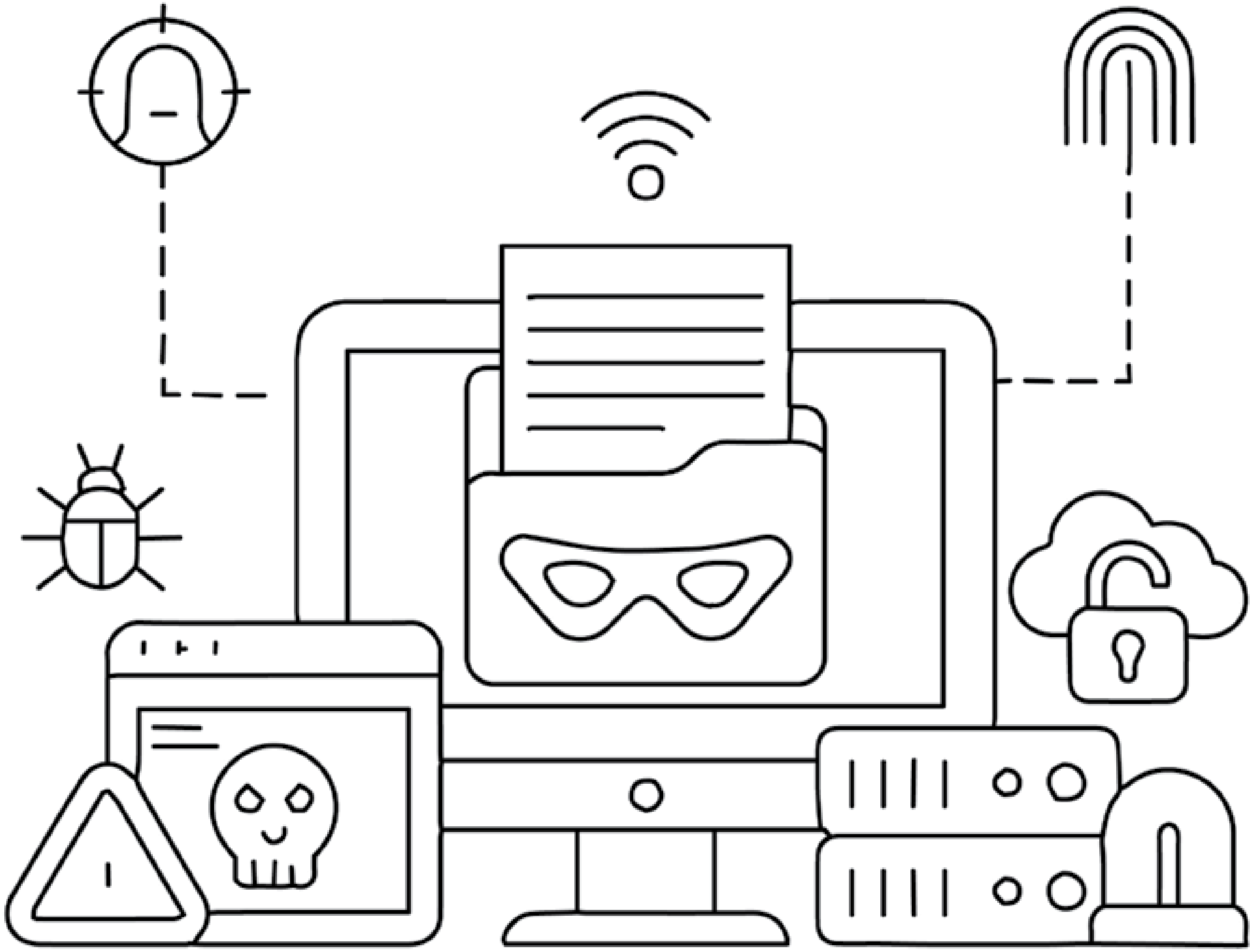
Content Security Policy (CSP) Implementation Steps:

A. Choose the web service provider for the website.

B. Add the Content Security Policy (CSP) to the HTTP response header of the website.

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

1. Using the browser, open the developer tools (use DevTools in Chrome), then navigate to the desired website and open the "Network" tab.
2. 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.
3. When clicking on the file, more information will appear, and here you start looking for the "200 OK" response code.
4. Below that, you will find the usage of Content Security Policy (CSP) or its absence.



To find the Content Security Policy, it is located in the HTML source:

1. Go to the page source, open the browser, and select the website.

2. Right-click on an empty area and choose "View Page Source."

3. Once the page source is displayed, search for the term "Content Security Policy" depending on the system. For Windows, press "Ctrl-F" on the keyboard and start searching for the term.

Competitions

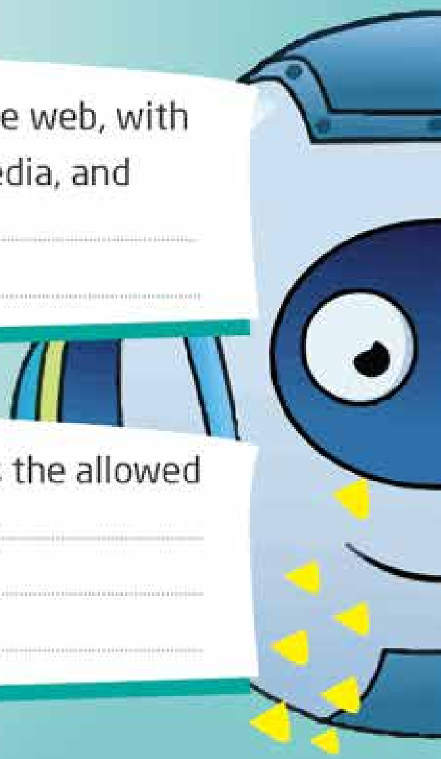
What is this?

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 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?

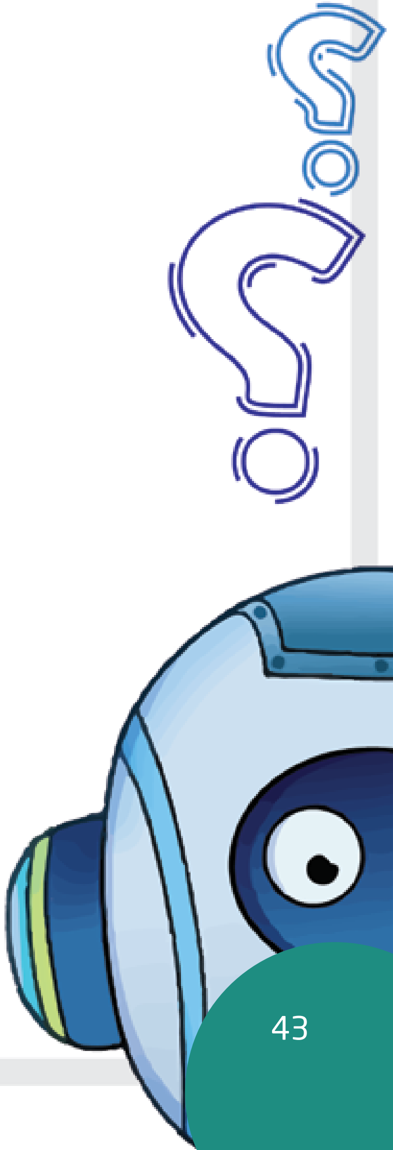
It refers to the storage of a script that is loaded onto target servers, such as in a database, visitor log, or comment field, and so on. The victim user then retrieves the malicious script from the server when requesting the stored text.

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 upgrade-insecure-requests directive instructs the browser to treat those URLs 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 that Google identifies as having malware.

- Internet users can receive warning notifications if their policy is violated, but without blocking content, by setting ………………. to 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.

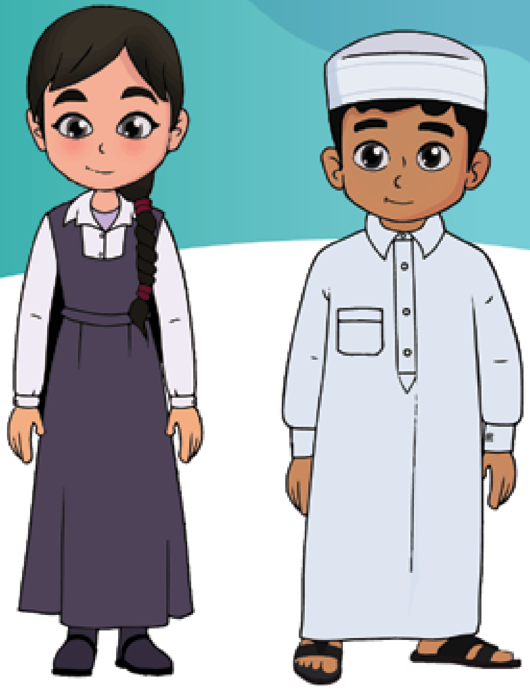
Cross-site scripting (XSS) attacks cause:

□ 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.

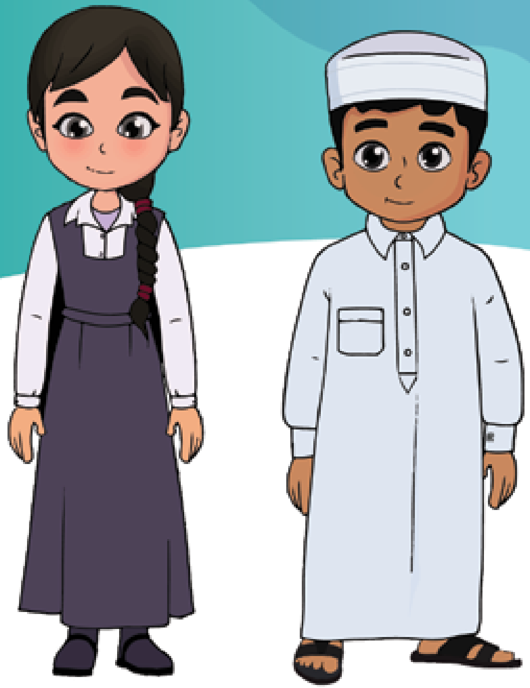
□ Reflected XSS attacks.

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.

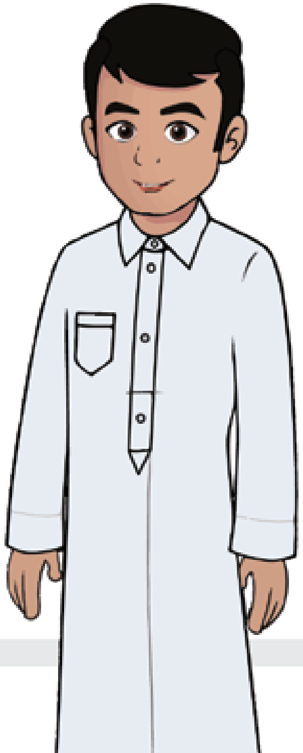
□ Transmission Control Protocol (TCP) session hijacking.

□ 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 parents, explaining what Content Security Policy is.



CyberEco

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency