CyberEco

معًا لدعم السلامة الرقمية

Together to support digital safety

سياسة أمَان المُحْتَوى (CSP)

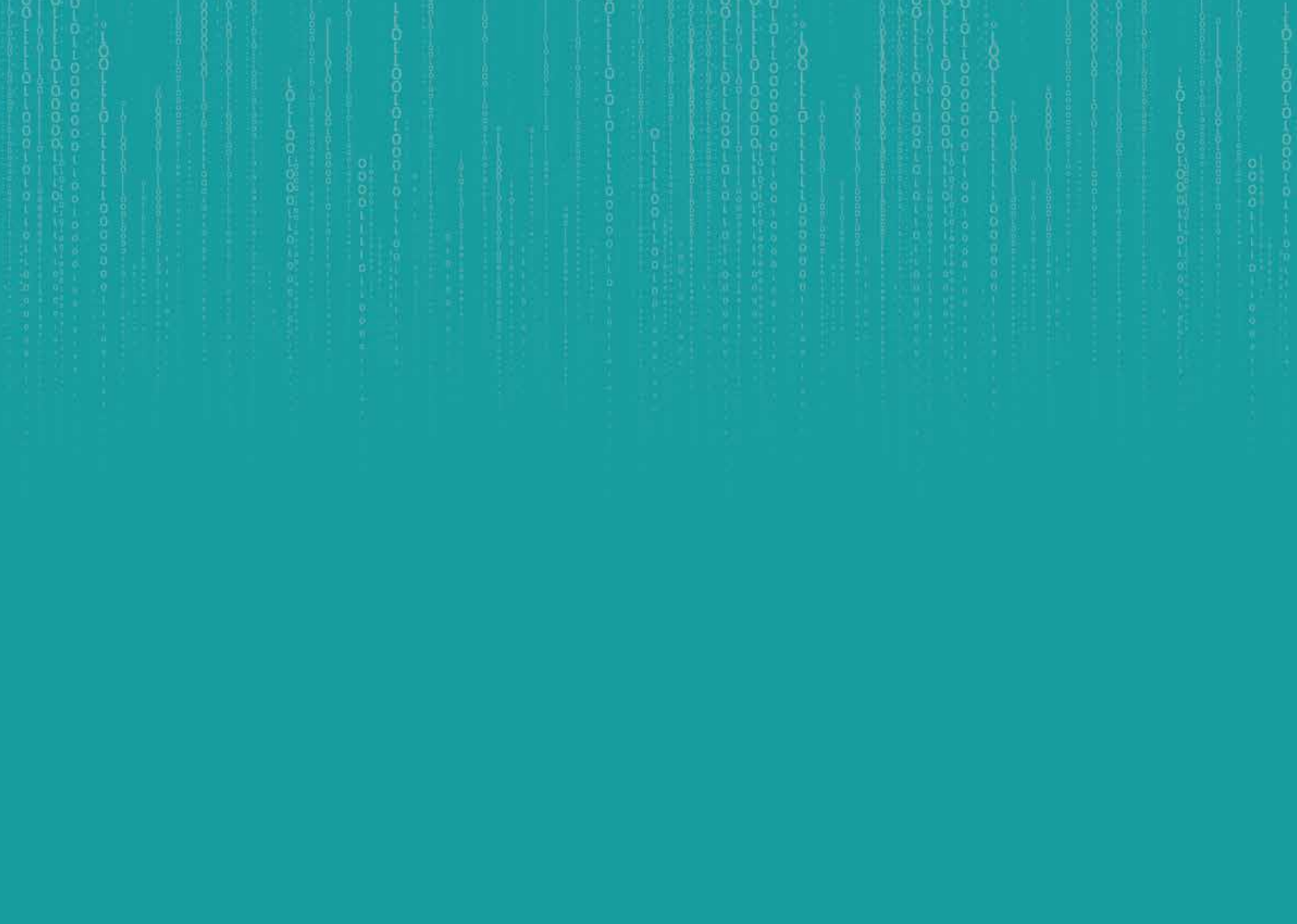
الحقيبة التَّدريبيَّة

تَمارين وتَدْريبَات الطَّالب

المرحلة الثَّانويَّة

الوكالة الوطنية للامن السيبراني

National Cyber Security Agency



سياسة أَمَان المُحْتَوَى (CSP)

الحقيبة التَّدريبيَّة / تمارين وتدريبات الطَّالِب

حُقُوق المِلْكِيَّة الفِكْرِيَّة

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

للاستفسار عن المُبادَرة أو البرنامج؛ يمكن التَّواصُل عن طريق المواقع الإلكترونيَّة أو الأرقام الهاتفيَّة التَّالية:

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

عزيزي الطَّالب

هـذا الكُتَيِّـب خـاصٌّ بـكَ، ولا بُـدّ أن يكـون معـكَ عنـد حُضُـورك جلسـات التَّدْريـب، سـيقوم مُدَرِّبُـك بإرشـادك لكيفيَّـة اسـتخدامه. يحتـوي هـذا الكُتَيِّـب علـى مَجْمُوعـة مـن التَّمَاريـن المُمْتِعَـة والمُفِيـدَة، والتـي سـتقوم بالإجابـة عنهـا إمَّـا خـلال الصَّـفّ أو فـي منزلـك.

كمـا يحتـوي الكُتَيِّـب علـى مجموعـة مـن المُسـابَقَات والبطاقـات التَّعليميَّـة، والمعلومـات العَامَّـة، والتـي سـتجد فيهـا فائـدةً ومُتْعَـةً، وسيرشـدك المُـدَرِّب لكيفيَّـة التَّعامُـل مـع هـذه المُسـابَقات التَّدريبيَّـة، كمـا سَـنُزَوِّدك فـي مَطْلـع كُلّ تمريـن أو مُسـابَقة بتوجيهـات عامَّـة لكيفيَّـة الإجابـة.

السَّادة أولياء أمور الطَّلَبة

هذا الكُتَيِّب خاصّ بالطَّالب، وسيرافقه خلال التَّدريب الذي سيتلقَّاه في المدرسة، وهو يحتوي على مجموعة من التَّمارين والتَّدريبات والمسابقات والبطاقات التَّدريبيَّة، التي تتمحور جميعها حول المفاهيم ذات الصِّلة بسياسَة أمان المُحتَوى وفَهْم آليَّة عملها.

الهدف من هذا الكُتَيِّب وما يحتوي عليه من تدريبات وأنشطة ذهنيَّة تكريس وترسيخ المعلومات التي تلقَّاها الطَّالب خلال محاضرة التَّدريب، وذلك لتحقيق هدفٍ رئيسٍ؛ يتمثَّل في تعزيز قدرة الطَّالب على استخدام الإنترنت والتِّكنولوجيا بفاعليَّة وأمان.

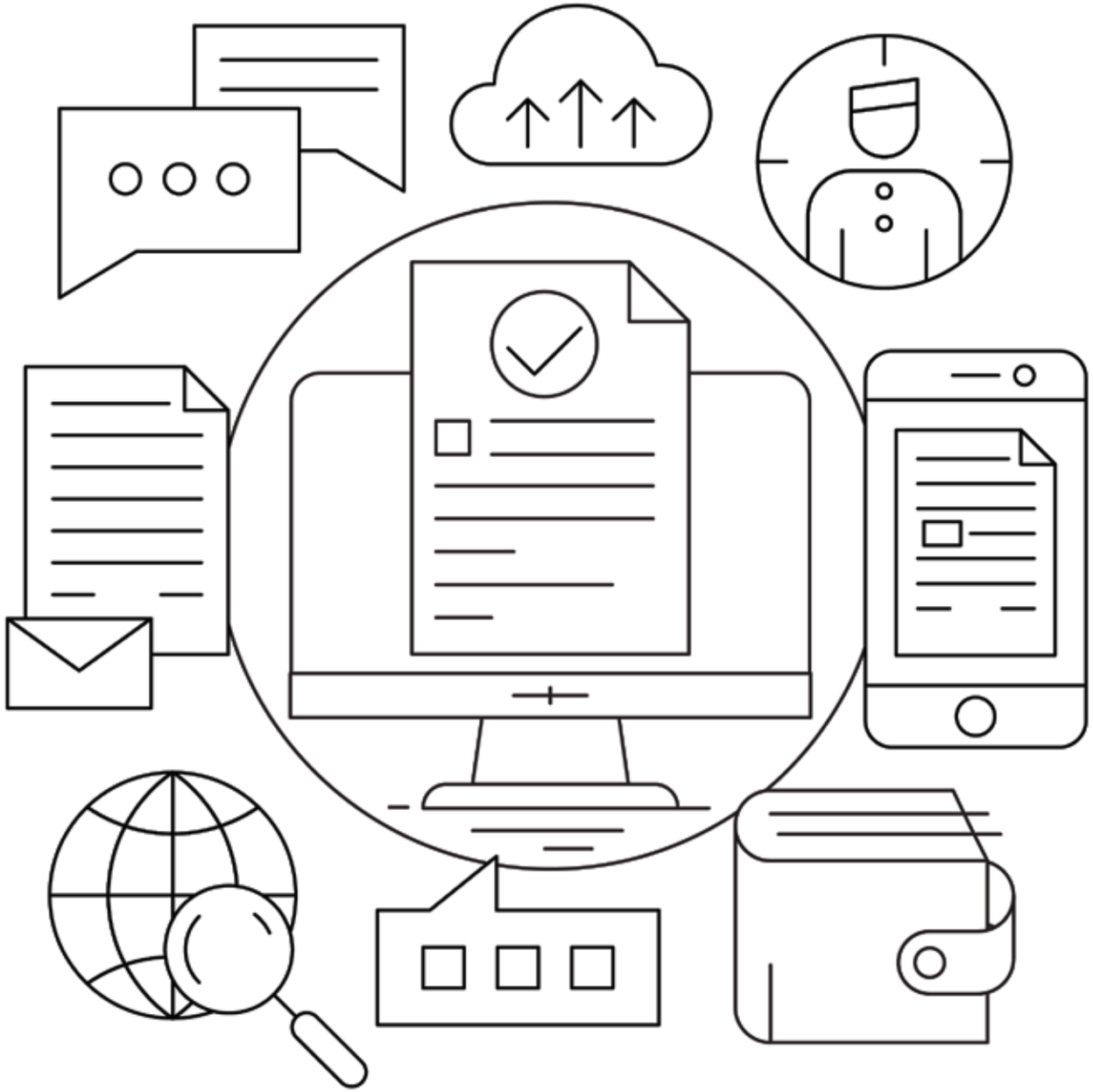
كلّ التَّمرينات والتَّدريبات الموجودة في الكُتَيِّب ستكون مرفقة بتَوْجِيهات عامَّة لكيفيَّة الإجابة عنها، أمَّا المسابقات التَّدريبيَّة فالمدرِّب هو مَن سيُقدِّم للطَّالب تَوْجِيهات حلِّها، كما أنّ الكُتَيِّب يحتوي على بعض التَّدريبات والتَّمارين اللَّاصفِّيَّة، وهذه التَّمارين سيقوم بالإجابة عنها بالمنزل، وهي الأخرى ستكون مرفقة بتَوْجِيهات للحلّ.

يُرجى منكم الإشراف غير المباشر على الطَّالب خلال تعامله مع الكتاب، وفي حال توجَّه الطَّالب إليكم بسؤال أو استفسار حول أحد التَّمارين أو التَّدريبات، يُرجى قراءة التَّوْجِيهات الخاصَّة بكلّ تمرين، وتقديم العون للطَّالب في ضَوْء هذه التَّوْجِيهات.

أولًا: التَّمارين الصَّفِّيَّة

هل تعلم؟

يُفَضَّل استخدام **سياسة أمان المُحْتَوَى CSP** للتَّطبيقات التي تُدِير البيانات الحسَّاسة، مثل واجهات المُستخدِم الإداريَّة ووحدات تَحَكُّم إدارة الأجهزة، أو المُنْتَجات التي تَسْتَضِيف المستندات أو الرَّسائل أو ملفَّات الوسائط التي أَنْشَأها المُستخدِم.



التَّمرين الأوَّل

أكْمِل الجُمَل التَّالية:

1. سياسة ..... المحتوى، هي ..... أمان أجهزة الحاسوب، وتمَّ ابتكارها من أجل مَنْع ..... البرمجيَّات ..... أو الضَّارَّة عبر المواقع.

2. تُعدّ هجمات ..... النَّصِّيَّة عبر المواقع ..... نوعًا من التَّعليمات البرمجيَّة الخبيثة والضَّارَّة في ..... الموثوقة، وغالبًا ما تُستخدَم في مهاجمة مواقع ..... الإلكترونيَّة.

3. يمكن تحديد سياسة أمان ..... في HTTP response header؛ وذلك حين يطلب عميل ويب.

4. سياسة أمَان المَحْتَوى CSP اختصارٌ لجُمْلَة ..... باللُّغة الإنجليزيَّة.

5. سياسة ..... المحتوى مُهمَّة جدًّا لأصحاب ..... الإلكترونيَّة.

انْتَبِه!

مفهوم سياسة أمَان المُحْتَوَى (CSP)

تُعدّ سياسة أمَان المُحتوى (CSP) طبقة إضافيَّة من الأمان تُساعد في اكتشاف أنواع مُعيَّنة من الهجمات الإلكترونيَّة والحدّ منها، بما في ذلك هجمات البرمجة النَّصيَّة للمواقع المشتركة (XSS) وهجمات الحَقن التي تقوم بسرقة البيانات وتشويه المواقع وهجمات البَرْمَجيَّات الضَّارَّة.

التَّمرين الثَّاني:

ضع علامة (✓) بجانب العبارة الصَّحيحة، وعلامة (✗) بجانب العبارة الخاطئة:

1. سياسة أمَان المَحْتَوَى CSP عبارة عن برنامج يُشبه البرامج المضادَّة للفيروسات. — ✓
2. تساعد سياسة أمَان المَحْتَوَى في الكشف فقط عن هجمات الويب. — ✗
3. لا يمكن لسياسة أمَان المَحْتَوَى أن تساعد في منع حالات سرقة البيانات. — ✗
4. لا علاقة بين سياسة أمَان المَحْتَوَى وبين الهجمات الإلكترونيَّة التي تحدث على المواقع. — ✗
5. تُوفِّر سياسة أمَان المَحْتَوَى مجموعة شاملة من توجيهات السِّياسة التي تُساعد في التَّحكُّم في الموارد التي يُسْمَح لصَفْحة الموقع بتحميلها. — ✗

6 عند تشغيل سياسة أمَان المُحْتَوَى لموقع ويب تُؤثِّر سلبًا على الاتِّصالات والبرامج النَّصِّيَّة والخطوط.

7 تستمرّ سياسة أمَان المُحْتَوَى في العمل بشكلٍ افتراضيّ طوال الوقت.

8 تُعدّ سياسة أمَان المُحْتَوَى إضافةً غير مُهمَّة إلى المواقع الإلكترونيَّة.

9 سياسة أمَان المُحْتَوَى عبارة عن طبقة إضافيَّة من الأمان تُساعد على كَشْف الهجمات الإلكترونيَّة.

10 يحتاج عدد كبير من المواقع إلى سياسة أمَان المُحْتَوَى؛ لزيادة سرعة الموقع.

انْتَبِه!

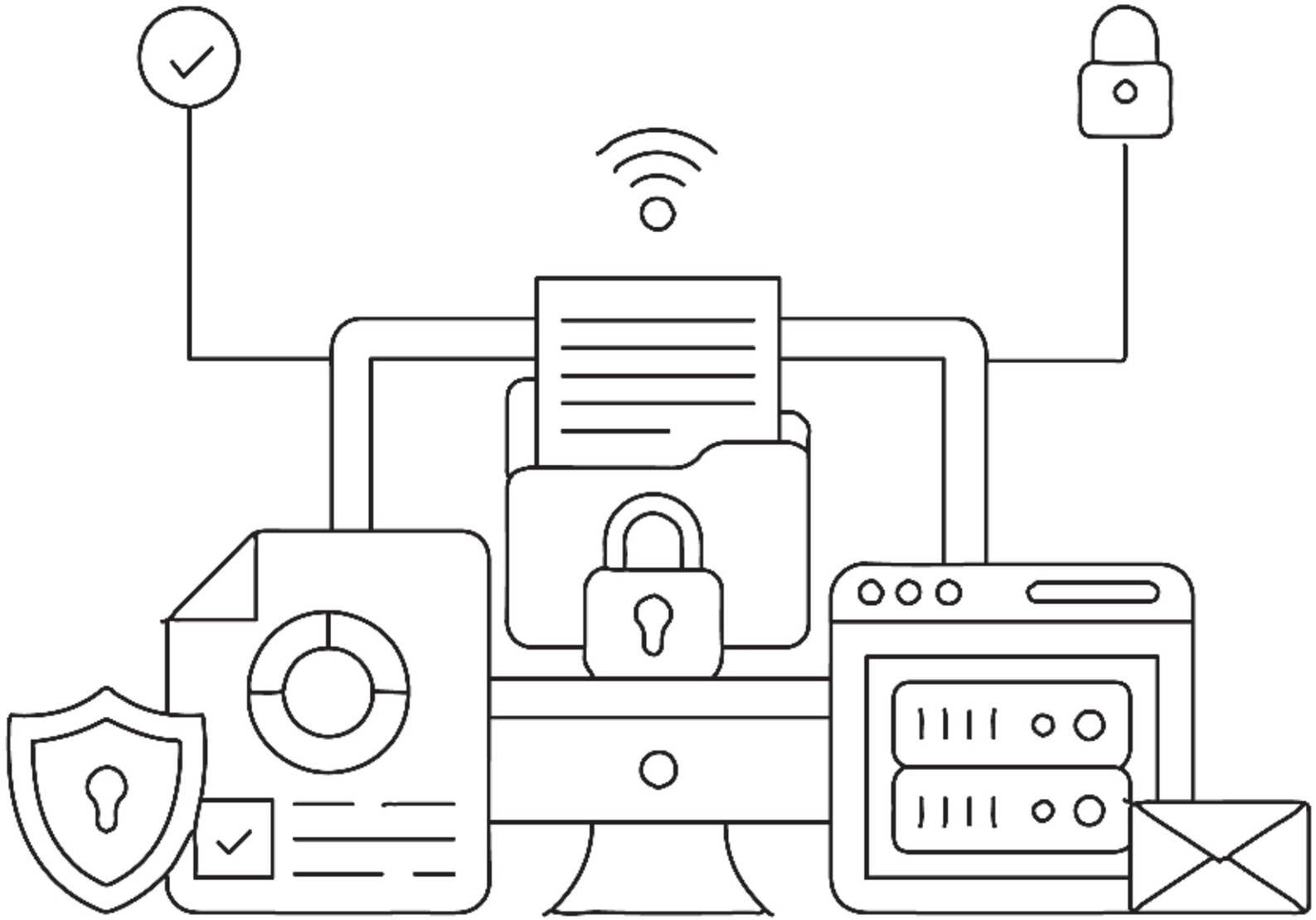
أفضل طريقة لإضافة سياسة أمَان المُحْتَوَى CSP بأَثَر رَجْعِيّ إلـى مـوقـع ويـب بالـكامـل

هي تحديد قائمة بيضاء فارغة تمامًا، لحَظْر كلّ شيء، والمطلوب هو تَشْغِيل تلك السِّياسة مبدئيًّا في وَضْع التَّقرير فقط، ليبدأ المُتصفِّح تقييم القواعد أوَّلًا قبل حَظْر المحتوى، حينها يمكن للمستخدم مراجعة الأخطاء وتَصْنِيف كلّ منها في قائمة المسموح به أو غير المسموح به.

التَّمرين الثَّالث:
صِلْ بين العِبَـارَات فـي العمـود الأوّل
وما يَنْسَجم معها في العمـود الثَّاني

توجيه
اقـرأ العبـارات الموجـودة فـي العمـود الأوّل مـن الجـدول أدنـاه، ثُـم صِـلْ كلّ عبـارة بمـا يناسبها من العمود الثّاني.

Default-Source	لمنع تحميل JavaScript على موقع الويب.
Child-Source	يُوفِّر قائمة بالمصادر الصَّالحة لأوراق الأنماط المتتالية، ويُقصَد بها: لغة تنسيق لصفحات الويب تهتمّ بشكل وتَصْميم المواقع.
Script-Source	هذا التَّوجيه مسؤولٌ عن تحديد عناوين URL التي يتمّ تَحْميلها باستخدام البرامج النَّصّيَّة.
Object-Source	يُحدِّد عناوين URL المسموح بها في العُنصر الأساسيّ للمُستَند.
Style-Source	التَّوجيه الاحتياطيّ لجميع توجيهات الإحضار، ويُحدِّد قائمة المصادر الافتراضيَّة لتوجيهات الجلب الأخرى.
Img-Source	في حال الرَّغْبة في مَنْع تحميل إطارات على موقع الويب يتمّ استخدامه.
Frame-Source	هذا التَّوجيه مسؤول عن تحديد مصادر البرامج النَّصّيَّة المُدْرَجَة في القائمة البيضاء لمسار التَّصفُّح المُتضمّن في الإطارات وعمال الويب.
Connect-Source	يُحدِّد المصادر المسموح بها لعناصر <applet> و<embed> و<object>.
Base-Url	لتقييد المحتوى بخلاف الصُّور على مواقع الويب.



انْتَبِه!

من الوظائف التي تُنفِّذها سياسة أمَان المُحْتَوَى

الحدّ من هجمات استنشاق الحزم -وهي هجمات إلكترونية يُنفِّذُها المُتسلِّلون لاعْتِراض حركة المرور على الشَّبكة ومراقبتها، وتَستهدِف رسائل البريد الإلكترونيّ غير المُشَفَّرة وبيانات تسجيل الدُّخول والمعلومات الماليَّة-، فتلك السِّياسة تعمل على تقييد النِّطاقات التي يمكن تحميل المحتوى منها عبر تحديد الخادم للبروتوكولات المسموح باستخدامها.

هل تعلم؟

تُمكِّن **سياسة أمَان المُحْتَوَى (CSP)** مسؤولي الخادم من التَّخفيف من الأضرار التي يمكن أن يُحْدِثها هجوم XSS، عن طريق إظهار المصادر الصَّالحة للبرامج النَّصِّيَّة أمام المُتصفِّح والقابلة للتَّنفيذ.

انْتَبِه!

هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS)

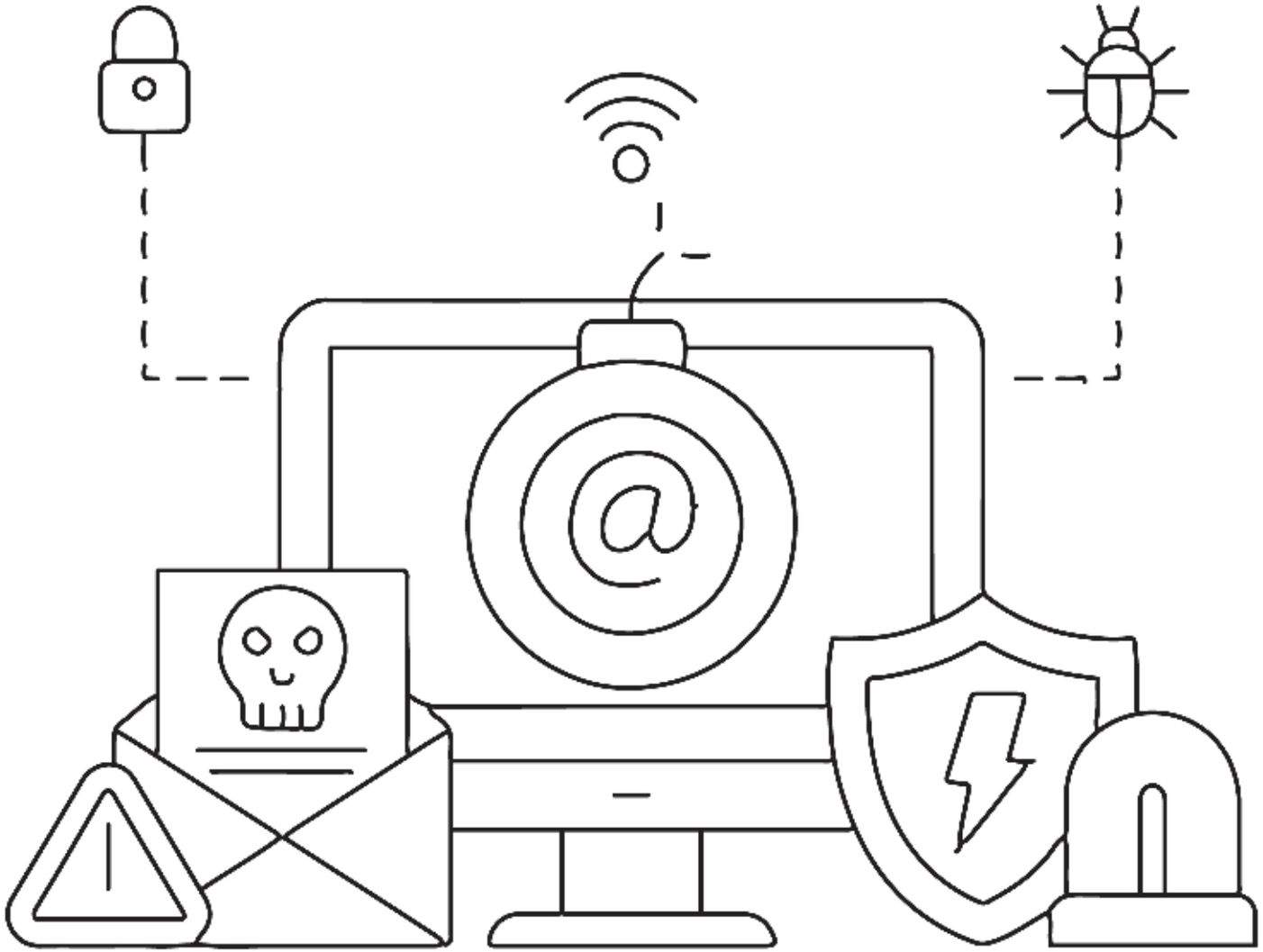
هي نوع من أنواع الحقن؛ إذ يقوم المهاجم الإلكتروني بحَقْن البرمجيَّات النَّصِّيَّة الضَّارَّة في مواقع الويب الموثوقة، ويَقَع الهجوم عندما يَسْتَخْدِم المُهاجِم تطبيق ويب لإرسال تعليمات برمجيَّة ضارَّة في شكل برنامجٍ نَصِّيٍّ من جانب المُتصفِّح إلى المُستخدِم.


ثانيًا: التَّمارين اللَّاصَفِّيَّة

انْتَبِه!

هجمات XSS المخزنة

يُقْصَد بها تخزين برنامجٍ نَصّيٍّ محقون بشَكْلٍ دائمٍ على الخوادم المُستهدَفة، كما هو الحال في قاعدة البيانات، أو سجلّ الزّائرين، أو حقل التّعليق، وما إلى ذلك. وبعد ذلك يبدأ المُستخدِم الضّحيّة باستعادة البرنامج النّصّيّ الضّارّ من الخادم عندما يَطْلُب النّصّ المُخَزَّن.



أضرار هجمات البرمجة النَّصِّيَّة عبر المواقع XSS

- تعديل عَرْض المحتوى.
- خرق الحساب بالكامل.
- تَثْبِيت برمجيات حصان طروادة.
- إعادة تَوْجيه المُسْتخدِم إلى صفحة أخرى أو موقع آخر.
- التَّلاعُب بالتَّقارير الماليَّة التي تصدرها وتنشرها

المؤسَّسات على مواقعها الإلكترونيَّة.

التَّمرين الأوَّل

ضع علامة (✓) بجانب العبارة الصَّحيحة،
وعلامة (✗) بجانب العبارة الخاطئة:

يمكن العُثور على سياسة أمَان المُحْتَوَى CSP في علامة التَّعريف للموقع.	✓
من الضَّروري تمكين بيئة تطوير / اختبار بسبب خطورة سياسة أمَان المُحْتَوَى.	
عليك بتَشْغيل سياسة أمَان المُحْتَوَى فورًا دون تجربة.	
تحتاج سياسة أمَان المُحْتَوَى على الأقلّ إلى 48 ساعة لكي تَعْمل.	
لا يمكن لخدمة أمَان المُحْتَوَى إعداد التَّقارير أو توضيح أماكن المشكلات أو الثَّغرَات.	
تَتَسبّب هجمات البرمجة النَّصيَّة عبر المواقع XSS في مشكلات تَصل حتَّى خرق الحساب بالكامل.	
يُستخدَم هجوم الاستنشاق النشط لحزم الاتصال على الشَّبكات الصَّغيرة.	
لا يمكنك أبدًا التَّحكُّم في التَّوجيهات الفرديَّة داخل السِّياسة.	

انْتَبِه!

تُساعِد **سياسة أمَان المُحْتَوَى** في حماية الموقع الخاصّ بالمُستخدِم من الوَضْع في القائمة المَحْظورَة التي تَفْرِضُها محرّكات البحث مثل جوجل Google عند التّعرُّف على أيٍّ من البرمجيّات الضّارّة، وهو ما يؤثّر في عدد الزّيارات والعملاء، ومن ثمّ يؤثّر في سمعة العلامة التّجاريّة والأرباح.

هل تعلم؟

يمكن لمُستخدِمي الإنترنت تلقّي إشعارات تنبيهيَّة في حال تمّ **انتهاك سياسة أمان المحتوى**، لكن دون حَظْر المحتوى، من خلال ضَبْط رأس استجابة HTTP على تقرير سياسة أمَان المُحْتَوَى فقط.

انْتَبِه!

البرمجة النَّصِّيَّة عبر المواقع العمياء

إحدى الطُّرق الأكثر شيوعًا التي تُصيب بها الرُّوبوتات جهاز الحاسوب الخاصّ بالمُستخدِم، حيث يتمّ تثبيت **البرمجيّات** الضَّارَّة بتنسيق التَّنزيل عبر وسائل التَّواصل الاجتماعيّ أو رسائل البريد الإلكترونيّ التي تنصح بالنَّقر فوق الرَّابط، وغالبًا ما يكون الرَّابط على شكل صورة أو فيديو، ويحتوي إمَّا على فيروسات وإمَّا على **برمجيات ضارة** أخرى.

التَّمرين الثَّاني

استخـرج الكلمـات التَّالية من الجـدول:

توجيه

اقْرأ الكلمات الواردة أدناه بتمعُّن، وابحث في الجدول عن حروف متتالية تُشكِّل هذه الكلمات، وأدناه مثال عن كلمة **"التطبيقات"** وكيف تمّ إيجاد أحرف الكلمة في الجدول:

ا	ل	ت	ط	ب	ي	ق	ا	ت	أ	ع
ل	م	و	ق	ع	غ	ف	ل	ق	م	ن
س	ي	ا	س	ة	ه	ى	ت	ا	ا	ر
ح	ا	ل	س	ر	ي	ة	ش	ر	ن	أ
ا	ل	ا	ص	ل	ا	ح	ف	ي	ة	د
ب	ه	ج	م	ا	ت	ب	ي	ر	ه	و
ة	ش	ك	ا	ل	ث	غ	ر	ا	ت	ا
ا	ل	ا	س	ت	ج	ا	ب	ة	ع	ت
ا	ل	ب	ن	ي	ة	ف	ل	ا	ف	ل
ا	ل	م	ح	ت	و	ى	ن	ي	و	ن

التَّطبيقات - أمان - السَّحابة - التَّشْفير - الإصلاح - الاستجابة - البنية - الثَّغرات
سياسة - المحتوى - موقع - السِّرِّيَّة - هجمات - تقارير - أدوات.

انْتَبِه!

خدمات معلومات الإنترنت IIS manager:

IIS manager هو خادم ويب من Microsoft يعمل على نظام التَّشغيل Windows، ويُسْتَخْدَم لتَبَادُل محتوى الويب الثَّابت والدِّيناميكيّ مع مُستخدِمي الإنترنت، ويمكن استخدامه أيضًا لاستضافة تطبيقات الويب ونَشْرها وإدارتها.

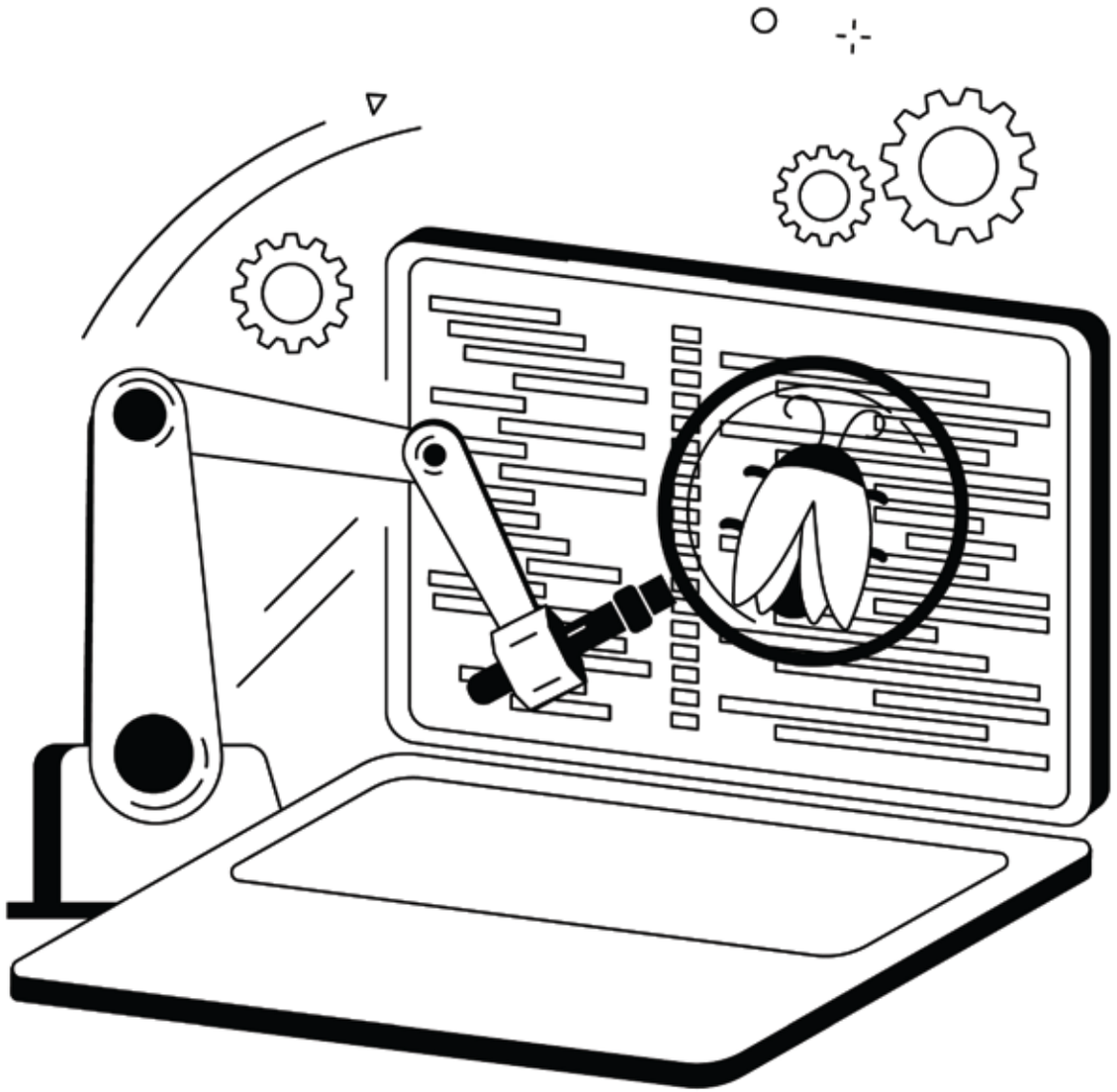
هل تعلم؟

تُسْهِم **سياسة أمان المُحْتَوَى** في تمكين أصحاب مواقع الويب من وَضْع قواعدهم الخاصَّة التي تُناسِب احتياجات موقعهم، فضلًا عن كونها تَمْنَعُ وصول غير المُصرَّح لهم إلى المعلومات المهمَّة.

انْتَبِه!

هجوم استشاق الحزم:

أسلوب قرصنة يعمل على جَمْع حزم البيانات التي تَنْتَقِل عَبْر شبكة حاسوب غير مُشَفَّرة؛ إذ يُراقِب المُتسلِّلون السِّيبرانيُّون حزم البيانات في حركة مرور الشَّبكة؛ بهدف اعتراض المعلومات الحسَّاسة مثل التَّفاصيل الماليَّة أو بيانات تسجيل الدُّخول، لبَيْعِها أو لاستخدامها في هجمات أخرى.



خطوات تنفيذ سياسة أمَان المُحْتَوَى CSP:

1. اختيار مُزوّد الخدمة الخاصّ بموقع الويب.
2. إضافة سياسة أمان المُحْتَوَى CSP إلى رأس استجابة HTTP الخاصّ بموقع الويب.

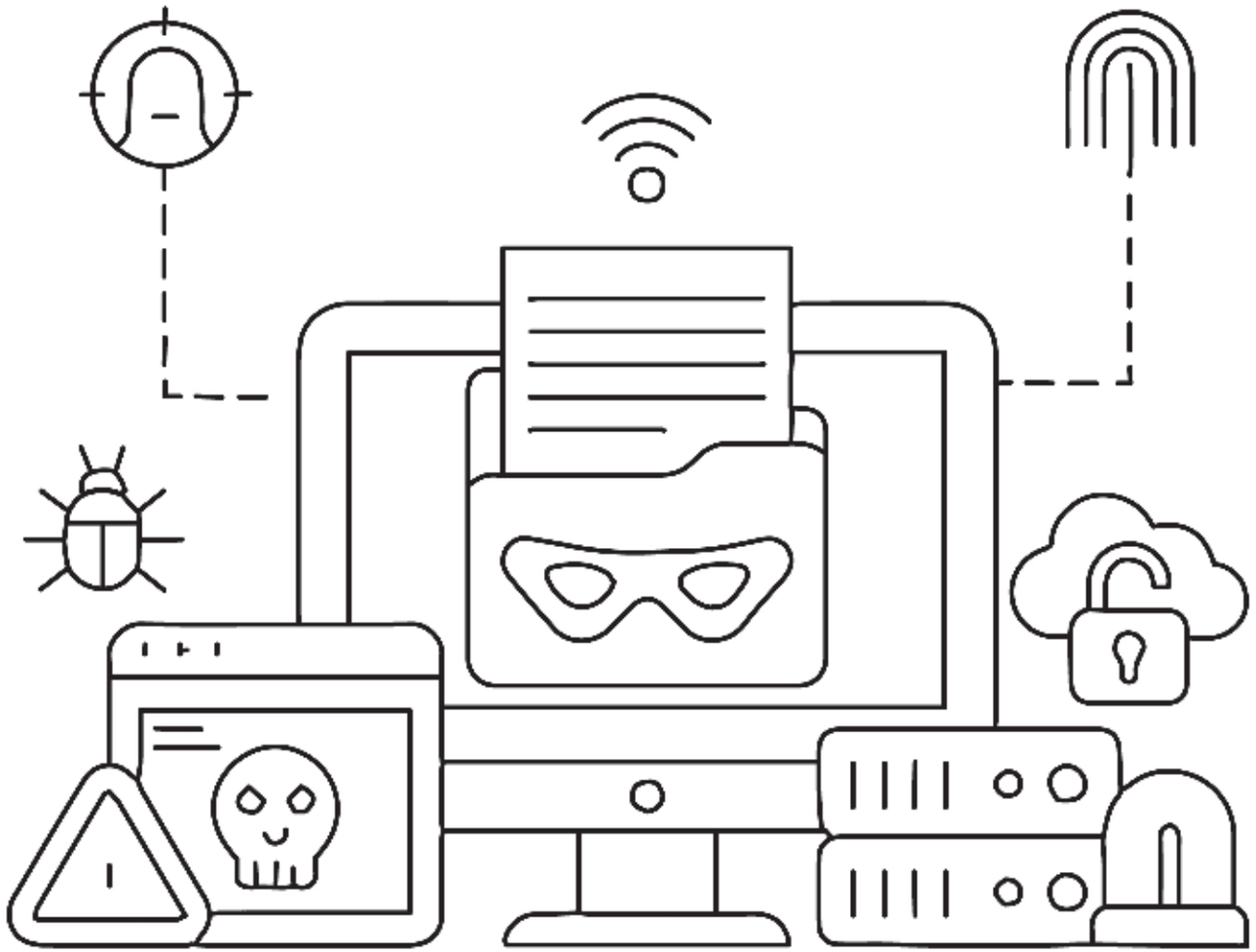
للعثور على سياسة أمان المُحْتَوَى في رؤوس الاستجابة يمكن اتِّباع الخطوات التَّالية:

باستخدام المُتصفِّح، افْتَح أدوات المُطوِّرين (اسْتَخْدِم أدوات DevTools في Chrome) ثمّ انْتَقِل إلى موقع الويب الذي تَخْتاره، وافْتَح علامة التَّبويب "الشَّبكة".

ابْحَث عن الملفّ الذي يُنْشِئ الصَّفحة، الذي يكون له نطاق موقع الويب نفسه الذي تَتَصَفَّحُه، وهو في الأغلب يكون العنصر الأوَّل في علامة التَّبويب "الشَّبكة".

عند النَّقر على الملفّ يَظْهَر مزيد من المعلومات، وحينها تبدأ عمليّة البحث عن رمز الاستجابة 200OK.

وفي الأسفل سيَظْهَر استخدام سياسة أمان المُحْتَوَى من عدمه.



للعثور على سياسة أمَان المُحْتَوَى CSP من علامة التَّعريف

1. انْتَقِل إلى مصدر الصَّفحة وافْتَح المُتصفِّح واخْتَر موقع الويب.
2. انْقُر بِزِرّ الفأرة (mouse) الأيمن على منطقة فارغة وحَدِّد "عَرْض مصدر الصَّفحة".
3. بمجرَّد عَرْض مصدر الصَّفحة، أجْرِ بحثًا حسب نوع النِّظام، ففي ويندوز Windows اضْغَط على أزرار (Ctrl-F) من لوحة المفاتيح، وابْدَأ عمليَّة البحث عن مصطلح "سياسة أمَان المُحْتَوَى".


أسئلة
المسابقات

مـا هــو؟

طبقة إضافيّة من الأمان تُساعد في اكتشاف أنواع مُعيّنَة من الهجمات الإلكترونيّة والحدّ منها.

هجمات إلكترونيّة يُنفّذها المُتسلّلون لاعتراض ومُراقَبَة حركة المرور على الشّبكة، وتستهدف رسائل البريد الإلكترونيّ غير المُشفّرة وبيانات تسجيل الدُّخول والمعلومات الماليّة.

سلسلة تتضمّن التّوجيهات التي تَصِف سياسة أمَان المُحْتَوَى الخاصّة بالمُستخدِم على الويب؛ حيث تُوجد مجموعة من التّوجيهات لعدّة أنواع من العناصر، أي يكون لكلّ نوع سياسته الخاصّة، بما في ذلك الخطوط والصُّور ووسائط الصّوت والفيديو والبرامج النّصّيّة.

إحدى فئات توجيهات سياسة أمَان المُحْتَوَى التي تُحدّد المواقع التي يتمّ منها تحميل أنواع مُحدّدة من الموادّ.

مـا هــو؟

إحدى فئات توجيهات سياسة أمان المَحْتَوى التي تساعد في التَّحكُّم بخصائص بيئة العمل.

خادم ويب من Microsoft يعمل على نظام التَّشغيل Windows ويُستخدَم لتبادُل محتوى الويب الثَّابت والديناميكيّ مع مُستخدِمي الإنترنت، ويمكن استخدامه أيضًا لاستضافة تطبيقات الويب ونَشْرها وإدارتها.

خادم ويب مسؤول عن قَبُول طلبات الدَّليل (HTTP) من مُستخدِمي الإنترنت وإرسال المعلومات المطلوبة إليهم في شَكْل ملفَّات وصفحات ويب.

مكانان يمكن العُثور في أيٍّ منهما على مُقدِّمي الخِدْمات المُفعَّلة لسياسة أمان المحتوى.

مـا هــو؟

يُقصَد بها تخزين برنامج نصّيّ محقون بشكلٍ دائمٍ على الخوادم المَستهدَفة، كما هو الحال في قاعدة البيانات، أو سِجِلّ الزّائرين، أو حَقْل التّعليق، وما إلى ذلك. وبعد ذلك يبدأ المَستخدِم الضَّحيَّة استرجاع البرنامج النَّصّيّ الضّارّ من الخادم عندما يَطلب النَّصّ المَخزَّن.

شَكل من أشكال هجمات XSS المَستمِرَّة، وتتمّ عند حِفْظ بَرْمَجيّات المَهاجِم على الخادم، وإعادتها إلى الضَّحيَّة، فمثلًا في "نماذج البيانات" يقوم المَهاجِم بإرسال برمجيّات ضَارّة، وبمُجرَّد فَتْح المَستخدِم للنّموذج يبدأ التّنفيذ.

يُعرَف بأنّه أسلوب قَرْصنة يعمل على جَمْع حزم البيانات التي تَنْتقل عبر شبكة حاسوب غير مُشفَّرة؛ حيث يُراقب المُتسلِّلون حزم البيانات في حركة مرور الشّبكة؛ بهدف اعتراض المعلومات الحسّاسة مثل التّفاصيل الماليّة أو بيانات تسجيل الدُّخول؛ لبيعها أو لاستخدامها في هجمات أخرى.

أكمل العبارات التّالية:

- تهدف طبقة الأمان الإضافيّة المَتمثّلة في سياسة أمَان المَحْتَوَى (CSP) إلى .....
- تُمَكّن سياسة أمَان المَحْتَوَى (CSP) مسؤولي الخادم من تَخفيف الأضرار التي يمكن أن يُحْدثها هجوم XSS عن طريق .....
- من الوظائف التي تُنفّذها سياسة أمَان المَحْتَوَى أيضًا الحدّ من هجمات ..... ، وهي هجمات إلكترونية يُنفّذها المَتسلّلون لاعتراض ومُراقَبَة حركة المرور على الشَّبكة.
- يتمّ تعريف توجيهات سياسة أمَان المَحْتَوَى في ..... التي تُسمَّى رؤوس CSP ومَهمّتها إرشاد المُتصفّح إلى مصادر المحتوى الموثوق بها، كما تتضمَّن قائمة بالمصادر التي ينبغي مَنْع الوصول إليها.
- تساعد توجيهات المستند في التَّحكُّم بخصائص بيئة العمل وتشمل: ..... و .....
- تُعدّ توجيهات الإبلاغ المسؤولة عن توثيق انتهاكات سياسة أمَان المَحْتَوَى والإبلاغ عنها، وتشمل .....

- قد تتضمَّن بعض مواقع الويب عناوين URL قديمة غير آمِنَة، لذا تقوم سياسة التَّوجيه ..... بإرشاد المُتصَفِّح للتَّعامُل مع تلك العناوين واستبدالها بأخرى أكثر أمنًا HTTPS .

- إنَّ أفضل طريقة لإضافة سياسة أمَان المُحْتَوَى CSP بأثرٍ رجعيّ إلى موقع ويب بالكامل هي تحديد ..... لحظر كُلّ شيءٍ.

- تُساعد سياسة أمَان المُحْتَوَى في حماية الموقع الخاصّ بالمُستخدِم من الوَضْع في ..... التي تَفْرضها مُحرّكات البحث مثل جوجل Google عند التَّعرُّف على أيٍّ من البرمجيَّات الضَّارَّة عليه.

- يمكن لمُستخدِمي الإنترنت تلقِّي إشعارات تنبيهيَّة في حال تمَّ انتهاك سياستهم، لكنْ دُون حَظْر المحتوى، من خلال ضَبْط ..... على تقرير سياسة أمَان المُحْتَوَى فقط.

اختر الإجابة الصَّحيحة

1. في هذه الفئة من هجمات البرمجة النَّصّيَّة عبر المواقع يقوم المُهاجِم بتخزين برنامج نصّيّ مَحْقُون بشكلٍ دائمٍ على الخوادم المُستهدَفة، كما هو الحال في قاعدة البيانات، أو سِجلّ الزَّائرين، أو حَقْل التَّعليق، وما إلى ذلك.

- ☐ هجمات XSS المُخزَّنة.
- ☐ هجمات XSS المنعكسة.
- ☐ البرمجة النَّصّيَّة عبر المواقع العمياء.
- ☐ هجمات استنشاق الحزم.

2. تتسبَّب هجمات البرمجة النَّصّيَّة عَبْر المواقع XSS في .....

- ☐ خرق الحساب بشَكْلٍ جزئيّ.
- ☐ تَثْبيت برمجيَّات الفدية.
- ☐ الفشل في تَوْجيه المُستخدِم إلى صفحة أخرى أو موقع آخر.
- ☐ تعديل عَرْض المحتوى.

3. يُسْتَخْدَم هذا النَّوع من الهجوم على الشَّبكات الأكبر حجمًا؛ فمع اتِّصال مزيدٍ من الأجهزة بشبكة واحدة، تصبح هناك حاجة إلى مُحَوِّل الشَّبكة .....

- [ ] البرمجة النَّصِّيَّة عَبْر المواقع العمياء.
- [ ] الاستنشاق النشط لحزم الاتصال.
- [ ] هجمات XSS المنعكسة.

4. يلْجَأ المُهاجِمون في حال فَشَل هجمات استنشاق كلمات المرور إلى استخدام هجمات .....، وهي نوع من هجمات خرق الشَّبكة لجَمْع بيانات كلمة المرور.

- [ ] خَرق جلسة اتِّصالات بروتوكول التَّحكُّم في الإرسال.
- [ ] استنشاق JavaScript.
- [ ] هجمات التَّنصُّت الوسيط.

5. هجمات إلكترونيّة يقوم فيها المُهاجِم بإدخال تعليمات برمجيّة ضارّة عند نقطة الشّراء على مواقع التّجارة الإلكترونيّة .....

- ☐ خَرق جلسة اتّصالات بروتوكول التّحكُّم في الإرسال.
- ☐ استنشاق JavaScript.
- ☐ هجمات التّنصُّت الوسيط.

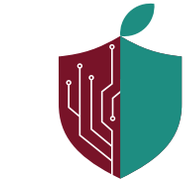
6. بمجرّد إنشاء اتّصال بين المُرسِل والمُستقبِل، يقوم المُهاجِم بالاختراق ونَقْل البيانات الموثوقة التي تتمّ واستنشاق حركة مرور الشّبكة .....

- ☐ انتحال بروتوكول تحليل العنوان (ARP).
- ☐ خَرق جلسة اتّصالات بروتوكول التّحكُّم في الإرسال.
- ☐ استنشاق JavaScript.

مشروع التَّخرُّج

مشروع التَّخرُّج هو واجب يقوم به الطَّالب بمفرده أو بالاشتراك مع زميل أو أكثر، ويقوم من خلاله وتحت إشراف المُدرِّب بأحد الواجبات التَّالية:

- كتَابَة قصَّة أو تقرير أو مقال تَشْرح فيه المَفاهيم ذات الصِّلة بسياسَة أمَان المُحْتَوَى.
- يَتَقَمَّص الطَّالب دَوْر المُدَرِّب ويَكْتُب تَوْجِيهاتٍ عامَّةً لزملائه أو أَهْله يُوضِّح لهم فيها الإجراءات المطلوبة للاستفادة من سياسَة أمَان المُحْتَوَى، وأهمِّيَّة هذا الأمر.



CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency