CyberEco

معًا لدعم السلامة الرقمية

Together to support digital safety

سياسة أمان المحتوى (CSP)

الحقيبة التدريبية

خاصة بالمدرب

المرحلة الثانوية

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

سياسة أمَان المُحْتَوَى (CSP)

المَرْحَلة الثَّانويَّة

المادَّة التَّدريبيَّة

(حَقيبَة خاصَّة بالمُدَرِّب)

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

المحتوى العام للحقيبة

أولاً: مدخل عام للحقيبة

ثانياً: المادة العلمية

أولًا: مَدْخل عامّ إلى الحَقيبَة التَّدْريبيَّة

فيما يلي تبيان لبعض التَّفاصيل ذات الصِّلَة المُباشِرَة بأهداف الحَقيبَة التَّدْريبيَّة، مع توجيهات عامَّة للمُدَرِّب حول كيفيَّة التَّعامُل مع هذه الحَقيبَة وتزويده بالمحتوى العِلْميّ الذي سيَعْتَمِد عليه في التَّدريب.

الفكرة العامَّة

تقوم فِكْرة هذه الحَقيبَة التَّدريبيَّة على تزويد المُدَرِّب بأدوات ووسائل تدريبيَّة؛ بحيث يسهل عليه تقديم المعلومات للمُتَدَرِّبين. وبِشَكْلٍ عامّ، فإنَّ كُلّ مادَّة تدريبيَّة تكون على جُزْأين؛ جُزْء لدى المُتَدَرِّب وجُزْء آخر لدى المُدَرِّب، والحَقيبَة التَّدريبيَّة تُعدّ مُوجِّهًا عامًّا للمُدَرِّب وداعِمًا له، ومحتواها العِلْمِيّ هو ذاته لدى المُتَدَرِّب، ولكنْ هنا يتمّ عَرْض ذات المحتوى التَّدريبيّ، ولكنْ بأسلوب عَرْضٍ مُخْتَلِفٍ؛ إضافةً إلى تزويد المُدَرِّب بأدواتٍ ووسائل تدريب تَدْعَمه في عمليَّة التَّدريب.

أهداف الحَقيبَة التَّدْريبيَّة

1. تَزويد المُدَرِّب بوسائل تدريب تُساعده على إيصال المحتوى التَّدريبيّ للطَّلَبة.
2. تَقديم المعلومات والمحتوى التَّدريبيّ بشكلٍ سَهْل ومُبسَّط.
3. تَقْديم المحتوى التَّدريبيّ الخاصّ بسياسة أمان المحتوى مُرفَقًا بأدوات ووسائل تدريب متعدِّدة.

محتوى الحَقيبَة التَّدْريبيَّة

تتضمَّن الحَقيبَة التَّدريبيَّة عدَّة أدوات تدريبيَّة، فيما يلي تبيان لها:

1. **ملفّ العَرْض.**
2. **ألعاب تدريبيَّة** ، كالكلمات المُتَقاطِعَة والمُسابَقات، يعرضها المُدَرِّب على الطَّلَبة؛ بهدف ضمان تَفاعُلهم مع المحتوى التَّدريبيّ.
3. **فيديوهات تَعليميَّة.**
4. **مُسابَقات،** وهي على شَكْل أسئلة استنتاجيَّة يَعْرضها المُدرِّب على الطَّلبة.
5. **بطاقات تدريبيَّة،** وهي على شَكْل معلومات عامَّة مُرْفَقة بصُوَر تعبيريَّة، يَعْرضها المُدَرِّب على الطَّلَبة.
6. **إسكتشات،** تتضمَّن معلومات حول المَحاوِر الرَّئيسة في المُحتَوى التَّدريبيّ.

فهرس المحتوى العِلْمِيّ

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
مُقدِّمة عامَّة	5 دقائق
الجانب النَّظريّ من المادَّة	25 دقيقة
عَرْض الفيديوهات التَّعليميَّة	25 دقيقة
استراحة قصيرة	20 دقيقة
تنفيذ الأَلْعَاب التَّدريبيَّة	25 دقيقة
حِوَار ونِقَاش مع الطَّلَبة	15 دقيقة
مَشروع التَّخرُّج	5 دقائق
المُدَّة الزَّمنيَّة للورشَة	ساعتان

دليل إرشادي للمُدَرِّب

فيما يلي تبيان لبعض الإرشادات العامَّة للمُدَرِّب، والتي تتمحور حول كيفيَّة اسْتِخدام هذه الحَقيبَة.

1. المحتوى العِلْمِيّ للحقيبة قد يَفُوق قُدْرة الطَّلبة على الاستيعاب؛ خاصَّة المصطلحات والمفاهيم العامَّة؛ لذلك لا بُدَّ للمُدرِّب من تبسيط هذه المفاهيم وتقديمها لطلبة المرحلة الثَّانويَّة بصورةٍ قابلةٍ للفَهْم.
2. يقوم المُدرِّب بعَرْض شرائح العَرْض عند كلّ نقطة يتحدَّث عنها، فمثلًا عند الحديث عن مفهوم سياسة أمَان المُحْتَوَى يتمّ عَرْض الشَّريحة التي تتناول ذات النُّقطة.
3. في أثناء شرح الفَصْل الأوَّل يتمّ توزيع الصُّور المصمَّمة خصوصًا لفقرة "هل تعلم؟".
4. يَعرِض المُدَرِّب الجزء الخاص بـ "إسكتشات" أثناء قيام الطَّلبة بحل التَّمارين والتَّدريبات.
5. في نهاية التَّدريب يتمّ عَرْض أسئلة المسابقات المذكورة في نهاية الملفّ.
6. في أثناء عرض المادَّة العِلْمِيّة لكلّ فَصْل يتمّ استقطاع فترة من الوقت المُخصَّص له لعَرْض عددٍ من الرَّوَابِط ذات الصِّلَة بمضمون الفصل.
7. يقوم المُدرِّب بعَرْض الفيديوهات -المذكورة في ملفّ منفصل- على الطَّلبة في نهاية كلّ فصل، أو في الموضع الذي يراه مناسبًا.
8. يُرْجى فَتْح باب المناقشة مع الطَّلبة في المواضع التي يراها المُدرِّب مناسبة.
9. فيما يخصُّ التَّمارين المُوجَّهة للطَّلبة؛ سيتمّ إرفاق ملفّ بالتَّمارين في نهاية هذه الحقيبة، وهذه التَّمارين تُقسَّم إلى جزأين؛ جُزْء يتمّ تقديمه للطَّلبة خلال التَّدريب، وهو تمارين صَفِّيَّة، والجزء الآخر يُكلَّف الطَّلبة بالإجابة عنه في المنزل، وهي تمارين لا صَفِّيَّة، وسيتمّ توضيح هذه الجزئيَّة في نهاية هذه الحقيبة.

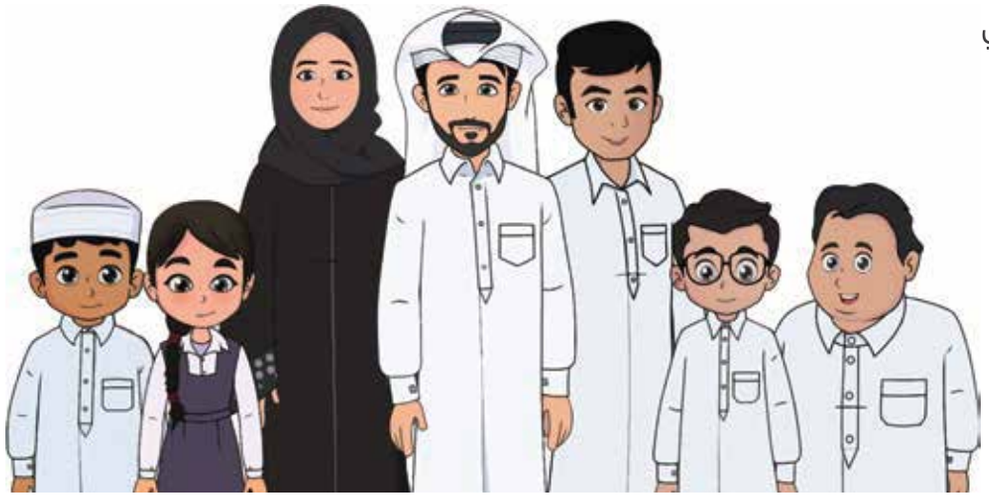
مشروع التَّخرُّج

مشروع التَّخرُّج هو عملٌ يَقُوم به الطَّالب، ويهدف لتحقيق عدَّة أهداف، فيما يلي تبيان لأهمّها:

- التَّأكُّد من أنَّ الطَّالب قد استوعَب المعلومات والأفكار التي قَدَّمها المُدَرِّب له، وأنَّه بات قادرًا على الاستفادة منها في حياته اليَوْميَّة.
- ترسيخ المعلومات والأفكار التي قَدَّمها المُدَرِّب للطَّالب.
- المشروع بمثابة رَبْط بين الأفكار والمعلومات النَّظريَّة بالواقع العَمَليّ والتَّطبيقيّ.

فيمـا يَتعلَّـق بآليَّـة تكليـف الطَّلَبـة بالمشـروع، وكيفيَّـة تنفيـذه، يمكـن تقديـم التَّوجيهـات التَّاليـة:

- يمكن أن يكون مشروع التَّخرُّج فَرْديًّا أو جَماعيًّا، وفي حال كان جَماعيًّا يجب ألَّا يَتجاوز عدد الطَّلَبة المُشْتَرِكين في مشروعٍ واحدٍ ثلاثة طلاب.
- اختيـار موضوع المشـروع يكون مِن قِبَل الطَّلبة، ويمكـن للمُدرِّب تقديم بعض المُساعَدة أو الأفكار في هذا المجال.
- موضوع مشروع التَّخرُّج لا بُدّ أن يكون مُنسجمًا مع المحتوى التَّدريبيّ الذي تمّ تقديمه للطَّلبة.
- يمكن أن يكون مشروع التَّخرُّج ضِمْن أحد التَّصوُّرات التَّالية، وهي تَصوُّرات غير مُلْزِمَة، فيمكن للمُدرِّب اختيار تَصوُّرات أخرى يراها مُناسِـبَة، وفيما يلي تبيان لبعض المُقْتَرحات:
  - كتابة قصَّة قصيرة أو مقال أو تقرير حول سياسة أمن المحتوى.
  - يَتَقَمَّص الطَّالب دَوْر المُدَرِّب ويَكْتُب تَوْجِيهاتٍ عامَّةً لزملائه أو أَهْله يُوضِّح لهم سياسة أمَان المُحْتَوَى.



ثانيًا: المادَّة العِلْمِيَّة

مُقدِّمة

مع التَّطوُّر التِّكنولوجيّ الهائل الذي يشهده العالم باتت المحتويات المعروضة على صفحات الويب أكثر عرضةً للاختراق والسَّرقة والتَّلاعب بها واستغلالها من قِبل المُتسلِّلين السِّيبرانيِّين، وهو ما دَفَعَ الشَّركات إلى اعتماد سلسلة من الآليَّات التِّقنيَّة المُتطوِّرة للحدّ من الهجمات السِّيبرانيَّة التي أصبحت جزءًا من حياة مُتصفِّحي الشَّبكة العالميَّة "الإنترنت"، الذين يُجْرون معاملاتهم اليوميَّة من محادثات وأعمال ومراسلات، وغير ذلك.

ومن الآليَّات التِّقنيَّة التي تمّ اعتمادها ما يُعرَف بسياسة أمَان المُحْتَوَى Content security policy (CSP)، وهي آليَّة أمان للمتصفِّح الهدف منها التَّخفيف من الهجمات الإلكترونيَّة مثل هجمات XSS؛ إذ تعمل عن طريق تقييد الموادّ المنتشرة على الإنترنت مثل النُّصوص والصُّور التي يَسْهُل تحميلها، وكذلك تقييد إمكانيَّة خرقها وسرقتها، وإنّ هجمات XSS أو البرمجة النَّصِّيَّة عبر المواقع التي تَستهدِف الموادّ النَّصِّيَّة والصُّور؛ هي عبارة عن ثغرة أمنيَّة على الويب تسمح للمُهاجِم السِّيبرانيّ باختراق المستخدمين انطلاقًا من استغلال نقاط الضَّعف في التَّطبيقات والأجهزة التقنية.

إذ تسمح هجمات XSS للمُتسلِّلين السِّيبرانيِّين بالتَّحايل والتَّنكُّر كمستخدمين ضحايا وتنفيذ الإجراءات نفسها التي قد يتَّبعها المستخدم العاديّ للوصول إلى بيانات الضَّحايا المُستهدَفين، فمثلًا في حال كان المستخدم الأصليّ يمكنه الوصول إلى التَّطبيقات، فإنّ المُتسلِّل يمكنه التَّحكُّم بالكامل في جميع بيانات ووظائف تلك التَّطبيقات؛ حينها تظهر أهمِّيَّة سياسة أمَان المُحْتَوَى في حماية الموادّ النَّصِّيَّة والصُّور من هذا النَّوع من الهجمات السِّيبرانيَّة.

الفَصْل الأَوَّل

مفهوم سياسة أمَان المُحْتَوَى (CSP) وآليَّة عملها

- أوَّلًا: مفهوم سياسة أمَان المُحْتَوَى (CSP)
- ثانيًا: آليَّة عمل سياسة أمَان المُحْتَوَى (CSP)

01

أولًا: مفهوم سياسة أمَان المُحْتَوَى (CSP)

تُعَدّ سياسة أمَان المُحْتَوَى (CSP) طبقة إضافيَّة من الأمان تُساعِد في اكتشاف أنواع معيَّنة من الهجمات السِّيبرانيَّة والحدّ منها، بما في ذلك هجمات البرمجة النَّصِّيَّة للمواقع المشتركة (XSS) وهجمات الحقن التي تقوم بسرقة البيانات وتشويه المواقع وتوزيع البَرمَجيَّات الضَّارَّة؛ وتُعَدّ هجمات (XSS) نوعًا من أنواع الحَقْن؛ إذ يقوم المُهاجِم السِّيبرانيّ بحَقْن البَرمَجيَّات النَّصِّيَّة الضَّارَّة في مواقع الويب الموثوقة، ويَقَعُ الهجوم عندما يَستخدم المُهاجِم تطبيق ويب لإرسال تعليمات برمجيَّة ضارَّة في شكل برنامج نصّيّ من المُتصفِّح إلى المستخدم.[1]

فطبقة الأمان الإضافيَّة المُتمثِّلة في سياسة أمَان المُحْتَوَى (CSP) تَهْدُف إلى الحدّ من هجمات البرمجة النَّصِّيَّة عبر المواقع والإبلاغ عنها؛ إذ يَسْتغلّ هذا النَّوع من الهجمات السِّيبرانيَّة ثقة المُتصفِّح بالمحتوى المُستَلَم من الخادم، ليبدأ تنفيذ الهجوم الضَّارّ بواسطة مُتصفِّح الضَّحيَّة؛ لذا تُمكِّن سياسة أمَان المُحْتَوَى (CSP) مسؤولي الخادم من التَّخفيف من الأضرار التي يمكن أن يُحْدِثها هجوم XSS عن طريق إظهار المصادر الصَّالحة للبَرمَجيَّات النَّصِّيَّة أمام المُتصفِّح، والقابلة للتَّنفيذ، فوفق ذلك يقوم المُتصفِّح المتوافق مع سياسة أمَان المُحْتَوَى بتنفيذ البَرمَجيَّات النَّصِّيَّة المُستَلَمة من النِّطاقات المسموح بها فقط.[2]

ومن الوظائف التي تُنفِّذها سياسة أمَان المُحْتَوَى أيضًا الحدّ من هجمات استنشاق الحزم، -وهي هجمات سيبرانيَّة يُنفِّذها المُتسلِّلون لاعتراض حركة مرور البيانات على الشَّبكة ومراقبتها وتَستهدِف رسائل البريد الإلكترونيّ غير المُشفَّرة وبيانات تسجيل الدُّخول والمعلومات الماليَّة-، فتلك السِّياسات تعمل على تقييد النِّطاقات التي يمكن تحميل المحتوى منها عبر تحديد الخادم للبروتوكولات المسموح باستخدامها، فمثلًا يمكن للخادم فَرْض تحميل كلّ المحتوى باستخدام HTTPS فهنا لا يتضمَّن الأمر عمليَّة نَقْل البيانات فقط، بل يمتدّ إلى وَضْع علامة على جميع ملفَّات تعريف الارتباط بالسِّمة الآمنة وتوفير عمليَّات إعادة التَّوجيه التِّلقائيّ من صفحات HTTP إلى صفحات HTTPS؛ لضمان الاتِّصال المُشفَّر بالمُتصفِّحات[3]؛ فالتَّصميم الصَّحيح لسياسة أمَان المُحْتَوَى يُسْهِم في حماية الصَّفحات على الويب من هجوم البرمجة النَّصِّيَّة عبر المواقع، وغيرها من الهجمات السِّيبرانيَّة.

1. Content Security Policy (CSP). On site: https://cutt.us/7Dcv2.
2. Content Security Policy in Cybersecurity. On site: https://cutt.us/QBfJJ.
3. ما هجمات الاستنشاق وكيف يمكن منعها؟ متاح على الرَّابط: https://cutt.us/NzcrB.

ويُقصَد بالسِّياسة: سلسلة تتضمَّن توجيهات السِّياسة التي تَصِف أمَان المُحْتَوَى الخاصّ بالمستخدم على الويب؛ حيث توجد مجموعة من التَّوجيهات لعدَّة أنواع من العناصر، أي يكون لكلّ نوع سياسته الخاصَّة، بما في ذلك الخطوط والصُّور ووسائط الصَّوت والفيديو والبَرمَجيَّات النَّصِّيَّة؛ ويتمّ تعريف توجيهات سياسة أمَان المُحْتَوَى في رؤوس استجابة HTTP التي تُسمَّى رؤوس CSP، ومهمَّتها إرشاد المُتصفِّح إلى مصادر المحتوى الموثوقة، كما تتضمَّن قائمة بالمصادر التي ينبغي مَنْع الوصول إليها.

وهناك عدَّة فئات يَنْدَرِج ضمنها توجيهات سياسة أمَان المُحْتَوَى CSP التي تختلف وفق حالة الاستخدام وسمة المحتوى، وهي:

- **إحضار التَّوجيهات؛** حيث تُحدِّد هذه التَّوجيهات المواقع التي يتمّ منها تحميل أنواع محدَّدة من الموادّ، **وتتضمَّن ما يلي:**

1. Child-Source: وهذا التَّوجيه مسؤول عن تحديد مصادر البَرمَجيَّات النَّصِّيَّة المُدْرَجة في القائمة البيضاء لمسار التَّصفُّح المتضمَّن في الإطارات وعُمَّال الويب.
2. Connect-Source: هذا التَّوجيه مسؤول عن تحديد عناوين URL التي يتمّ تحميلها باستخدام البَرمَجيَّات النَّصِّيَّة.
3. Default-Source: التَّوجيه الاحتياطيّ لجميع توجيهات الإحضار، ويُحدِّد قائمة المصادر الافتراضيَّة لتوجيهات الجلب الأخرى.
4. Object-Source: يُحدِّد المصادر المسموح بها لعناصر <applet> و<embed> و<object>.
5. Style-Source: يُوفِّر قائمة بالمصادر الصَّالحة لأوراق الأنماط المتتالية، ويُقصَد بها: لغة تنسيق صفحات الويب التي تهتمّ بشكل المواقع وتصميمها.

- **توجيهات المستند،** التي تُساعِد على التَّحكُّم بخصائص بيئة العمل (المستند)، **وتشمل:**

1. وَضْع الحماية: فهو يحمي موردًا مُحدَّدًا مشابهًا لعناصر البرنامج النَّصِّيّ المضمَّنة.
2. base-uri: يُحدِّد عناوين URL المسموح بها في العنصر الأساسيّ للمستند.

- **توجيهات التَّصفُّح،** هذه التَّوجيهات تُسيطر على مواقع إرسال المستند (أي تنقُّلاته)، وتشمل:

1. إجراء المستند: وهو يُحدِّد عناوين URL التي تُرسِل عناصر المستند.
2. أصول الإطار: وتعمل على تقييد الأصول التي يتمّ تضمينها في صفحة الويب.

- **توجيهات الإبلاغ، وهي المسؤول عن توثيق انتهاكات سياسة أمَان المُحْتَوَى والإبلاغ عنها، وتشمل:**

1. تقرير إلى: بدء عمليَّة انتهاك سياسة الأمان.
2. تقرير URI: يُوجِّه بيئة المستخدم إلى الإبلاغ عن أيّ محاولة لانتهاك مواصفات سياسة أمَان المُحْتَوَى CSP.
3. require-sri-for: يَفْرِض استخدام تكامل الموارد الفرعيَّة (SRI) لسمة النَّمط ومصادر البرنامج النَّصّيّ للصَّفحة.
4. الأنواع الموثوقة trusted-types: تقوم بتحديد قائمة بالقيم المكتوبة غير القابلة للتَّحايل من قِبل المُهاجِمين السِّيبرانيِّين؛ ما يحدّ من هجمات XSS .
5. المُطالَبة بأنواع موثوقة من أجل require-trusted-types-for: يقوم توجيه السِّياسة هذا على فَرْض سياسة الأنواع الموثوقة على البَرمَجيَّات النَّصِّيَّة.
6. طلبات التَّرقية غير الآمنة upgrade-insecure-requests: قد تتضمَّن بعض مواقع الويب عناوين URL قديمة غير آمنة، لذا تقوم سياسة التَّوجيه هذه بإرشاد المتصفِّح للتَّعامُل مع تلك العناوين واستبدالها بأكثر أمنًا HTTPS.[1]

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

ثانيًا: آليَّة عمل سياسة أمَان المُحْتَوَى (CSP)

إنّ أفضل طريقة لإضافة سياسة أمَان المُحْتَوَى CSP بأثر رجعيّ إلى موقع ويب بالكامل هي تحديد قائمة بيضاء فارغة تمامًا، لحَظْر كلّ شيء. والمطلوب هو تشغيل تلك السّياسات مبدئيًّا في وَضْع التَّقرير فقط، ليبدأ المُتصفِّح بتقييم القواعد أوَّلًا قبل حَظْر المحتوى، حينها يمكن للمستخدم مراجعة الأخطاء وتصنيف كلّ منها في قائمة المسموح به أو غير المسموح به.

فعند تحميل المُتصفِّح إحدى الصَّفحات التي تتضمَّن سياسة أمَان المُحْتَوَى، فإنَّه يتحقَّق منCSP للتَّأكُّد من أنّ المحتوى مصرَّح به، وفي حال كان غير مُصرَّح به يقوم المُتصفِّح حينها بحَظْر تحميله عارضًا رسالة تُفيد بالخطأ، وهذا الإجراء يُسْهِم في مَنْع المُهاجِمين من إدخال تعليمات برمجيَّة ضارَّة إلى الصَّفحة، وبالتَّالي يؤدِّي إلى حماية مستخدمي الويب من الهجمات الخبيثة، وتُساعِد سياسة أمَان المُحْتَوَى أيضًا في حماية الموقع الخاصّ بالمستخدم من الوَضْع في القائمة المحظورة التي تَفْرِضها محرِّكات البحث مثل جوجل Google عند التَّعرُّف على أيّ من البرمجيَّات الضَّارَّة عليه، وهو ما يؤثِّر في عدد الزِّيارات والعملاء، ومن ثمّ يؤثِّر في سمعة العلامة التِّجاريَّة والأرباح؛ ولا بُدّ هنا من الإشارة إلى أنّ سياسة أمَان المُحْتَوَى CSP لا تُوفِّر الحماية المتكاملة لمواقع الويب، لذا ينبغي فَحْص المواقع بحثًا عن أيّ تهديداتٍ أمنيَّةٍ.[1]

ولتنفيذ سياسة أمَان المُحْتَوَى CSP هناك عدَّة خطوات

أ. اختيار مزوِّد الخدمة الخاصّ بموقع الويب

تختلف التَّوجيهات المُتضمَّنة في سياسة أمَان المُحْتَوَى لذا يُفضَّل تخصيص السِّياسة التي تتناسب مع احتياجات كلّ مستخدم على موقع الويب الخاصّ به أو التَّطبيق، ومن أجل ذلك ينبغي إنشاء قائمة بالتَّوجيهات (أو السِّياسات) لتحديد الموارد التي سيُسْمَح بها أو لن يُسْمَح بها على موقعك.

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

ومن مزوّدي خدمات الاتّصالات (CSP) المتخصّصين في سيناريوهات أمان مواقع الويب الشّائعة:

- في حال الرّغبة في مَنْع تحميل إطارات iframes على موقع الويب يتمّ استخدام frame-Source، لتصبح الصّيغة كالآتي: Content-Security-Policy:frame-Source’ none’.

وهنا يجب التّأكُّد من فَصْل التّوجيهات المتعدّدة بفاصلة منقوطة عند إنشاء CSP.

- استخدام script-Source لمَنْع تحميل JavaScript على موقع الويب، لتصبح الصّيغة كالآتي: Content-Security Policy:script-Source none”.
- ولتقييد المحتوى بخلاف الصُّور على مواقع الويب الخاصّة بالمستخدمين يتمّ استخدام img-Source، لتصبح الصّيغة كالآتي:

Content-Security-Policy: default-Source ‘self’; img-Source.

ويجب التّنبيه على أهمّيّة التّعيين الافتراضيّ Source على “self” أو “none” وإدراج الموارد المسموح بها بشَكْلٍ واضحٍ؛ لعدم التّعيين الافتراضيّ لجميع الصُّور بالمرور، وإنّ كلمة “self” لا تتضمَّن أيًّا من النّطاقات الفرعيّة.

وللسّماح بالمحتوى نفسه فقط من المصدر نفسه وموقع الويب الخاصّ بالمستخدم ونطاقاته الفرعيّة يتمّ استخدام default-Source. لتصبح الصّيغة كالآتي:

Content-Security-Policy: default-Source ‘self’ *.sucuri.net.

والسّماح فقط للوسائط أو البَرمَجيّات النّصّيّة الأخرى القابلة للتّنفيذ من المصدر نفسه، لتصبح الصّيغة كالآتي:

Content-Security-Policy: default-Source ‘self’; img-Source *; media-Source sucuri.net; script-Source sucuri.net.

وينبغي اختبار سياسة أمان المستخدم CSP الخاصّ بالمستخدم قبل تنفيذها؛ للتّأكُّد من عدم نسيان تضمين أيّ أصل موثوق لموقع الويب.[1]

ويمكن لمستخدمي الإنترنت تلقّي إشعارات تنبيهيّة في حال تمّ انتهاك سياستهم، لكن دون حَظْر المحتوى، من خلال ضَبْط رأس استجابة عن HTTP على تقرير سياسة أمَان المُحْتَوَى فقط.

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

ب. إضافة سياسة أمْن المُحْتَوَى CSP إلى رأس استجابة HTTP الخاصّ بموقع الويب

تختلف التَّوجيهات المُتضمَّنة في سياسة أمَان المُحْتَوَى لذا يُفضَّل تخصيص السِّياسة التي تتناسب مع احتياجات كلّ مستخدم على موقع الويب الخاصّ به أو التَّطبيق، ومن أجل ذلك ينبغي إنشاء قائمة بالتَّوجيهات (أو السِّياسات) لتحديد الموارد التي سيُسْمَح بها أو لن يُسْمَح بها على موقعك.

تتمّ أغلب التَّعديلات على رأس استجابةHTTP ، ويجب أوَّلًا معرفة الخادم الخاصّ بموقع الويب الخاصّ بالمستخدم قبل تعيين HTTP؛ وللتَّعرُّف على الخادم الذي يعمل عليه موقع الويب الخاصّ بكلّ مستخدم يمكنك تسجيل الدُّخول إلى cPanel الخاصّ به والتَّحقُّق من واجهة معلومات الخادم لمعرفة ذلك؛ إذ تُوفِّر cPanel النِّظام الأساسيّ لإدارة الخوادم والمواقع الأكثر موثوقيَّة.[1]

واختصارًا، توجد عدَّة خيارات متاحة لفعل ذلك

1. تعيين سياسة أمْن المُحْتَوَى CSP باستخدام IIS (خدمات معلومات الإنترنت)

IIS manager خدمات معلومات الإنترنت هو خادم ويب من Microsoft يعمل على نظام التَّشغيل Windows، ويُستخدَم لتبادل محتوى الويب الثَّابت والدِّيناميكيّ مع مستخدمي الإنترنت، ويمكن استخدامه أيضًا لاستضافة تطبيقات الويب ونَشْرها وإدارتها.

2. قُمْ بتعيين CSP الخاصّ بك باستخدام Apache

Apache هو خادم ويب مسؤول عن قبول طلبات الدَّليل HTTP من مستخدمي الإنترنت وإرسال المعلومات المطلوبة إليهم في شكل ملفَّات وصفحات ويب.

3. تطبيق سياسة أمَان المُحْتَوَى

تُنفَّذ سياسات أمَان المُحْتَوَى بواسطة رأس HTTP خاصّ يتمّ إرساله مع الاستجابة من الخادم، الذي يتضمَّن قواعد تلك السِّياسات التي تُفْرَض فيما بعد عبر المُتصفِّح؛ وهناك طريقتان للقيام بذلك، **هما:**

- إضافة سياسات أمَان المُحْتَوَى الخاصَّة بموقع الويب عبر علامات وصفيَّة لتعمل على جميع المُتصفِّحات، وللقيام بذلك في حال عدم وجود حقّ الوصول لتكوين خادم الويب الخاصّ بموقع المستخدم يمكن استخدام علامة HTML لتمكين سياسة أمْن المُحْتَوَى الخاصّ بالموقع داخل HTML الخاصّ بالصَّفحة.
- تعيين تلك السِّياسات الخاصَّة بموقع المستخدم بواسطة رأس استجابة HTTP، وهذه الطَّريقة تَدْعم معظم المُتصفِّحات، باستثناء Internet Explorer وبعض الإصدارات الأقدم من المُتصفِّحات. [2]

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

الفَصْل الثَّاني

كيفيَّة تفعيل سياسة أمَان المُحْتَوَى (CSP) والمخاطر الرَّقميَّة التي تحدّ منها

- أوَّلًا: كيفيَّة تفعيل سياسة أمَان المُحْتَوَى (CSP)
- ثانيًا: المخاطر الرَّقميَّة التي تحدّ منها سياسة أمَان المُحْتَوَى (CSP)

02

أولًا: كيفيَّة تفعيل سياسة أمَان المُحْتَوَى (CSP)

لأنّ سياسة أمَان المُحْتَوَى هي أفضل وسيلة للحماية من الهجمات الخبيثة التي يُطْلِقها المُتسلِّلون السِّيبرانيُّون ضدّ مُستخدِمي الإنترنت، والجيِّد في الأمر أنَّه يمكن للمُستخدِم التَّأكُّد من وجود تلك السِّياسات وتفعيلها على موقع الويب. وهناك مكانان يمكن العثور فيهما على مُقدِّمي الخدمات المُفعِّلة لتلك السِّياسات التَّوجيهيَّة، وهما رؤوس الاستجابة، والعلامات الفوقيَّة.

وللعثور على سياسة أمْن المُحْتَوَى في رؤوس الاستجابة يمكن اتِّباع الخطوات التَّالية:

1. باستخدام المُتصفِّح، افْتَح أدوات المُطوِّرين (اسْتَخْدِم أدوات DevTools في Chrome) ثمّ انْتَقِل إلى موقع الويب الذي تختاره، وافْتَح علامة التَّبويب "الشَّبكة".
2. ابْحَث عن الملفّ الذي يُنشئ الصَّفحة، الذي يكون له نطاق موقع الويب نفسه الذي تتَصَفَّحه، وهو في الأغلب يكون العنصر الأوَّل في علامة التَّبويب "الشَّبكة".
3. عند النَّقر على الملفّ يَظْهَر مزيد من المعلومات، حينها تبدأ عمليَّة البحث عن رمز الاستجابة OK200.
4. وفي الأسفل سيَظْهَر استخدام سياسات أمْن المُحْتَوَى من عدمه.[1]

مثال: تطبيق هذه الخطوات على منصة X.

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

المكان الثّاني للعثور على سياسة أمَان المُحْتَوَى CSP يكون في علامة التّعريف

1. انْتَقِل إلى مصدر الصَّفحة وافْتَح المُتصفِّح واخْتَر موقع الويب.
2. انْقُر بِزِرّ الفأرة (الماوس) 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".

أدوات مجّانيَّة تُساعِد على إنشاء سياسة أمَان المُحْتَوَى وتقييمها ومراقبتها

1. تتضمَّن أدوات تدقيق w3af مُكوِّنًا إضافيًّا لتدقيق تطبيقات الويب بشَكْلٍ تلقائيّ للتَّأكُّد من تفعيل سياسات أمْن المُحْتَوَىCSP.
2. اختبار CSP (امتداد المُتصفِّح) لبناء السِّياسة الخاصَّة بتطبيق موقع الويب الخاصّ بالمستخدم واختبارها.
3. مُوَلِّد سياسة أمْن المُحْتَوَى CSP Generator لإنشاء السِّياسات تلقائيًّا (امتداد Chrome/Firefox).
4. مُقيم CSP لتقييم سياسات أمَان المُحْتَوَى الحاليَّة.
5. أداة تجميع تقارير Csper لمُراقَبة سياسة أمَان المُحْتَوَى باستخدام تقرير uri.[1]

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

ثانيًا: المخاطر الرَّقميَّة التي تحدّ منها سياسة أمَان المُحْتَوَى (CSP)

بواسطة سياسة أمَان المُحْتَوَى يمكن إيقاف الهجمات السِّيبرانيَّة، مثل هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS)، ما يُساعِد أصحاب مواقع الويب على تحديد الموارد الآمنة وغير الآمنة، وتُسْهِم تلك السِّياسات أيضًا في تمكين أصحاب مواقع الويب من وَضْع قواعدهم الخاصَّة التي تناسب احتياجات موقعهم، فضلًا عن كونها تَمْنَع وصول غير المُصرَّح لهم إلى المعلومات المهمَّة، وهذا بالإضافة إلى توفير أدوات إعداد التَّقارير والتَّحليلات التي تبحث عن الثَّغرات الأمنيَّة بعد تثبيت سياسة أمَان المُحْتَوَى CSP.

ومن الهجمات التي تحدّ منها تلك السِّياسات:

- هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS)

تُعَدّ هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS) نوعًا من أنواع الحقن؛ إذ يقوم المُهاجِم السِّيبرانيّ بحَقْن البَرمَجيَّات النَّصِّيَّة الضَّارَّة في مواقع الويب الموثوقة، ويَقَعُ الهجوم عندما يستخدم المُهاجِم تطبيق ويب لإرسال تعليمات برمجيَّة ضارَّة في شكل برنامجٍ نَصِّيٍّ من جانب المُتصفِّح إلى المستخدم.

ويتمّ التَّحايل في هذا الهجوم؛ إذ يَظْهَر البرنامج النَّصِّيّ الضَّارّ كأنَّه من مصدر موثوق، ومن هنا يتمكَّن البرنامج النَّصِّيّ الضَّار من الوصول إلى أيّ ملفَّات تعريف ارتباط أو معلومات حسَّاسة يحتفظ بها المُتصفِّح ويستخدمها في موقع الويب، ويمكن لهذه البَرمَجيَّات النَّصِّيَّة إعادة كتابة محتوى صفحة HTML .[1]

وتنقسم هذه الهجمات السِّيبرانيَّة إلى:

1. هجمات XSS المنعكسة

في هذه الفئة يَنْعَكِس البرنامج النَّصِّيّ الضَّارّ الذي تمّ إدخاله على خادم الويب، كما هو الحال في رسالة خطأ أو نتيجة بحث أو أيّ استجابة أخرى تتضمَّن بعض المدخلات المُرْسَلة إلى الخادم -أو كلّها- كجزء من الطَّلب.
ويتمّ تسليم هجمات XSS المنعكسة إلى الضَّحايا من خلال طريق آخر، مثل رسالة بريد إلكترونيّ، أو على بعض مواقع الويب الأخرى، وبمجرَّد نَقْر المُستخدِم على الرَّوابط الضَّارَّة أو تَصَفُّح الموقع المُتضرِّر يتمّ انتقال التَّعليمات البرمجيَّة المحقونة إلى موقع الويب الضَّعيف، ما يَعْكِس الهجوم مرَّة أخرى على مُتصفِّح المُستخدِم، ثمّ يبدأ المُتصفِّح تنفيذ التَّعليمات البرمجيَّة لأنَّها جاءت من خادم "موثوق" وهي عمليَّة خداع [1].

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

2. هجمات XSS المخزَّنة

يُقْصَد بها تخزين برنامج نَصّيّ محقون بشَكْلٍ دائمٍ على الخوادم المُستهدَفة، كما هو الحال في قاعدة البيانات، أو سجلّ الزَّائرين، أو حقل التَّعليق، وما إلى ذلك. وبعد ذلك يبدأ المُستخدِم الضَّحيَّة استرداد البرنامج النَّصّيّ الضَّارّ من الخادم عندما يَطْلُب النَّصّ المُخَزَّن.

3. البرمجة النَّصِّيَّة عبر المواقع العمياء

هي شكل من أشكال هجمات XSS المستمرَّة، وتتمّ عند حِفْظ بَرمَجيَّات المُهاجِم على الخادم وإعادتها إلى الضَّحيَّة، فمثلًا في "نماذج البيانات" يقوم المُهاجِم بإرسال بَرمَجيَّات ضارَّة، وبمجرَّد فَتْح المُستخدِم للنَّموذج يبدأ التَّنفيذ.

وتتسبَّب هجمات البرمجة النَّصِّيَّة عبر المواقع XSS في عدد من المشكلات للمُستخدِمين الضَّحايا، **تَصِل إلى:**

- اختراق الحساب بالكامل.
- تَثْبيت بَرمَجيَّات حصان طروادة.
- إعادة تَوْجيه المُستخدِم إلى صفحة أخرى أو موقع آخر.
- تعديل عَرْض المحتوى.
- تعديل بيان صحفيّ أو خَبَر على سِعْر سَهْم المؤسَّسة؛ ما يتسبَّب في تقليل ثقة المستهلك بها.[1]

هجوم استنشاق الحزم a packet sniffing attack

يُعْرَف هجوم استنشاق الحزم بأنَّه 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.

يُعَدّ هذا الهجوم من هجمات التَّجسُّس التي تعمل بشَكْلٍ جيِّدٍ على الشَّبكات غير المُشَفَّرة.

وتوجد فئتان من هجمات استنشاق الحزم، هما:

1. الاستنشاق النَّشِط لحُزَم الاتِّصال Active packet sniffing

يُسْتَخْدَمُ هذا النَّوع من الهجوم على الشَّبكات الأكبر حجمًا؛ فمع اتِّصال مزيدٍ من الأجهزة بشبكة واحدة، تصبح هناك حاجة إلى مُحَوِّل الشَّبكة، وهنا تبدأ الشَّبكة توجيه حركة مرور الإنترنت إلى حيث من المفترض أن تذهب؛ كي لا يُسَيْطِر حَجْم حركة المرور على كلّ جهازٍ متَّصلٍ بها.

ويقوم هجوم الاستنشاق النَّشِط لحُزَم الاتِّصال في هذه الحالة بإدخال حركة مرور إضافيَّة إلى الشَّبكة المُستهدَفة والانتظار حتى يقوم مُحَوِّل الشَّبكة بإعادة تَوْجيه حركة المرور المشروعة؛ ليَتَمَكَّن المُهاجِم السِّيبرانيّ من الوصول إلى مُحَوِّل الشَّبكة وبدء هجومه، ويُعَدّ هذا النَّوع النَّشِط من هجمات الاستنشاق أكثر قابليَّةً للاكتشاف؛ لأنَّه يجب أن يُعلِن عن نفسه.

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

2. الاستنشاق غير النَّشِط لحُزَم الاتِّصال

يُنَفَّذُ هذا الهجوم في الشَّبكات الأصغر حجمًا؛ إذ تكون جميع الأجهزة مُتَّصِلَة بمركز شبكة واحد، وهنا لا يحتاج الهجوم إلى الاعتماد على مُحَوِّلات الشَّبكة لتَوْجيه حركة المرور، ولا يحتاج إلى الكَشْف عن نفسه؛ لذا يَصْعُب اكتشاف هؤلاء المُهاجِمين.

كيفيَّة تنفيذ هجوم استنشاق الحزم

يقوم المُهاجِم السِّيبرانيّ في هجمات استنشاق الحزم باستهداف مناطق معيَّنة في الشَّبكة أو منافذ الأجهزة أو مواقع الويب، وهناك عدَّة طُرُق لمراقبة حركة مرور الشَّبكة، فيما يلي تبيان لأهمِّها:

1. استنشاق كلمة المرور

يقوم المُهاجِم بجَمْع حزم البيانات التي تحتوي على كلمات المرور وبيانات تسجيل الدُّخول الأخرى في هدوء؛ إلَّا أنّ قيام مواقع الويب الشَّرعيَّة باستخدام تشفير https وَفَّر الأمان لكلمات المرور، لذا يَلْجَأ المُهاجِمون إلى استخدام هجمات التَّنصُّت الوسيط man-in-the-middle attacks، وهي نوع من هجمات التَّنصُّت على الشَّبكة لجَمْع بيانات كلمات المرور.

2. تزوير DNS

هو نوع من الهجمات المزيَّفة التي تستخدم أداة شمّ الحزم لإعادة تَوْجيه حركة مرور الإنترنت نحو موقع ويب ضارّ.

3. استنشاق JavaScript

يحدث استنشاق JavaScript أو Formjacking عندما يقوم المُهاجِم بإدخال تعليمات برمجيَّة ضارَّة عند نقطة الشِّراء على مواقع التِّجارة الإلكترونيَّة، وتُشْبِه بَرمَجيَّاتJavaScript النُّسخة الإلكترونيَّة من كاشطات بطاقات الصَّرَّاف الآليّ لجَمْع المعلومات الماليَّة.

4. تزوير بروتوكول تحليل العنوان (ARP)

يحدث عندما ينتحل أحد المُتسلِّلين عنوان IP الخاصّ بمُضِيفٍ أو جهازٍ على شبكة محليَّةٍ، لتنتهي حركة المرور إلى المُتسلِّل بدلًا من الوِجْهة الصَّحيحة.

5. خرق جلسة اتِّصالات بروتوكول التَّحكُّم في الإرسال TCP

بمجرَّد إنشاء اتِّصال بين المُرسِل والمُستقبِل، يقوم المُهاجِم بخرق جلسة TCP ونَقْل البيانات الموثوقة التي تتمّ واستنشاق حركة مرور البيانات على الشَّبكة.[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.

متى يُفضَّل استخدام سياسات أمَان المُحْتَوَى CSP؟

يُوصَى باستخدام تلك السِّياسات للتَّطبيقات التي تُدِير البيانات الحسَّاسة، مثل واجهات المُستخدِم الإداريَّة ووحدات تحكُّم إدارة الأجهزة، أو المُنْتَجات التي تَسْتَضيف المستندات أو الرَّسائل أو ملفَّات الوسائط التي أنشأها المُستخدِم.

أمَّا التَّطبيقات الثَّابتة دون أيّ وظائف أو ملفَّات تعريف ارتباط لتسجيل الدُّخول؛ فلا يُفضَّل استخدام تلك السِّياسات معها، وكذلك التَّطبيقات الكبيرة التي لها تاريخٌ مع هجمات XSS، فإنّ تلك السِّياسات ستكون آليَّة أمان إضافيَّة، لكنّ الأساس هو التَّعليمات البرمجيَّة المُصَمَّمة للحماية من هذه الهجمات السِّيبرانيَّة.

ونضيف إلى ذلك أنّ سياسات CSP لا تكون مفيدة في حال أُنْشِئَت سياسة تَسْمَحُ بالبَرمَجيَّات النَّصِّيَّة المُضمَّنة أو تَسْمَحُ بتحميل البَرمَجيَّات النَّصِّيَّة من مجالات غير موثوقة، ففي هذه الحالة هي لا تحمي من هجمات XSS.[1]

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

تمارين وتَدْريبَات

تُعدّ التَّمَارِين جزءًا رئيسًا من عمليَّة التَّدريب، وهي تُحقِّق عدَّة أهداف وغايات، فيما يلي تبيان لأهمّها:

- التَّمَارِين أداة فعَّالة لمعرفة مدى استفادة الطَّلبة من المحتوى التَّدريبيّ، ومدى الأثر الذي حقَّقته على المخزون المعرفيّ لدى الطَّلبة .
- أداة مُهمَّة لترسيخ المعلومات والمعارف لدى الطَّلبة ؛ كونها تُمثِّل مُراجَعَة سريعة للمحتوى التَّدريبيّ.
- اكتشاف الفُرُوق المعرفيَّة بين الطَّلبة .
- تُمثِّل تغذيةً عكسيَّة للمُدرِّب، وتُقدِّم له معلومات حول فاعليَّة الحقيبة التَّدريبيَّة وفاعليَّة أسلوبه التَّدريبيّ.

منهجيَّة التَّعامُل مع التَّمَارِين

التَّمَارِين المذكورة في هذا القسم شاملة للمحتوى التَّدريبيّ في هذه الحقيبة، وفيما يلي توضيح للمنهجيَّة المُقترَحَة للتَّعامُل معها:

- خلال التَّدريب يقوم المُدَرِّب وبعد الانتهاء من فِكْرةٍ ما بالطَّلب من الطَّلبة فَتْح الكُتَيِّب الخاصّ بهم، والقيام بالإجابة عن السُّؤال المُحدَّد، والذي يرتبط بشكلٍ مُباشِر بالفكرة أو الموضوع الذي يُقدِّمه لهم.
- التَّمَارِين مُختَارة بعناية، بحيث تكون مُبسَّطة وسهلة الفَهْم، وقابلة للحلّ مِن قِبَل طلبة المرحلة الثَّانويَّة، وهنا من الممكن للمُدَرِّب تقديم الدَّعْم الطَّلبة في الإجابة عن بعض التَّمَارِين في حال اقتضت الضَّرورة، وهذا الأمر يُتْرَك لتَقْدير المُدَرِّب.
- التَّمَارِين ستكون على جزأين؛ جزءٌ خاصّ بالصَّفّ، وتُسمَّى بالتَّمَارِين الصَّفِّيَّة، وآخر لا صَفِّيّ، يقوم الطَّالب بالإجابة عنها كواجبٍ منزليّ.
- تمَّ إضافَة الحَلّ الخاصّ بكُلّ تَمْرين، مع تمييز الإجَابَة بلَوْن مُختَلف.

وفيما يلي تبيان للتَّمارين الخاصَّة بالحقيبة، مُرتَّبة وفقًا للفصول ووفقًا لطبيعتها الصَّفِّيَّة واللَّاصَفِّيَّة، مع العِلْم بأنَّ ذات التَّمَارِين وبصيغتها الموجودة هنا هي ذاتها موجودة في الكُتَيِّب الخاص بالطَّالب.

أولًا: التَّمارين الصَّفيَّة

التَّدريبات هنا مَرْفَقة بالحَلّ، بينما في كُتَيِّب الطَّالب مَكْتوبة بدون حَلّ، ومَرْفَق معها تَوجيه للطَّالب لكيفيّة الحلّ، وذلك حيث تقتضي الضَّرورة.

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.

أكْمِل الجُمَل التَّالية:

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

2. تُعدّ هجمات ..... **البرمجة** ..... النَّصِّيَّة عبر المواقع ..... **المُشْتَرَكة (XSS)** ..... نوعًا من التَّعليمات البرمجيَّة الخبيثة والضَّارَّة في ..... **المواقع غير** ..... الموثوقة، وغالبًا ما تُستخدَم في مهاجمة مواقع ..... **التِّجارة** ..... الإلكترونيَّة.

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

4. سياسة أمَان المَحْتَوَى CSP اختصارٌ لجُمْلَة ..... **Content security policy** ..... باللُّغة الإنجليزيَّة.

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

6. عند تشغيل سياسة أمَان المُحْتَوَى لموقع ويب تُؤثّر سلبًا على الاتّصالات والبرامج النّصّيّة والخطوط.

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

8. تُعدّ سياسة أمَان المُحْتَوَى إضافةً غير مُهمّة إلى المواقع الإلكترونيّة.

9. سياسة أمَان المُحْتَوَى عبارة عن طبقة إضافيّة من الأمان تُساعد على كَشْف الهجمات الإلكترونيّة.

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

انْتَبِه!

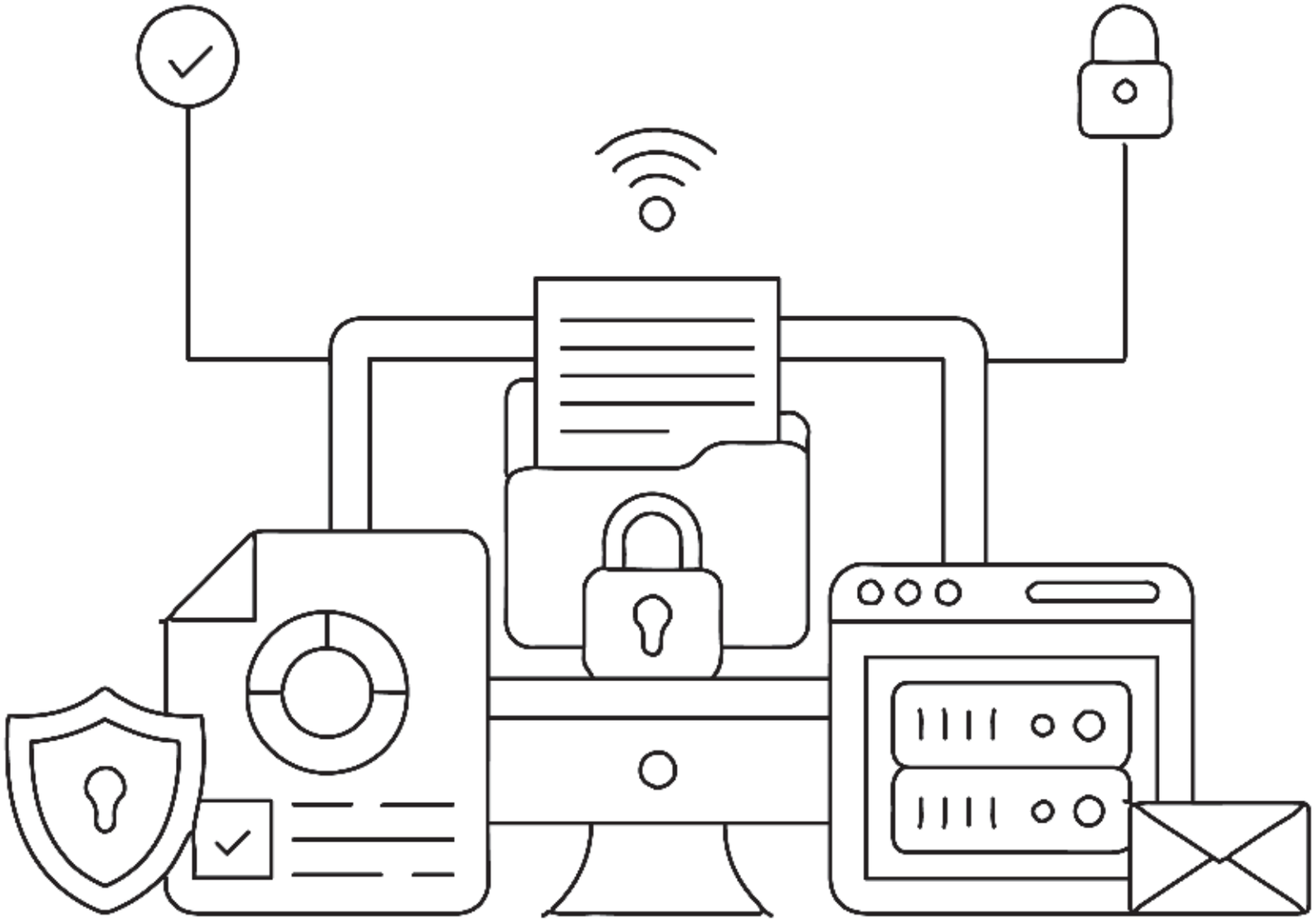
أفضل طريقة لإضافة سياسة أمَان المُحْتَوَى CSP بأَثَر رَجْعِيّ إلـى مـوقـع ويـب بالـكامـل

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

Default-Source	التَّوجيه الاحتياطيّ لجميع توجيهات الإحضار، ويُحدِّد قائمة المصادر الافتراضيَّة لتوجيهات الجلب الأخرى.
Child-Source	وهذا التَّوجيه مسؤول عن تحديد مصادر البرامج النَّصِّيَّة المُدْرَجَة في القائمة البيضاء لمسار التَّصفُّح المُتضمَّن في الإطارات وعُمَّال الويب.
Script-Source	لمَنْع تحميل JavaScript على موقع الويب.
Object-Source	يُحَدِّد المصادر المسموح بها لعناصر <applet> و<embed> و<object>.
Style-Source	يُوفِّر قائمة بالمصادر الصَّالحة لأوراق الأنماط المتتالية، ويُقصَد بها: لغة تنسيق صفحات الويب، التي تهتمّ بشكل المواقع وتصميمها.
Img-Source	لتقييد المحتوى بخلاف الصُّور على مواقع الويب.
Frame-Source	في حال الرَّغبة في مَنْع تحميل إطارات على موقع الويب يتمّ استخدامه.
Connect-Source	هذا التَّوجيه مسؤول عن تحديد عناوين URL التي يتمّ تحميلها باستخدام البرامج النَّصِّيَّة.
Base-Url	يُحدِّد عناوين URL المسموح بها في العنصر الأساسيّ للمستند.



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)

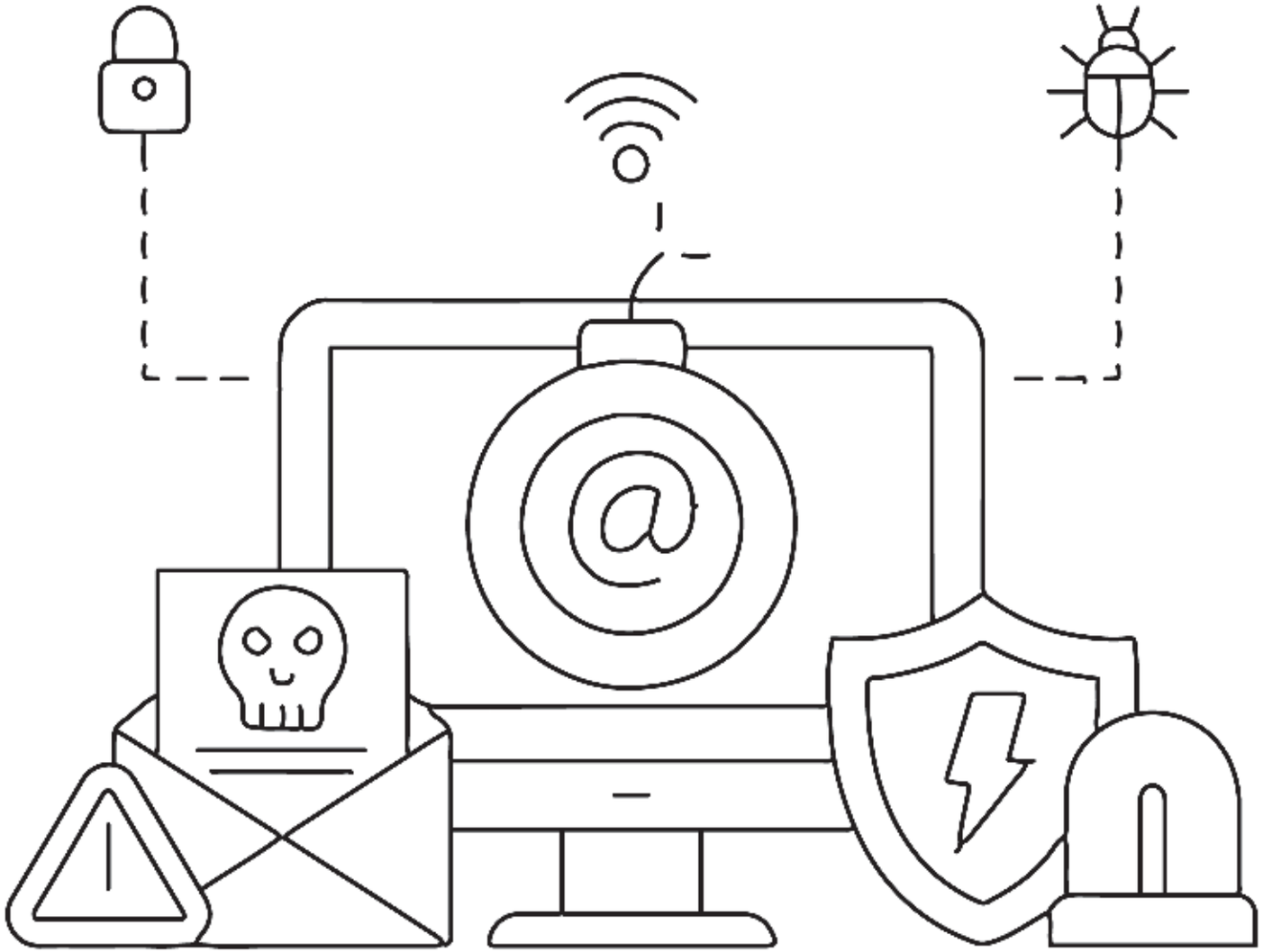
هي نوع من أنواع الحقن؛ إذ يقوم المهاجم الإلكتروني بحَقْن البرمجيَّات النَّصِّيَّة الضَّارَّة في مواقع الويب الموثوقة، ويَقَع الهجوم عندما يَسْتَخْدِم المُهاجِم تطبيق ويب لإرسال تعليمات برمجيَّة ضارَّة في شكل برنامجٍ نَصِّيٍّ من جانب المُتصفِّح إلى المُستخدِم.


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.
- تَثْبيت 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 محرِّكات البحث مثل جوجل Google عند التَّعرُّف على أيٍّ من البرمجيّات الضَّارَّة، وهو ما يؤثِّر في عدد الزِّيارات والعملاء، ومن ثمّ يؤثِّر في سمعة العلامة التِّجاريَّة 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

استخرج الكلمات التَّالية من الجدول:

~~التَّطبيقات~~ - أمان - السَّحابة - التَّشفير - 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.

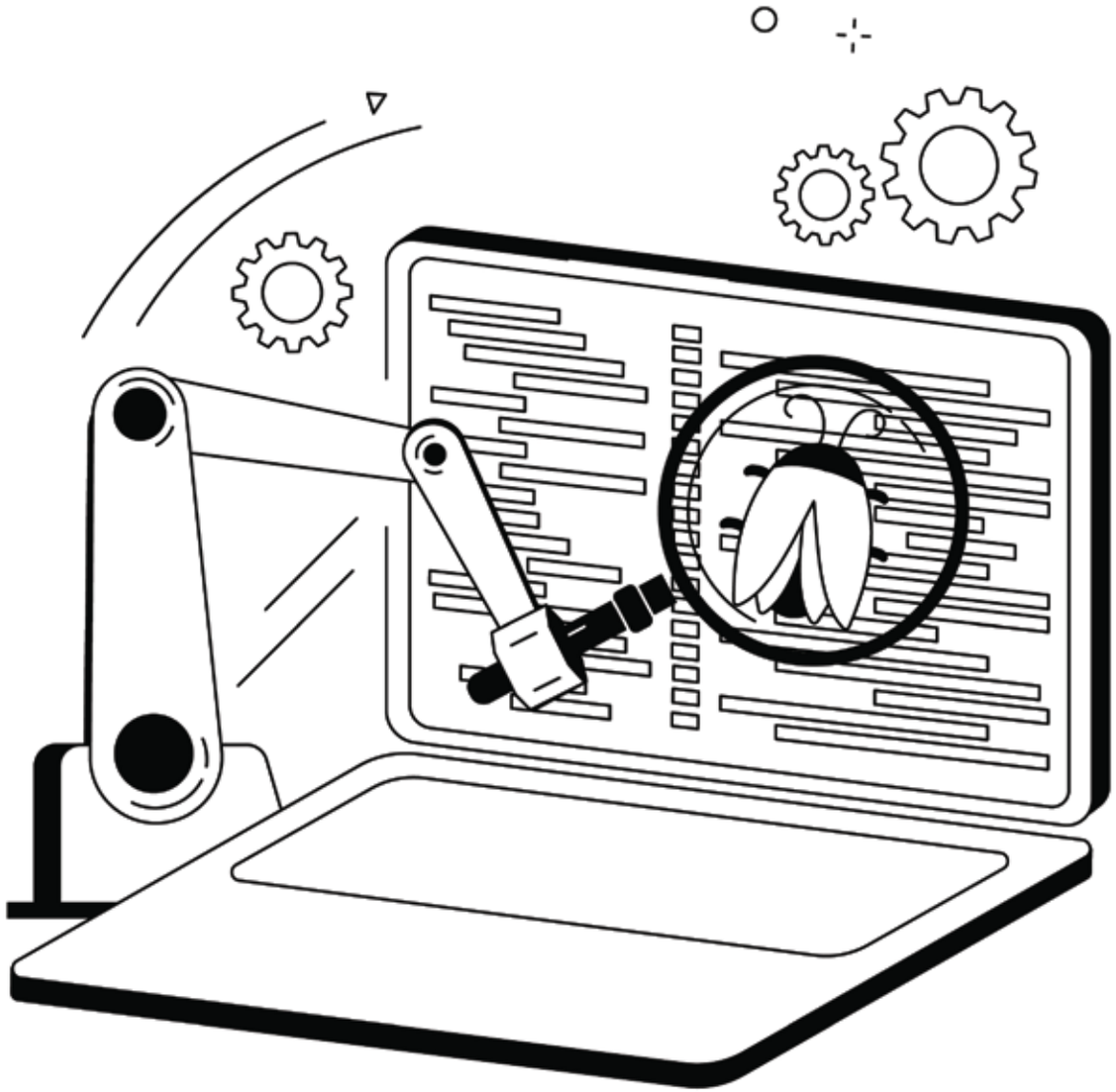
هل تعلم؟

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 استنشاق 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.

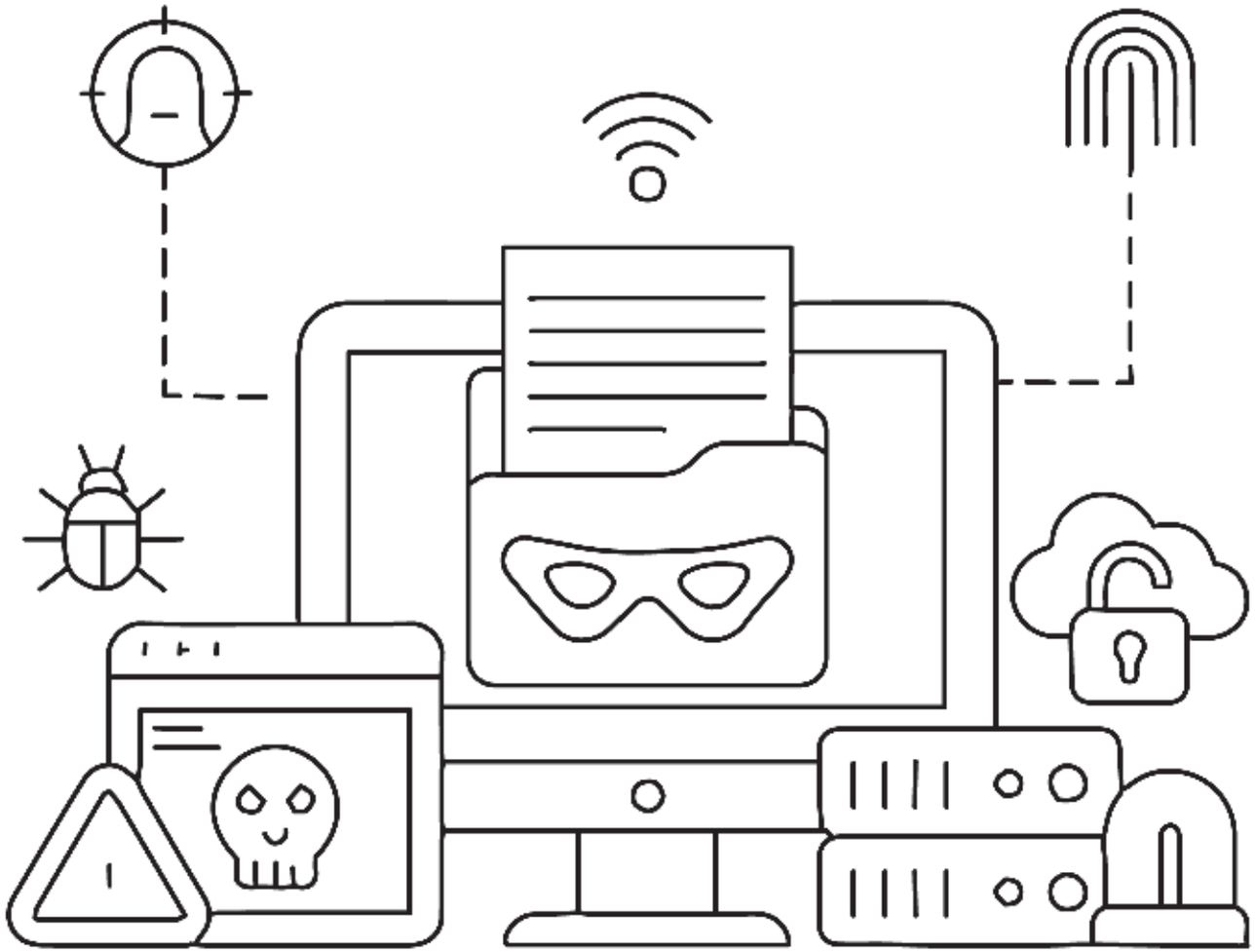
للعثور على سياسة أمان المُحْتَوَى في رؤوس الاستجابة يمكن اتّباع الخطوات التّالية:

باستخدام المُتصفّح، افْتَح أدوات المُطوّرين (اسْتَخْدِم أدوات DevTools في Chrome) ثمّ انْتَقِل إلى موقع الويب الذي تَخْتاره، وافْتَح علامة التّبويب "الشّبكة".

ابْحَث عن الملفّ الذي يُنْشِئ الصّفحة، الذي يكون له نطاق موقع الويب نفسه الذي تَتَصَفّحه، وهو في الأغلب يكون العنصر الأوّل في علامة التّبويب "الشّبكة".

عند النّقر 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 مُعيّنة من الهجمات الإلكترونيّة والحدّ منها.
الإجابة: سياسة أمان المُحتَوى.

هجمات إلكترونيّة يُنفّذها المُتسلّلون لاعتراض ومُراقبة حركة المرور على الشّبكة، وتستهدف رسائل البريد الإلكترونيّ غير المُشفّرة وبيانات تسجيل الدُّخول والمعلومات الماليّة.
الإجابة: هجمات استنشاق الحزم.

سلسلة تتضمّن التّوجيهات التي تَصِف سياسة أمان المُحتَوى 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. **الإجابة: السّياسات.**

إحدى فئات توجيهات سياسة أمان المُحتَوى التي تُحدّد المواقع التي يتمّ منها تحميل أنواع مُحدّدة من الموادّ. **الإجابة: إحضار التّوجيهات.**

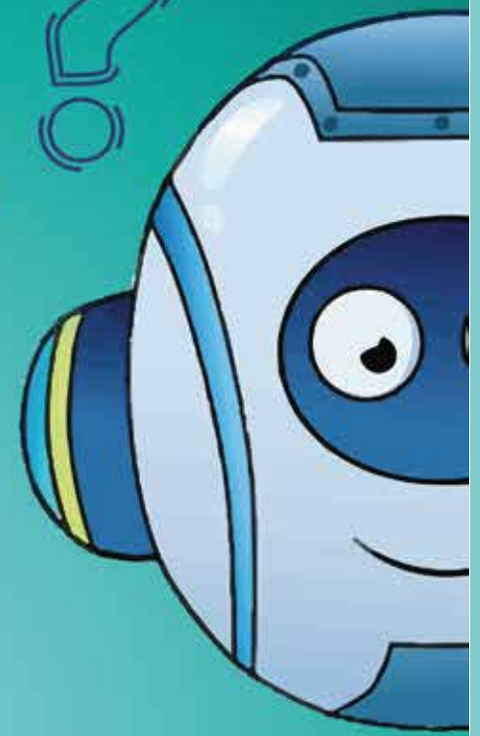
مـا هــو؟

إحدى فئات توجيهات سياسة أمَان المُحْتَوى التي تساعد في التَّحكُّم بخصائص بيئة العمل.
الإجابة: وَضْع الحماية، وbase-uri.

هو 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. **الإجابة: خدمات معلومات الإنترنت IIS manager.**

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

مكانان يمكن العُثور في أيٍّ منهما على مُقدِّمي الخِدْمات المُفعَّلة لسياسة أمان المحتوى.
الإجابة: رؤوس الاستجابة، والعلامات الفوقيّة.



مـا هــو؟

يُقصَد بها تخزين برنامج نصّيّ محقون بشكلٍ دائمٍ على الخوادم المُستهدَفة، كما هو الحال في قاعدة البيانات، أو سِجلّ الزّائرين، أو حَقْل التّعليق، وما إلى ذلك. وبعد ذلك يبدأ المُستخدِم الضَّحيَّة استرجاع البرنامج النَّصّيّ الضّارّ من الخادم عندما يَطلب النَّصّ المُخزَّن. **هجمات XSS المخزَّنة**

هي شَكل من أشكال هجمات XSS المُستمِرَّة، وتتمّ عند حِفْظ بَرْمَجيّات المُهاجِم على الخادم، وإعادتها إلى الضَّحيَّة، فمثلًا في "نماذج البيانات" يقوم المُهاجِم بإرسال برمجيّات ضَارّة، وبمُجرَّد فَتْح المُستخدِم للنّموذج يبدأ التّنفيذ. **البرمجة النَّصّيَّة عبر المواقع العمياء**

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

أكمل العبارات التّالية:

- تهدف طبقة الأمان الإضافيَّة المُتمثِّلة في سياسة أمَان المُحْتَوَى (CSP) إلى **الحدّ من هجمات البرمجة النَّصّيَّة عبر المواقع والإبلاغ عنها**
- تُمَكِّن سياسة أمَان المُحْتَوَى (CSP) مسؤولي الخادم من تَخفيف الأضرار التي يمكن أن يُحْدثها هجوم XSS عن طريق **إظهار المصادر الصَّالحة للبرامج النَّصّيَّة أمام المُتصفِّح والقابلة للتَّنْفيذ**
- من الوظائف التي تُنفِّذها سياسة أمَان المُحْتَوَى أيضًا الحدّ من هجمات **استنشاق الحزم**، وهي هجمات إلكترونية يُنفِّذها المُتسلِّلون لاعتراض ومُراقَبَة حركة المرور على الشَّبكة.
- يتمّ تعريف توجيهات سياسة أمَان المُحْتَوَى في **رؤوس استجابة HTTP** التي تُسمَّى رؤوس CSP ومَهمّتها إرشاد المُتصفِّح إلى مصادر المحتوى الموثوق بها، كما تتضمَّن قائمة بالمصادر التي ينبغي مَنْع الوصول إليها.
- تساعد توجيهات المستند في التَّحكُّم بخصائص بيئة العمل وتشمل: **وَضْع الحماية، base-uri.**
- تُعدّ توجيهات الإبلاغ المسؤولة عن توثيق انتهاكات سياسة أمَان المُحْتَوَى والإبلاغ عنها، وتشمل **تقرير Report-to, تقرير URI**

- قد تتضمَّن بعض مواقع الويب عناوين URL قديمة غير آمِنَة، لذا تقوم سياسة التَّوجيه **طلبات التَّرقية غير الآمنة** 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 **قائمة بيضاء فارغة** لحظر كُلّ شيءٍ.

- تُساعد سياسة أمَان المُحْتَوَى في حماية الموقع الخاصّ بالمُستخدِم من الوَضْع في **القائمة المحظورة** 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 **رأس استجابة HTTP** 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.

- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] استنشاق JavaScript.
- [ ] هجمات التّنصُّت الوسيط.

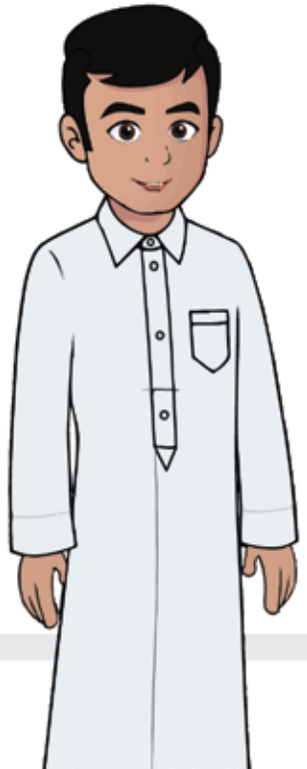
6. بمجرّد إنشاء اتّصال بين المُرسِل والمُستقبِل، يقوم المُهاجِم بالاختراق ونَقْل البيانات الموثوقة التي تتمّ واستنشاق حركة مرور الشّبكة .....

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

مشروع التَّخرُّج

مشروع التَّخرُّج هو واجبٌ تقوم به بمُفْرَدك أو بالاشتراك مع زميل أو زميلين من زُمَلائك، وتقوم من خلاله وتحت إشراف المُدرِّب بأحد الواجبات التَّالية:

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



مراجـــــع

المحتوى العلمي

في الحـــــقيبة

المراجع العربيَّة:

1. ما هي هجمات الاستنشاق؟ وكيف يمكن منعها؟ مُتَاح علَى الرَّابط: https://cutt.us/NzcrB

المراجع الأجنبيَّة:

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/e92IS
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