سياسة أمَان المُحْتَوى (CSP)

شرائح العَرْض

حَقِيبَة خاصَّة بالمُدَرِّب

المرحلة الثَّانويَّة

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

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

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
تمهيد	5 دقائق
الجُزْء 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

فهرس المحتوى العِلْمِيّ

الفَصْل الأَوَّل
مفهوم سياسة أمَان المُحْتَوَى (CSP) وآليَّة عملها

مفهوم سياسة أمَان المُحْتَوَى (CSP)

تُعدّ سياسة أمَان المُحْتَوَى (CSP) طبقة إضافيَّة من الأمان تُساعد في اكتشاف أنواع مُعيَّنة من الهجمات السّيبرانيَّة والحدّ منها، بما في ذلك هجمات البرمجة النَّصِّيَّة للمواقع المشتركة (XSS) وهجمات حَقْن البَيَانات التي تقوم بسرقة البيانات وتشويه المواقع وتوزيع البرمجيات الضَّارَّة.

تُمكِّن سياسة أمَان المُحْتَوَى (CSP) مسؤولي الخادم من تخفيف الأضرار التي يمكن أن يُحدثها هجوم XSS؛ عن طريق إظهار المصادر الصَّالحة للبرامج النَّصِّيَّة أمام المُتَصَفِّح والقابلة للتَّنفيذ، فوفق ذلك يقوم المُتَصَفِّح المُتوافِق مع سياسة أمَان المُحْتَوَى بتنفيذ البرامج النَّصِّيَّة المُستَلَمة من النِّطاقات المسموح بها فقط.

ويُقصَد بالسِّياسَة

سلسلة تتضمَّن توجيهات السِّياسَة التي تَصِف سياسة أمَان المُحْتَوَى الخاصَّة بالمُسْتَخْدِم على الويب؛ حيث توجد مجموعة من التَّوجيهات لعدَّة أنواع من العناصر، أي يكون لكلّ نوع سياسته الخاصَّة؛ بما في ذلك الخُطُوط والصُّور ووسائط الصّوت والفيديو والبرامج النَّصِّيَّة.

يتمّ تعريف توجيهات سياسة أمَان المُحْتَوَى في رؤوس استجابة HTTP التي تُسمَّى رؤوس CSP، ومَهمتها إرشاد المُتَصَفِّح إلى مصادر المحتوى الموثوقة، كما تتضمَّن قائمة بالمصادر التي ينبغي مَنْع الوصول إليها.

وهناك عدَّة فئات تندرج ضِمْنها توجيهات سياسة أمَان المُحْتَوَى CSP التي تختلف وَفْق حالة الاستخدام وسِمَة المحتوى، وهي:

إحضار التَّوجيهات؛ وتتضمَّن ما يلي:

Child-Source

وهذا التَّوجيه مسؤول عن تحديد مصادر البرامج النَّصِّيَّة المُدْرَجَة في القائمة البيضاء لمسار التَّصفُّح المُتضمّن في الإطارات وعمال الويب.

Connect-Source

هذا التَّوجيه مسؤول عن تحديد عناوين URL التي يتمّ تحميلها باستخدام البرامج النَّصِّيَّة.

Default-Source

التَّوجيه الاحتياطي لجميع توجيهات الإحضار، ويُحدِّد قائمة المصادر الافتراضيَّة لتَوجيهات الجلب الأخرى.

Object-Source

يُحدِّد المصادر المسموح بها لعناصر <applet> و<embed> و<object>.

Style-Source

يُوفِّر قائمة بالمصادر الصَّالحة لأوراق الأنماط المتتالية، ويُقصَد به: لغة تنسيق لصفحات الويب تهتمّ بشكلِ وتصميم المواقع.

توجيهات المستند، التي تساعد في التَّحكُّم بخصائص بيئة العمل (المستند)، وتشمل:

01

وَضْع الحماية: فهو يَحْمي موردًا مُحدَّدًا مُشابهًا لعناصر البرنامج النَّصِّيّ المُضمَّنة.

02

base-uri: يُحدِّد عناوين URL المسموح بها في العنصر الأساسيّ للمُستَنَد.

توجيهات التَّصفُّح، هذه التَّوجيهات تسيطر على مواقع إرسال المُستنَد (أي تنقُّلاته)، وتشمل:

01

إجراء المستند: وهو يُحدِّد عناوين URL التي تُرسل عناصر المُستنَد.

02

أصول الإطار: وتَعْمل على تقييد الأصول التي يَتمّ تضمينها في صفحة الويب.

توجيهات الإبلاغ، وهي المسؤولة عن توثيق انتهاكات سياسة أمَان المُحْتَوَى والإبلاغ عنها، وتشمل:

01

تقرير إلى: بَدْء عمليَّة انتهاك سياسة الأمان.

02

تقرير URI: يُوجّه بيئة المُسْتَخْدِم للإبلاغ عن أيّ محاولة لانتهاك مُواصفات سياسة أمَان المُحْتَوَى CSP.

من توجيهات الإبلاغ عن انتهاكات سياسة أمَان المُحْتَوَى

require-sri-for

يَفرض استخدام تكامُل الموارد الفرعيَّة (SRI) لسمة النَّمط، ومَصادر البرنامج النَّصِّيّ للصَّفحة.

الأنواع الموثوقة trusted-types

تقوم بتحديد قائمة بالقِيَم المكتوبة غير القَابلة للخرق مِن قِبَل المُهَاجِمين الإلكترونيِّين، ممَّا يَحُدّ من هجمات XSS.

المُطالَبة بأنواع موثوقة من أجل require-trusted-types-for

يقوم توجيه السِّياسة هذا على فَرْض سياسة الأنواع الموثوقة على البرامج النَّصِّيَّة.

طلبات التَّرقية غير الآمنة upgrade-insecure-requests

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

آليَّة عمل سياسة أمَان المُحْتَوَى (CSP)

إنَّ أفضل طريقة لإضافة سياسة أمَان المُحْتَوَى CSP بأثرٍ رجعيّ إلى موقع ويب بالكامل هي تحديد قائمة بيضاء فارغة تمامًا لحَظْر كلّ شيءٍ. والمطلوب هو تشغيل تلك السِّياسات مبدئيًّا في وَضْع التَّقرير فقط، ليبدأ المُتَصَفِّح بتقييم القواعد أولًا قبل حَظْر المحتوى. ومن هنا يمكن للمُسْتَخْدِم مُراجَعَة الأخطاء وتصنيف كلّ منها في قائمة المسموح به وغير المسموح به.

عند تحميل المُتَصَفِّح لإحدى الصَّفَحات التي تتضمَّن سياسة أَمَان المُحْتَوَى،

فإنه يتحقَّق من CSP للتَّأكُّد من أنَّ المحتوى مُصرَّح به، وفي حال كان غير مُصرَّح به؛ يقوم المُتَصَفِّح حينها بحَظْر تَحْميله عارضًا رسالة تُفيد بالخطأ، وهذا الإجراء يُسْهم في مَنْع المُهَاجِمين من إدخال تعليمات برمجيَّة ضَارَّة إلى الصَّفْحَة، وبالتَّالي حماية مُستخدِمِي الويب من الهجمات الخَبيثة.

تُساعد سياسة أمَان المُحْتَوَى على حماية الموقع الخاصّ بالمُسْتَخْدِم

من الوضع في القائمة المحظورة التي تَفرضها مُحَرِّكات البحث، مثل جوجل Google، عند التَّعرُّف على أيٍّ من البرمجيات الضَّارَّة عليه، وهو ما يُؤثِّر على عدد الزِّيارات والعُملاء، وبالتَّالي سُمْعَة العلامَة التّجاريَّة والأرباح.

خطوات تنفيذ سياسة أمَان المُحْتَوَى CSP

اختيار مُزوّد الخدمة الخاصّ بموقع الويب

يُفضّل تخصيص السِّياسَة التي تتناسب مع احتياجات كلّ مُسْتَخْدِم على موقع الويب الخاصّ به أو التَّطبيق، ومن أجل ذلك ينبغي إنشاء قائمة بالتَّوجيهات (السياسات) لتحديد الموارد المسموح بها أو غير المسموح بها على مَوْقعك.

ومن مُزوِّدي خدمات الاتّصالات (CSP) المُتخصِّصين في أمان مواقع الويب الشَّائعة:

1	2	3	4	5
في حال الرَّغبة في مَنْع تحميل إطارات iframes على موقع الويب يتمّ استخدام frame-source.	استخدام script-source لمَنْع تحميل JavaScript على موقع الويب.	لتقييد المحتوى بخلاف الصُّوَر على مواقع الويب الخاصَّة بالمُسْتَخْدِمين يتمّ استخدام img-source.	للسَّماح بنفس المحتوى فقط من نَفْس المَصْدر وموقع الويب الخاصّ بالمُسْتَخْدِم ونطاقاته الفرعيَّة يتمّ استخدام default-source.	السَّماح فقط للوسائط أو البرامج النَّصِّيَّة الأخرى القابلة للتَّنفيذ من نفس المصدر.

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.

إضافة سياسة أمان المُحْتَوَى CSP إلى رأس استجابة HTTP الخاصّ بموقع الويب

تتمّ أغلب التَّعديلات على رأس استجابة HTTP، ويجب أولًا معرفة الخادم الخاصّ بموقع الويب الخاص بالمُسْتَخْدِم قبل تعيين HTTP.

وللتَّعرُّف على الخادم الذي يعمل عليه موقع الويب الخاصّ بكلّ مُستخدِم، يمكنك تسجيل الدُّخول إلى cPanel الخاصّ به، والتَّحقُّق من واجهة معلومات الخادم لمعرفة ذلك؛ حيث تُوفِّر cPanel النِّظام الأساسيّ لإدارة الخوادم والمواقع الأكثر موثوقيَّة.

واختصارًا، هناك عدَّة خيارات للقيام بذلك:

تعيين سياسة أمان المُحْتَوَى CSP باستخدام IIS manager (خدمات معلومات الإنترنت)

IIS manager خدمات معلومات الإنترنت هو خادم ويب من Microsoft يعمل على نظام التشغيل Windows ويُستخدم لتبادل محتوى الويب الثابت والديناميكي مع مستخدمي الإنترنت، ويمكن استخدامه أيضًا لاستضافة تطبيقات الويب ونشرها وإدارتها.

CyberEco

تعيين سياسات CSP الخاص بك باستخدام Apache

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

تطبيق سياسة أمَان المُحْتَوَى

تُنفّذ سياسات أمان المُحْتَوَى بواسطة رأس HTTP خاصّ يتمّ إرساله مع الاستجابة من الخادم، الذي يتضمَّن قواعد تلك السِّياسات التي تُفرض فيما بعد عبر المُتَصَفِّح، وهناك طريقتان للقيام بذلك:

- إضافة سياسات أمان المُحْتَوَى الخاصَّة بموقع الويب عبر علامات وَصْفيَّة لتعمل على جميع المُتَصَفِّحات.
- تَعيين تلك السِّياسات الخاصَّة بموقع المُسْتَخْدِم بواسطة رأس استجابة HTTP، وهذه الطَّريقة تدعم معظم المُتَصَفِّحات باستثناء Internet Explorer وبعض الإصدارات الأقدم من المُتَصَفِّحات.

الفَصْل الثَّاني
كيفيَّة تفعيل سياسة أمَان المُحْتَوَى (CSP) والمَخاطِر الرَّقميَّة التي تَحُدّ منها

كيفيَّة تفعيل سياسة أمَان المُحْتَوَى (CSP)

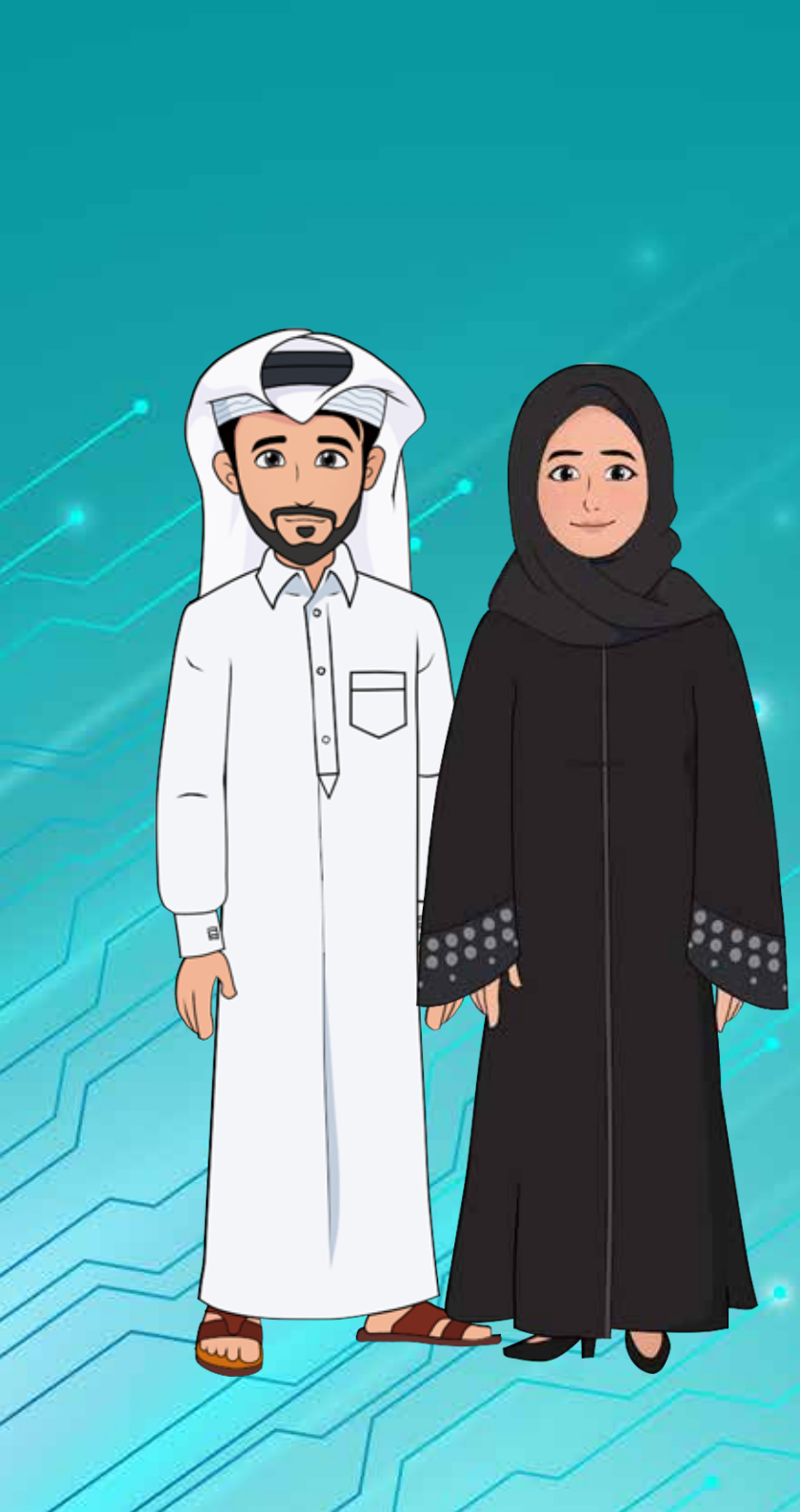
للعثور على سياسة أمان المُحْتَوَى في رؤوس الاستجابة يمكن اتِّباع الخطوات التَّالية:

01
باستخدام المُتَصَفِّح، نقوم بفتح أدوات المطوِّرين (نستخدم أدوات DevTools في Chrome)، ثم نشتقل إلى موقع الويب الذي نختاره، ونفتح علامة التَّبويب "الشَّبكة".

02
ابحث عن الملف الذي يُنشئ الصَّفْحَة، الذي يكون له نفس نطاق موقع الويب الذي تتصفّحه وهو في الأغلب يكون العنصر الأوَّل في علامة التبويب "الشَّبكة".

03
عند النَّقر على الملفّ يظهر مزيد من المعلومات، ومن هنا تبدأ عمليَّة البحث عن رمز الاستجابة 200 OK.

04
وفي الأسفل سيظهر استخدام سياسات أمان المُحْتَوَى من عدمه.



المكان الثَّاني للعثور على سياسة أمَان المُحْتَوَى CSP يكون في علامة التَّعريف

1. ننتقل إلى مصدر الصَّفْحَة، ويتمّ فَتْح المُتَصَفِّح، ونختار موقع الويب.
2. ننقر بزرّ الماوس الأيمن على منطقة فارغة، ونُحدِّد "عرض مصدر الصَّفْحَة".
3. بمُجرَّد عرض مصدر الصَّفْحَة، نُجري بحثًا حسب نوع النظام ففي ويندوز Windows نضغط على أزرار (Ctrl-F) من على لوحة المفاتيح، ونبدأ عمليَّة البحث عن مصطلح "سياسة أمَان المُحْتَوَى".

أدوات مجانيَّة تساعد في إنشاء وتقييم ومراقبة سياسة أمَان المُحْتَوَى

تتضمَّن أدوات تدقيق w3af مكونًا إضافيًّا لتدقيق تطبيقات الويب بشكلٍ تلقائيّ؛ للتَّأكد من تفعيل سياسات أمان المُحْتَوَى CSP.

اختبار CSP (امتداد المُتَصَفِّح) لبناء واختبار السِّياسَة الخاصَّة بتطبيق موقع الويب الخاصّ بالمستخدم.

مولد سياسة أمان المُحْتَوَى CSP Gener-ator لإنشاء السِّياسات تلقائيًّا (امتداد Chrome/ Firefox).

مُقيم CSP لتقييم سياسات أمَان المُحْتَوَى الحاليَّة.

أداة تجميع تقارير Csper لمراقبة سياسة أمَان المُحْتَوَى باستخدام تقرير uri.

المَخاطِر الرَّقميَّة التي تَحُدّ منها سياسة أمَان المُحْتَوَى (CSP)

هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS)

تُعدّ هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS) نوعًا من أنواع حقن البيانات؛ إذ يقوم المُهَاجِم الإلكترونيّ بحَقْن البرمجيات النَّصِّيَّة الضَّارَّة في مواقع الويب الموثوقة، ويقع الهجوم عندما يستخدم المُهَاجِم تطبيق ويب لإرسال تعليمات برمجيَّة ضارَّة في شكلِ برنامج نَصِّيّ من جانب المُتَصَفِّح إلى المُستخدِم.

ويتمّ الاحتيال في هذا الهجوم؛ إذ يظهر البرنامج النَّصِّيّ الضَّارّ كأنه من مصدر موثوق، ومن هنا يتمكَّن البرنامج النَّصِّيّ الضَّارّ من الوصول إلى أيّ ملفَّات تعريف ارتباط أو معلومات حسَّاسة يحتفظ بها المُتَصَفِّح ويستخدمها في موقع الويب، كما يمكن لهذه البرمجيات النَّصِّيَّة إعادة كتابة محتوى صفحة HTML.

تنقسم هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS) إلى:

هجمات XSS المنعكسة

في هذه الفئة ينعكس البرنامج النَّصّيّ الضَّارّ الذي تمَّ إدخاله على خادم الويب، كما هو الحال في رسالة خطأ أو نتيجة بحث أو أيّ استجابة أخرى تتضمَّن بعض أو كلّ المُدْخَلات المُرْسَلة إلى الخادم كجزءٍ من الطلب.

يتمّ تسليم هجمات XSS المنعكسة إلى الضحايا من خلال طريق آخر، مثل رسالة بريد إلكترونيّ أو على بعض مواقع الويب الأخرى، وبمُجرَّد نَقْر المُسْتَخْدِم على الرَّوابط الضَّارَّة أو تصفُّح الموقع المُتضرِّر يتمّ انتقال التَّعليمات البرمجيَّة المحقونة إلى موقع الويب الضَّعيف، ممَّا يعكس الهجوم مرَّة أخرى إلى مُتَصَفِّح المُستخدِم، ثم يبدأ المُتَصَفِّح تنفيذ التَّعليمات البرمجيَّة؛ لأنها جاءت من خادم "موثوق"، وهي عمليَّة خداع.

هجمات XSS المُخزّنة

يُقصَد بها تخزين برنامج نصيّ مَحْقُون بشكلٍ دائمٍ على الخوادم المُستهدَفَة، كما هو الحال في قاعدة البيانات، أو سِجِلّ الزائرين، أو حَقْل التَّعليق، وما إلى ذلك. وبعد ذلك يبدأ المُسْتَخْدِم الضحيَّة استعادة البرنامج النَّصِّيّ الضَّارّ من الخادم عندما يطلب النَّصّ المُخزن

البرمجة النَّصِّيَّة عبر المواقع العمياء

هي شَكْل من أشكال هجمات XSS المُستمِرَّة، وتتمّ عند حِفْظ برمجيات المُهَاجِم على الخادم وإعادتها إلى الضحيَّة، فمثلًا في "نماذج البيانات"، يقوم المُهَاجِم بإرسال البرمجيات الضَّارَّة وبمُجرَّد فَتْح المُسْتَخْدِم للنَّمُوذج يبدأ التَّنفيذ.

أضرار هجمات البرمجة النَّصِّيَّة عبر المواقع XSS

01 خرق الحساب بالكامل.

02 تثبيت برمجيَّات حصان طروادة.

03 إعادة توجيه المُسْتَخْدِم إلى صفحة أو موقع آخر.

04 تعديل عَرض المحتوى.

05 تعديل بيان صحفيّ أو خبر عن سعر سهم المُؤسَّسَة؛ ما يتسبَّب في تقليل ثقة المُستهلِك بها.

هجوم استنشاق الحزم A packet sniffing attack

هو أسلوب قَرْصَنة يعمل على جَمْع حزم البيانات التي تنتقل عبر شبكة حاسوب غير مُشفَّرة؛ حيث يُراقِب المُتَسَلِّلون السّيبرانيُّون حزم البيانات في حركة مرور الشَّبكة، بهدف اعتراض المعلومات الحسَّاسة مثل التَّفاصيل الماليَّة أو بيانات تسجيل الدُّخول؛ لبيعها أو لاستخدامها في هجمات أخرى.

ويُعدّ هذا الهجوم من هجمات التَّجسُّس التي تعمل بشكلٍ جيِّد على الشَّبكات غير المُشفَّرة، الأمر الذي يستدعي الحذر في أثناء استخدام شبكة Wi-Fi عامَّة لتشفير الاتِّصال ومَنْع تَعقُّب المُستخدِمِين وبياناتهم.

أنواع هجمات استنشاق الحزم

الاستنشاق النَّشِط لحُزَم الاتِّصال

Active packet sniffing

يُستخدم هذا النَّوع من الهجوم على الشَّبكات الأكبر حجمًا؛ حيث مع اتِّصال المزيد من الأجهزة بشبكةٍ واحدةٍ، تصبح هناك حاجة إلى مُحوّل الشَّبكة، وهنا تبدأ الشَّبكة في توجيه حركة مرور الإنترنت إلى حيث من المفترض أن تذهب؛ كي لا يسيطر حجم حركة المرور على كلّ جهاز متَّصل بها، ويُعدّ هذا النَّوع النَّشط من هجمات الاستنشاق أكثر قابليَّة للاكتشاف؛ لأنه يجب أن يُعلِن عن نفسه من أجل البَدْء في الاستنشاق.

الاستنشاق السلبي لحُزَم الاتِّصال

يُنفّذ هذا الهجوم في الشَّبكات الأصغر حجمًا، والتي تكون جميع الأجهزة فيها متَّصلة بمركز شبكة واحد، وهنا لا يحتاج الهجوم إلى الاعتماد على مُحوّلات الشَّبكة لتوجيه حركة المرور، ولا يحتاج إلى الكشف عن نفسه؛ لذا يَصْعُب اكتشاف هؤلاء المُهَاجِمين.

متى يُفضَّل استخدام سياسات أمان المُحْتَوَى CSP؟

يُوصَى باستخدام تلك السِّياسات للتَّطبيقات التي تُدير البيانات الحسَّاسة؛ مثل واجهات المُسْتَخْدِم الإداريَّة، ووحدات تحكُّم إدارة الأجهزة، أو المُنتَجات التي تَستضيف المستندات أو الرَّسائل أو ملفَّات الوسائط التي أنشأها المُستخدِم.

أمَّا التَّطبيقات الثَّابتة دون أيّ وظائف أو ملفَّات تعريف ارتباط لتسجيل الدُّخول، فلا يُفضّل استخدام تلك السِّياسات معها، وكذلك التَّطبيقات الكبيرة التي لها تاريخ مع هجمات XSS؛ فإنَّ تلك السِّياسات ستكون آليَّة أمان إضافيَّة، لكنَّ الأساس هو التَّعليمات البرمجيَّة المُصمَّمة للحماية من هذه الهجمات الإلكترونيَّة.

تَمارين وتَدْريبات

أولًا: التَّمَارين الصَّفِّيَّة

هل تعلم؟

يُفَضِّل استخدام **سياسة أمان المُحْتَوَى CSP** للتّطبيقات التي تُدِير البيانات الحسّاسة، مثل واجهات المُستخدِم الإداريّة ووحدات تَحَكُّم إدارة الأجهزة، أو المُنْتَجات التي تَسْتَضِيف المستندات أو الرّسائل أو ملفّات الوسائط التي أَنْشَأها المُستخدِم.

التَّمرين الأوَّل

أكْمِل الجُمَل التَّالية:

1. سياسة ..... المحتوى، هي ..... أمان أجهزة الحاسوب، وتمّ ابتكارها من أجل مَنْع ..... البرمجيّات ..... أو الضّارّة عبر المواقع.
2. تُعدّ هجمات ..... النّصّيّة عبر المواقع ..... نوعًا من التّعليمات البرمجيّة الخبيثة والضّارّة في ..... الموثوقة، وغالبًا ما تُستخدَم في مهاجمة مواقع ..... الإلكترونيّة.
3. يمكن تحديد سياسة أمان ..... في HTTP response header؛ وذلك حين يطلب عميل ويب.
4. سياسة أمان المُحْتَوى CSP اختصارٌ لجُمْلة ..... باللُّغة الإنجليزيّة.
5. سياسة ..... المحتوى مُهمّة جدًّا لأصحاب ..... الإلكترونيّة.

انْتَبِه!

مفهوم سياسة أمَان المُحْتَوَى (CSP)

تُعدّ سياسة أمَان المُحتوى (CSP) طبقة إضافيّة من الأمان تُساعد في اكتشاف أنواع مُعيّنة من الهجمات الإلكترونيّة والحدّ منها، بما في ذلك هجمات البرمجة النّصيّة للمواقع المشتركة (XSS) وهجمات الحَقن التي تقوم بسرقة البيانات وتشويه المواقع وهجمات البَرْمَجيّات الضّارّة.

التَّمرين الثَّاني:

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

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

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

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

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

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

10. يحتاج عدد كبير من المواقع إلى سياسة أمَان المُحْتَوى؛ 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 مبدئيًا في وَضْع التَّقرير فقط، ليبدأ المُتصفِّح تقييم القواعد أوّلًا قبل حَظْر المحتوى، حينها يمكن للمستخدم مراجعة الأخطاء وتَصْنِيف كلّ منها في قائمة المسموح به أو غير المسموح به.

التمرين الثالث:
صِلْ بين العِبارات في العمود الأوّل
وما يَنسجم معها في العمود الثّاني

توجيه
اقرأ العبارات الموجودة في العمود الأوّل من الجدول أدناه، ثُم صِلْ كلّ عبارة بما يناسبها من العمود الثّاني.

Default-Source	لمنع تحميل JavaScript على موقع الويب.
Child-Source	يُوفّر قائمة بالمصادر الصّالحة لأوراق الأنماط المتتالية، ويُقصَد بها: لغة تنسيق لصفحات الويب تهتمّ بشكل وتَصْميم المواقع.
Script-Source	هذا التّوجيه مسؤولٌ عن تحديد عناوين URL التي يتمّ تَحْميلها باستخدام البرامج النّصّيّة.
Object-Source	يُحدّد عناوين URL المسموح بها في العُنصر الأساسيّ للمُستَند.
Style-Source	التّوجيه الاحتياطيّ لجميع توجيهات الإحضار، ويُحدّد قائمة المصادر الافتراضيّة لتوجيهات الجلب الأخرى.
Img-Source	في حال الرّغْبة في مَنْع تحميل إطارات على موقع الويب يتمّ استخدامه.
Frame-Source	هذا التّوجيه مسؤول عن تحديد مصادر البرامج النّصّيّة المُدْرَجَة في القائمة البيضاء لمسار التّصفُّح المُتضمّن في الإطارات وعمال الويب.
Connect-Source	يُحدّد 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 الماليّة-، 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 التّخفيف من الأضرار التي يمكن أن يُحْدِثها هجوم XSS، عن طريق إظهار المصادر الصّالحة للبرامج النّصّيّة أمام المُتصفِّح والقابلة للتّنفيذ.

انْتَبِه!

هجمات البرمجة النَّصِّيَّة عبر المواقع (XSS)

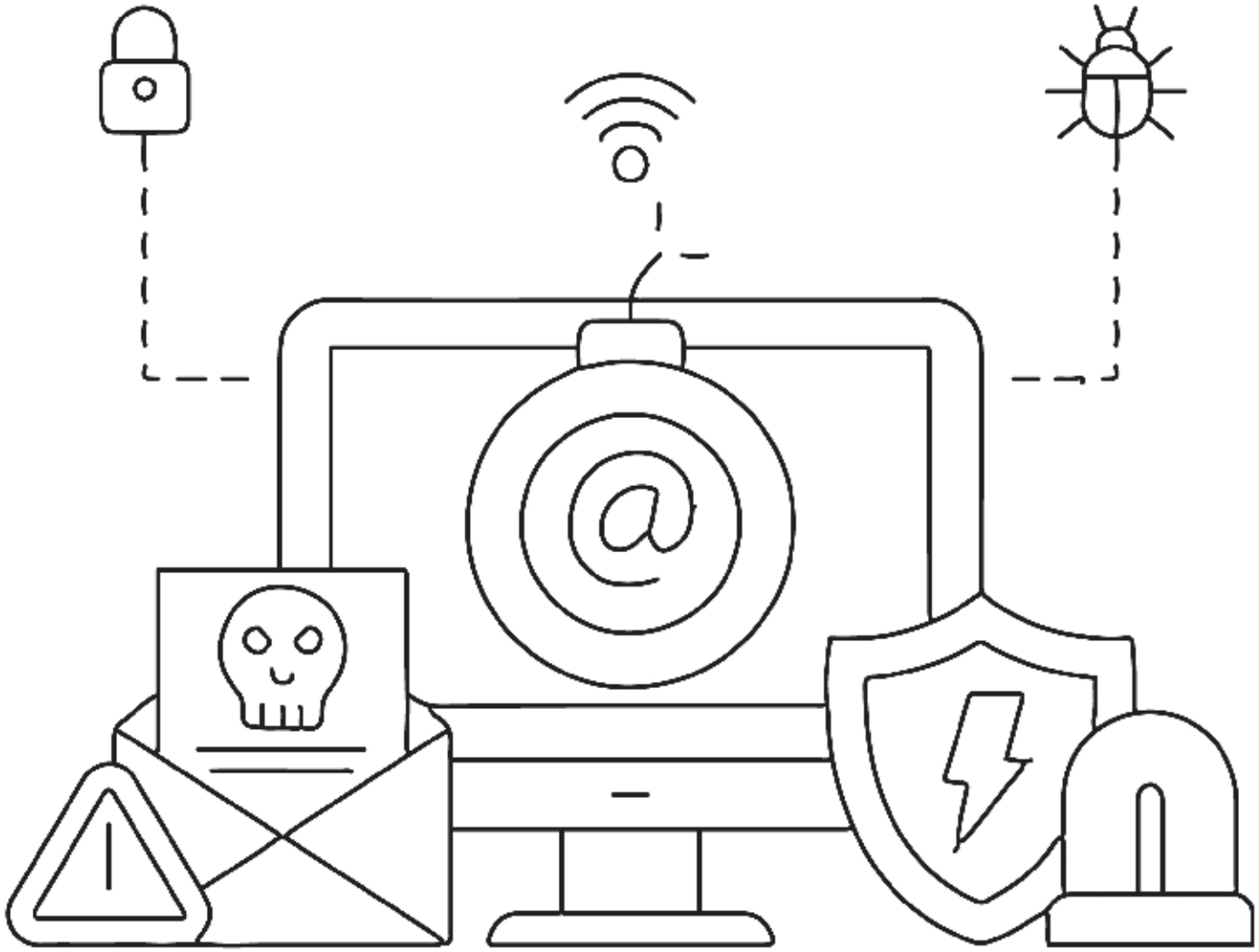
هي نوع من أنواع الحقن؛ إذ يقوم المهاجم الإلكتروني بحَقْن البرمجيّات النّصّيّة الضّارّة في مواقع الويب الموثوقة، ويقع الهجوم عندما يَسْتَخْدِم المُهاجِم تطبيق ويب لإرسال تعليمات برمجيّة ضارّة في شكل برنامج نَصّيّ من جانب المُتصفِّح إلى المُستخدِم.


ثانيًا: التَّمارين اللَّاصفيَّة

انْتَبِه!

هجمات XSS المخزنة

يُقْصَد بها تخزين برنامج نَصِّيّ 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 المُخَزّن.



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.
- التّلاعُب بالتّقارير الماليّة التي تصدرها وتنشرها المؤسّسات على مواقعها الإلكترونيّة.

التّمرين الأوّل

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

يمكن العُثور على سياسة أمان المُحْتَوى CSP في علامة التّعريف للموقع.	✓
من الضّروري تمكين بيئة تطوير / اختبار بسبب خطورة سياسة أمان المُحْتَوى.	
عليك بتَشْغيل سياسة أمان المُحْتَوى فورًا دون تجربة.	
تحتاج سياسة أمان المُحْتَوى على الأقلّ إلى 48 ساعة لكي تَعْمل.	
لا يمكن لخدمة أمان المُحْتَوى إعداد التّقارير أو توضيح أماكن المشكلات أو الثّغرات.	
تَتَسبّب هجمات البرمجة النّصّيّة عبر المواقع XSS في مشكلات تَصل حتّى خرق الحساب بالكامل.	
يُستخدَم هجوم الاستنشاق النشط لحزم الاتصال على الشّبكات الصّغيرة.	
لا يمكنك أبدًا التّحكُّم في التّوجيهات الفرديّة داخل السّياسة.	

انْتَبِه!

تُساعِد **سياسة أمَان المُحْتَوى** في حماية الموقع الخاصّ بالمُستخدِم من الوَضْع في القائمة المَحْظورَة التي تَفْرِضُها محرِّكات البحث مثل جوجل Google عند التّعرُّف على أيٍّ من البرمجيّات الضّارّة، وهو ما يؤثِّر في عدد الزِّيارات والعملاء، ومن ثمّ يؤثِّر في سمعة العلامة التِّجاريّة والأرباح.

هل تعلم؟

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

انْتَبِه!

البرمَجة النَّصِّيَّة عبر المواقع العمياء

إحدى الطُّرق الأكثر شيوعًا التي تُصيب بها الرُّوبوتات جهاز الحاسوب الخاصّ بالمُستخدِم، حيث يتمّ تثبيت **البرمجيَّات** الضّارّة بتنسيق التّنزيل عبر وسائل التّواصل الاجتماعيّ أو رسائل البريد الإلكترونيّ التي تنصح بالنّقر فوق الرّابط، وغالبًا ما يكون الرّابط على شكل صورة أو فيديو، ويحتوي إمّا على فيروسات وإمّا على **برمجيات ضارة** أخرى.

التمرين الثاني
استخرج الكلمات التالية من الجدول:

توجيه
اقْرأ الكلمات الواردة أدناه بتمعُّن، وابحث في الجدول عن حروف متتالية تُشكّل 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	ي	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	ج	ت
ا	ل	ب	ن	ي	ة	ف	ل	ا	ف	ل
ا	ل	م	ح	ت	و	ي	ن	ي	و	ن

التّطبيقات - أمان - السّحابة - التّشفير - الإصلاح - الاستجابة - البنية - الثّغرات
سياسة - المحتوى - موقع - السرّيّة - هجمات - تقارير - أدوات.

انْتَبِه!

خدمات معلومات الإنترنت IIS manager:

IIS manager هو خادم ويب من Microsoft يعمل على نظام التّشغيل Windows، ويُسْتَخْدَم لتبادُل محتوى الويب الثّابت والدّيناميكيّ مع مُستخدِمي الإنترنت، ويمكن استخدامه أيضًا لاستضافة تطبيقات الويب ونَشْرها وإدارتها.

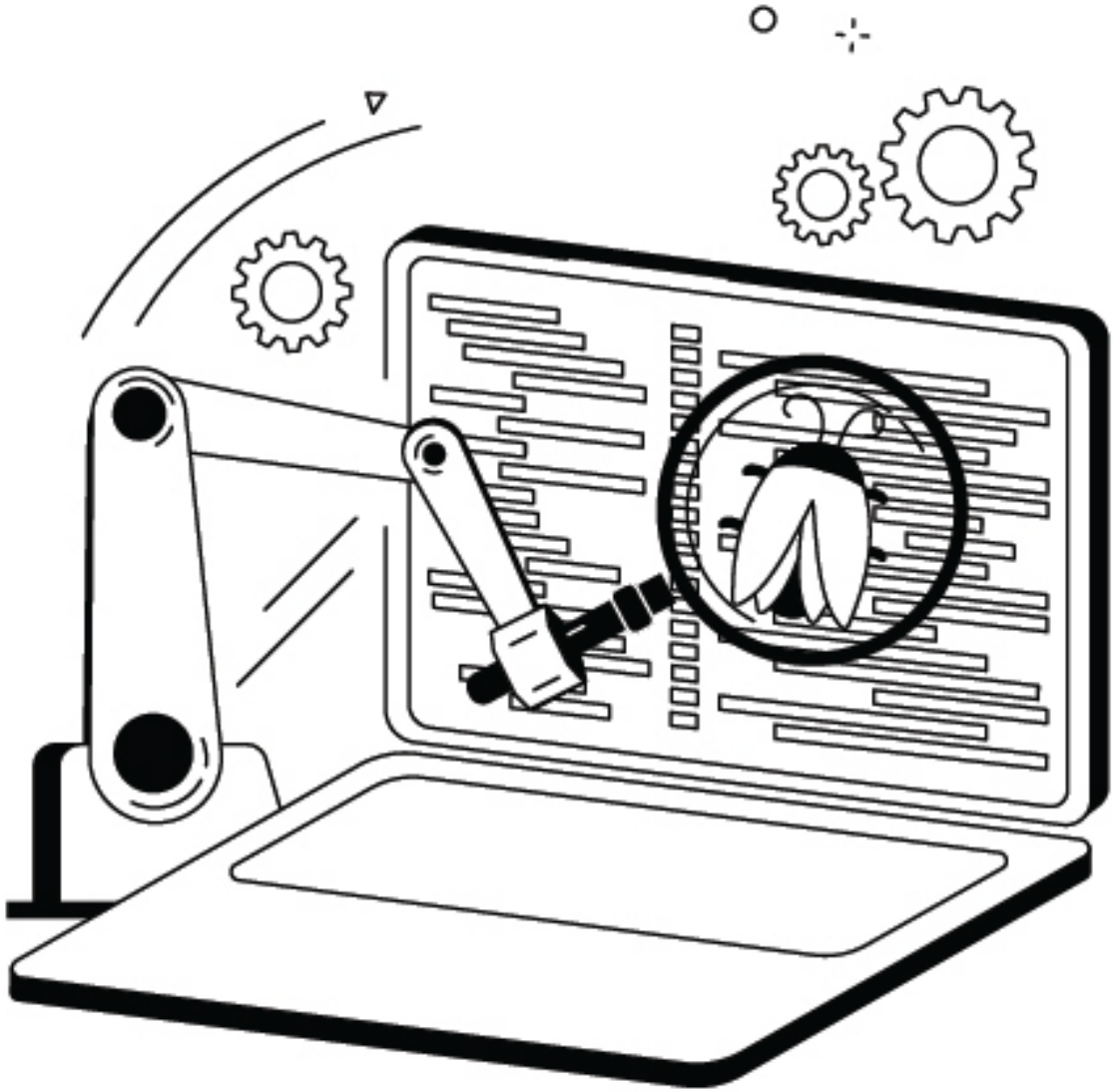
هل تعلم؟

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

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.

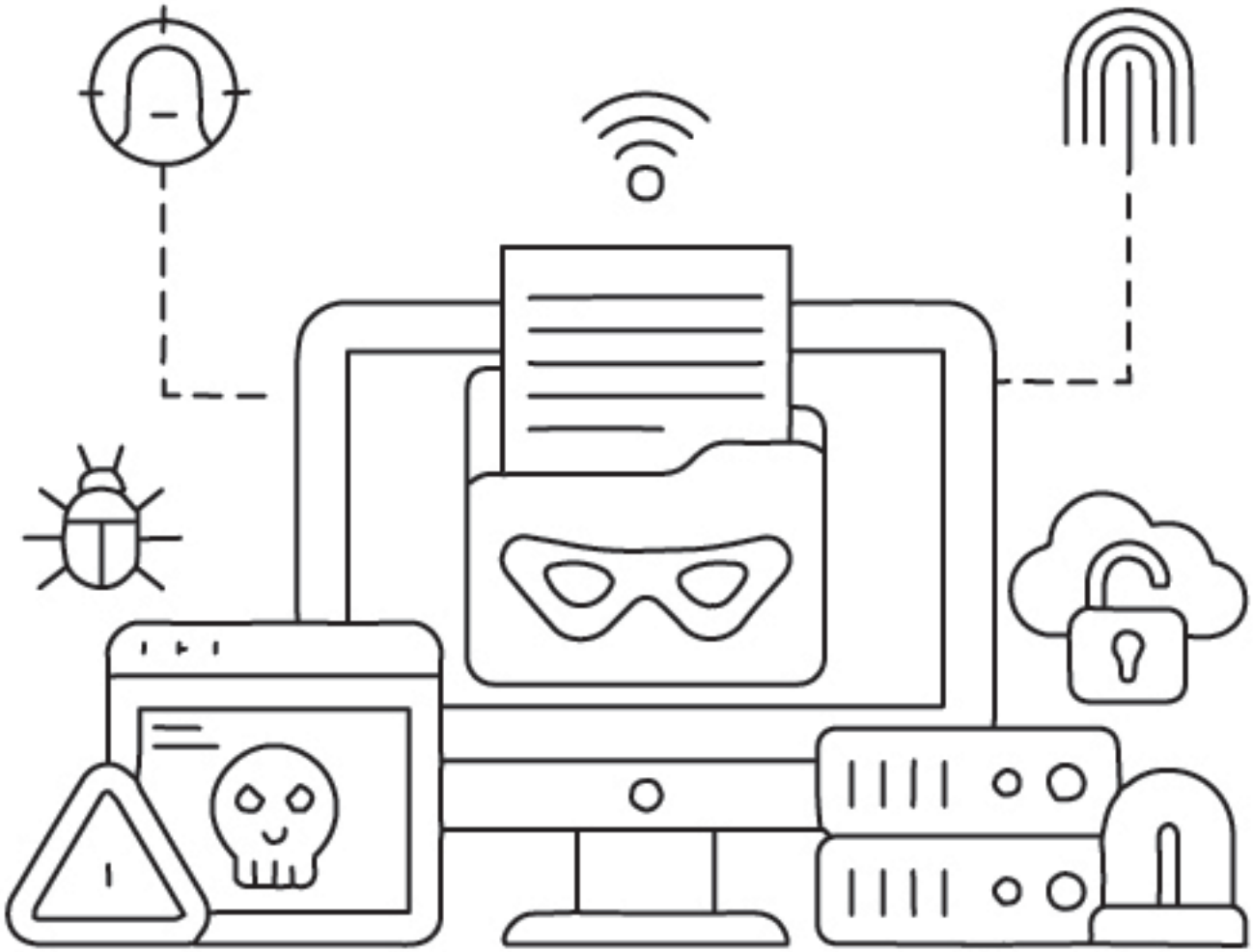
للعثور على سياسة أمان المُحْتَوَى في رؤوس الاستجابة يمكن اتِّباع الخطوات التّالية:

باستخدام المُتصفِّح، افْتَح أدوات المُطوِّرين (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 تَتَصَفَّحه، 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 المُحْتَوى من عدمه.



للعثور على سياسة أمَان المُحْتَوَى CSP من علامة التَّعريف

1. انْتَقِل إلى مصدر الصَّفحة وافْتَح المُتصفِّح واخْتَر موقع الويب.
2. انْقُر بِزرّ 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".


أسـئلة
المسابقات

مـا هــو؟

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

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

سلسلة تتضمّن التّوجيهات التي تَصِف سياسة أمَان المُحْتَوى 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 المُحْتَوى التي تُحدّد المواقع التي يتمّ منها تحميل أنواع مُحدّدة من الموادّ.

مـا هــو؟

إحدى فئات توجيهات سياسة أمان المُحْتَوى التي تساعد في التّحكُّم بخصائص بيئة العمل.

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

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

مكانان يمكن العُثور في أيّ منهما على مُقدّمي الخِدْمات المُفعّلة لسياسة أمان المحتوى.

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 الضّحيّة استرجاع البرنامج النّصّيّ الضّارّ من الخادم عندما يَطلب النّصّ المُخزّن.

هي شَكل من أشكال هجمات XSS المُستمِرّة، وتتمّ عند حِفْظ تِرْمِجيّات المُهاجِم على الخادم، وإعادتها إلى الضّحيّة، فمثلًا في "نماذج البيانات" يقوم المُهاجِم بإرسال برمجيّات ضّارّة، وبمُجرّد فَتْح المُستخدِم للنّموذج يبدأ التّنفيذ.

يُعرّف بأنّه أسلوب قَرْصنة يعمل على جَمْع حزم البيانات التي تَنْتقل عبر شبكة حاسوب غير مُشفّرة؛ حيث يُراقب المُتسلّلون 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 المُتمثّلة في سياسة أمان المُحْتَوى (CSP) إلى .....
- تُمكّن سياسة أمان المُحْتَوى (CSP) مسؤولي الخادم من تخفيف الأضرار التي يمكن أن يُحْدثها هجوم XSS عن طريق .....
- من الوظائف التي تُنفّذها سياسة أمان المُحْتَوى أيضًا الحدّ من هجمات .....، وهي هجمات إلكترونية يُنفّذها المُتسلّلون لاعتراض ومُراقبة حركة المرور على الشّبكة.
- يتمّ تعريف توجيهات سياسة أمان المُحْتَوى في ..... التي تُسمّى رؤوس CSP ومَهمّتها إرشاد المُتصفّح إلى مصادر المحتوى الموثوق بها، كما تتضمّن قائمة بالمصادر التي ينبغي مَنْع الوصول إليها.
- تساعد توجيهات المستند في التّحكُّم بخصائص بيئة العمل وتشمل: ..... و.....
- تُعدّ توجيهات الإبلاغ المسؤولة عن توثيق انتهاكات سياسة أمان المُحْتَوى والإبلاغ عنها، وتشمل: .....

- قد تتضمّن بعض مواقع الويب عناوين URL قديمة غير آمِنَة، لذا تقوم سياسة التّوجيه ..... بإرشاد المُتصَفّح للتّعامُل مع تلك العناوين واستبدالها بأخرى أكثر أمنًا HTTPS .

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

- تُساعد سياسة أمَان المُحْتَوى في حماية الموقع الخاصّ بالمُستخدِم من الوَضْع في ..... التي تَفْرضها مُحرّكات البحث مثل جوجل Google عند التّعرُّف على أيّ من البرمجيّات الضّارّة عليه.

- يمكن لمُستخدِمي الإنترنت تلقّي إشعارات تنبيهيّة في حال تمّ انتهاك سياستهم، لكنْ دُون حَظْر المحتوى، من خلال ضَبْط ..... على تقرير سياسة أمَان المُحْتَوى فقط.

اختر الإجابة الصَّحيحة

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

- ☐ هجمات XSS المُخزّنة.
- ☐ هجمات XSS المنعكسة.
- ☐ البرمجة النَّصّيّة عبر المواقع العمياء.
- ☐ هجمات استنشاق الحزم.

2. تتسبّب هجمات البرمجة النَّصّيّة عَبْر المواقع XSS في .....

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

3. يُسْتَخْدَم هذا النّوع من الهجوم على الشّبكات الأكبر حجمًا؛ فمع اتّصال مزيدٍ من الأجهزة بشبكة واحدة، تصبح هناك حاجة إلى مُحَوّل الشّبكة .....

- [ ] البرمجة النّصّيّة 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 الشّبكة لجَمْع بيانات كلمة المرور.

- [ ] خَرق جلسة اتّصالات بروتوكول التّحكُّم في الإرسال.
- [ ] استنشاق JavaScript.
- [ ] هجمات التّنصُّت 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.

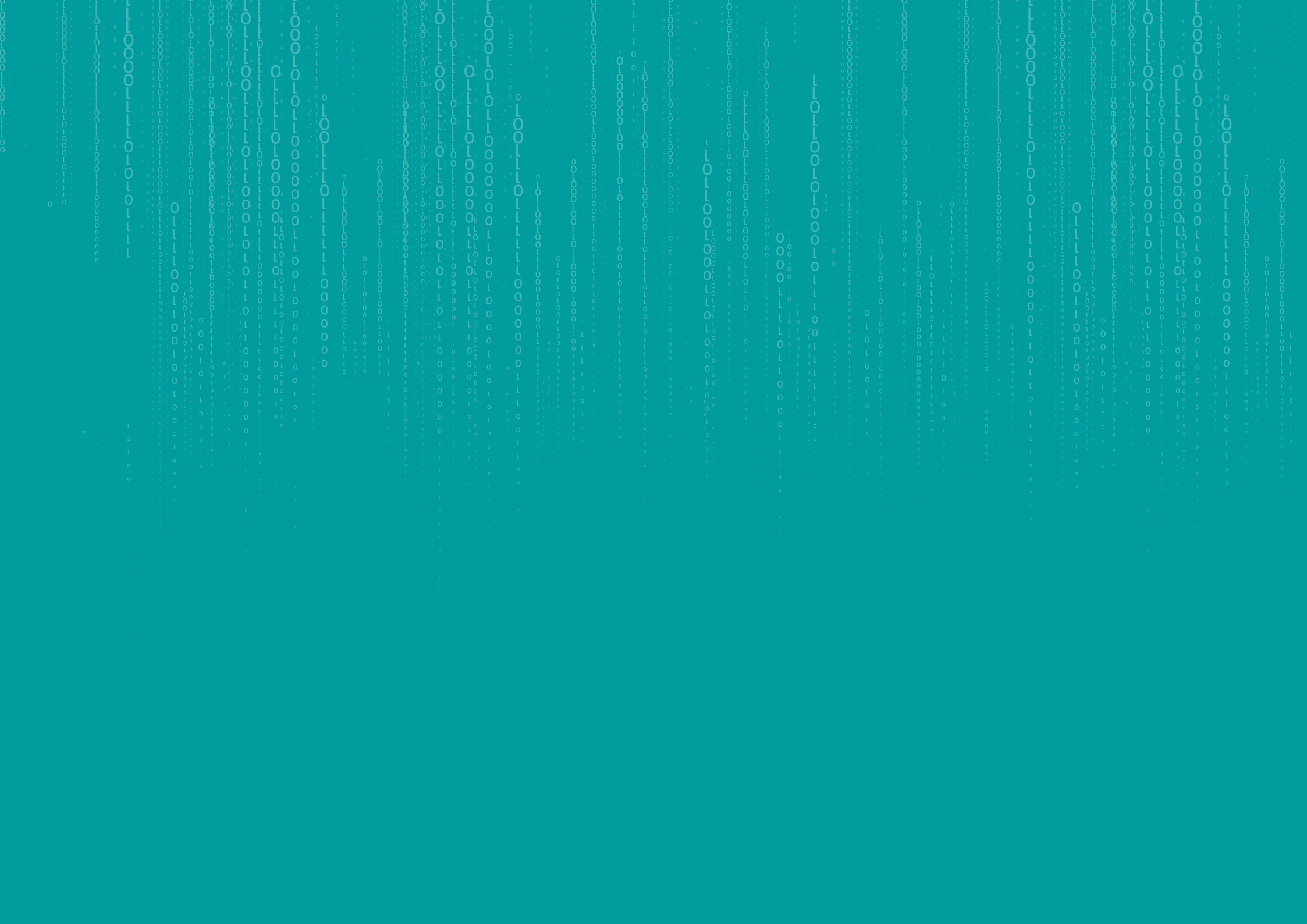
6. بمجرّد إنشاء اتّصال بين المُرسِل والمُستقبِل، يقوم المُهاجِم بالاختراق ونَقْل البيانات الموثوقة التي تتمّ واستنشاق حركة مرور الشّبكة .....

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

مشروع التَّخرُّج

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

- كتَابَة قصّة أو تقرير أو مقال تَشْرح فيه المَفاهيم ذات الصّلة بسياسَة أمَان المُحْتَوَى.
- يَتَقَمّص الطّالب دَوْر المُدَرّب ويَكْتُب تَوْجِيهاتٍ عامّةً لزملائه أو أَهْله يُوضّح لهم فيها الإجراءات المطلوبة للاستفادة من سياسَة أمَان المُحْتَوَى، وأهمّيّة هذا الأمر.



CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency