Content Security Policy (CSP)

Training kit

Trainer's booklet

CyberEco

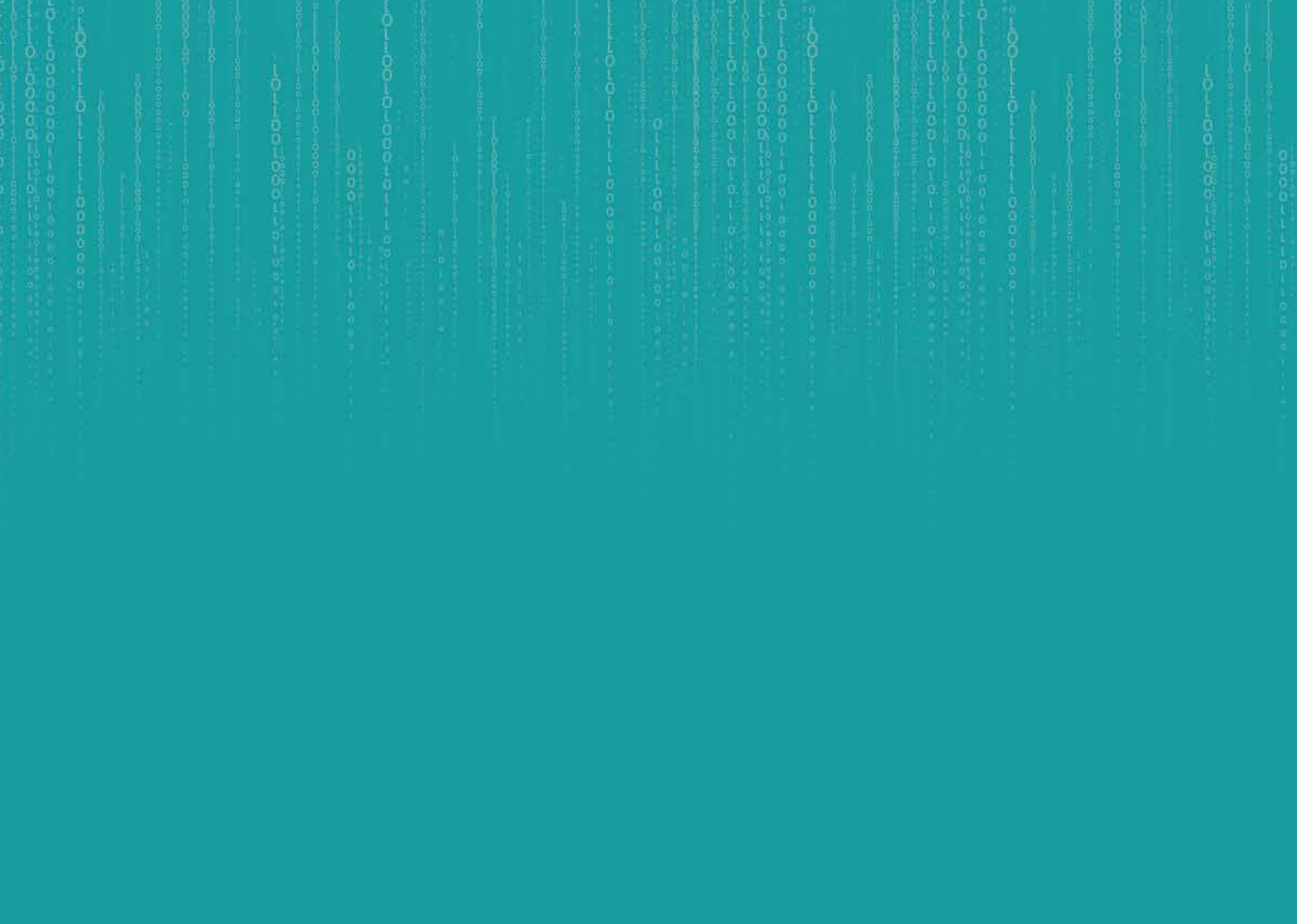
معًا لدعم السلامة الرقمية

Together to support digital safety

High School

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency



Content Security Policy (CSP)

High School

Training Kit

Trainer's booklet

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

General content of the Kit

First: General Introduction to the training kit

Second: Scientific content

First: General Introduction to the Training Kit

Below is an explanation of some details relevant to the objectives of the training kit, along with general guidelines for the trainer on how to handle this kit, while providing him with the scientific content that will be relied upon during the training.

General Idea

The concept of this training kit is to equip the trainer with tools and training resources, making it easier for him to deliver information to the trainees. In general, each training material consists of two parts: One part for the trainee and another for the trainer. The training kit serves as a general guide and support for the trainer, and its scientific content is the same as that of the trainee, but here the training content is presented differently. Additionally, the kit equips the trainer with training tools and methods that support him in the training process.

Objectives of the Training Kit

1. Providing the trainer with training tools that help him deliver the training content to the students.
2. To present information and training content in an easy and simple manner.
3. To offer training content on content security policy along with multiple training tools and methods.

Contents of the Training Kit

The training kit includes several training tools, as detailed below:

1. **Presentation files.**
2. **Training games,** such as shape coloring, drawings and crossword puzzles, which the trainer presents to the students to ensure their interaction with the training content.
3. **Educational videos.**
4. **Competitions,** Contests in the form of inferential questions presented by the trainer to encourage interaction between the students.
5. **Training cards,** comprising general information accompanied by illustrative images, presented by the teacher to the students.
6. **Sketches,** including information about the main topics in the training content.

Content of the Training Kit

WorkShop Timetable

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

Trainer's Guidance Manual

The following is an explanation of some general guidelines for the trainer, revolving around how to use this training kit:

1. The scientific content of the kit may exceed the student's ability to comprehend, especially in terms of general concepts. Therefore, the trainer must simplify these concepts and present them in a way that is understandable to high school students.
2. The trainer presents slides for each point discussed. For example, when talking about the concept of the Content security policy, the corresponding slide is presented, and the same applies to all scientific content.
3. During the explanation of the first chapter, specially designed images for the "Did you know that..?" section are distributed.
4. The trainer displays "Sketches" while the students solve the exercises.
5. At the end of the training, the mentioned competition questions are presented.
6. During the presentation of the scientific material for each chapter, a portion of the allocated time is used to present several links related to the content of the chapter.
7. The trainer displays some of the videos - mentioned in a separate file - to the students at the end of each chapter, or in the place he deems appropriate
8. It is encouraged to open a discussion with the students to hear their opinions.
9. Regarding exercises directed towards students; a file with exercises will be attached at the end of this kit. These exercises are divided into two parts: a part to be given to students during training, which are In-Classroom exercises, and the other part assigned for students to answer at home, which are Non-Classroom exercises. This division will be explained at the end of this kit.

Graduation Project

The graduation project is a task carried out by the student, aimed at achieving several goals, here is an explanation of the most important ones:

- Ensure that the student has absorbed the information and ideas presented and is capable of applying them in their daily life.
- Consolidate the information and ideas that were presented to the student.
- The project serves as a link between theoretical information and practical real-world application.

Regarding the mechanism for assigning students to the project, and how to implement it, the following guidance can be provided:

- The graduation project can be individual or group-based, in case of a group project; the number of students participating in one project should not exceed three students.
- The students choose the project topic, and the trainer can provide some assistance or ideas in this field.
- The topic of the graduation project must be consistent with the training content that was presented to the students.
- The graduation project can be within one of the following scenarios, which are non-binding concepts. The trainer can choose other concepts that he finds suitable. Here are some suggestions:

1. Writing a short story, report, or article in which the student explains the concept of content security policy.
2. The student takes on the role of the trainer and writes general guidelines to his colleagues or family members, explaining to them the concept of content security policy, and how to benefit from it.

Second: Scientific Content

Introduction

With the tremendous technological advancements in the world, web content has become more susceptible to hacking, theft, manipulation, and exploitation by cyber intruders. This has prompted companies to adopt a series of advanced technological mechanisms to mitigate cyber-attacks, which have become part of the lives of internet users who conduct their daily transactions, conversations, and communications online And so on.

One of the adopted technological mechanisms is known as Content Security Policy (CSP). It is a security mechanism for web browsers aimed at reducing electronic attacks such as Cross-Site Scripting (XSS) attacks. CSP works by restricting the content distributed on the internet, such as text and easily downloadable images, as well as limiting the possibility of hacking and theft.

XSS attacks, also known as script-based attacks, target textual and image content. They are web vulnerabilities that allow cyber attackers to exploit weaknesses in applications and software.

XSS attacks enable cyber intruders to deceive and impersonate victims, executing the same actions that regular users would take to access the targeted victims' data. For example, if the original user has access to applications, the intruder can gain full control over all the data and functions of those applications. This highlights the importance of Content Security Policy in protecting textual and image content from such cyber-attacks.

Chapter 1

Concept of Content Security Policy (CSP) and its Mechanism

- Concept of Content Security Policy (CSP)
- Operation Mechanism of Content Security Policy (CSP)

01

First: Concept of Content Security Policy (CSP)

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, data injection attacks that steal data, distort websites, and distribute malware. 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 malicious script instructions from the browser to the user(1).

The additional security layer provided by Content Security Policy (CSP) aims to mitigate XSS attacks and report them. This type of cyber attack exploits the browser's trust in content received from the server to initiate a malicious attack through the victim's browser. CSP enables server administrators to mitigate the potential damage caused by XSS attacks by specifying valid sources of executable scripts to the browser. Accordingly, a CSP-compliant browser executes only scripts received from allowed domains (2).

Content Security Policy also helps mitigate packet sniffing attacks, which are cyber attacks executed by intruders to intercept and monitor network traffic, targeting unencrypted email messages, login credentials, and financial information. These policies restrict the domains from which content can be loaded by specifying the server's allowed protocols. For example, a server can enforce loading all content using HTTPS. This not only includes data transmission but also extends to marking all cookies with the secure attribute and providing automatic redirection from HTTP pages to HTTPS pages to ensure encrypted connections with browsers(3). Properly designing Content Security Policy contributes to protecting web pages from XSS attacks and other cyber attacks.

The term "policy" refers to a set of policy directives that describe the user's web content security. There are different directives for

1. Content Security Policy (CSP). On site: https://cutt.us/7Dcv2.
2. Content Security Policy in Cybersecurity. On site: https://cutt.us/QBfJJ.
3. What are inhalation attacks and how can they be prevented? On site: https://cutt.us/NzcrB

various types of elements, meaning each type has its own policy, including fonts, images, audio and video media, and scripts. Content Security Policy directives are defined in HTTP response headers called CSP headers, and their purpose is to guide the browser to trusted content sources. They also include a list of sources that should be blocked from access.

There are several categories that fall under Content Security Policy (CSP) directives, which vary depending on the usage and content characteristics. They are as follows:

1. **Fetch directives:** These directives specify the sites from which specific types of content are allowed to be loaded. **They include the following:**

- **Child-Source:** Responsible for specifying the sources of script content included in the browsing context's whitelist, including frames and web workers.
- **Connect- Source:** Responsible for specifying the URL addresses that can be loaded using script content.
- **Default- Source:** The fallback directive for all fetch directives, which defines the default list of 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 cascading style sheets (CSS), which define the appearance and design of web pages.

2. **Document directives:** These directives help control the environment (document) properties **and include:**

- **Sandbox:** Protects a specific resource similar to inline script elements.
- **Base-uri:** Specifies the allowed URL addresses in the document's base element.

3. **Navigation directives:** These directives control the document's navigation, including its origins. They include:

- **Frame-ancestors:** Specifies the origins that can embed the document as a frame.
- **Form-action:** Defines the URL addresses to which form submission is allowed.

4. **Reporting directives:** These directives are responsible for documenting and reporting violations of the CSP **and include**

1. **Report-to:** Initiates the process of reporting CSP violations.
2. **Report-uri:** Directs the user agent to report any attempts to violate the CSP specifications.
3. **Require-sri-for:** Enforces the use of Sub resource Integrity (SRI) for style and script sources on the page.
4. **Trusted-types:** Specifies a list of non-bypassable trusted values to mitigate XSS attacks.
5. **Require-trusted-types-for:** Imposes a trusted types policy on script content.
6. **Upgrade-insecure-requests:** Some websites may contain insecure, outdated URL addresses. This directive guides the browser to handle those addresses and replace them with more secure HTTPS equivalents[1].

1. Content Security Policy Reference. On site: https://cutt.us/xko67.

second: Content Security Policy (CSP) Mechanism

The best way to retroactively add a Content Security Policy (CSP) to an entire website is to start with an empty whitelist, blocking everything. Initially, the CSP should be set to report-only mode, allowing the browser to evaluate the rules before blocking content. This allows the user to review errors and categorize them as either allowed or disallowed.

When a browser loads a page that includes a Content Security Policy, it verifies the CSP to ensure that the content is allowed. If the content is not allowed, the browser blocks it and displays an error message. This process helps prevent attackers from injecting malicious code into the page, thus protecting web users from malicious attacks. Additionally, the CSP helps protect the user's website from being flagged by search engines like Google for hosting malicious software.

This can impact the number of visits, customers, brand reputation, and profits. It's important to note that CSP does not provide comprehensive protection for websites, so it is necessary to regularly scan websites for any security threats[1].

To implement a Content Security Policy (CSP), there are several steps:

A. Choose the website's CSP provider:

The directives included in a Content Security Policy can vary, so it is recommended to customize the policy to meet the specific needs of each user or application. To do this, create a list of directives (or policies) to specify the resources that are allowed or disallowed on your website.

1. Using Content Security Policy (CSP) to Secure Web Applications. On site: https://cutt.us/fuMF9.

Some specialized Content Security Policy (CSP) service providers for common website security scenarios include:

- If you want to block the loading of iframes on your website, use the frame- Source directive. The format would be: Content-Security-Policy: Frame- Source 'none'. Make sure to separate multiple directives with a semicolon when creating the CSP.
- To prevent the loading of JavaScript on your website, use the Script- Source directive. The format would be: Content-Security-Policy: Script- Source 'none'.
- To restrict content other than images on user-specific websites, use the Img- Source directive. The format would be: Content-Security-Policy: Default- Source 'self'; Img- Source.

It is important to emphasize the significance of setting the default source to either "self" or "none" and explicitly including the allowed resources to avoid defaulting to all images, as the word "self" does not include any subdomains.

To allow only content from the same source, the user's own website, and its subdomains, use .default-src. The format would be: Content-Security-Policy: default-src 'self' *.sucuri.net;.

To only allow other executable media or scriptable programs from the same source, use the following format: Content-Security-Policy: default-src 'self'; img-src *; media-src sucuri.net; script-src sucuri.net.

It is important to test the user's CSP before implementation to ensure that no trusted origin for the website is overlooked[1].

Internet users can receive alert notifications if their policy is violated without content blocking by setting the HTTP response header to report-only mode for the Content Security Policy.

1. How to Set Up a Content Security Policy (CSP) in 3 Steps. On site: https://cutt.us/e92IS.

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

Most modifications to the HTTP response header are done on the user's web server. To set up the HTTP response header, it is necessary to first identify the user's web server. To determine the server hosting a 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[1].

In summary, there are several available options to accomplish this:

1. Setting up Content Security Policy (CSP) using IIS (Internet Information Services):

IIS (Internet Information Services) is a web server from Microsoft that runs on the Windows operating system. It is used to serve static and dynamic web content to internet users and can also be used to host and manage web applications.

2. Set up your CSP using Apache:

Apache is a web server responsible for accepting HTTP directory requests from internet users and sending the requested information to them in the form of web files and pages.

3. Implementing Content Security Policy

Content Security Policy policies are enforced through a specific HTTP header sent with the response from the server. This header includes the rules of the policies that will be subsequently enforced by the browser. **There are two ways to do this:**

- Adding Content Security Policy to the website through meta tags to work across all browsers. If access rights to configure the user's web server are not available, an HTML tag can be used to enable the Content Security Policy within the HTML of the page.
- Setting up the user's specific policies through the HTTP response header. This method is supported by most browsers, except for Internet Explorer and some older versions of browsers[2].

1. cPanel. On site: https://cpanel.net/
2. Content Security Policy (CSP). On site: https://cutt.us/Sdgpu.

Chapter 2

How to Enable Content Security Policy (CSP) and Digital Risks Mitigated by it.

- First: How to Enable Content Security Policy
- Second: Digital Risks Mitigated by Content Security Policy

02

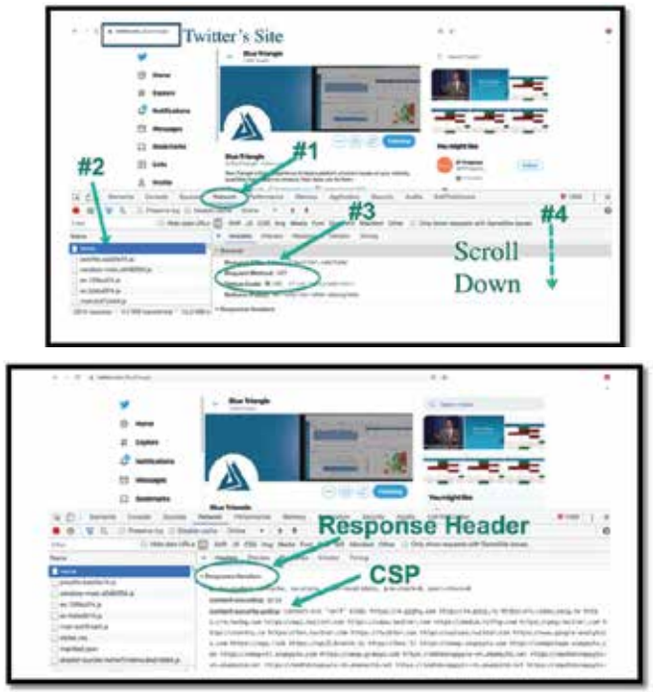
First: How to Enable Content Security Policy (CSP)

Content Security Policy is the best method for protecting against malicious attacks launched by cybercriminals against internet users. The good news is that users can ensure the presence and activation of these policies on their website. There are two places where you can find providers that enable these directive policies: response headers and meta tags.

To find Content Security Policy in response headers, follow these steps:

1. Using your browser, open the developer tools (use DevTools in Chrome) and navigate to the desired website. Open the "Network" tab.
2. Look for the file that creates the webpage, which usually has the same domain as the website you are browsing. It is typically the first item in the "Network" tab.
3. When you click on the file, more information will appear, and you start searching for the 200 OK response code.
4. At the bottom, you will see whether Content Security Policy is being used or not[1]

Example: Applying these steps to X platform.



1. How to find out if a Site has a Content Security Policy (CSP) deployed. On site: https://cutt.us/G1EJs.

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

1. Go to the page source and open it in the browser by selecting the website.
2. Right-click on a blank area and choose "View Page Source."
3. Once the page source is displayed, search for the term "Content Security Policy" using the search function (Ctrl-F) in Windows.

Free Tools to Help Create, Evaluate, and Monitor Content Security Policy (CSP):

1. The w3af Audit Tools include an additional component for automatically auditing web applications to ensure the activation of CSP.
2. CSP Tester (Browser Extension) is used to build and test the CSP policy for the user's website application.
3. CSP Generator is a tool that automatically generates CSP policies (Chrome/Firefox extension).
4. CSP Evaluator evaluates the current Content Security Policy policies.
5. Csper Report Aggregation Tool is used for monitoring Content Security Policy using a reporting URI[1].

1. Content Security Policy. On site: https://cutt.us/A9Mnj.

Second: Digital Risks Mitigated by Content Security Policy (CSP)

Content Security Policy (CSP) policies can help prevent cyber attacks, such as Cross-Site Scripting (XSS) attacks. They assist website owners in identifying safe and unsafe resources, and these policies also enable website owners to customize their own rules to fit their site›s needs. Additionally, CSP policies restrict unauthorized access to sensitive information and provide tools for configuring reports and conducting analyses that identify security vulnerabilities after implementing CSP.

The attacks mitigated by these policies include:

- Cross-Site Scripting (XSS) Attacks

Cross-Site Scripting (XSS) attacks are a type of injection attack where 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.

This attack involves deception, as the malicious script appears to come from a trusted source. Consequently, the malicious script can access any stored cookies or sensitive information held by the browser and manipulate the content of an HTML page[1].

XSS attacks can be categorized as follows:

1. 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 user input as part of the request. The delivered XSS attacks reach victims through another means, such as an email or other websites. When the user clicks on the malicious links or browses the compromised website, the injected script is returned to the vulnerable web server, thereby reflecting the attack back to the user's browser. The browser then executes the script, assuming it came from a "trusted" server, falling for the deception.

1. Types of Cross-Site Scripting (XSS) Attacks. On site: https://cutt.us/ySnS4.

2. Stored XSS Attacks:

Stored XSS attacks involve permanently storing a malicious script on targeted servers, such as in a database, visitor log, comment field, etc. Subsequently, the victim user retrieves the stored malicious script when accessing the stored text.

3. Blind XSS Attacks:

Blind XSS attacks are a form of persistent XSS attacks. They occur when the attacker stores the payload on the server and delivers it back to the victim. For example, in "data forms," the attacker sends malicious scripts, and when the user opens the form, the script starts executing.

XSS attacks pose several problems for victim users, including:

- Complete account compromise.
- Installation of Trojan horses.
- User redirection to other pages or websites.
- Modification of content display.
- Alteration of press releases or news affecting stock prices, leading to decreased consumer trust[1].

1. Cross Site Scripting (XSS). On site: https://cutt.us/DyAza.

Packet sniffing attack

Packet sniffing attack is defined as a method of hacking that involves capturing data packets that are transmitted over an unencrypted computer network. Cyber attackers monitor the data packets in network traffic with the aim of intercepting sensitive information such as financial details or login credentials, either for sale or for use in other attacks, this attack falls under the category of espionage attacks that work well on unencrypted networks[1].

There are two types of packet sniffing attacks:

1. Active packet sniffing:

This type of attack is used in larger networks where multiple devices are connected to a single network. As more devices connect to a network, the need for a network switch arises. The network switch directs internet traffic to its intended destinations to prevent traffic congestion on connected devices.

In the case of active packet sniffing, the attacker introduces additional traffic into the targeted network and waits for the network switch to redirect legitimate traffic. This allows the cyber attacker to access the network switch and initiate their attack. Active packet sniffing

is more detectable as it requires the attacker to announce itself in order to start sniffing[1]

2. Passive packet sniffing:

This attack is executed in smaller networks where all devices are connected to a single network hub. In this case, the attack does not rely on network switches to direct traffic, and it does not need to announce itself. Consequently, it becomes more difficult to detect these attackers.

Methods of executing a packet sniffing attack

Cyber attackers targeting specific areas of a network, device ports, or websites employ various methods to monitor network traffic. The following are the most significant methods:

1. Password sniffing:

Attackers quietly collect data packets containing passwords and other login information. However, legitimate websites that use HTTPS encryption provide security for passwords. As a result, attackers resort to man-in-the-middle attacks, which are a type of network hijacking attacks used to gather password data.

2. DNS forgery:

This is a type of deceptive attack that uses packet sniffing to redirect internet traffic to a malicious website.

3. JavaScript sniffing:

JavaScript sniffing, also known as formjacking, occurs when attackers inject malicious code at the point of purchase on e-commerce websites. These JavaScript programs resemble electronic skimmers used to collect financial information.

4. Address Resolution Protocol (ARP) spoofing:

This occurs when an attacker impersonates the IP address of a host or device on a local network, causing traffic to be redirected to the attacker instead of the correct destination.

5. TCP session Hacking:

By exploiting a TCP session between a sender and receiver, the attacker can intercept and sniff network traffic containing reliable data[2].

1. What is a packet sniffing attack? A cybersecurity guides. On site: https://cutt.us/Kbz3p.
2. The Effective Guide to Creating a Content Security Policy. On site: https://cutt.us/Pjrxe.

When is it recommended to use Content Security Policy (CSP)?

It is recommended to use 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.

However, static applications without any functionality or login cookies do not require the use of CSP. Similarly, large applications with a history of XSS attacks can benefit from CSP as an additional security mechanism, but the primary focus should be on implementing secure coding practices to protect against cyber attacks[1].

It is important to note that CSP policies are not effective if a policy allows for embedded scripts or allows the loading of scripts from untrusted domains, as it does not protect against XSS attacks.

1. Content Security Policy. On site: https://cutt.us/FujwG.

Exercices and Trainings

Exercises are a major part of the training process, and they achieve several goals and aims, as follow:

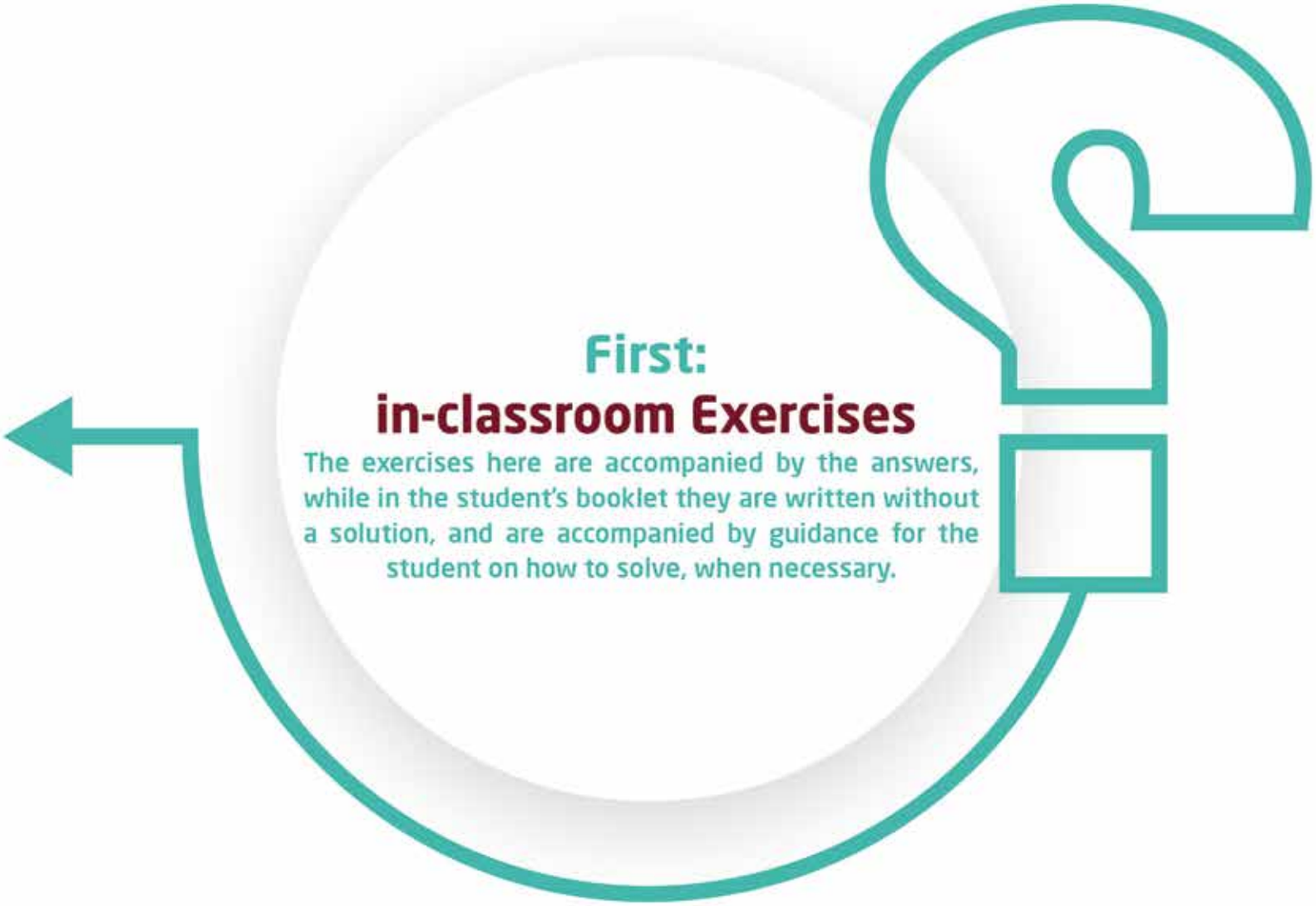
- Exercises are an effective tool to assess students' utilization of the training content and its impact on their cognitive inventory.
- They serve as a vital means to reinforce information and knowledge, constituting a rapid review of the training content.
- They help to identify knowledge gaps among students.
- They act as a form of feedback for the trainer, providing information on the effectiveness of the training kit and the training method.

Approach to Dealing with Exercises

The exercises mentioned in this section are comprehensive of the training content in this kit, here's an outline of the proposed methodology for dealing with them:

- During the training, after introducing an idea, the trainer will request students to open their respective booklet and answer the specific question, directly related to the presented idea or subject.
- The exercises are carefully selected to be simple, easily understood, and solvable by high school students. The trainer may offer support to students in answering some exercises if necessary, at their discretion.
- The exercises are divided into two parts; one for in-cassroom use, called classroom exercises, and another is non-classroom, to be completed at home by the students.
- The answers for each exercise are provided, highlighted in a different color.

Below is an explanation of exercises specific to high school students, arranged according to chapters and classified as in-classroom and homework exercises (Non-classroom Exercises). These exercises, in the form presented here, are the same as those in the students' booklet.



First:
in-classroom Exercises

The exercises here are accompanied by the answers, while in the student's booklet they are written without a solution, and are accompanied by guidance for the student on how to solve, when necessary.

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 ...**security**.... is a ...**mechanism** .... for securing computer systems and was developed to prevent ....**scripts** ....or malware ....**attacks**.... through websites.

2. ...**Cross-Site Scripting (XSS)** .... attacks are a type of malicious and harmful code in untrusted ...**websites**..., often used to attack ...**e-commerce** .... sites.

3. The..**content** .. security policy (CSP) can be specified in the HTTP response header When the web client requests.

4. CSP stands for "...**Content Security Policy**..." in English.

5. Content .....**security** .... policy is very important for owners of ...**e-commerce** .... 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 malware attacks.

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 cyber 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!

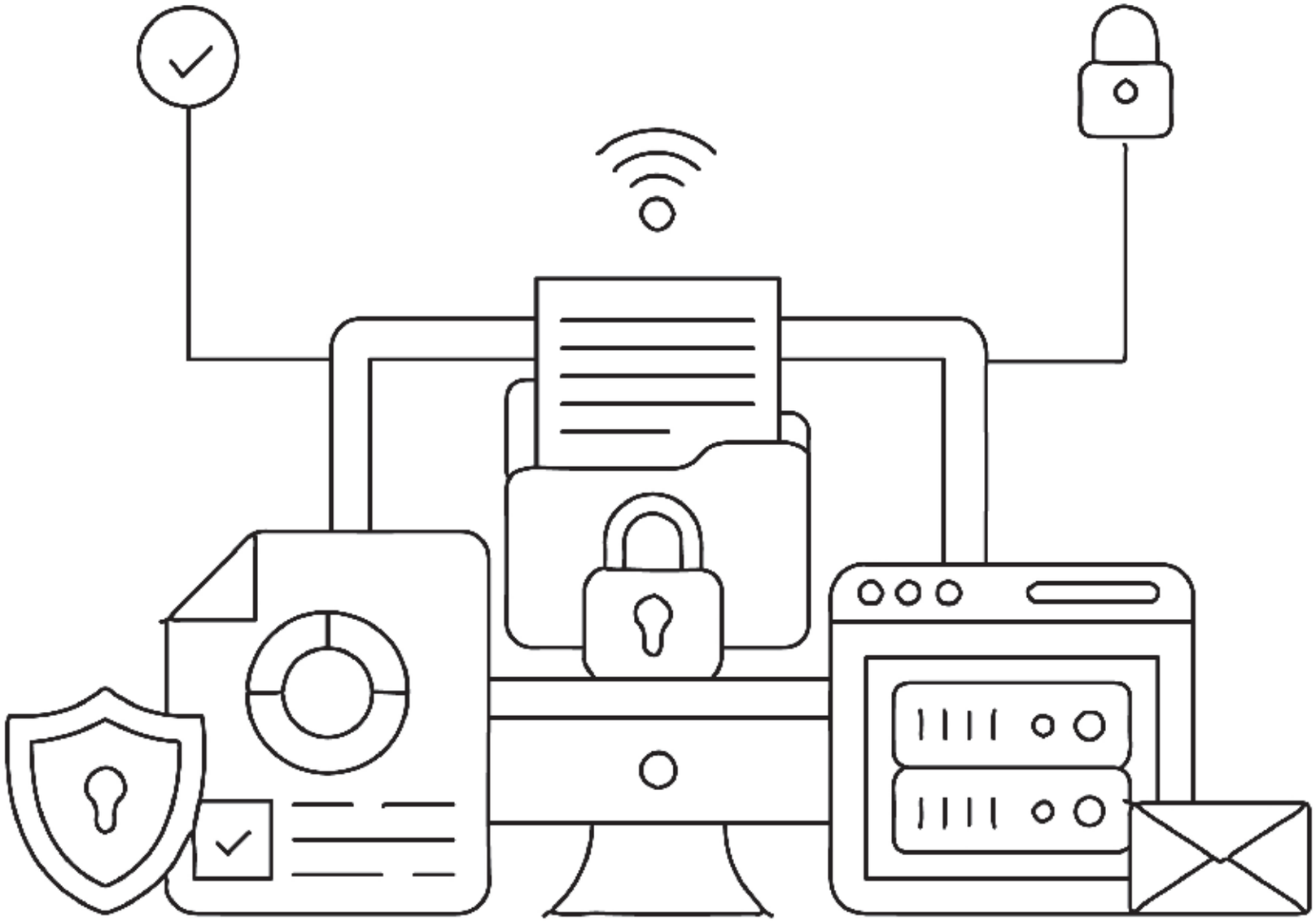
The best way to add Content Security Policy (CSP) with retroactive effect to an entire website

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:

Default-Source	Backup guidance for all habeas corpus directives, identifying list of default sources for other fetch directions.
Child-Source	This directive is responsible for identifying the sources of the scripts included in the white list of the browsing route included in the frames and web workers.
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, It means: web page format language, which is concerned with the format and design of websites
Img-Source	Restricts content other than images on the website.
Frame-Source	it is used in case of wanting to prevent the loading of frames on the website.
Connect-Source	This directive is responsible for determining which URLs are uploaded using scripts.
Base-Url	Specifies the permitted URL addresses in the core element of the document.



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

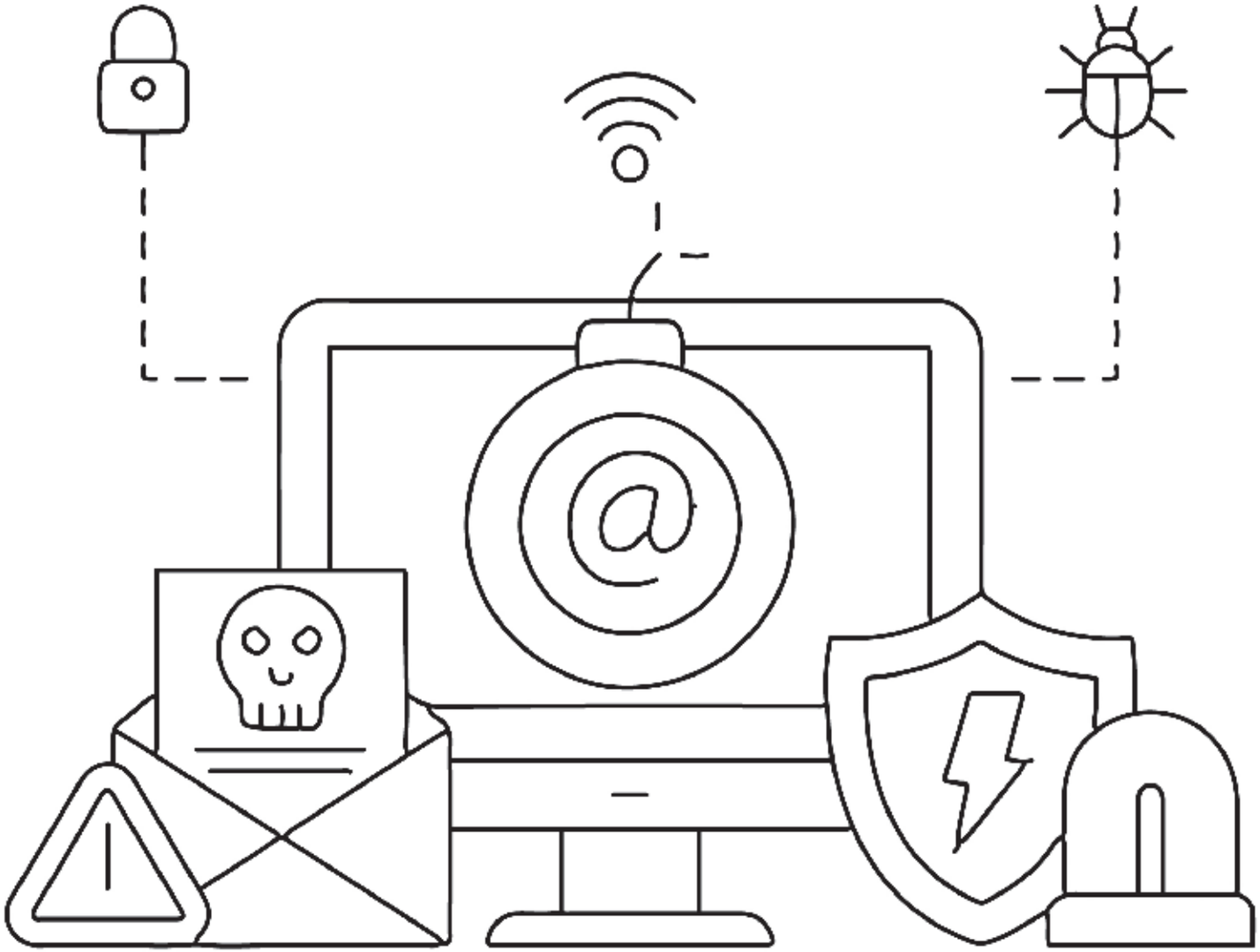
XSS attacks are a type of injection attack in which a cyber attacker injects malicious scripts into being and trusted websites. The attack occurs when the attacker uses a web application to send malicious script instructions from the browser's side to the user.


Second:
Non-classroom
Exercises

Pay Attention!

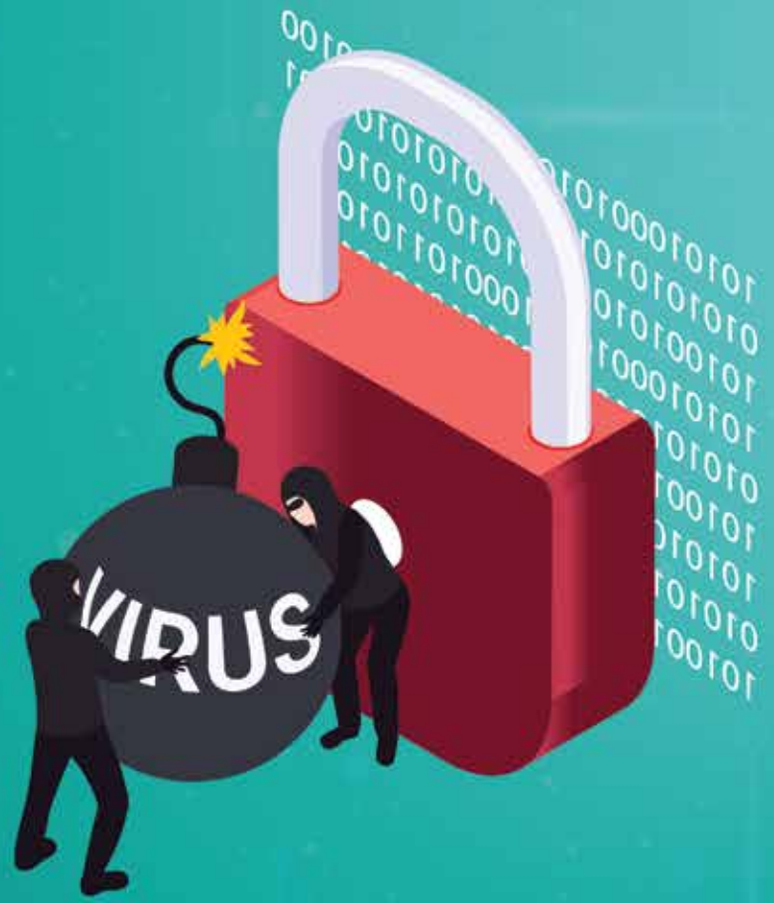
Stored XSS Attacks

These refer to the permanent storage of a malicious script on targeted servers, such as in a database, visitor log, comment field, etc. Subsequently, the victim user retrieves the malicious script from the server when accessing the stored text.



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.
- Manipulation of financial reports issued and published by institutions on their websites.



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.

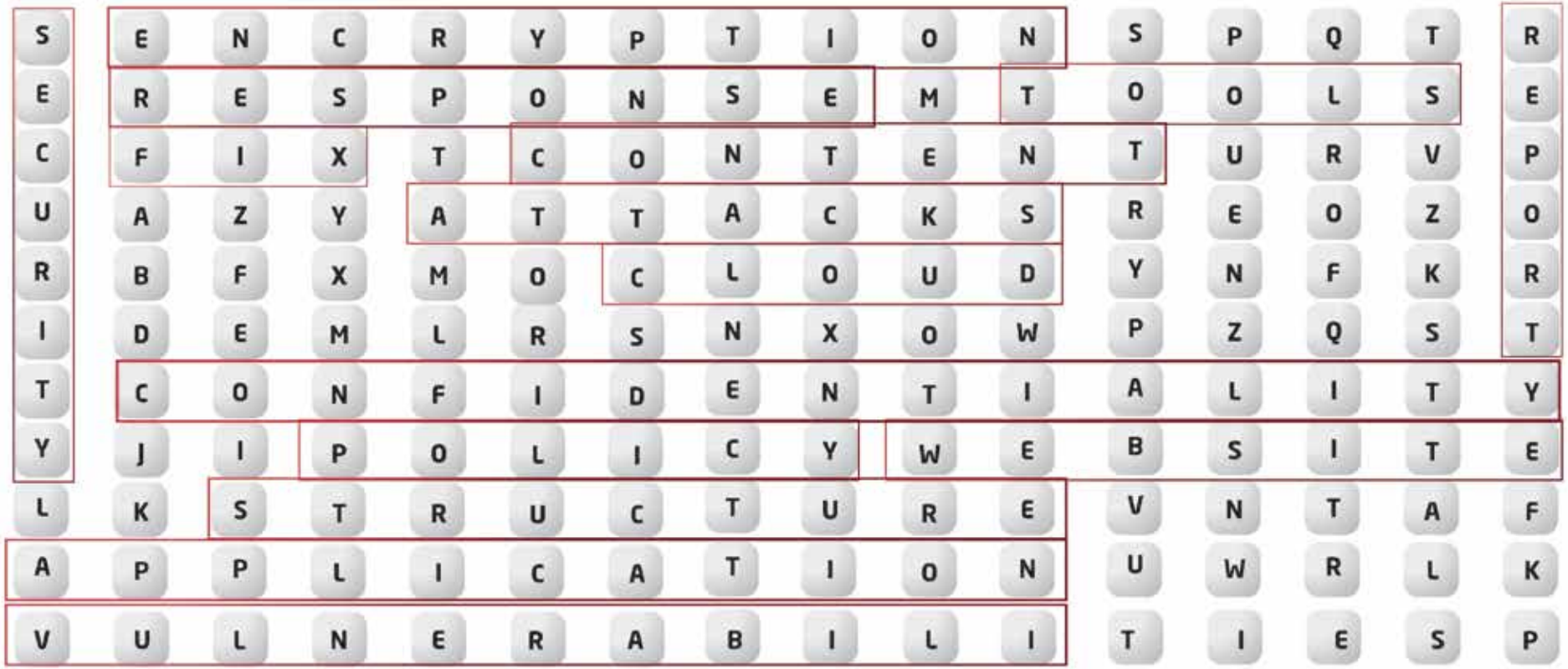
Pay Attention!

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



Application - Security - Cloud - Encryption - Fix - Response - Structure - Vulnerabilities

Policy - Content - Website - Confidentiality - Attacks - Report - 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.

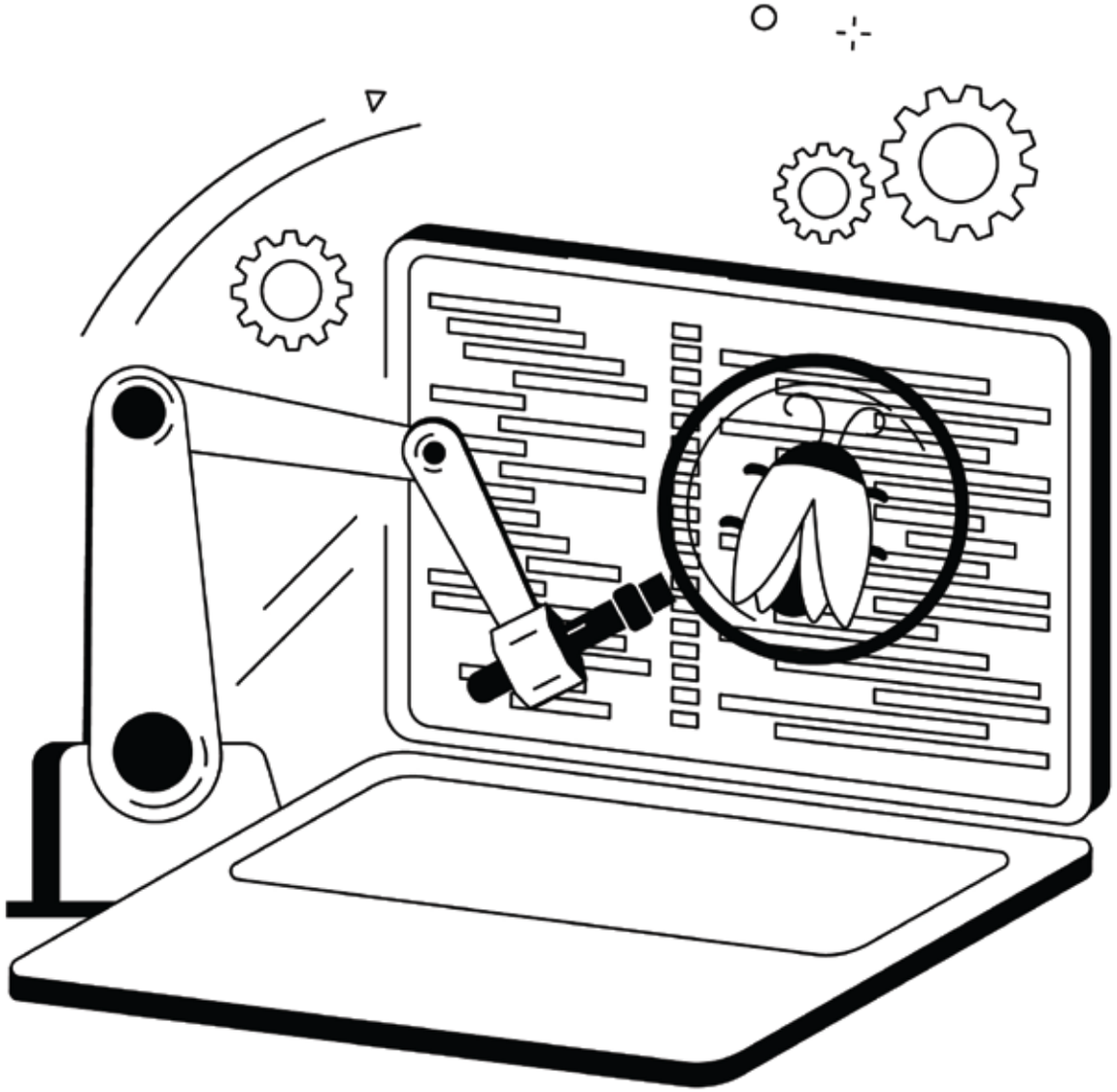
Did you know that .....?

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.

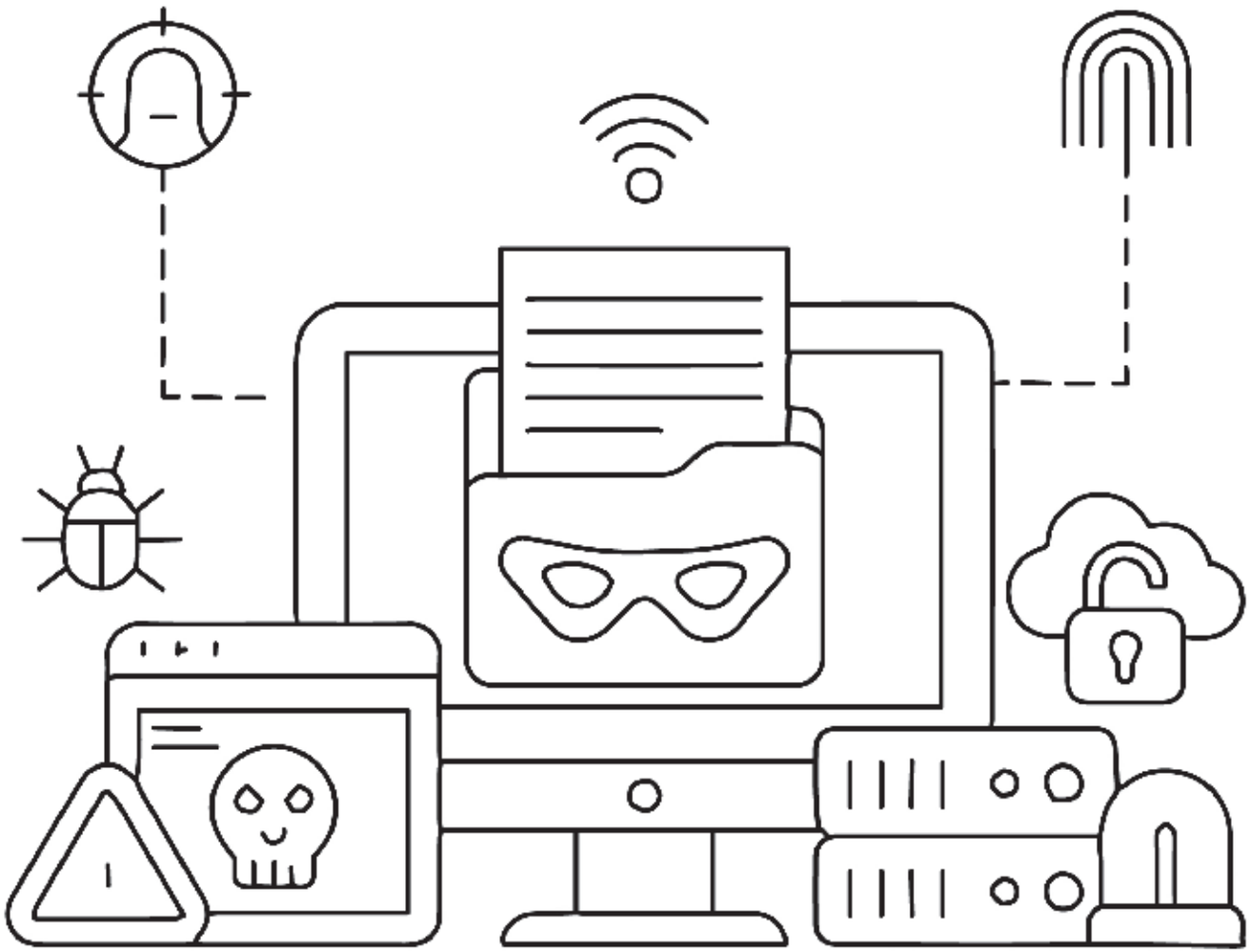
To find the Content Security Policy in the response headers, you can follow the following steps:

Using the browser, open the developer tools (use DevTools in Chrome), then navigate to the desired website and open the "Network" tab.

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.

When clicking on the file, more information will appear, and here you start looking for the "200 OK" response code.

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

Content Security Policy (CSP)

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

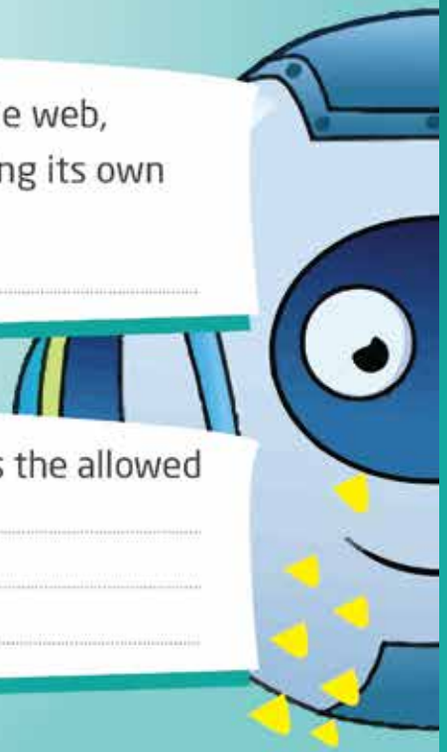
Packet sniffing attacks.

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

Policies

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

picking up directives



What is this?

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

content Security Policy sandbox directive.

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.

Internet information services (IIS) Manager.

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

Apache.

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

Response headers and meta tags.

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.

Stores XSS attacks.

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 malware, and as soon as the user opens the form, the execution begins

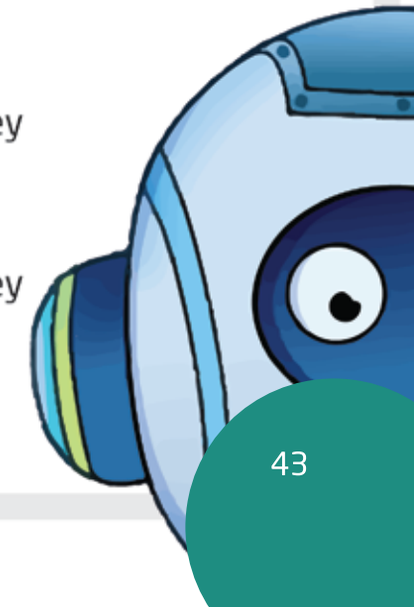
Blind XSS.

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.

Packet sniffing attacks.

Complete the following sentences:

- The additional security layer provided by Content Security Policy (CSP) aims to...**Mitigate cross-site scripting (XSS) attacks and report them**.... .
- Content Security Policy (CSP) allows server administrators to mitigate the damage that can be caused by an XSS attack by.....**Specifying valid executable script sources to the browser**.....
- One of the functions that Content Security Policy also performs is to limit ....**Packet sniffing attacks**.... , which are cyberattacks carried out by attackers to intercept and monitor network traffic.
- Content Security Policy directives are defined in ....**HTTP response headers**....., 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.
- directives help to control the properties of the working environment (document), and they include: ...**security policies**....., and....**base-uri**....
- Reporting directives are responsible for documenting and reporting violations of CSP, and they include: ...**report-to**...., and.....**report-uri**.....



- Some websites may contain old, insecure URLs, so the upgrade-insecure-requests directive instructs the browser to treat those URLs as HTTPS. **insecure upgrade requests**

- The best way to add CSP retroactively to an entire website is to specify ..**an empty whitelist**.., to block everything.

- CSP helps to protect a user's site from being placed in ...**the blacklist**..., 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 ..**HTTP response headers**.. 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.

- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] JavaScript sniffing.
- [ ] Man-in-the-middle.

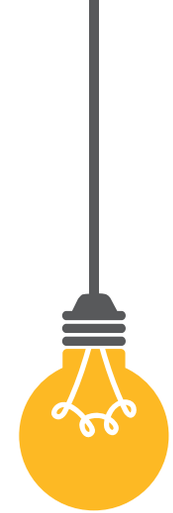
6. Once a connection is established between the sender and the receiver, the attacker hacks in and transfers the trusted data, sniffing the network traffic .....

- [ ] Address Resolution Protocol (ARP) spoofing.
- [x] 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.
- The student takes on the role of the trainer and write general instructions for his classmates or parents, explaining what Content Security Policy is.



References

Arabic references

1. What are inhalation attacks and how can they be prevented? On site: https://cutt.us/NzcrB

English references:

1. The Effective Guide to Creating a Content Security Policy. On site: https://cutt.us/Pjrxe
2. -What is a packet sniffing attack? A cybersecurity guides. On site: https://cutt.us/Kbz3p
3. Cross Site Scripting (XSS). On site: https://cutt.us/DyAza
4. Packet Sniffing: Types, Methods, Examples, and Best Practices. On site: https://cutt.us/yTA3a
5. 3 Types of Cross-Site Scripting (XSS) Attacks. On site: https://cutt.us/ySnS4
6. Content Security Policy. On site: https://cutt.us/A9Mnj
7. How to find out if a Site has a Content Security Policy (CSP) deployed. On site: https://cutt.us/G1EJs
8. Content Security Policy (CSP). On site: https://cutt.us/Sdgpu
9. cPanel. On site: https://cpanel.net/
10. How to Set Up a Content Security Policy (CSP) in 3 Steps. On site: https://cutt.us/e92lS
11. Using Content Security Policy (CSP) to Secure Web Applications. On site: https://cutt.us/fuMF9
12. Content Security Policy Reference. On site: https://cutt.us/xko67
13. Content Security Policy (CSP). On site: https://cutt.us/7Dcv2
14. Content Security Policy in Cybersecurity. On site: https://cutt.us/QBfJJ


CyberEco


الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency