الجمهورية العربية السورية

وزارة التعليم العالي

الجامعة السورية الخاصة

كشف التصيد في شبكات التواصل الاجتماعي

Phishing Detection in Social Media

(فصلي)

إعداد

سيدره النزال صباح خربوطلي

اشراف

د.وسيم جنيدي

أكتوبر – 2025

Table of Contents

List of Tables

List of Forms

1.1 مقدمة الفصل

تزداد هجمات التصيّد الاحتيالي بشكل متكرر على الرغم من الجهود الكبيرة المبذولة لمواجهتها. يجد المحتالون سهولة في استهداف الضحايا غير المشتبه بهم وخداعهم للتخلي عن معلومات حساسة. ومن خلال استغلال التلاعب بالسلوك البشري المعروف باسم "الهندسة الاجتماعية" [1][2]، يُجبر الأفراد على التصرف بطرق تؤدي إلى "تسريب" معلومات لأغراض مالية. أكثر أشكال الهندسة الاجتماعية شيوعاً هو التصيّد عبر البريد الإلكتروني، عناوين المواقع (URLs)، والمواقع الإلكترونية [3].

كما أن بعض أشكال التصيّد الأخرى الأقل انتشاراً بدأت تكتسب زخماً، مثل التصيّد عبر الرسائل القصيرة (Smishing) [4] والتصيّد الصوتي (Vishing) [5].

في عام 2024، كان التصيّد الاحتيالي أكثر أشكال الجرائم الإلكترونية شيوعاً. ووفقاً لتقرير مجموعة مكافحة التصيّد الاحتيالي (APWG) [1]، فقد أُشير إلى أنه بحلول الربع الثالث من عام 2024، كان هناك المزيد من هجمات التصيّد مقارنة بالربع السابق. وبالمثل، أعلنت جمعية تدقيق ومراقبة نظم المعلومات (ISACA) في تقريرها للأمن السيبراني لعام 2024 [6] أن التصيّد الاحتيالي، باستخدام أساليب الهندسة الاجتماعية المعقدة، يُعد أكثر أنواع الجرائم الإلكترونية شيوعاً.

خلال العقد الماضي، ركّزت الأبحاث بشكل متزايد على دراسة التصيّد، خصوصاً عبر البريد الإلكتروني واكتشاف المواقع الاحتيالية، وذلك بسبب إدخال تقنيات جديدة في الذكاء الاصطناعي مثل التعلم الآلي (ML)، التعلم العميق (DL)، ومعالجة اللغة الطبيعية (NLP). وفي المقابل، فإن متجهات الهجوم تتزايد، ما يزيد من سطح الهجوم. ومع تزايد تدابير الحماية ضد رسائل البريد الإلكتروني والمواقع الاحتيالية، يحوّل المهاجمون هجماتهم نحو الرسائل القصيرة والصوتية [7]. ومع ذلك، لا تزال الحماية ضد هذه الهجمات محدودة. إذ تُجرى العديد من هجمات التصيّد عبر خدمات التواصل الاجتماعي (SNS)، ولم تُولَ هذه المنصات الاهتمام الكافي من الباحثين. إن فهم هذا النوع المتغير من متجهات الهجوم أمر بالغ الأهمية لتطوير تدابير مضادة فعّالة لحماية منصات التواصل من هذه التهديدات الناشئة.

في الآونة الأخيرة، أصبحت منصات التواصل الاجتماعي هدفًا متزايدًا لهجمات التصيّد الاحتيالي، حيث استغل المهاجمون الشعبية الواسعة لهذه المنصات للوصول إلى مستخدمين عاديين وشركات على حد سواء. تشير التقارير إلى أن هجمات التصيّد عبر منصات التواصل الاجتماعي قد شكلت 22.5% من إجمالي الهجمات في الربع الرابع من عام 2024، مما يجعلها ثاني أكثر القطاعات استهدافًا بعد خدمات البريد الإلكتروني والخدمات السحابية .

تتسم هذه الهجمات بالابتكار، حيث يستخدم المهاجمون تقنيات متقدمة مثل الذكاء الاصطناعي لإنشاء رسائل احتيالية تبدو موثوقة، مما يزيد من صعوبة اكتشافها. على سبيل المثال، يمكن للمهاجمين استخدام نماذج الذكاء الاصطناعي لتوليد رسائل احتيالية مخصصة تستهدف مستخدمين محددين بناءً على بياناتهم الشخصية المتاحة على الإنترنت.

بالإضافة إلى ذلك، ظهرت تقنيات جديدة مثل هجمات التصيّد عبر الروابط المختصرة التي تظهر في معاينات الروابط على منصات التواصل الاجتماعي، مما يجعل من الصعب على المستخدمين التمييز بين الروابط الحقيقية والمزيفة.

1.2 المشكلة العلمية

على الرغم من التطور الملحوظ في أدوات الكشف ومنع الهجمات الإلكترونية، فإن التصيّد الاحتيالي (Phishing) لا يزال يُصنف كأكثر أشكال الجرائم السيبرانية شيوعًا على مستوى العالم [1], [6]. ويعتمد المهاجمون بشكل متزايد على أساليب الهندسة الاجتماعية لاستغلال السلوك البشري وخداع المستخدمين للإفصاح عن بياناتهم الشخصية أو المالية [2]. وتشير تقارير حديثة إلى أن المهاجمين يوسّعون نطاق أنشطتهم من البريد الإلكتروني إلى قنوات جديدة مثل الرسائل النصية القصيرة (Smishing) [4] والتصيّد الصوتي (Vishing) [5]، مما يزيد من سطح الهجوم وصعوبة الكشف,وفي سياق منصات التواصل الاجتماعي، تُظهر الأبحاث أن المستخدمين أكثر عرضة للتأثر بهجمات التصيّد بسبب طبيعة هذه المنصات القائمة على الثقة وتبادل المعلومات بسرعة [7]. كما تبيّن أن المهاجمين يستغلون تقنيات الذكاء الاصطناعي والروابط المختصرة لتصميم هجمات يصعب على المستخدمين التمييز بينها وبين المحتوى الشرعي [3]. ومع ذلك، تبقى الحلول الأمنية الحالية محدودة في مواجهة هذه التهديدات الديناميكية، خصوصًا مع انخفاض مستوى وعي المستخدمين وعدم وجود أنظمة فعّالة للكشف المبكر [7],بالتالي، تتمثل المشكلة العلمية في غياب آليات ذكية وفعّالة للتصدي لهجمات التصيّد الاحتيالي عبر قنوات متعددة، خاصة شبكات التواصل الاجتماعي، مما يترك الأفراد والمؤسسات عرضة لتسريب البيانات الشخصية والمعلومات الحساسة.

1.3 الهدف

تسعى هذه الدراسة إلى مواجهة واحدة من أخطر التحديات الأمنية في العصر الرقمي، وهي عمليات التصيّد الاحتيالي عبر مواقع التواصل الاجتماعي. ومع تزايد اعتماد الأفراد والمؤسسات على هذه المنصات في التواصل وتبادل المعلومات، أصبحت بيئة خصبة للمهاجمين لتنفيذ هجمات احتيالية تهدف إلى سرقة الحسابات أو البيانات الشخصية. ينطلق المشروع من فكرة بناء بيئة اختبار تعليمية وآمنة يتم من خلالها محاكاة سيناريوهات التصيّد عبر إنشاء صفحات وهمية مشابهة لمواقع التواصل الاجتماعي الشهيرة. ومن خلال هذه البيئة يتم جمع بيانات واقعية تمثل عينات من الروابط والنصوص الاحتيالية، ليصار إلى تحليلها باستخدام أحدث التقنيات. يستند المشروع إلى دمج تقنيات الذكاء الاصطناعي والتعلم الآلي ضمن برامج الكشف المعتمدة، حيث يتم تدريب نماذج قادرة على التعرف على الأنماط المميزة لهجمات التصيّد سواء من خلال خصائص الروابط أو من خلال البنية اللغوية للرسائل المرافقة. هذا الدمج يتيح للنظام القدرة على الكشف الاستباقي للهجمات بنسبة دقة أعلى مقارنة بالأساليب التقليدية التي تعتمد على الفحص اليدوي أو السمات السطحية. الغاية النهائية للمشروع هي تطوير نظام ذكي وفعّال قادر على رفع مستوى الأمان الرقمي للمستخدمين عبر

مواقع التواصل الاجتماعي، والحد من فرص نجاح المهاجمين في اختراق الحسابات أو الوصول إلى بيانات حساسة، بما ينعكس إيجاباً على أمن المعلومات وسلامة بيئة التواصل الافتراضي.

1.4 مراجعة أدبية

مع تزايد حالات هجمات التصيّد الإلكتروني، أصبح الكشف عن التصيّد أمرًا بالغ الأهمية لحماية المستخدمين من محاولات الاحتيال التي تهدف إلى سرقة المعلومات الحساسة. إن فهم تقنيات الكشف الشائعة عن التصيّد يعتبر أساسيًا. تشمل تقنيات الكشف التقليدية تلك المعتمدة على القوائم (list-based) وتقنيات تعتمد على تحليل المحتوى (content-based filtering). أما تقنيات الكشف المعاصرة فهي تعتمد على التعلم الآلي (machine learning)، الشبكات العصبية العميقة (deep neural networks)، والشبكات الالتفافية العميقة (graph convolutional networks).

الطرق المعتمدة على القوائم تتضمن إدراج روابط التصيّد المعروفة في قوائم سوداء وفحص الروابط الجديدة بمقارنتها مع تلك القوائم [8]. وتُستخدم هذه الطريقة بشكل واسع في المتصفحات الشهيرة وخدمات البريد الإلكتروني [8], [9]. غير أن أحد عيوب هذه التقنية هو أن القوائم السوداء تحتاج إلى تحديث مستمر لإضافة روابط التصيّد الجديدة، مما يعني أن هذه التقنية لا تستطيع كشف روابط التصيّد التي لم يتم إدراجها بعد في القوائم.أما تقنيات تصفية المحتوى (content-based filtering) فهي تعتمد على تقييم المواقع الإلكترونية المشبوهة استنادًا إلى خصائص متعددة، لكن هذه الطريقة تواجه صعوبة في كشف هجمات التصيّد التي تستخدم أساليب جديدة لم تُسجل بعد.أظهرت الدراسات السابقة أن تقنيات التعلم الآلي والشبكات العصبية العميقة توفر أداءً واعدًا في معالجة هذه القصور. هناك عدة أشكال مختلفة من التصيّد تتم معالجتها من خلال الرسائل الإلكترونية، مواقع الويب، الرسائل النصية (SMS)، والصوت/الصورة [10]. توضح مراجعتنا الأولية أن التصيّد عبر مواقع الويب والروابط الإلكترونية هو الأسلوب الأكثر دراسة [11]. التصيّد عبر الرسائل القصيرة SMS والصوت آخذ بالازدياد مؤخرًا. فقد أصبحت منصات التواصل الاجتماعي (SNS)تتعرض جديدًا لهجمات التصيّد التي يمكن تنفيذها عبر نصوص، صور، أو فيديو [7], [12], [13]. الطبيعة المتطورة باستمرار لهذه الهجمات تستدعي حلولاً مبتكرة لمكافحة التصيّد وحماية المستخدمين بشكل فعال.كشفت عملية المسح الأولي أن معظم الأبحاث تركزت على التصيّد عبر الروابط (URL-based) أو البريد الإلكتروني (web-based phishing)، مع وجود أبحاث أقل بكثير تناولت التصيّد عبر الرسائل النصية SMS أو المكالمات الصوتية. من بين حوالي 430 مقالة تمت مراجعتها من قاعدة بيانات Scopus باستخدام كلمة البحث "Phishing Detection"، كانت معظم المقالات المنشورة بين 2018 و2025 (حوالي 246 مقال، أي ما يعادل 57.6%) تتناول التصيّد عبر الروابط أو الويب. في حين تناولت 52 مقالة فقط (12%) التصيّد عبر البريد الإلكتروني، و46 مقالة تناولت التصيّد عبر الرسائل النصية القصيرة SMS، و15 مقالة درست التصيّد الصوتي (voice-based phishing)، بالإضافة إلى 105 مقالات مراجعة شاملة (survey/review articles) [15].

لمواجهة التصيّد عبر الروابط أو المواقع الإلكترونية، تم اقتراح حلول مبتكرة بالاعتماد على التعلم الآلي والتعلم العميق. تشمل هذه الحلول تقنيات التعلم الآلي التقليدية [14], [15], [16], تقنيات التعلم العميق المتقدمة [18], [19], [20], [21], [22]، والشبكات العميقة القائمة على الرسوم البيانية [23], [24], [25], [26]. رغم ذلك، فإن تقنيات التعلم الآلي تعاني من محدودية الأداء في حال عدم اختيار الخصائص بدقة، حيث أن البيانات غير الضرورية أو المشوشة قد تؤدي إلى فرط التكيّف (overfitting) وانخفاض الدقة. من ناحية أخرى، تتطلب تقنيات التعلم العميق بيانات ضخمة وتكلفة حسابية عالية أثناء التدريب [27], [28]. للتغلب على هذه المشكلات، تم اقتراح استراتيجيات بديلة مثل اختيار الخصائص (feature selection) [20], [29], [30], [31] بهدف إزالة الخصائص غير المفيدة وتحسين الدقة، لكن هذه الاستراتيجيات تعاني من مشكلات في قابلية التوسع. في مجال كشف التصيّد عبر البريد الإلكتروني، أظهرت تقنيات التعلم العميق المدمجة مع معالجة اللغة الطبيعية (NLP) أداءً أفضل من طرق التعلم الآلي التقليدية. على سبيل المثال، في دراسة Melendez وآخرين [33] تم اختبار عدة نماذج مثل:

RoBERTa بدقة (99.43%)

XLNet بدقة (98.84%)

BERT بدقة (99.11%)

وقد تفوقت جميعها على نماذج التعلم الآلي التقليدية في كشف رسائل التصيّد.

معظم هذه الدراسات ركزت على خصائص الروابط (URLs)، نموذج كائن المستند (Document Object Model – DOM)، لغة JavaScript، المحتوى النصي، ترويسات البريد الإلكتروني، أو التمثيلات البصرية. إلا أنه لا توجد دراسات كافية تناولت الكشف متعدد الوسائط (multimodal detection) للتصيّد على شبكات التواصل الاجتماعي، وهو ما يمثل فجوة بحثية مهمة تسعى هذه الدراسة إلى سدّها.

جدول 1:اهم مقالات الدراسة في كشف التصيد

SL. No.	Pub Year	Author(s)	Title	Pub title	Dol
1	2024	Albishri, A.A.; Dessouky, M.M.	دراسة مقارنة لتقنيات التعلّم الآلي في كشف هجمات التصيّد الاحتيالي عبر عناوين المواقع (URLs)	Technology and Applied Science Research	10.48084/etasr.8920
2	2024	Duy, P.T.; Minh, V.Q.; Dang, B.T.H.; Son, N.D.H.; Quyen, N.H.; Pham, V.-.H	دراسة حول مقاومة العينات الهجومية وآليات الدفاع للكشف عن مواقع التصيّد الاحتيالي بالاعتماد على التعلم متعدد الوسائط	IEEE Access	10.1109/ACCESS.2024.3436812
3	2022	Chai, Y.; Zhou, Y.; Li, W.; Jiang, Y.	نموذج تفسيري متعدد الوسائط قائم على الانتباه الهرمي لتطوير استخبارات التهديدات في التصيّد الاحتيالي	IEEE Transactions on Dependable and Secure Computing.	10.1109/TDSC.2021.3119323
4	2022	Rao, Routhu Srinivasa; Umarekar,	تطبيق تقنيات تمثيل الكلمات والتعلّم الآلي في كشف مواقع التصيّد الاحتيالي	Telecommunication Systems	10.1007/s11235-021-00850-6

		Amey; Pais, Alwyn Roshan			
5	2024	Tsinganos, N.; Fouliras, P.; Mavridis, I.; Gritzalis, D.	CSE-ARS: دمج متأخر قائم على التعلّم العميق للمعلومات متعددة الأنماط من أجل التعرّف على هجمات الهندسة الاجتماعية المعتمدة على المحادثات	IEEE Access	10.1109/ACCESS.2024.3359030
6	2024	Avci, Cigdem; Tekinerdogan, Bedir; Cat	تصميم التكتيكات لتكييف بنى المحوّلات (Transformers) مع التحديات في مجال الأمن السيبراني	Cluster Computing	10.1007/s10586-024-04355-0
7	2023	Rustam, Furqan; Saher, Najia; Mehmood, Arif; Lee, Ernesto; Washington, Sandrilla; Ashraf, Imran	اكتشاف الرسائل البريدية الشرعية وغير المرغوب فيها باستخدام دمج الخصائص ونماذج التعلم الآلي المشرف	Multimedia Tools Appl.	10.1007/s11042-023-14814-2
8	2024	Dharini, N.; Sudarsan, E.P.V.;	تحسين كشف التصيّد الاحتيالي: دمج خوارزمية الغابة العشوائية مع تحليل النطاق لتعزيز الأمن السيبراني الاستباقي	8th International Conference on I-SMAC (IoT in Social, Mobile,	10.1109/I-SMAC61

		Praveen, B.; Thirugnanam, D.; Sibi, K		Analytics and Cloud), I-SMAC 2024 - Proceedings	858.2024.10714859
9	2023	Sun, Y.; Liu, G.; Han, X.; Zuo, W.; Liu, W.	FusionNet: إطار فعّال لكشف مواقع التصيّد الاحتيالي الشبكية قائم على الدمج متعدد الوسائط	IEEE International Conference on High Performance Computing Communications, Data Science Systems, Smart City Dependability in Sensor, Cloud Big Data Systems Application	10.1109/HPCC-DSS-SmartCity-DependSys60770.2023.00071
10	2022	Nam, S.-G.; Jang, Y.; Lee, D.-G.; Seo, Y.-S.	الميزات الهجينة من خلال دمج المعلومات البصرية والنصية لتحسين أداء تصفية الرسائل المزعجة	Electronics (Switzerland)	10.3390/electronics11132053
11	2020	Azeez, Nureni Ayofe; Salaudeen, Balikis	اكتشاف هجمات التصيد في شبكات الاتصال باستخدام ميزات اتساق عناوين المواقع (URLs)	Int. J. Electron. Secur. Digit. Forensic	**10.1504/ijesdf.2020.106318**

		Bolanle; Misra, Sanjay; Damaševičius, Robertas; Maskeliūnas, Rytis			
12	2023	Muralidharan, Trivikram; Nissim, Nir	تحسين كشف رسائل البريد الإلكتروني الخبيثة من خلال هياكل عميقة مبتكرة مخصصة بالاعتماد على محتوى البريد الإلكتروني بالكامل	Neural Network	**10.1016/j.neunet.2022.09.002**
13	2024	Trad, Fouad; Chehab, Ali	وكلاء متعددة الوسائط واسعة النطاق للكشف الدقيق عن هجمات التصيد الاحتيالي باستخدام رموز محسّنة	Optimization and Cost Reduction	**Arxiv•DOI:arXiv:2412.02301**
14	2024	Liu, Ruofan; Lin, Yun; Teoh, Xiwen; Liu, Gongshen; Huang, Zhiyong; Dong, Jin Song	معرفة أقل تحديدًا وإنذارات أكثر دقة: اكتشاف التصيد الاحتيالي بالاعتماد على المراجع دون قائمة مرجعية محددة مسبقًا	Proceedings of the 33rd USENIX Conference on Security Symposium	**Not available**

15	2024	Gallagher, S.; Gelman, B.; Taoufiq, S.; Vörös, T.; Lee, Y.; Kyadige, A.; Bergeron, S	التصيد الاحتيالي والهندسة الاجتماعية في عصر نماذج اللغة الضخمة (LLMs)	Large Language Models in Cybersecurity: Threats, Exposure and Mitigation	**10.1007/978-3-031-54827-7_8**
16	2021	Anupam, Sagnik; Kar, Arpan Kumar	اكتشاف مواقع التصيّد الاحتيالي باستخدام آلات متجه الدعم وخوارزميات التحسين المستوحاة من الطبيعة	Telecommun. System	**10.1007/s11235-020-00739-w**
17	2024	Prasad, Arvind; Chandra, Shalini	إطار PhiUSIIL: منظومة لاكتشاف روابط التصيّد الاحتيالي مدعومة بملف أمني متنوع، تعتمد على مؤشر التشابه والتعلم التدريجي	Computer Security	**10.1016/j.cose.2023.103545**
18	2023	Vo Quang, M.; Bui Tan Hai, D.; Tran Kim Ngoc, N.; Ngo Duc Hoang, S.; Nguyen Huu, Q.; Phan The,	Shark-Eyes: إطار دمج متعدد الوسائط للكشف عن مواقع التصيّد الاحتيالي اعتماداً على المنظور متعدد المشاهدات	ACM International Conference Proceeding Series	**10.1145/3628797.3629003**

		D.; Pham, V.-H			
19	2022	Tanha, Jafar; Zarei, Zahra	خوارزمية تحسين نحلة الطنان (Bombus-terrestris) لاختيار الميزات	Applied Intelligence	**10.1007/s10489-022-03478-4**
20	2024	Singh, Tejveer; Kumar, Manoj; Kumar, Santosh	استعراض تقنيات كشف التصيّد الاحتيالي	Computer Electrical Engineering	**10.1016/j.compeleceng.2024.109374**
21	2024	Lee, Jehyun; Lim, Peiyuan; Hooi, Bryan; Divakaran, Dinil Mon	نماذج اللغة الكبيرة متعددة الوسائط لكشف وتحديد صفحات الويب الاحتيالية (التصيّد)	APWG Symposium on Electronic Crime Research (eCrime)	**10.1109/eCrime66200.2024.00007**
22	2021	Van Dooremaal, Bram; Burda, Pavlo; Allodi, Luca;	دمج الخصائص النصية والبصرية لتحسين التعرف على صفحات الويب المستنسخة من أجل الكشف المبكر عن هجمات التصيّد	Proceedings of the 16th International Conference on Availability, Reliability and Security	**10.1145/3465481.3470112**

		Zannone, Nicola			
23	2023	Mishra, S.; Soni, D.	DSmishSMS: نظام لكشف رسائل التصيّد الاحتيالي عبر الرسائل القصيرة (Smishing SMS)	Neural Computing and Applications	**10.1007/s00521-021-06305-y**
24	2023	Tan, Colin Choon Lin; Chiew, Kang Leng; Yong, Kelvin S.C.; Sebastian, Yakub; Than, Joel Chia Ming; Tiong, Wei King	كشف التصيّد الاحتيالي الهجين باستخدام الهوية المشتركة البصرية والنصية	Expert Systems with Applications	**10.1016/j.eswa.2023.119723**
25	2023	Belfedhal, Alaa Eddine	التعلّم العميق متعدّد الوسائط للكشف الفعّال عن صفحات الويب الخبيثة	Revue d'Intelligence Artificielle	**10.18280/ria.370422**
26	2024	Alsaedi, Mohammed ; Ghaleb, Fuad A.; Saeed, Faisal;	نموذج الشبكات العصبية الالتفافية المعتمد على التمثيل متعدّد الوسائط لكشف المواقع الإلكترونية الخبيثة	IEEE Access	**10.1109/ACCESS.2023.3348071**

		Ahmad, Jawad; Alasli, Mohammed			
27	2023	Al-Kabbi, H.A.; Feizi-Derakhshi, M.-R.; Pashazadeh	إطار عمل لاستخراج الميزات متعددة الأنواع والدمج المبكر لكشف الرسائل النصية المزعجة SMS Spam) (Detection	IEEE Access	**10.1109/ ACCESS .2023.332 7897**
28	2021	Zhang, Lei; Zhang, Peng; Liu, Luchen; Tan, Jianlong	إطار عمل لاستخراج الميزات متعددة الأنواع ودمجها المبكر للكشف عن الرسائل النصية القصيرة المزعجة (SMS Spam (Detection	IEEE Access	**10.1109/ ACCESS .2023.332 7897**
29	2024	Cao, Tri; Huang, Chengyu; Li, Yuexin; Wang, Huilin	PhishAgent: وكيل متعدد الوسائط وموثوق للكشف عن صفحات الويب الاحتيالية Phishing Webpage) (Detection	Proceedings of the AAAI Conference on Artificial Intelligence	**10.1609/a aai.v39i2 7.35003**
30	2022	Zhang, Sirui; Yan, Zhiwei; Dong, Kejun; Li, Hongtao;	الكشف عن أسماء النطاقات الاحتيالية بالاعتماد على الدمج الهرمي للميزات متعددة الوسائط	IEEE 16th International Conference on Big Data Science and Engineering (BigDataSE)	**10.1109/ BigData SE56411. 2022.000 10**

		Yuchi, Xuebiao			
31	2024	Yoon, Jun-Ho; Buu, Seok-Jun; Kim, Hae-Jung	الكشف عن صفحات الويب الاحتيالية من خلال التكامل متعدد الوسائط بين رسوم HTML البيانية وميزات عناوين DOM الروابط (URLs) بالاعتماد على الشبكات الالتفافية البيانية وشبكات المحولات	Electronics	el/10.3390 ectronics131633 44
32	2025	Çolhak, Furkan; Ecevit, Mert İlhan; Uçar, Bilal Emir; Creutzburg, Reiner; Dağ, Hasan	الكشف عن مواقع الويب الاحتيالية من خلال التحليل متعدد النماذج لمحتوى HTML	Proceedings of International Conference on Theoretical and Applied Computing	**10.1007/9 78-981- 97-6957- 5_15**

1.5 التحديات

في الدراسة الحديثة " Staying ahead of phishers: a review of recent advances and challenges in phishing detection" (2024)، أجرى الباحثون مراجعة منهجية لأحدث تقنيات كشف التصيّد الاحتيالي، مسلطين الضوء على أبرز التحديات التقنية والبحثية التي تحد من كفاءة هذه الأنظمة. توضح الدراسة أن الاعتماد على القوائم السوداء (Blacklists) أو تقنيات الكشف الثابتة يفتقر إلى القدرة على التعامل مع هجمات Zero-Day، إذ لا تتمكن هذه الأساليب من التكيف بالسرعة الكافية مع الروابط الضارة الجديدة. كما تشير الدراسة إلى أن الهجمات المتحوّلة (Adversarial Attacks) تمثل تهديدًا جوهريًا، حيث يمكن للمهاجمين إدخال تعديلات طفيفة في هيكل الرابط أو المحتوى لتمويه أنظمة الكشف وتجاوزها. ولاكن ، لاحظ الباحثون أن النماذج التقليدية المعتمدة على الخصائص اليدوية (Feature Engineering) تعاني من ضعف القدرة على التكيف مع أنماط التصيّد الناشئة، رغم فعاليتها النسبية. وتوصي الدراسة بتطوير أنظمة هجينة (Hybrid Models) تجمع بين قوة التعلم العميق ومرونة النماذج الإحصائية، مع التركيز على إنشاء خصائص مقاومة للتلاعب، بهدف تعزيز دقة الكشف مع الحد من معدلات الإنذار المخادعة.

1.6 التطبيقات العملية

خلال الفترة من 2023 إلى 2024، شهدت الأبحاث الأكاديمية تقدمًا كبيرًا في تطوير تطبيقات عملية لكشف التصيّد الاحتيالي، خاصة فيما يتعلق بالبيئات الحقيقية مثل البريد الإلكتروني وشبكات التواصل الاجتماعي. على سبيل المثال، قدمت دراسة PhishIntel نموذجًا متقدمًا يعتمد على تقسيم المهام إلى سريعة وبطيئة، مما يتيح كشفًا فوريًا للروابط الاحتيالية مع الحفاظ على دقة عالية، وقد تم اختبار هذا النظام فعليًا على بيئة Microsoft Outlook لإظهار قابليته للتطبيق العملي.

في السياق نفسه، طوّر PhishLang إطارًا للكشف على جانب العميل باستخدام نموذج MobileBERT، حيث ركّز الباحثون على إنشاء نظام سريع وخفيف الموارد قادر على معالجة آلاف الروابط في الوقت الفعلي، ما يجعله مناسبًا للاستخدام المباشر على الأجهزة المحمولة دون الحاجة إلى خوادم مركزية.

كما استعرضت دراسة KnowPhish إمكانية دمج نماذج اللغة الكبيرة مع الرسوم المعرفية متعددة الوسائط لتعزيز الكشف عن الروابط الاحتيالية، مما أتاح للنظام تحليل المحتوى النصي والصوري بشكل متكامل وزيادة فعالية اكتشاف الهجمات المتقدمة. وبالموازاة، استخدمت دراسة Prompted Contextual Vectors تقنيات حديثة لإنشاء تمثيلات سياقية للمستندات باستخدام نماذج اللغة الكبيرة، موجهة بشكل خاص للكشف عن رسائل التصيّد الموجه (Spear-Phishing)، وهو ما يعالج التحديات المرتبطة بالهجمات المخصصة للأفراد أو المؤسسات.

توضح هذه الدراسات أن تطبيقات كشف التصيّد الحديثة لا تقتصر على خوارزميات نظرية، بل تمتد إلى نماذج قابلة للتنفيذ العملي في بيئات واقعية متنوعة، سواء على البريد الإلكتروني، الشبكات الاجتماعية، أو الأجهزة المحمولة. كما تؤكد هذه الأعمال على أهمية الجمع بين السرعة والدقة، وتحليل الروابط والمحتوى بطريقة شاملة، لتقديم حلول متكاملة تحمي المستخدمين من الهجمات الاحتيالية المتطورة.

الفصل الأول

2.1 ما هي وسائل التواصل الاجتماعي؟

شهدت السنوات الأخيرة تطورًا ملحوظًا في استخدام وسائل التواصل الاجتماعي، حيث أصبحت أداة أساسية للتواصل بين الأفراد والمؤسسات، ومصدراً مهماً لنشر الرسائل والوصول إلى جمهور واسع. ووفقًا لتقرير صادر عن معهد ماكينزي العالمي في يوليو 2012، بلغ عدد مستخدمي شبكات التواصل الاجتماعي حوالي 1.5 مليار مستخدم حول العالم، منهم ما يقارب 80% يتفاعلون بانتظام مع مستخدمين آخرين. هذا الانتشار الكبير، مدفوعًا برغبة الشركات في الوصول إلى عملائها، أدى إلى أن ما يقارب 70% من المؤسسات أصبحت تعتمد على هذه الوسائل في أنشطتها.لقد تحولت التكنولوجيا الاجتماعية إلى عنصر جوهري في حياتنا اليومية، سواء على مستوى التواصل الاجتماعي أو في بيئة الأعمال. ومع ذلك، ورغم كون وسائل التواصل الاجتماعي أداة فعّالة للتفاعل، فإن العديد من الأفراد والمنظمات اندفعوا نحو استخدامها دون إدراك كافٍ للمخاطر المرتبطة بها. هذه التهديدات قد تؤثر بشكل مباشر على السلامة الشخصية، والمسار الوظيفي، واستمرارية الأعمال.ومن هنا تبرز أهمية التعمق في فهم طبيعة وسائل التواصل الاجتماعي، ومراحل تطورها، قبل التطرق إلى المخاطر المحتملة وطرق الحد منها.

2.2 فهم وسائل التواصل الاجتماعي

تُعرف وسائل التواصل الاجتماعي بأنها مجموعة من التقنيات التي تهدف إلى تعزيز التفاعل والتعاون بين الأفراد، وتتميز بخصائصها الفريدة التي تميزها عن وسائل الإعلام التقليدية. بينما تعتمد وسائل الإعلام التقليدية، مثل الصحف والتلفزيون، على تقديم محتوى مُعد مسبقًا ومراجعته من قبل مختصين، فإن وسائل التواصل الاجتماعي تسمح للمستخدمين أو العلامات التجارية بإنشاء المحتوى ونشره دون الحاجة إلى تدقيق صارم، مما يتيح تواصلًا ثنائي الاتجاه مع الجمهور. تُعتبر التكلفة المنخفضة لاستخدام وسائل التواصل الاجتماعي، والتي قد تكون مجانية في بعض الحالات، من أبرز ميزاتها مقارنة بالإعلام التقليدي. كما أن الجانب الاجتماعي لوسائل التواصل الاجتماعي يتيح للمستخدمين إمكانية التعليق والمشاركة، مما يعزز الحوار المتبادل. فعلى سبيل المثال، يمكن للقراء الرد على المدونات مباشرةً، مما يحول المعلومات إلى تبادل غير رسمي للآراء. تُظهر هذه الخصائص كيف أن وسائل التواصل الاجتماعي قد كسرت الحدود التقليدية، حيث يمكن للقارئ أن يصبح كاتبًا بسهولة. وبالتالي، يُعتبر مصطلح "وسائل التواصل الاجتماعي" متغيرًا ومتطورًا باستمرار، مما يجعله أكثر اتساعًا من مجرد الإشارة إلى استخدام أو تصميم محدد.

2.3 الأنواع والتصنيفات المختلفة لوسائل التواصل الاجتماعي

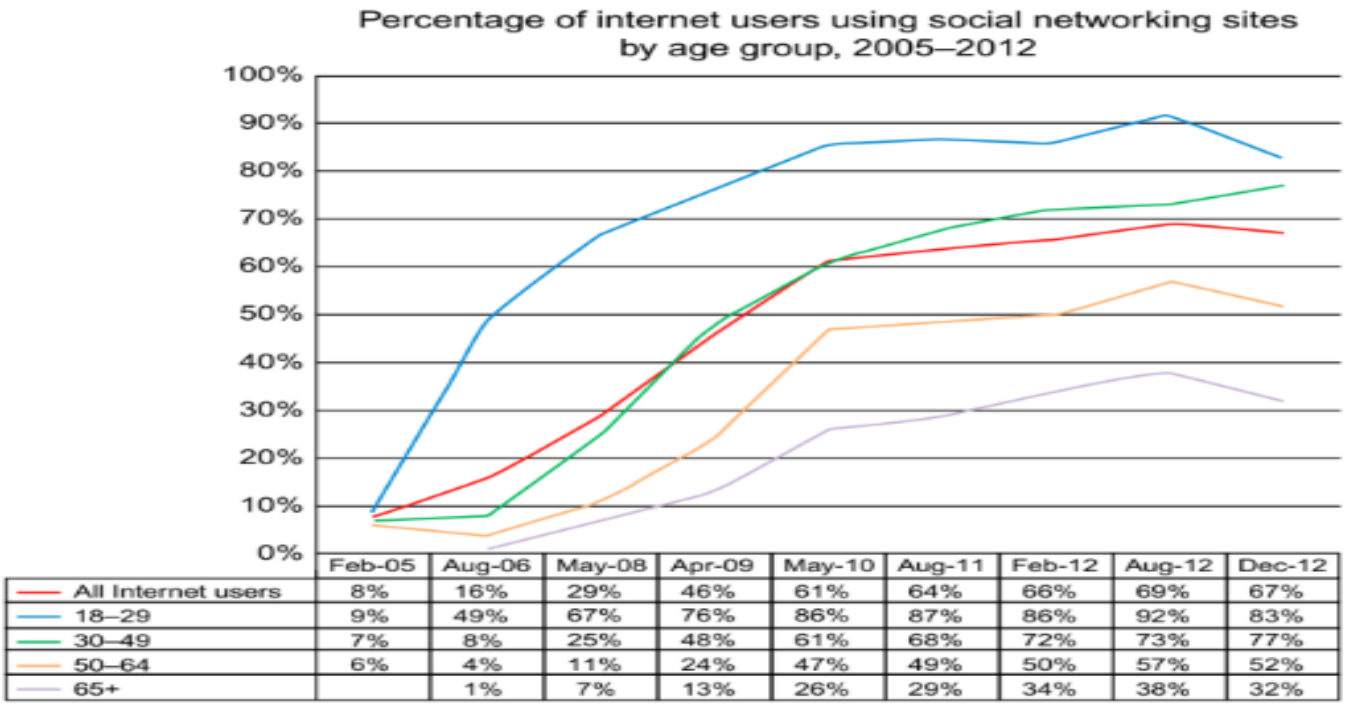
بمجرد البدء في دراسة وسائل التواصل الاجتماعي، سرعان ما يتضح أن هناك اختلافات كبيرة في الأهداف والوظائف بين المنصات المختلفة. فعلى سبيل المثال، قد يكون تويتر أداة فعّالة لإرسال رسائل قصيرة إلى جمهور واسع، ولكنه غير مناسب للتعاون في كتابة

مقالات طويلة. وبالمثل، إذا كان الهدف نشر محتوى مرئي بدلاً من النصوص، فسيكون موقع مثل يوتيوب الخيار الأمثل. ونظرًا لوجود مئات المواقع والتطبيقات الخاصة بوسائل التواصل الاجتماعي، فإن من المهم التمييز بينها. ويساعد تقسيم هذه المنصات إلى مجموعات محددة على توضيح أنواع وسائل التواصل الاجتماعي المتاحة، ومعرفة أي منها الأنسب لتحقيق غرض معين. في مقال نُشر عام 2010 في مجلة Business Horizons، قام أندرياس كابلان ومايكل هاينلاين بوضع مخطط تصنيفي لأنواع مختلفة من وسائل التواصل الاجتماعي. وبالاعتماد على النظريات القائمة في مجالي أبحاث الإعلام والعمليات الاجتماعية، قاما بتحديد ست فئات رئيسية:

1. المشاريع التعاونية (Collaborative Projects)
2. المدونات (Blogs)
3. مجتمعات المحتوى (Content Communities)
4. مواقع الشبكات الاجتماعية (Social Networking Sites)
5. عوالم الألعاب الافتراضية (Virtual Game Worlds)
6. العوالم الاجتماعية الافتراضية (Virtual Social Worlds)

2.4 قيمة وسائل التواصل الاجتماعي

على امتداد هذا الفصل، تمت مناقشة بعض فوائد وسائل التواصل الاجتماعي على المستويات الشخصية والتنظيمية، مع التأكيد على أن القيمة الحقيقية لاستخدامها تعتمد على كيفية استثمار الأفراد أو المؤسسات لهذه الوسائل. الخيارات المتخذة تحدد ما إذا كانت هذه الوسائل ستعود بفوائد ملموسة أو ستؤثر سلبًا على السمعة. وفقًا لدراسة أجرتها جامعة ماساتشوستس دارتموث عام 2013، تبين أن 73% من شركات Fortune 500 لديها حسابات على تويتر، و66% على فيسبوك، و62% تستخدم يوتيوب. يُظهر هذا الارتفاع في استخدام وسائل التواصل الاجتماعي بين الشركات الكبرى أنها أصبحت سمة أساسية في المؤسسات. بالإضافة إلى ذلك، أظهر استطلاع من وول ستريت جورنال وVistage International عام 2013 أن 30% من مالكي الشركات الصغيرة يستخدمون لينكدإن بانتظام، مع اعتبار 41% منهم أنها المنصة الأكثر فائدة لأعمالهم كما موضح في الشكل (1) فقد كانت معدلات استحدام المنصات الأخرى أقل كما اعتبرت أقل فائدة.



	Feb-05	Aug-06	May-08	Apr-09	May-10	Aug-11	Feb-12	Aug-12	Dec-12
All Internet users	8%	16%	29%	46%	61%	64%	66%	69%	67%
18–29	9%	49%	67%	76%	86%	87%	86%	92%	83%
30–49	7%	8%	25%	48%	61%	68%	72%	73%	77%
50–64	6%	4%	11%	24%	47%	49%	50%	57%	52%
65+		1%	7%	13%	26%	29%	34%	38%	32%

الشكل 1 : استخدام مواقع التواصل الاجتماعي من قبل شركات Fortune 500

2.5 تاريخ الشبكات الاجتماعية

رغم أن مصطلح "وسائل التواصل الاجتماعي" حديث نسبيًا، فإن جذوره تعود إلى بدايات الحوسبة الحديثة في سبعينيات القرن العشرين، حين بدأ المستخدمون بالتفاعل عبر الحواسيب لتبادل البيانات والمشاركة في المشاريع الجماعية. وشكّل نظام لوحات النشرات الإلكترونية (BBS) الذي أُطلق عام 1978 نقطة تحول مهمة، إذ أتاح التواصل وتبادل الملفات عبر خطوط الهاتف، ممهّدًا لظهور المجتمعات الرقمية الأولى. مع منتصف التسعينيات، تراجع استخدام أنظمة BBS لصالح الإنترنت، وظهرت منصات مثل GeoCities التي سمحت بإنشاء مواقع شخصية، وAOL وCompuServe التي قدمت بيئات تفاعلية مبكرة للتواصل. كما برز نظام Usenet كمنصة للنقاشات وتبادل الملفات عالميًا. وفي عام 1997 ظهر موقع SixDegrees، الذي يُعد أول شبكة اجتماعية بالمعنى الحديث، إذ مكّن المستخدمين من بناء علاقات رقمية مترابطة. خلال العقد الأول من الألفية الجديدة، تسارعت وتيرة التطور بظهور Wikipedia (2001) وLinkedIn (2003) وMySpace (2003) و Second Life (2003)، قبل أن تُطلق Facebook (2004) التي غيّرت مفهوم التواصل الرقمي جذريًا، تلاها YouTube (2005) لمشاركة الفيديو وTwitter (2006) للتدوين المصغر. ارتبط هذا التحول بمفهوم الويب 2.0 الذي مثّل انتقال

الإنترنت من المحتوى الثابت إلى المنصات التفاعلية التي ينشئ المستخدمون محتواها بأنفسهم، وهو المفهوم الذي بُنيت عليه تعريفات وسائل التواصل الاجتماعي الأكاديمية. في العقد الثاني من القرن الحادي والعشرين، هيمنت المنصات البصرية مثل Instagram (2010) وTikTok (2016)، لتتحول وسائل التواصل الاجتماعي إلى فضاءات متعددة الوسائط تؤثر في الثقافة والسياسة والاقتصاد العالمي. وهكذا، يُظهر المسار التاريخي أن الشبكات الاجتماعية لم تكن ابتكارًا مفاجئًا، بل نتاج تطور تدريجي بدأ من أنظمة النشرات الإلكترونية وصولًا إلى المنصات الحديثة، مع بقاء جوهر الفكرة ثابتًا: تمكين الأفراد من التواصل وتبادل المعرفة وبناء مجتمعات رقمية عابرة للحدود.

2.6 آلية تصميم منصّات التواصل الاجتماعي

تمثل منصّات التواصل الاجتماعي تفاعلًا متكاملًا بين الأبعاد الاجتماعية والسلوك البشري من جهة، والبنية التقنية والهندسية من جهة أخرى. وتُعتبر عملية تصميم هذه المنصات سلسلة مترابطة تبدأ من تحديد طبيعة المجتمع الرقمي، مرورًا ببناء الهوية الرقمية للمستخدمين وأنماط العلاقات، إلى إدارة دورة حياة المحتوى، البنية التقنية، الخوارزميات، إدارة المنصّة، والخصوصية.

في المراحل الأولى، ينطلق التصميم من تحديد الرؤية الاجتماعية للمنصّة، أي نوع التفاعل المتوقع وطبيعة المجتمع الذي سيُبنى. ويبرز هنا مفهوم أنماط التصميم الاجتماعي (Social Design Patterns) الذي يُوضح آليات بناء الهوية الرقمية للمستخدم، وأنماط العلاقات بين الأفراد (صداقة ثنائية أو متابعة أحادية)، بالإضافة إلى أساليب إدارة المحتوى وتنظيمه داخل المنصّة. بعد ذلك، يتم تصميم دورة حياة المحتوى (Content Lifecycle)، التي تشمل مراحل النشر، التفاعل (إعجاب، مشاركة، تعليق)، وإدارة النقاشات. ويتضمن ذلك آليات تحفيز المحتوى الإيجابي، مثل أنظمة التقييم أو التصويت، إلى جانب أدوات الحدّ من السلوكيات السلبية، مثل التبليغ عن الإساءة أو إدارة التعليقات المتداخلة التي تنظّم الحوار. ومن الناحية التقنية، تعتمد المنصات عادةً على بنية ثلاثية الطبقات، تشمل واجهة أمامية (Front-End) سهلة الاستخدام، وخدمات خلفية موزعة وقابلة للتوسّع (Back-End)، بالإضافة إلى قاعدة بيانات تدير الحسابات والمحتوى والشبكات. تهدف هذه البنية إلى ضمان الأداء والاستقرار، مع إبقاء التقنية في خدمة المجتمع الرقمي لا العكس.مع تطور المجتمع، تُدمج أنظمة الاكتشاف والتوصية (Recommendation Systems) لتسهيل وصول المستخدمين إلى المحتوى ذي الصلة، بالاعتماد على الاهتمامات الفردية، سمعة الناشرين، وحداثة المحتوى. ومع ذلك، قد يؤدي الإفراط في التخصيص إلى تكوين "غرف صدى" (Echo Chambers)، مما يستدعي إدماج أدوات الشفافية والتحكم الذاتي، مثل توضيح سبب ظهور منشور معيّن أو منح المستخدم القدرة على تعديل خوارزمية التوصية.إلى جانب ذلك، تشكّل إدارة المنصّة الرقمية عنصرًا جوهريًا في التصميم، وتشمل وضع القواعد العامة للنشر، توفير أدوات الإبلاغ المدمجة في الواجهة، وتطبيق سياسات الإشراف العادل والشفاف. يساهم دمج هذه السياسات ضمن تجربة المستخدم في جعل عملية الضبط المجتمعي جزءًا أصيلاً من المنصة نفسها.

أما من ناحية الأمان والخصوصية، فقد أصبح التعامل معها عنصرًا أساسيًا منذ مراحل التصميم الأولى. يشمل ذلك التشفير، الإعدادات الواضحة للتحكم بالخصوصية، وآليات الشفافية (Transparency by Design) لبناء الثقة مع المستخدمين، إذ تُعتبر الثقة الأساس لاستدامة المجتمعات الرقمية.بناءً على ذلك، يُمكن القول إن تصميم منصّات التواصل الاجتماعي عملية متكاملة تبدأ من الرؤية الاجتماعية، مرورًا بالهوية الرقمية وأنماط العلاقات، دورة حياة المحتوى، البنية التقنية والخوارزميات، إدارة المنصّة، وصولًا إلى الأمان والخصوصية، وهو التكامل الذي يميز المنصات الناجحة ويضمن قدرتها على النمو والاستدامة.

2.7 آلية عمل منصّات التواصل الاجتماعي

تعمل منصّات التواصل الاجتماعي ضمن منظومة متكاملة تجمع بين التكنولوجيا والسلوك البشري. تبدأ العملية من إنشاء الهوية الرقمية للمستخدم، والتي لا تقتصر على عرض الاسم أو الصورة، بل تشكّل الأساس الذي تُبنى عليه الخوارزميات لتحديد اهتمامات الفرد وبناء الروابط الاجتماعية المناسبة. تُبنى الشبكات الاجتماعية على الرسم البياني الاجتماعي، الذي يوضّح طبيعة الروابط بين الأعضاء، سواء كانت متبادلة كما في الصداقة على فيسبوك، أو أحادية كما في نظام المتابعة على تويتر. هذا الهيكل يمكّن المنصّة من فهم العلاقات الرقمية وتحديد المسافات بين الأفراد، بما يعزز دقة توصية المحتوى المناسب. ويمثّل المحتوى الركيزة الأساسية للمنصّة. فعند نشر نصوص، صور، أو فيديوهات، يخضع المحتوى لدورة حياة تشمل الرفع إلى الخادم الخلفي، ثم التوزيع للجمهور وفق معايير مثل حداثة المحتوى، حجم التفاعل المبكّر، وملاءمته لاهتمامات المستخدمين. تُقرر الخوارزميات ما يظهر على الصفحة الرئيسية للمستخدم وما يُنقل إلى الهامش، مع موازنة ثلاثة عناصر رئيسية: ارتباط المحتوى بالمستخدم، مستوى التفاعل، وحداثة المنشور، مع مراعاة أهداف المنصّة في التفاعل والانتباه. وتدمج المنصات أيضًا آليات الإشراف والضبط، بما يشمل استخدام الذكاء الاصطناعي لرصد الانتهاكات، وفرق بشرية لمراجعة البلاغات، لضمان بيئة آمنة. كما يُعتبر الأمان والخصوصية عنصرًا أساسيًا، حيث تعتمد المنصات على التشفير، إعدادات الخصوصية المدمجة، والشفافية لإبلاغ المستخدم بكيفية استخدام بياناته وسبب ظهور المحتوى.

أخيرًا، تعتمد المنصات على التحسين المستمر، من خلال مراقبة مؤشرات الأداء مثل معدلات الاستخدام ووقت التفاعل، وإجراء اختبارات لتطوير الخوارزميات والوظائف بما يتوافق مع سلوك المستخدمين. بذلك، يمكن القول إن آلية عمل منصات التواصل الاجتماعي تعتمد على سلسلة مترابطة تبدأ من الهوية الرقمية، مرورًا بالشبكات الاجتماعية، إدارة المحتوى والخوارزميات، الإشراف والخصوصية، وصولًا إلى التحسين المستمر، ما يجعلها فضاءات اجتماعية ديناميكية تعكس تعقيد السلوك البشري وتطوره.

2.8 المشكلات والتحديات المرتبطة بوسائل التواصل الاجتماعي

على الرغم من الفوائد الكبيرة التي تقدمها منصات التواصل الاجتماعي في تعزيز الحضور الرقمي للمؤسسات وتحسين التفاعل مع الجمهور، إلا أنّ استخدامها ينطوي على تحديات ومخاطر متعددة. من أبرز هذه المخاطر غياب الوعي الاستراتيجي لدى المستخدمين

والمؤسسات حول مستوى الأمان، اختيار المنصات المناسبة، ووضع سياسات واضحة للاستخدام، مما قد يؤدي إلى تسريب معلومات حساسة أو انتهاك خصوصية البيانات. كما يواجه المحتوى المنشور عبر المنصات التفاعلية مثل الويكيات تحديات الموثوقية والدقة، إذ يمكن أن يُنشر محتوى خاطئ أو مضلل لفترات طويلة قبل اكتشافه وتصحيحه، كما ظهر في حالات مثل جون سيغنثالَر وWikitorial بصحيفة Los Angeles Times.وتتضمن التحديات الأخرى المخاطر المؤسسية، حيث يمكن للمدونات أو الحسابات المرتبطة بالشركة أن تتحول إلى مصدر تهديد إذا لم تُحدد السياسات ما يمكن وما لا يمكن نشره، كما ظهر في حالة Robert Scoble أثناء عمله في مايكروسوفت. إضافة إلى ذلك، يُشكل انتهاك حقوق الملكية الفكرية تحديًا آخر، إذ يمكن إعادة استخدام الصور أو الفيديوهات المنشورة بدون إذن، ما يثير التوازن بين فقدان السيطرة على المحتوى والاستفادة من الانتشار التسويقي غير المباشر.

بشكل عام، تشير هذه المخاطر إلى أن تحديات وسائل التواصل الاجتماعي تمتد من الاستخدام الفردي إلى البنية المؤسسية والمجتمعية، وتشمل غياب الحوكمة الرقمية وضعف آليات التدقيق والمراجعة. لذلك، فإن الاستخدام الآمن والفعال لهذه المنصات يتطلب وعيًا استراتيجيًا متوازنًا بين الاستفادة من الفرص وتجنب التهديدات، مع اعتماد سياسات واضحة للمراقبة والإشراف والتحكم في المحتوى.

2.9 المخاطر الأمنية المرتبطة باستخدام وسائل التواصل الاجتماعي

يشكّل الأمن المعلوماتي أحد أبرز التحديات المرتبطة باستخدام وسائل التواصل الاجتماعي على المستويين الفردي والمؤسسي، نظرًا لتزايد الاعتماد على هذه الأدوات وانتشارها الواسع. وتشمل المخاطر الأساسية ما يلي:

1. البرمجيات الخبيثة (Malicious Code): احتمال إصابة الأجهزة أو الشبكات بفيروسات أو برامج تجسس عبر الروابط والملفات المتداولة.
2. الهندسة الاجتماعية (Social Engineering): التعرض لمحاولات خداع أو تصيّد تهدف إلى سرقة بيانات حساسة.
3. اختراق الحسابات: السيطرة على حسابات المستخدمين لنشر محتوى مزيف أو مسيء.
4. تسريب المعلومات الحساسة: نشر بيانات داخلية قد يضر بسمعة المؤسسة.
5. الجرائم الإلكترونية: الابتزاز، الاحتيال، أو سرقة الهوية الرقمية.
6. الوصول غير المصرح به إلى البيانات: تخزين المحتوى على خوادم عامة يعرضه للاختراق.
7. الإفراط في مشاركة المعلومات الشخصية: الكشف عن تفاصيل حساسة عبر المدونات أو الحسابات الاجتماعية.
8. المساءلة القانونية: قضايا متعلقة بالبحث عن الموظفين أو مشاركة البيانات الشخصية.
9. مخالفة التشريعات والأنظمة: انتهاك حقوق الملكية الفكرية أو قوانين حماية البيانات.

ولا تقتصر الاستجابة لهذه المخاطر على تقييد الوصول أو فرض ضوابط صارمة، بل تتطلب تحقيق توازن بين تمكين المستخدمين وتطبيق ضوابط أمنية فعّالة. كما يعتمد نجاح أي استراتيجية أمنية على وعي الموظفين والمستخدمين بأهمية هذه الإجراءات وفهمهم لأسبابها، مما يعزز الامتثال ويقلل احتمالية الانتهاك أو التحايل.

في عام 2004، تعرض حوالي 2 مليون مواطن أمريكي لعمليات سطو على حساباتهم الجارية بواسطة مجرمي الإنترنت. وقد قدرت الخسائر المتوسطة لكل حادثة بحوالي 1200 دولار، ليصل إجمالي الخسائر إلى نحو 2 مليار دولار. وقد شهدت نسبة رسائل البريد الإلكتروني للتصيّد، وهي الرسائل التي تهدف إلى سرقة اسم المستخدم وكلمة المرور عبر تقليد البريد الإلكتروني المرسل من مؤسسة مالية شرعية، زيادة بنسبة 4000% خلال الأشهر الستة الأخيرة. يجسد مصطلح "التصيّد" (Phishing) تقنية صيد البيانات، حيث يُستمد الـ "ph" من الأساليب المعقدة التي يستخدمها المهاجمون لتمييز أنشطتهم عن أساليب الصيد التقليدية والبسيطة.

على مر السنوات الأخيرة، أصبحت الخدمات المصرفية عبر الإنترنت، بما في ذلك دفع الفواتير، شائعة للغاية مع ازدياد عدد المؤسسات المالية التي تقدم خدمات مجانية عبر الإنترنت. ومع تزايد عمليات الاحتيال عبر الإنترنت وسرقة الهوية، تحولت الجرائم المالية من هجمات مباشرة إلى هجمات غير مباشرة. أي أن المهاجمين لم يعودوا يسرقون البنوك بشكل مباشر، بل بدأوا يستهدفون عملاء تلك البنوك. هذه الهجمات غير المباشرة تؤثر بشكل كبير على المؤسسات المالية نفسها، إذ أن عدم قدرتها على حماية أصول عملائها بشكل مناسب يؤثر سلبًا على سمعتها وثقة العملاء بها. كانت رسائل التصيّد في البداية تعرف بـ "carding" حيث كان المهاجمون يستخدمون تقنيات لسرقة معلومات البطاقات الائتمانية عبر البريد الإلكتروني. ورغم أن هذه الرسائل تعتبر من الآثار الجانبية غير المرغوب فيها لعصرنا الإلكتروني، فإنها تستمر في الانتشار بشكل غير مسبوق شهريًا. وفقًا لتقرير صادر عن شركة Symantec (تقرير تهديدات الإنترنت من Symantec، المجلد السابع، مارس 2005)، تم تصنيف 63% من 2.93 مليار رسالة بريد إلكتروني عبر برنامج Brightmail AntiSpam على أنها رسائل غير مرغوب فيها. وفي منتصف يوليو 2004، كانت فلاتر Brightmail AntiSpam تحظر حوالي 9 مليون محاولة تصيّد أسبوعيًا، ليرتفع الرقم إلى أكثر من 33 مليون محاولة في ديسمبر من نفس العام.وفقًا لإحصائيات أخرى من شركة Postini لمكافحة الرسائل غير المرغوب فيها، تم تصنيف 10 من كل 12 رسالة بريد إلكتروني على أنها رسائل غير مرغوب فيها رسميًا خلال فترة 24 ساعة في مارس 2005، كما كانت 1 من كل 82 رسالة تحتوي على فيروس.ورغم الإجماع العام على أن الرسائل غير المرغوب فيها تعتبر أمرًا سيئًا، يظل التساؤل قائمًا: لماذا لا تزال هذه الصناعة تعد واحدة من أسرع الصناعات نموًا؟ الجواب يكمن في أن المهاجمين يستمرون في إرسال الرسائل طالما أن 1 من كل 100,000 متلقي يستجيب فعليًا للروابط المرسلة في رسائل البريد الإلكتروني، مما يحفزهم على إرسال ملايين الرسائل الجديدة.

لقد تعرضت القضايا القانونية المرفوعة ضد مرسلي الرسائل المزعجة (سبام) لعدة معوقات، تشمل تتبع المصدر، وتحديد هوية المصدر، وتفسير القوانين الدولية في محاولات تقديمهم للمحاكمة. يعتقد العديد من خبراء الصناعة أن غالبية رسائل التصيّد والبريد المزعج (سبام) تأتي من خارج الولايات المتحدة. ومع ذلك، أفادت مزودات برامج مكافحة الفيروسات مثل سوفوس (Sophos) أن حوالي

60% من البريد المزعج الذي استقبله مركز أبحاث البريد المزعج التابع لها في سوفوس لابز حول العالم في عام 2004 كان مصدره الولايات المتحدة. وفقًا لسوفوس لابز، تم الإبلاغ عن أكثر من 1200 فيروس جديد خلال الشهرين الأولين من عام 2005، وهو زيادة كبيرة مقارنة بإحصائيات عام 2004.

وبالنسبة لقانون CAN-SPAM للتحكم في الهجمات التسويقية غير المرغوب فيها في الولايات المتحدة لعام 2003، فإنه يمكن استخدامه لمقاضاة مرسلي البريد المزعج. ومع ذلك، تبين أن أكثر من 60% من البريد المزعج الذي تم إرساله من الولايات المتحدة كان قد أُرسل من أجهزة كمبيوتر مصابة بتروجان وبرمجيات خبيثة تعمل كـ بريد مزعج عبر قنوات مصابة (spam-relay Trojans and worms). تسمح هذه الأدوات الخبيثة للمرسلين من جميع أنحاء العالم بإعادة توجيه رسائلهم عبر آلاف الأنظمة المصابة من دون أن يعلم مالكو الأجهزة بذلك.

2.10 التصيد الإلكتروني

التصيّد الإلكتروني هو أحد الأنواع الفرعية من فئة الاحتيال. في هجوم التصيّد، يتنكر المهاجمون في صورة شركات محترمة (الهدف) للحصول على بيانات حسابات العملاء، معلوماتهم، أو صلاحيات الوصول. باستخدام تقنيات التصنيف التي تم وصفها سابقًا، يمكننا تحديد مجموعات التصيّد الإلكترونية الخاصة. تشمل العناصر الرئيسية للتعرف ما يلي:

- أداة إرسال البريد الجماعي وخصائصها
- عادات إرسال البريد، بما في ذلك أنماط الإرسال والجداول الزمنية المحددة
- أنواع الأنظمة المستخدمة لإرسال البريد المزعج (مثل مضيف البريد الإلكتروني)
- أنواع الأنظمة المستخدمة لاستضافة خادم التصيّد
- تخطيط خادم التصيّد العدائي، بما في ذلك استخدام HTML، JS، PHP، والبرمجيات النصية الأخرى

حتى الآن، وفقًا لـ SSC، يوجد ما يُقدّر بحوالي أربعة دزينة من مجموعات التصيّد الإلكتروني على مستوى العالم، مع أكثر من نصف هذه المجموعات تستهدف العملاء في الولايات المتحدة. يوضح بقية الكتاب تقنيات تساعد في فهم وتتبع مرسلي التصيّد، وتمكين

إنشاء خط دفاع قوي ضد هؤلاء المجرمين الإلكترونيين، الذين يعتبرهم الكثيرون هجومًا ساحقًا. يبدأ الكتاب بنظرة عامة عامة، ثم ينتقل إلى مناقشات محددة جدًا وعميقة من كلا الجانبين، الجيد والسيئ.

2.11 تطور الجريمة الإلكترونية

من المحتمل أن تكون قد تلقيت رسالة تصيّد إلكتروني (Phishing) في بريدك الإلكتروني خلال الأشهر القليلة الماضية أو حتى في الأسبوع الماضي. وبحلول الوقت الذي يتم فيه نشر هذا الكتاب ووصوله إلى يديك، ستكون العمليات التي تتضمن عمليات الاحتيال عبر التصيّد قد تسارعت بسبب انتشار البرمجيات الخبيثة العدائية (التروجان، الفيروسات)، والشبكات الآلية (botnets)، والبنية التحتية العامة التي أنشأها هؤلاء المجرمون الإلكترونيون.

لنأخذ خطوة إلى الوراء للحظة. لقد تغير عالمنا بشكل كبير منذ أن كنت صغيرًا. قبل 10 سنوات فقط، كانت تطور مهارات القراصنة والأدوات المتاحة لهم محدودة إلى حد ما من الناحية الأمنية على المستويين الوطني والدولي. نعم، كان هناك جرائم إلكترونية، ولا يمكن إنكار ذلك، لكن لم تكن بهذا المستوى من الجرأة الذي نعيشه اليوم. كان اختراق الأنظمة الحاسوبية مدفوعًا بالحاجة إلى الاستكشاف، والحصول على المعلومات، والتعليم. كان هذا هو عالم القراصنة الذين يعملون في ساعات الليل المتأخرة بدافع التسلية، والذين أصبحوا الآن مجرد ذكرى (من كان يظن أننا سنشعر بالحنين إليهم في يوم من الأيام!).

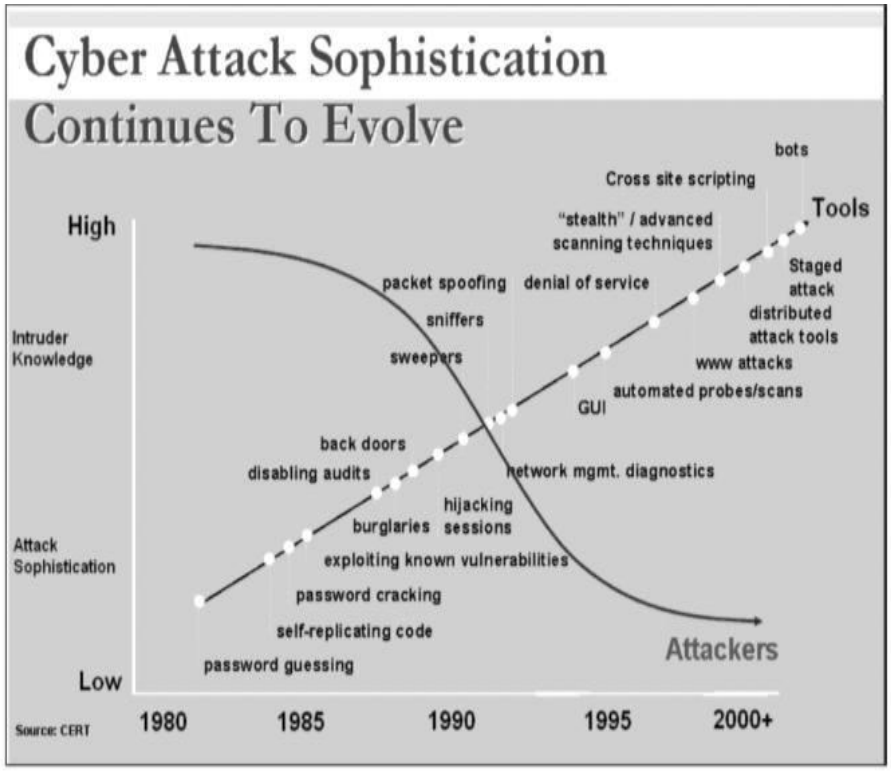
من المحتمل أن القراصنة الذين كانوا في الماضي يعملون الآن كمحترفي أمن معلومات، يحاولون إغلاق صندوق باندورا الذي ساهموا في فتحه منذ وقت ليس ببعيد. المعرفة التي قدمها القراصنة اليوم، الذين يُعرفون أيضًا باحثي الأمن، قد تم تشكيلها وفقًا للأخلاقيات والانضباط؛ حيث أصبحوا حذرين في نشر اكتشافاتهم، ليس بسبب ‘‘أنشطة مثيرة للجدل’’، ولكن بسبب المسؤوليات المطلوبة لحماية هذه الأداة ذات الحدين.

خلال العقد الأخير، شهدت الجريمة الإلكترونية تحولاً كبيراً في أساليبها ومنهجياتها. في الماضي، كان معظم القراصنة يستهدفون أنظمة خوادم مثل Windows NT وUNIX، غالبًا في سياقات بحثية أو تعليمية. ومع تطور الإنترنت وزيادة سرعة الاتصال، تغيرت أهداف الهجمات لتشمل جميع الأجهزة المعرضة للاختراق. ففي الوقت الذي كان فيه المهاجمون يستهدفون أجهزة الكمبيوتر المكتبية

عبر شبكات kbps14.4 مودم، فإن اليوم يتجهون إلى اختراق أجهزة الكمبيوتر الشخصية العادية التي تعمل بنظام Windows والتي باتت عرضة للعديد من البرمجيات الخبيثة.

يعد أطفال السكربتات (أو ما يُعرف بـ"script kiddies") من الفاعلين الرئيسيين في هذا المجال اليوم. هؤلاء هم أفراد في الغالب شباب، يفتقرون للإبداع والمهارات العميقة في القرصنة، لكنهم يمتلكون الوقت الكافي، الصبر، وقدرة كبيرة على استخدام الأكواد البرمجية الجاهزة التي يطورها الباحثون الأمنيون الأكثر مهارة. كما أن البنية التحتية التي يتيحها الإنترنت عالي السرعة تجعل هذه الأنشطة أكثر انتشارًا. في الواقع، أصبح معظم هؤلاء القراصنة يستخدمون هذه الأنظمة المخترقة لأغراض مختلفة، مثل تخزين وتبادل الملفات، أو لدعم أنشطة مثل التصيّد الإلكتروني والبريد المزعج (spam).

تشير البيانات من مراكز الأبحاث الأمنية مثل Internet Storm Center إلى أن الأجهزة التي لا يتم تحديثها أو ترقيتها بشكل مستمر قد تُخترق في غضون دقائق من الاتصال بالإنترنت. بالإضافة إلى ذلك، يُظهر الشكل التالي (2) كيف أصبح التصيّد جزءاً من النظام الاقتصادي العالمي للجريمة الإلكترونية، مع تزايد استخدام هذه الأساليب لتحقيق مكاسب مالية غير مشروعة عبر الإنترنت.



الشكل2: تطور تعقيد الهجمات الإلكترونية بشكل مستمر

2.12 ما هو التصيد ؟

التصيّد، المعروف أيضًا بال''كارديغ'' أو ''التقليد العلاماتي''، له العديد من التعريفات المختلفة. ومن المهم جدًا أن نكون دقيقين في تعريف هذا المصطلح نظرًا لأنه في حالة تطور مستمر. بدلاً من تقديم تعريف ثابت، سنستعرض الطرق البدائية للتصيّد ونلاحظ كيف أن هذا المجال في تطور مستمر من خلال الكتاب، مع إمكانية استكشاف الممارسات الحالية والمستقبلية.

في الوقت الحالي، يمكن تعريف التصيّد البدائي على أنه عملية إرسال بريد إلكتروني مزيف (باستخدام أدوات البريد الجماعي) إلى المرسل إليه، حيث يتم تقليد مؤسسة مشروعة بشكل زائف في محاولة للاحتيال على الضحية بهدف الحصول على معلومات خاصة، مثل أرقام بطاقات الائتمان أو كلمات مرور الحسابات البنكية. في معظم الحالات، يُطلب من الضحية زيارة موقع ويب لملء تلك المعلومات الخاصة. ولإضفاء الثقة على الضحية، يتم تصميم الموقع ليبدو وكأنه الموقع الإلكتروني للمؤسسة التي يزعم المحتال أنه يمثلها. بالطبع، الموقع ليس الموقع الفعلي للمؤسسة المشروعة، بل إنه مصمم خصيصًا لسرقة المعلومات الشخصية للضحية بغرض الحصول على مكاسب مالية.

التصيّد (Phishing) موجود منذ أكثر من 10 سنوات، حيث بدأ في عام 1995 مع خدمة ''أمريكا أونلاين'' (AOL). كان هناك برامج مثل AOHell التي قامت بأتمتة عملية التصيّد للحصول على معلومات الحسابات وبطاقات الائتمان. في ذلك الوقت، لم يكن التصيّد يُستخدم بشكل شائع عبر البريد الإلكتروني كما هو الحال اليوم، بل كان يتم بشكل رئيسي من خلال ''الدردشة عبر الإنترنت'' (IRC) أو نظام التنبيهات الذي كان يستخدمه AOL. كان المحتالون يقلدون مسؤولي AOL ويخبرون الضحية أن هناك مشكلة في الفاتورة ويطلبون منهم تحديد معلومات بطاقاتهم الائتمانية وكلمات المرور. في ذلك الوقت، نظرًا لأن أجهزة الكمبيوتر الشخصية المنزلية واستخدام الإنترنت كانا تجربة جديدة نسبيًا، كانت هذه الطريقة فعالة للغاية، ولكن لم تكن منتشرة كما هي اليوم.

تزايدت هجمات التصيّد ضد المؤسسات المالية في يوليو 2003، حيث كانت الأهداف الرئيسية هي شركات مثل E-loan، و-E gold، وWells Fargo، وCitibank. وأكثر ما يميز ظاهرة التصيّد هو أنها قدمت فئة جديدة من أساليب الهجوم التي تم تجاهلها في ميزانيات الأمان الخاصة بغالبية المؤسسات المالية: العنصر البشري. جميع الجدران النارية المكلفة، وشهادات SSL، وقواعد IPS، وإدارة التصحيحات لم تكن قادرة على منع استغلال الثقة عبر الإنترنت، وهو ما أدى إلى تعريض المعلومات الحساسة للمستخدمين للخطر، وله تأثير كبير على ثقة المستهلكين في وسائل الاتصال بين المؤسسات وعملائها.

من منظور تقني، لم يكن خبراء مكافحة البريد المزعج وأمن البريد الإلكتروني مندهشين من تأثير هذه التهديدات، حيث تم توثيقها جيدًا في RFC 2821 (بروتوكول نقل البريد البسيط أو SMTP)، وهو تحديث لـ RFC 821 الذي كتب في عام 1982.

التصيّد ينجح بسبب تلاقي ضعفَين متكاملَين: هشاشةُ القنوات التقنية (مثل إمكانية تزوير الرسائل وعناوين الويب) وتَعرُّضُ المستخدم البشري للخداع عبر الهندسة الاجتماعية. مع توفر أدوات جاهزة ونماذج إثبات المفهوم، يمكن حتى للمهاجمين غير الماهرين إطلاق حملات واسعة بتكلفة منخفضة، ما يجعل الهجوم مجزياً اقتصاديًا. نفس أساليب التزوير والروابط الشبيهة التي استهدفت البريد الإلكتروني تنتقل اليوم إلى منصات التواصل الاجتماعي، حيث تتيح الطبيعة الفورية والمرئية لتلك المنصات وصولاً أوسع وسيناريوهات خداع جديدة تستدعي تدابير دفاعية تقنية وبشرية مدموجة.

يعتمد عدد من مهاجمي التصيّد على استغلال الإدراك البشري وثغرات التمثيل النصي لعناوين الإنترنت (URLs) لخداع المستخدمين. تُستخدم تقنيات متعددة لجعل عنوان موقعٍ مزيف يبدو مشابهاً للعنوان الحقيقي — سواء عبر استخدام نطاقات شبيهة بصريًا أو عبر طرق تمويه تُغيّر مظهر العنوان لدى المستخدم دون أن تُنبّه المتصفح أو الضحية بوضوح. البشر عادةً يقرؤون الكلمات ككل، ولا يلتفتون دائمًا إلى ترتيب الحروف أو فروق بسيطة في النطاق؛ وهذا ما يستغله المخترِقون بوضع ''طُعم'' مرئي يخفي الفروق الحاسمة. بالإضافة إلى ذلك، قد يستغل المهاجمون ميزات بروتوكولات وقدرات المتصفحات (مثل التعامل مع أجزاء من العنوان التي تتضمن رموزًا خاصة) لتوجيه الضحايا إلى مواقع ضارة رغم ظهور عناوين تبدو مألوفة عند النظرة الأولى.

هذه الأساليب تمثل تهديدًا مهمًا لأنّها تهاجم كلًا من البنية التحتية البشرية والبصرية للمستخدمين، لا فقط الجانب التقني للأنظمة. لذلك، ينبغي أن يتضمن أي إطار دفاعي مزيجًا من أدوات تقنية (فلترة الروابط، التحقق من النطاقات، فحص الروابط قبل الوصول) وتدريبًا للمستخدمين على ملاحظة مؤشرات الحماية في المتصفحات وعدم الاعتماد على المظهر الظاهري للرابط وحده.

كان التلاعب بعناوين الويب إحدى الأساليب المبكرة والفعّالة لخداع المستخدمين غير الانتباهين، ولا سيما في هجمات التصيّد الموجّهة ضد المؤسسات المالية. استجاب مطورو المتصفحات لهذه الثغرات بإضافة تحذيرات وإشعارات، إلا أن هذه الحلول الجزئية لا تقطع الطريق على التكتيكات المتقدمة ولا تغني عن ضعف وعي المستخدم. لذا، تبرّر هذه الأمثلة الحاجة إلى استراتيجية دفاعية متعددة المستويات تجمع بين تحسين واجهات المتصفحات، وفحص الروابط على مستوى الخوادم، وتدريب المستخدمين على ملاحظة علامات الخداع.

2.13 طرق نسخ المواقع

2.13.1 نسخ واجهة البصرية:

نسخ الواجهة البصرية لموقع الويب (Visual Interface Duplication) هو نهج يركز على التقاط الحالة الظاهرة للوثيقة كما تُعرض للمستخدم النهائي في لحظة زمنية معينة، حيث يُنظَر إليها كمُتمِّم لطبقة العرض ضمن نموذج ثلاثي الطبقات للموقع (الأصول الثابتة، البيانات البنيوية، وسلوك التنفيذ)، ويهدف التحليل النظري لهذه الطريقة إلى توضيح عناصر التمثيل التي تُلتقط (شجرة DOM النهائية، السمات النمطية المرئية، مقتطفات النص الظاهر، والموارد الرسومية المرتبطة) وعلاقاتها الدلالية المحدودة. ومن منظور نمذجي، تُنتج هذه العملية تمثيلاً سطحيًا يعكس الشكل والتخطيط والتنسيق المرئيين دون نقل حالة الخادم أو منطق الأعمال أو بيانات الجلسات، وبالتالي فإن تقييم جودة النسخ البصري يعتمد على مؤشرات قياسية مثل الوفاء البصري (Visual Fidelity) المقاس عبر مقاييس تشابه صورية/نصية، قابلية الاسترجاع المحلي للموارد المرتبطة، ومعدل الاحتفاظ بالروابط والوظائف الأساسية للعرض، بينما تبرز قيود منهجية جوهرية تتمثل في عدم القدرة على استعادة التفاعلات الديناميكية أو المحتوى الذي يُولَّد لاحقًا بعد تفاعل المستخدم، والحساسية لحالة الجلسة والبيانات المخصصة التي قد تمنح نتائج عرضية غير ممثلة للشكل العام للموقع؛ علاوة على ذلك، هناك تحديات مفاهيمية في ضمان أن التمثيل المرئي المحفوظ لا يعرّض بيانات حساسة أو ميتاداتا مرتبطة بالمستخدم، ومن ثم يجب أن تُدرج اعتبارات حماية الخصوصية وإجراءات التعمية عند التعامل مع أي نسخ لأغراض بحثية أو أرشيفية، وأخيرا فإنه على مستوى الدفاع السيبراني يُعد فهم آليات النسخ البصري ذا قيمة بالغة لتطوير تقنيات الكشف عن المواقع المزيفة — مثل مقارنات التواقيع البصرية والتحقق متعدد القنوات لكن ينبغي أن يظل هذا الفهم مقترنًا بإطار امتثالي وأخلاقي يحدد حدود الاستخدام المشروع ويمنع التوظيف الخبيث لهذه المعرفة.

2.13.2 نسخ URL:

نسخ عنوان الرابط الموحد (URL) هو عملية استنساخ الرابط الكامل الذي يشير إلى مورد معين على الإنترنت، حيث يشمل هذا استنساخ جميع مكونات الرابط مثل البروتوكول (مثل HTTP أو HTTPS)، اسم المضيف (النطاق)، المسار إلى المورد، وأي استعلامات مرتبطة (مثل المعاملات أو باراميترات البحث)، إضافة إلى المرجع الداخلي (الـ Fragment) إذا كان موجودًا. الهدف من نسخ الـ URL هو إنتاج نسخة طبق الأصل من الرابط الذي يستخدمه المستخدم للوصول إلى المحتوى نفسه. عند نسخ هذا الرابط، يُحتفظ في الغالب بالبنية الخارجية للرابط بشكل مشابه لما يظهر للمستخدم، لكن يُمكن أن يحتوي الرابط المستنسخ على معطيات حساسة قد تكون موجودة ضمن الاستعلامات أو المعاملات مثل معرّفات الجلسات أو رموز التتبع. وهذه المعطيات يمكن أن تحتوي على معلومات شخصية مثل اسم المستخدم أو تفاصيل الحسابات، مما يجعل من الضروري التعامل معها بحذر شديد.

عملية نسخ الـ URL يمكن أن تؤدي إلى تسريب بيانات حساسة إذا لم يتم التعامل مع الرابط بشكل سليم. على سبيل المثال، يمكن أن تحتوي الروابط على معرّفات فريدة مرتبطة بجلسات المستخدم أو تفاصيل حسابات قد تكون عرضة للاستغلال إذا تم إعادة استخدام الرابط أو توزيعه بشكل غير آمن. عند استخدام هذه الروابط في سيناريوهات مختلفة، يجب التأكد من أنه تم إخفاء أو تعميم هذه المعطيات الحساسة للحفاظ على سرية البيانات وحمايتها من التسريب أو الاستخدام غير المصرح به.في السياق الأمني، يعتبر نسخ الـ URL وسيلة رئيسية يمكن للمهاجمين استخدامها في هجمات التصيّد الاحتيالي (Phishing). يقوم المهاجمون في هذا النوع من الهجمات بنسخ روابط من مواقع إلكترونية موثوقة لاستهداف الضحايا عبر مواقع مزيفة تبدو مشابهة تمامًا للمواقع الأصلية. يتم استخدام هذه الروابط في رسائل بريد إلكتروني احتيالية أو مواقع ويب مزيفة بهدف خداع المستخدمين ليدخلوا بياناتهم الشخصية أو المالية. مثل هذه الهجمات تعتمد بشكل رئيسي على تقليد شكل الرابط الأصلي، مما يجعل من الصعب على المستخدمين التمييز بين الرابط الحقيقي والمزور. عند نسخ الـ URL، من الضروري أن يتم فحص الرابط بعناية لضمان أنه يؤدي إلى المورد الصحيح دون وجود أي تغييرات قد تُؤثر على الوصول إلى البيانات أو المحتوى. كذلك يجب التأكد من أن الرابط لا يحتوي على معطيات قد تكون معرضة للاستغلال مثل معرّفات الجلسات أو رموز التتبع، حيث أن أي تسريب لتلك البيانات قد يعرض المستخدمين لخطر السرقة أو الاحتيال. وبهذا فإن عملية نسخ الـ URL تتطلب اهتمامًا خاصًا من حيث الأمان، وتحتاج إلى تقنيات متقدمة للكشف عن الروابط المزيفة مثل فحص التوقيعات الرقمية أو التأكد من التحقق عبر بروتوكولات الأمان مثل SSL/TLS.

بذلك، فإن نسخ الـ URL يتطلب فحصًا دقيقًا لضمان سلامة الرابط وحمايته من الاستغلال في الهجمات الإلكترونية، ولا سيما التصيّد الاحتيالي. وبغض النظر عن نوع الهجوم، يظل من المهم توظيف آليات للكشف المبكر عن هذه الروابط المزيفة لضمان عدم وقوع المستخدمين ضحايا لهجمات قد تضر بخصوصياتهم أو أموالهم.

2.13.3 نسخ المحتوى الديناميكي:

نسخ المحتوى الديناميكي يشير إلى عملية استنساخ العناصر التي يتم تحميلها وتحديثها بشكل مستمر استجابة لتفاعل المستخدم أو تغييرات تحدث في البيئة المحيطة بالموقع. يتضمن هذا النوع من المحتوى البيانات التي يتم توليدها في الوقت الفعلي بواسطة الخوادم، مثل النصوص المخصصة للمستخدم، نتائج البحث التفاعلية، التعليقات الحية، أو أي معلومات يتم جلبها من قواعد البيانات عبر تقنيات مثل واجهات برمجة التطبيقات (APIs) أو AJAX. تعد هذه العملية أكثر تعقيدًا من نسخ المحتوى الثابت، حيث أن المحتوى الديناميكي لا يُعرض مباشرة عند تحميل الصفحة بل يتم تحميله استجابةً لتفاعلات المستخدم، مثل التمرير عبر الصفحة أو النقر على عناصر معينة. لذلك، يتطلب نسخ هذا المحتوى تقنيات متقدمة تشمل محاكاة العمليات التفاعلية بين المستخدم والخادم، مثل محاكاة النقرات على الأزرار أو إرسال طلبات إلى الخادم لجلب البيانات بشكل دوري.عند استنساخ المحتوى الديناميكي، يجب أن يتمكن المهاجم أو الأداة المستخدمة من التقاط استجابات الخادم التي تُعيد تحميل المحتوى ديناميكيًا بناءً على طلبات المستخدم. يتم ذلك عبر تقنيات مثل زحف واجهات برمجة التطبيقات (APIs) أو محاكاة التفاعل مع الصفحة باستخدام أدوات مثل الأتمتة البرمجية التي

تحاكي تصرفات المستخدم في البيئة الحية. هذه الأدوات تتفاعل مع المكونات الديناميكية للموقع التي لا يتم تحميلها بشكل مباشر، بل تُجلب عن طريق تفاعل المستخدم مع الموقع، مما يجعل عملية النسخ أكثر تعقيدًا. على سبيل المثال، في المواقع التي تحتوي على بيانات مخصصة للمستخدمين مثل الرسائل الشخصية أو تفاصيل الحسابات، يتطلب الأمر الحصول على رموز الجلسة أو معرّفات التتبع الخاصة بالمستخدم للوصول إلى هذا المحتوى، مما قد يؤدي إلى تسريب معلومات حساسة إذا تم التعامل معها بشكل غير آمن.

من الناحية الأمنية، يُعد نسخ المحتوى الديناميكي أداة رئيسية في تنفيذ هجمات التصيّد الاحتيالي. في هذه الهجمات، يقوم المهاجمون بنسخ المحتوى الديناميكي لموقع موثوق مثل موقع مصرفي أو موقع للتجارة الإلكترونية بهدف خلق نسخة مزيفة من الموقع لخداع المستخدمين. قد تتضمن هذه النسخ المزيفة محتوى ديناميكي مشابه جدًا للمحتوى الأصلي، مثل تفاصيل الحسابات أو البيانات الشخصية المحدثة في الوقت الفعلي، مما يجعل من الصعب على المستخدمين التمييز بين الموقع الحقيقي والموقع المزيف. هذه الأنواع من الهجمات تعتمد بشكل كبير على قدرة المهاجمين في استنساخ كل التفاصيل الدقيقة في الصفحة الديناميكية، بما في ذلك البيانات التي تُعرض للمستخدم في جلسات متعددة.

بالإضافة إلى ذلك، تتطلب عملية نسخ المحتوى الديناميكي اتخاذ تدابير احترازية لضمان عدم تسريب بيانات حساسة قد تكون موجودة في هذه العمليات. أي تقنيات تُستخدم في النسخ يجب أن تكون قادرة على التعامل مع معرّفات الجلسات بشكل آمن، ودمج أدوات حماية تضمن أن المعلومات الشخصية أو البيانات المخصصة لا يتم استغلالها أو تسريبها خلال عملية النسخ. في النهاية، يعتبر نسخ المحتوى الديناميكي خطوة معقدة تتطلب خبرة متقدمة في التعامل مع تقنيات الزحف والأتمتة، ويجب أن يتم استخدامها بحذر شديد لتجنب مخاطر الأمان التي قد تنتج عن استنساخ أو تسريب بيانات حساسة.

2.13.4 نسخ بريد الكتروني:

نسخ البريد الإلكتروني هو عملية استنساخ رسائل البريد الإلكتروني أو محتويات البريد التي يتم إرسالها أو تلقيها عبر الأنظمة الإلكترونية. يتضمن هذا النوع من النسخ استنساخ الرسائل نفسها مع كافة تفاصيلها مثل عنوان المرسل، موضوع الرسالة، نص الرسالة، المرفقات، والتوقيت الزمني لإرسال الرسالة. بالإضافة إلى ذلك، يمكن أن يتضمن نسخ البريد الإلكتروني استنساخ العناوين المرتبطة بالمرسلين والمستلمين ضمن الرسالة، وكذلك أي روابط أو محتوى ديناميكي موجود داخل الرسالة. تعتبر هذه العملية، التي غالبًا ما تتم عبر تقنيات الزحف الإلكتروني أو أدوات الأتمتة، أساسية في العديد من الهجمات الإلكترونية مثل التصيّد الاحتيالي (Phishing) أو الهندسة الاجتماعية، حيث يتم نسخ رسائل البريد الإلكتروني الموثوقة بشكل زائف لاستهداف الضحايا.

عند نسخ البريد الإلكتروني، تتطلب العملية القدرة على تكرار كل جزء من محتوى الرسالة بدقة. في حالة الهجمات الإلكترونية، يسعى المهاجمون إلى استنساخ الرسائل الأصلية التي قد تحتوي على روابط احتيالية أو مرفقات تحتوي على برمجيات خبيثة. تُستخدم تقنيات

مثل أدوات الأتمتة الخاصة بالبريد الإلكتروني أو برامج الزحف إلى الويب لنسخ محتوى البريد الإلكتروني المرسل أو المستلم من حسابات البريد الإلكتروني المستهدفة. هذه الأدوات قد تقوم أيضًا بجمع البريد الإلكتروني من الخوادم أو من الحسابات عبر بروتوكولات مثل IMAP أو POP3، ثم تقوم بإنشاء نسخ طبق الأصل من الرسائل التي يتم تخزينها أو إرسالها بعد ذلك باستخدام تقنيات تلاعب. يعتبر نسخ البريد الإلكتروني تهديدًا كبيرًا في سياق الهجمات السيبرانية. على سبيل المثال، قد يقوم المهاجم بنسخ رسائل بريد إلكتروني تحتوي على بيانات حساسة مثل كلمات المرور، التفاصيل المالية، أو المعلومات الشخصية الخاصة بالمستخدمين. قد يتم أيضًا استنساخ الرسائل التي تحتوي على روابط مزيفة لسرقة بيانات المستخدمين في عمليات التصيّد، حيث يتم إرسال بريد إلكتروني زائف يبدو أنه من جهة موثوقة، مثل بنك أو مؤسسة حكومية، بهدف إقناع المستخدمين بالكشف عن معلوماتهم السرية. هذه الهجمات تعتمد على النسخ المتقن للرسائل لجعلها تبدو طبيعية وموثوقة للمستخدمين المستهدفين. عند نسخ البريد الإلكتروني، قد تتضمن العملية أيضًا إعادة استخدام محتويات الرسائل المستنسخة في الهجمات اللاحقة. على سبيل المثال، قد يقوم المهاجم بإرسال رسالة مزيفة مشابهة جدًا للبريد الإلكتروني الأصلي، مع روابط أو مرفقات ضارة، مستفيدًا من الثقة التي يضعها المستلم في المرسل الحقيقي. لذلك، يتم استخدام تقنيات تحليل البريد الإلكتروني للكشف عن الرسائل المزيفة عبر فحص الأنماط البريدية والتوقيعات الرقمية للمرسلين.بالإضافة إلى ذلك، يتطلب نسخ البريد الإلكتروني تدابير أمان لضمان حماية البيانات الشخصية والحساسة التي قد تحتوي عليها هذه الرسائل. يجب أن يتم التعامل مع البريد الإلكتروني المستنسخ بحذر شديد لضمان عدم تسريب المعلومات الخاصة بالمستخدمين أو تعرضهم للخداع. من خلال تكامل آليات تشفير البيانات والتحقق من الهوية، يمكن الحد من مخاطر تسريب المعلومات أو استخدامها في الهجمات الإلكترونية.

2.13.5 نسخ المواقع عبر أدوات التنزيل:

نسخ المواقع عبر أدوات التنزيل يُعرَّف كمقاربة منهجية تعتمد على برمجيات آلية لاسترجاع موارد الويب عبر بروتوكول HTTP/HTTPS وإعادة تنظيمها محلياً في هيكل ملفات يعكس البنية الظاهرة للموقع؛ من المنظور العلمي، تعمل هذه المقاربة على معالجة رسمٍ بيانيٍ للموارد (عقد تمثل الصفحات وحواف تمثل الروابط) وفق سياسات اختيار محددة ثم تحويل المراجع النسبية والروابط الداخلية لتُشير إلى النسخ المحلية، وبذلك توفر تمثيلاً قابلاً للتصفح لغرض الأرشفة أو التحليل البنيوي، أما مؤشرات قياس نجاحها فتشمل نسبة التغطية للمصادر القابلة للوصول، درجة الاتساق البنيوي للحوسبة المحلية مع الرسم البياني الأصلي، والوفاء البصري/الوظيفي للصفحات بعد إعادة التركيب؛ في المقابل، تُواجه هذه المنهجية قيوداً نظرية متجذرة في طبيعة الويب الحديث، إذ قد تفشل في استنساخ المحتوى المولَّد جانب العميل أو المحتوى المرتبط بحالة الجلسة، كما تطرح اعتبارات منهجية تتعلق بضبط أثر التحميل على الخادم المصدر والامتثال لسياسات الوصول الآلي وحماية البيانات الشخصية المستخرجة، ومن ثم يتطلب تطبيقها البحثي أو المؤسسي إطار حوكمة يتضمن معايير تعمية البيانات، حدود معدل الطلبات، وآليات امتثال قانوني تضمن أن إجراء النسخ لا ينتهك خصوصية المستخدمين أو يعطل خدمات المورد.

2.13.6 نسخ المواقع باستخدام السكريبتات :

نسخ مواقع الويب باستخدام السكريبتات يُعرَّف منهجيًا على أنه نهج آلي قائم على نصوص تنفيذية تُؤتمت عمليات جلب وتمثيل وتجميع الموارد الشبكية بغرض إعادة بناء تمثيل محلي للبنية الظاهرة أو البنيوية للموقع، حيث تُمثّل هذه النصوص طبقة وسيطة تنفذ سياسات اختيار الموارد وتتعامل مع حالات الطلب والاستجابة وتحويل المراجع وإدارة الحالة المؤقتة، ويتيح هذا النهج إمكانيات عالية في التحكم بمنطق التجميع وتخصيص سياسات التصفية والجدولة والقياس، كما يقدّم مرونة في معالجة المحتوى المولَّد ديناميكيًا عبر نماذج تتضمن انتظار اكتمال التوليد أو استهلال استدعاءات بيانات داخلية، إلّا أنّه من منظور علمي يواجه قيودًا منهجية أساسية تتعلق بضمان اتساق snapshots الزمنية بين الطبقات المختلفة (الملفات والبيانات)، وبإمكانية استعادة التفاعلات المعتمدة على حالة جلسات المستخدم، فضلاً عن متطلبات الحوكمة لجهات التشغيل نتيجة أثر الحمل على مزود الخدمة ووجود معطيات حساسة ضمن الطلبات أو الاستجابات، وتُقاس كفاءة هذا الأسلوب بمعايير كمية تشمل نسبة التغطية للمصادر القابلة للوصول، سلامة البنية المرجعية الداخلية للنسخة المحلية، درجة الوفاء البصري/الوظيفي بالمظهر الأصلي، زمن الانجاز واستهلاك الموارد، ومعدل التأثير على الخدمة الأصلية، ومن ثم ينبغي توظيف هذا النهج في سياقات مشروعة مع ضوابط تعمية البيانات، وضوابط لمعدل الطلبات، وإطار امتثالي يضمن حماية الخصوصية والالتزام بحقوق الملكية ومنع الاستخدام الخبيث للمخرجات.

2.13.7 خدمات الاستنساخ عبر الإنترنت :

خدمات الاستنساخ عبر الإنترنت تُعرَّف كنموذجٍ استثماري تشغيلي يوفر واجهاتٍ مستضافة تُمكّن المستخدمين من إنشاء نسخٍ من مواقع الويب أو أجزاءٍ منها دون الحاجة إلى إدارة بنى تحتية محلية، وتعتمد هذه الخدمات من الناحية المفاهيمية على تجميعٍ متكامل لعمليات الاكتشاف، الجلب، التحويل، والتخزين في طبقاتٍ متراصة تتضمن طبقة التحكم وسياسات الاختيار، طبقة التنفيذ المسؤولة عن التعامل مع طلبات بروتوكول الويب وتحويل المراجع، وطبقة التخزين التي تحتفظ بالنسخ والميتاداتا المصاحِبة لها؛ من منظور علمي، تتيح هذه البنية مرونةً في ضبط نطاق الاستنساخ، جدولة العمليات، وإدارة معدلات الطلبات لتقليل التأثير على خوادم المصدر، كما توفر آليات للتعامل مع المحتوى الديناميكي عبر تنفيذٍ منظم لمنطق جانب العميل أو الاستفادة من واجهات برمجة التطبيقات المعلنة، فيما تقاس جودة أداء هذه الخدمات بمقاييس معيارية تشمل نسبة التغطية للمصادر القابلة للوصول، الاتساق الزمني بين طبقات الملفات والبيانات، الوفاء البصري والوظيفي للنسخ المستعادة، زمن الإنجاز، واستهلاك الموارد وتأثيره على متانة الخدمة الأصلية. إلى جانب ذلك تبرز متطلبات حوكمة صارمة حول الخصوصية وحماية البيانات وحقوق الملكية الفكرية تفرض سياسات تعمية وإخفاء المعطيات الحساسة، متطلبات تراخيص أو صلاحيات من ملاك المحتوى، وإجراءات امتثال قانونية لتنظيم الاستخدام المشروع، ولهذا فإن تقييم هذه الخدمات يستلزم مراجعة فنية وقانونية متوازنة تضمن فاعليتها كموردٍ للأرشفة أو الترحيل أو التحليل دون أن تتحول إلى وسيلةٍ لاستغلال المحتوى أو الإضرار بمقدمي الخدمة.

2.14 طرق الكشف عن نسخ المواقع:

2.14.1 كشف استنساخ المواقع بالاعتماد على URL:

كشف استنساخ المواقع باستخدام عنوان URL يعتمد على تحليل شامل لمكونات الرابط للكشف عن أي تلاعب أو تغيير قد يشير إلى أن الموقع هو نسخة مزيفة أو تهدف إلى انتحال هوية موقع حقيقي. تبدأ العملية بفحص اسم النطاق في URL للتأكد من عدم وجود تغييرات خفية قد تكون مصممة لخداع المستخدمين. المهاجمون غالبًا ما يستخدمون أساليب تحايل مثل استبدال الحروف أو إضافة رموز مشابهة بصريًا للنطاق الأصلي، بهدف جعل الموقع المزيف يبدو موثوقًا. بعد ذلك، يتم التحقق من البروتوكول المستخدم في الموقع، حيث أن المواقع الأصلية عادةً ما تستخدم بروتوكول HTTPS وتوفر شهادة SSL لضمان الأمان. بالمقابل، تفتقر المواقع المزيفة إلى هذه الشهادات، مما يعرض البيانات للخطر ويجعلها عرضة لهجمات سرقة البيانات. كما يتم فحص مسار URL و المعاملات الاستعلامية المرفقة به، حيث قد تحتوي على تعديلات تهدف إلى محاكاة الموقع الأصلي أو قد تشمل معلمات خبيثة لجمع بيانات حساسة من المستخدمين. بالإضافة إلى ذلك، يُعد فحص سلسلة إعادة التوجيه جزءًا أساسيًا من عملية الكشف، حيث يتم تتبع أي تحويلات تحدث على طول مسار URL للتأكد من عدم توجيه المستخدم إلى مواقع مشبوهة أو غير موثوقة. أخيرًا، يتم التحقق من سجلات WHOIS الخاصة بالنطاق للكشف عن تاريخ التسجيل والمعلومات المتعلقة به، حيث أن المواقع المزيفة غالبًا ما تُسجل لفترات قصيرة أو بشكل مؤقت، ما يجعل هذه السجلات أداة قوية للكشف عن المواقع المزيفة. من خلال تنفيذ هذه الفحوصات الشاملة لمكونات URL، يمكن الكشف المبكر عن المواقع المزيفة ومنع هجمات التصيد الاحتيالي والتهديدات الإلكترونية.

2.14.2 كشف الاستنساخ البصري للمواقع:

كشف الاستنساخ البصري للمواقع يرتكز على تحليل تمثيل الواجهة الظاهرية لصفحات الويب بغية تمييز النسخ المزيفة عن الأصلية عبر قياس درجات التشابه البصرية والهيكلية؛ من الناحية العلمية يتضمن ذلك استخلاص سمات متعددة المستويات تمثّل الخصائص البصرية (تخطيط الصفحة، توزيع النصوص والعناصر الرسومية، استخدام الألوان، أحجام وخطوط النص، ومظاهر الأزرار والقوائم) والخصائص الهيكلية للعرض (ترتيب العقد في شجرة العرض والـ DOM، تسلسل التحميل للموارد، ووجود عناصر تفاعلية مرئية)، ثم مقارنة هذه السمات بين الصفحة المراد فحصها ونموذج مرجعي معتمد باستخدام مؤشرات كمية تُقيِّم التشابه الصوري ونمط توزيع العناصر؛ تُستخدم في هذا الإطار مفاهيم مثل البصمة البصرية للصفحة (visual fingerprinting)، ومقاييس تشابه الصور والنماذج الهيكلية، وتحليل فروق الألوان والتباين، إلى جانب تحليل مصادر الموارد الرسومية (مثل مصدر الصور وأوراق الأنماط) للتحقق من توافقها مع النسخة الأصلية، كما تُؤخذ في الاعتبار عناصر ديناميكية ذات أثر بصري كالمحتوى المحمّل لاحقًا ووجود وسائط تفاعلية،

بحيث تُكَوَّن نتيجة تجمع دلائل مرجحة لتمثيل الثقة البصرية؛ يقاس أداء آليات الكشف البصري من خلال مؤشرات متعددة منها الوفاء البصري (مقدار التشابه المرئي)، سلامة البنية (حفظ ترتيب وارتباط العناصر)، ومعدل الإنذارات الخاطئة/الحقيقية، ويستدعي التطبيق العملي إطار امتثالي وأخلاقي صارم يشمل حماية البيانات الشخصية داخل النسخ المرجعية وتعميتها قبل المقارنة، كما يجب أن يُوظّف الكشف البصري كطبقة تكاملية ضمن نظام كشف متعدد القنوات لا يعتمد حصراً على المؤشرات المرئية وإنما يجمعها مع فحوصات هوية النطاق والشهادات والسلوك الشبكي لضمان كشف فعال ومستدام للاستنساخ الضار دون المساس بخصوصية المستخدمين.

2.14.3 كشف استنساخ المواقع عبر المؤشرات السلوكية والشبكية:

كشف استنساخ مواقع الويب بالاعتماد على مؤشرات سلوكية وشبكية يركز على تحليل أنماط التفاعل والشبكة المصاحبة للوصول إلى الموقع لاكتشاف الانتحال بدلاً من الاعتماد الحصري على الخصائص البصرية أو هوية العنوان. ومن المنظور العلمي، يقوم هذا النهج بنمذجة سلوك الجلسات والزوار وسلوك حركة المرور الصادرة والواردة كدلائل تفاضلية بين الموقع الأصلي والموقع المستنسخ. يتضمن ذلك دراسة توقيتات الاستجابة، تتابع الطلبات إلى واجهات الخدمة، نمط توزيع الطلبات عبر نقاط النهاية، تكرار ونمط إعادة التوجيهات، ومقاييس التشتت في مصادر الموارد عبر النطاقات المختلفة. كما يتم تحليل سلوكيات التفاعل الظاهرة مثل تسلسل الأحداث التي يرسلها العميل إلى الخادم، طلبات تحميل موارد محددة، استدعاءات بيانات لاحقة، ومعدلات إعادة المحاولة لاستخلاص توقيع سلوكي يمكن مقارنته بنموذج مرجعي. ويُقاس نجاح آليات الكشف السلوكي والشبكي عبر مؤشرات مثل معدل الاكتشاف الحقيقي، معدل الإنذارات الخاطئة، زمن الكشف من لحظة الانتحال، وحجم البيانات المطلوبة للتثبت.

من الناحية التطبيقية، يوفر هذا النهج ميزة مقاومة الخداع البصري لأن الاستنساخ قد يحاكي الواجهة دون إعادة إنتاج سلوك الخادم أو بنية الدعائم الخلفية. بيد أن فاعليته تتطلب بنية قياس ومراقبة شبكية والالتزام بسياسات خصوصية صارمة، لأن جمع وتحليل سجلات الشبكة والجلسات قد يكشف عن بيانات حساسة. لذا يجب أن يندرج ضمن إطار حوكمة قانوني وأخلاقي يتضمن تعمية البيانات، حدود الاحتفاظ، وضوابط الوصول، وأن يُدمج الكشف السلوكي مع فحوصات هوية النطاق والشهادة والتحقق البصري لتكوين نظام كشف متعدد الطبقات ذا قدرة أعلى على التمييز بين المواقع الأصلية والمزيفة.

2.14.4 كشف استنساخ مواقع الويب باستخدام الذكاء الاصطناعي:

يكشف نظام الكشف عن مواقع الويب المستنسخة القائم على تقنيات الذكاء الاصطناعي عبر بناء أنموذج تحليلي متعدد الأبعاد يستخلص الميزات الهيكلية والبصرية والنصية والسلوكية والشبكية من كل صفحة ثم يُعالجها ضمن خط أنابيب تعلم آلي منظم؛ تبدأ

العملية باستخلاص الميزات الدلالية المشتقة من عنوان المورد وسمات النطاق وسجلات نظام الأسماء، والميزات البصرية الممثلة في تخطيط الصفحة وتوزيع العناصر والألوان وبصمات الموارد الرسومية، والميزات النصية المتمثلة في الأنماط اللغوية والميتا داتا، إضافة إلى الميزات السلوكية والشبكية المتمثلة في توقيتات الاستجابة، تسلسل الاستدعاءات إلى نقاط النهاية، وسلاسل إعادة التوجيه، ثم تُجرى عملية تطبيع وتجميع لهذه الميزات لتكوين تمثيل عددي موحد يصلح للتعلّم. تُستخدم أساليب خاضعة للإشراف لتدريب مصنفات مثل الغابات العشوائية والمحولات العصبية العميقة لمعالجة السمات المختلطة، كما تُوظف شبكات تلافيفية لمعالجة الملامح البصرية وشبكات تحويلية لمعالجة النصوص، ويمكن استخدام شبكات سيامية أو نماذج كشف الشذوذ لتقييم مدى تشابه الصفحة مع مرجع موثوق بدلاً من التصنيف الثنائي الصرف. يقاس أداء الأنظمة بمعايير معيارية تشمل الدقة، الاستدعاء، معدل الإنذارات الكاذبة، والمنحنى تحت منحنى الاستقبال، كما تُقاس زمنية الكشف واستهلاك الموارد لتقييم جدوى النشر في بيئات الزمن الحقيقي. من متطلبات التصميم دمج طبقات متعددة للقرار بحيث توفر طبقة أولية سريعة قائمة على قواعد أو مؤشرات خفيفة لفرز العينات ثم طبقة تحليل عميق للعناصر المشتبه بها، وإدراج آليات تفسيرية لتبرير إنذارات النظام لأغراض الاستجابة التشغيلية والامتثال القانوني. تفرض خصوصية البيانات وحوكمة النماذج قيوداً على جمع سجلات الشبكة والمحتوى الذي يحتوي بيانات شخصية، مما يستلزم سياسات تعمية، حدود حفظ، وإجراءات تحكم في الوصول، بينما تبرز أيضاً حاجة إلى مقاومة الهجمات العدائية ضد النماذج عبر تدريب تحسيني، توليد أمثلة اصطناعية لاختبار التحمل، وتحديث دوري لمجموعات التدريب لمواجهة انجراف التوزيع والتقنيات الجديدة للتزييف، وبذلك يصبح الذكاء الاصطناعي مكوّناً فعالاً ضمن نظام كشف متعدد القنوات يوازن بين الدقة والسرعة والامتثال الأخلاقي والقانوني.

2.14.5 كشف استنساخ المواقع من خلال مؤشرات المتصفح:

يكشف النهج المعتمد على المتصفح عن مواقع الاستنساخ من خلال مراقبة مؤشرات الأمان والسلوك الظاهرية والمهيكلة التي يوفرها المتصفح نفسه كقناة تحقق أولية ومباشرة للمستخدم، حيث يشتمل التحليل على تدقيق شريط العنوان لتحديد تطابق اسم النطاق ووجود تمييز مرئي للنطاق الفعلي، وفحص مؤشر الاتصال المشفّر ومعلومات الشهادة الرقمية للتحقق من صاحب الشهادة وسلسلة الثقة ووجود سياسات الحماية مثل HSTS والشهادات الظاهرة في سجلات الشهادات الشفافة، بالإضافة إلى مراقبة تحذيرات المتصفح الظاهرة مثل تحذيرات المحتوى المختلط أو صفحات التحميل غير الآمن أو تحذيرات البرمجيات الخبيثة. على مستوى الموارد والتفاعل يتم فحص سلوك التحميل عبر أدوات المطوّر لمعرفة مصادر الموارد ونطاقاتها ومطابقتها للمصدر المعلن، والتحقق من سياسات أمان المحتوى التي يفرضها المورد مثل Content Security Policy لمعرفة حدوث انتهاكات أو إعادة توجيهات وسيطة، كما تُراجع سمات النماذج وحقول الإدخال مثل خاصية action والعلامات المتعلقة بالإكمال التلقائي والوجود الآمن لخاصيات الحماية في الكوكيز مثل Secure وHttpOnly وSameSite لمعرفة عدم اتساقها مع المعايير المتوقعة للموقع الحقيقي. كما يجري تحليل سجلات وحدة التحكم للعثور على أخطاء تحميل موارد أو قيود سياسات تشير إلى تحميل عناصر من نطاقات مشبوهة، ومتابعة تسجيلات خدمة العمل أو سجل التخزين المحلي التي قد تدل على محاكاة بيئة العميل أو استعمال وسطاء خارجيين، ويُقاس

اكتشاف الاستنساخ على مستوى المتصفح عبر مؤشرات مثل وجود عدم تطابق بين النطاق المعروض ومصدر الموارد، ظهور تحذيرات الأمان، وحالات انتهاك سياسات المحتوى أو تعارضات شهادات TLS، وينبغي دمج هذه الفحوصات كطبقة تكاملية مع فحوصات مستوى النطاق والمقارنة البصرية والسلوكية لتقليل الإنذارات الخاطئة، مع مراعاة قواعد خصوصية صارمة عند جمع أي بيانات جلسة أو سجلات متصفح لضمان الامتثال القانوني والأخلاقي.

2.14.6 تحليل متغيرات HTTP headers:

يُعد تحليل HTTP headers من الأدوات الفعّالة في الكشف عن استنساخ المواقع، حيث يوفر بروتوكول HTTP مجموعة من الحقول التي تحمل معلومات حيوية بين العميل (المتصفح) والخادم (السيرفر). من خلال فحص هذه الحقول، يمكن اكتشاف التلاعبات أو التغييرات التي قد تشير إلى محاولات انتحال هوية أو استنساخ للموقع. يبدأ التحليل بفحص متغير Host للتأكد من تطابق النطاق الذي يظهر في المتصفح مع النطاق الفعلي للموقع. أي اختلاف بين النطاقين قد يشير إلى محاولة لتحويل المستخدم إلى موقع مزيف باستخدام اسم نطاق مختلف. إلى جانب ذلك، يُعتبر متغير User-Agent من العناصر الأساسية، حيث يعرض معلومات عن نوع المتصفح ونظام التشغيل المستخدم. إذا تم التلاعب بهذا المتغير في المواقع المستنسخة، فقد يُستخدم لتقليد سلوك متصفح موثوق وإخفاء هوية المتصفح الفعلي للمهاجم، مما يساعد في تضليل المستخدم. كما يُستخدم Referer للكشف عن وجود روابط مشبوهة أو إعادة توجيه غير مصرح بها، وهي تقنية قد يستخدمها المهاجمون لنقل المستخدمين من مواقع شرعية إلى مواقع مستنسخة عبر روابط وهمية. يساعد فحص X-Frame-Options في اكتشاف محاولات استنساخ المواقع من خلال محاكاة واجهات المستخدم عبر clickjacking، حيث قد لا تكون هذه الإعدادات مضبوطة بشكل صحيح في المواقع المستنسخة. يُضاف إلى ذلك أهمية فحص Cache-Control، الذي يحدد كيفية تخزين المحتوى في الذاكرة المؤقتة. مواقع الاستنساخ قد تستخدم سياسات تخزين غير مناسبة لتخزين محتوى مزيف أو بيانات حساسة. كما يساعد تحليل Content-Type في الكشف عن التلاعب في نوع البيانات المرسلة من الخادم إلى العميل، مما يشير إلى احتمالية وجود استنساخ أو تلاعب في المحتوى.

يعد تحليل Set-Cookie من العناصر الهامة الأخرى، حيث يساعد في اكتشاف التغييرات غير المصرح بها في إدارة الجلسات بين العميل والسيرفر. إذا كانت ملفات cookies تحمل بيانات غير متوافقة، فإن ذلك يشير إلى وجود تباين في سياسة إدارة الجلسات بين الموقع الأصلي والموقع المستنسخ. أخيرًا، يساهم فحص سياسات Content-Security-Policy (CSP) و Strict-Transport-Security (HSTS) في اكتشاف المواقع المستنسخة التي قد تفتقر إلى معايير الأمان الصحيحة، مثل الحماية ضد تحميل المحتوى من مصادر غير موثوقة أو استخدام الاتصال المشفر بشكل غير صارم. من خلال تحليل هذه الحقول والبحث عن التباينات في القيم بين الموقع الأصلي والمستنسخ، يمكن الكشف عن محاولات الاستنساخ وتعزيز أمان الشبكة وحماية المستخدمين من مواقع التصيد الإلكتروني.

2.14.7 مقارنة استعلامات محركات البحث:

توظِّف مقارنة استعلامات محركات البحث منهجًا تحليليًا لاكتشاف استنساخ المواقع عبر استغلال قدرة محركات البحث على فهرسة ونمذجة التكرار والتشابه في المحتوى الرقمي؛ يقوم الأسلوب على تشكيل مجموعات استعلامية معيارية تمثّل عبارات مفتاحية وعناوين وقطع نصية مميزة للموقع المرجعي، ثم إجراء استعلامات منظمة للحصول على قوائم النتائج ومقارنة الروابط والعناوين والمقتطفات المعروضة مع الموارد الأصلية من حيث التطابق النصي، التكرار البنيوي، وتواتر الظهور عبر نطاقات متعددة، كما تستفيد المقارنة من دلائل زمنية وإشارات السمعة (مثل ترتيب الظهور ونسب النقر) لاستخلاص أنماط غير طبيعية تشير إلى نسخ أو إعادة نشر غير مصرح به للمحتوى . تُعالَج نتائج الاستعلامات إحصائيًا أو عبر نماذج قياس التشابه لتحديد مؤشرات قوية لاستنساخ المحتوى، وتُستخدم تحليلات التفريق بين المصادر (source attribution) لتقدير الأصلية والتكرار، ويُقاس أداء هذه المقاربة بمؤشرات مثل الحساسية والنوعية ومعدل الإنذارات الكاذبة ووقت الكشف، مع مراعاة قيود التغطية الزمنية لفرز النتائج وتباين سياسات الفهرسة لمحركات البحث؛ وبالنظر إلى أن مراقبة الاستعلامات تجمع بيانات عن المحتوى المتاح علناً فقط، فمن الضروري تطبيق سياسات أخلاقية وقانونية تحكم نطاق البحث وطرق الاحتفاظ بالبيانات، ودمج هذه المقاربة كطبقة مساعدة ضمن نظام كشف متعدد القنوات يشتمل على فحوصات الهوية البنائية والبصرية والسلوكية لرفع دقة الكشف وتقليل الإنذارات الكاذبة.

الفصل الثاني

3.1بيئة العمل

3.1.1المتصفحات المتاحة لاختبار الإضافة

تتطلب عملية تطوير الإضافات البرمجية لمتصفحات الويب فهماً عميقاً للمتصفحات المختلفة وأدوات التطوير المتاحة فيها. يختلف كل متصفح عن الآخر في دعمه للتقنيات والواجهات البرمجية الخاصة بالإضافات، وبالتالي فإن اختيار المتصفح المناسب لاختبار الإضافة يعد أمراً حيوياً لضمان فاعلية الاختبارات ودقتها.

من بين المتصفحات التي كانت في قائمة الخيارات لاختبار الإضافة، كان Google Chrome هو المتصفح الأكثر شهرة واستخداماً في العالم، ويعد الخيار الأول لمعظم المطورين. يمتاز Chrome بتقديمه دعمًا كبيرًا للإضافات من خلال واجهات برمجة التطبيقات (APIs)، مما يسهل عملية تطوير الإضافات واختبارها. ومع ذلك، شهد Chrome في الآونة الأخيرة تغييرات جوهرية مع إصدار Manifest v3، الذي فرض قيودًا جديدة على الإضافات تتعلق بصلاحيات الوصول إلى بيانات الكوكيز والمعلومات الحساسة الأخرى. هذه القيود قد تؤدي إلى صعوبة في تنفيذ بعض المهام الأمنية التي يتطلبها المشروع، مما يجعله غير الخيار المثالي في بعض الحالات. أما Mozilla Firefox، فقد كان أيضًا من المتصفحات المدعومة بقوة من قبل المطورين نظراً لكونه مفتوح المصدر ويقدم دعماً جيدًا للإضافات. لكن على الرغم من مرونته، يعاني Firefox من بعض القيود فيما يتعلق بالوصول إلى بيانات الكوكيز والمحتوى الخاص بالموقع عند العمل على بعض الإضافات. كما أن دعمه للإصدار Manifest v3 قد يختلف عن Chrome، مما يتسبب في مشكلات توافق بين المتصفحات المختلفة. بالنسبة لـ Microsoft Edge، فقد تم اعتماده في الآونة الأخيرة كخيار قوي في تطوير الإضافات، خصوصاً بعد انتقاله إلى محرك Chromium، مما جعله مشابهًا في العديد من الجوانب لـ Chrome. يدعم Edge الإضافات بشكل جيد ويوفر بيئة مستقرة لتطوير الإضافات، ولكنه قد يواجه بعض المشاكل في التوافق بينه وبين Chrome، خاصة عندما يتطلب الأمر استخدام أدوات أو صلاحيات متقدمة. أما بالنسبة لـ Safari، الذي يعد المتصفح الرسمي على نظام macOS، فيوفر أيضًا دعمًا للإضافات، لكنه يظل يفتقر إلى الدعم الكامل للإصدار Manifest v3 مقارنة بـ Chrome و Firefox. بالإضافة إلى ذلك، يتطلب Safari معايير محددة لتطوير الإضافات، مما يجعل من الصعب استخدامه بشكل فعال في العديد من الحالات، خصوصاً عندما يتعلق الأمر بالإضافات التي تحتاج إلى صلاحيات خاصة أو الوصول إلى بعض الموارد الحساسة.

بالنظر إلى هذه المتصفحات المختلفة، كان من الواضح أن كل متصفح يقدم مزايا وقيوداً معينة تتعلق بتطوير واختبار الإضافات، مما يفرض الحاجة إلى اختيار المتصفح الأنسب بناءً على الأهداف المحددة للمشروع.

3.1.2اختيار المتصفح Brave

في إطار تطوير مشروعنا المتعلق بكشف التصيد في مواقع التواصل الاجتماعي، كان من الضروري اختيار بيئة عمل تتسم بالكفاءة والدقة في معالجة المهام الأمنية. ومن بين المتصفحات المتاحة، تم اختيار متصفح Brave ليكون البيئة الرئيسية لاختبار الإضافة، بناءً على مجموعة من العوامل التقنية التي تجعله الخيار الأنسب.

يتميز Brave بعدة خصائص تقنية تجعله من الأدوات المثالية لاختبار الإضافات المتعلقة بالأمان، مما يجعله الخيار الأول للمشروع. يعتمد Brave على محرك Chromium، وهو ما يعني دعمه الكامل للإصدار Manifest v3. وهذا الدعم الكامل للإصدار الأخير من Manifest يعد من العوامل الحاسمة، حيث يتطلب تطوير الإضافات الحديثة استخدام تقنيات متقدمة مثل JavaScript و HTML5، ولا بد من ضمان التوافق مع أحدث معايير واجهات البرمجة. ومن خلال استخدام Brave، يمكن تجنب المشاكل المتعلقة بالتوافق مع المعايير القديمة التي قد تظهر في المتصفحات الأخرى. إضافةً إلى ذلك، يتميز Brave بتركيزه الكبير على الأمان وحماية الخصوصية، وهي ميزة أساسية في مجال العمل الأمني. يقوم Brave بحظر الإعلانات والكوكيز غير المرغوب فيها بشكل افتراضي، مما يخلق بيئة مثالية لاختبار المكونات البرمجية التي تهتم بالكشف عن التصيد، وتعزيز الأمان العام. هذا التركيز القوي على الأمان كان عاملاً مهمًا في اختيار Brave كبيئة اختبار للمكون. ومن أبرز مزايا Brave أيضًا، هي إمكانية تحميل الإضافات محليًا، حيث يدعم المتصفح تحميل الإضافات غير المعبأة (unpacked extensions). هذه الميزة توفر للمطورين فرصة لاختبار الإضافات بشكل سريع وفعال في بيئة عمل حية دون الحاجة لنشر الإضافة على منصات مثل متجر Chrome. يتيح ذلك سرعة التعديل والاختبار الفوري لأي تغييرات تجريها، مما يحسن سير العمل ويسهم في تسريع عملية التطوير.

علاوة على ذلك، نظراً لأن Brave يعتمد على محرك Chromium، فإنه يتوافق تمامًا مع واجهات برمجة التطبيقات (APIs) الخاصة بـ Chrome. هذا التوافق يوفر دعمًا كاملًا لأدوات Chrome Developer Tools، مما يسهل تصحيح الأخطاء واكتشاف المشكلات في الكود بشكل أسرع وأكثر كفاءة. يساعد ذلك المطورين في إجراء اختبارات دقيقة وتحليل الأداء بشكل أفضل، مما يساهم في تحسين جودة الإضافة.

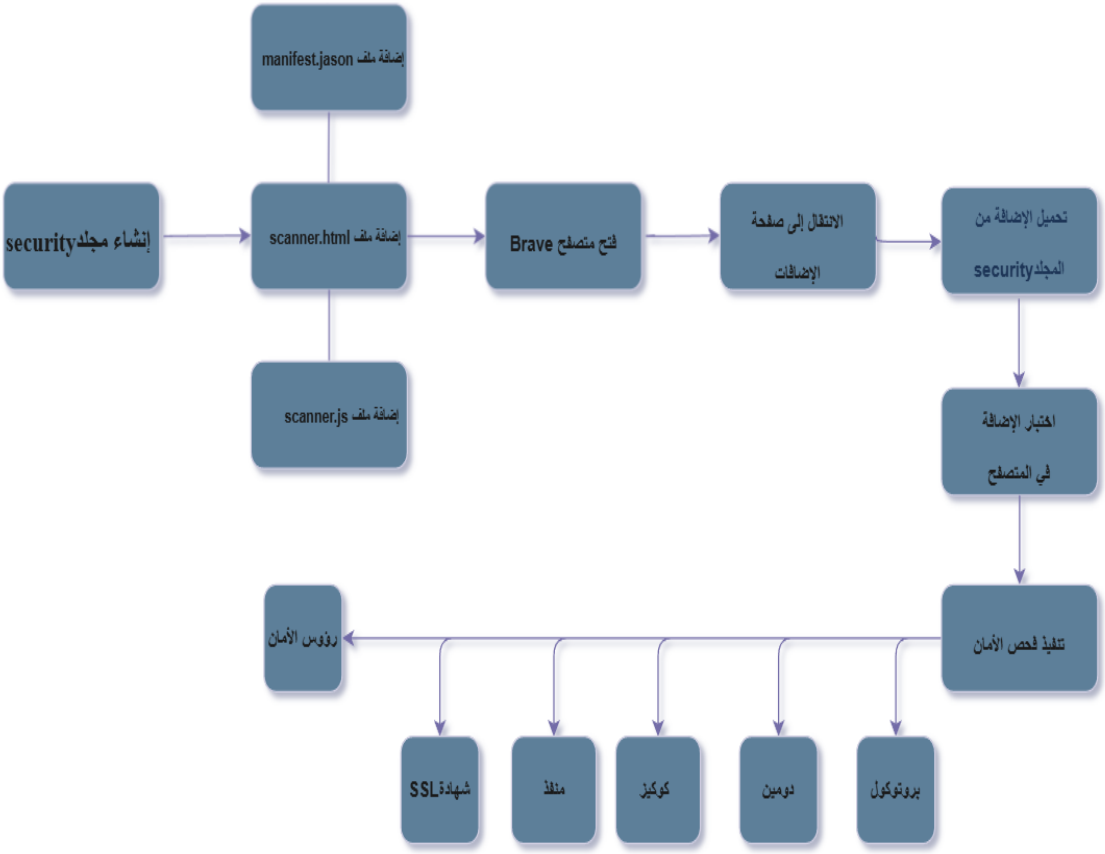
جدول2: مقارنة بين المتصفحات لاختبار الإضافة

المتصفح	الدعم الكامل لـ Maneifest v3	الأمان والخصوصية	دعم تحميل الإضافات محليا	التوافق مع Chrome APIs	التحديات
Google Chrome	نعم	متوسط (حماية محدودة)	نعم	كامل	قيود على بعض الصلاحيات بعد إصدار Maneifest v3
Mozilla Firfox	نعم	عالي (مرونة في التحكم بالخصوصية)	نعم	محدود	قيود في الوصول إلى الكوكيز والمحتوى الخاص بالموقع
Microsoft Edge	نعم	متوسط (يركز على حماية الخصوصية)	نعم	كامل	مشاكل توافق مع بعض الأدوات المتقدمة بين Chrome و Edge
Safari	لا (دعم محدود)	متوسط (يركز على حماية الخصوصية)	نعم	محدود	يحتاج معايير خاصة لتطوير الإضافات على نظام macOS
Brave	نعم	عالي (حظر الإعلانات والكوكيز الغير امنة)	نعم	كامل	قيود الوصول إلى الكوكيز والمحتوى (تم تجاوزها)

الفصل الثالث

4.1 المقدمة

في هذا الفصل، سيتم عرض مخطط سير العمل الذي يوضح الخطوات الرئيسية التي تم اتباعها أثناء تطوير الإضافة الخاصة بفحص الأمان في متصفح Brave. يهدف المخطط إلى توضيح الإجراءات المتبعة من بداية إنشاء الإضافة وحتى اختبارها في بيئة العمل، مرورًا بتطوير الكود وتنفيذ الفحوصات المختلفة للتحقق من الأمان. كما يتضمن المخطط جميع المراحل المتتابعة بدءًا من تجهيز الملفات الأساسية للإضافة وصولاً إلى اختبار النتائج وتحليلها، مما يسهم في فهم سير العملية بشكل منظم ودقيق كما هوا موضح في الشكل(3).



الشكل 3: مخطط العمل لتطوير واختبار إضافة فحص الأمان

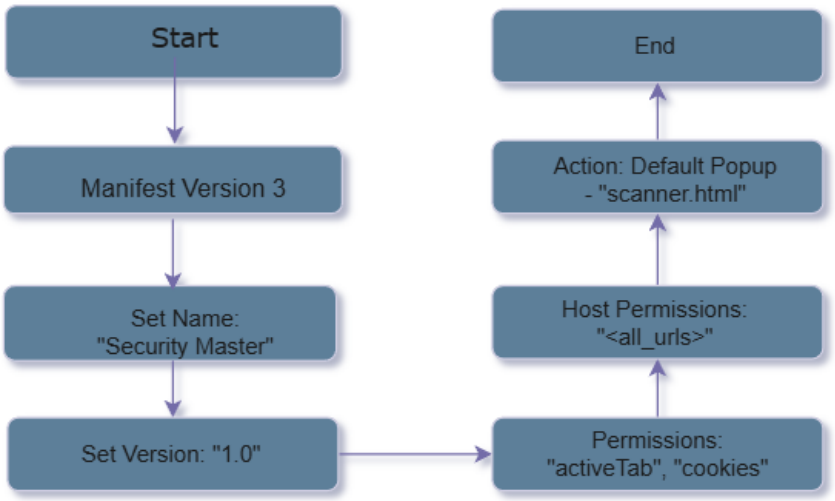
4.2الشرح التفصيلي للمكونات

في سياق تطوير الأنظمة البرمجية التي تهدف إلى تحسين الأمان السيبراني، تُعد الإضافات البرمجية لمتصفحات الإنترنت أدوات أساسية لتحليل وتقييم التهديدات الأمنية المحتملة في المواقع الإلكترونية. في هذا الفصل، نقدم شرحًا تفصيليًا للمكونات الأساسية التي تشكل الإضافة الخاصة بفحص الأمان، والتي تم تصميمها لتحليل العديد من الجوانب الأمنية للموقع، بما في ذلك فحص البروتوكولات، الدومينات، الكوكيز، المنافذ، الشهادات الأمنية، ورؤوس الأمان. إن الهدف من هذه الإضافة هو تقديم أداة قوية للمستخدمين تساعدهم على تقييم مستوى الأمان لمواقع الإنترنت التي يتصفحونها، باستخدام تقنيات حديثة مثل Manifest v3 و JavaScript و Chrome Extension APIs. من خلال هذا الشرح التفصيلي، سيتم تسليط الضوء على كيفية تكامل كل مكون من مكونات الإضافة لتحقيق هذه الأهداف، بالإضافة إلى تبرير سبب اختيار كل مكون وفقًا لمتطلبات الأمان المحددة. يُعتبر هذا الفصل بمثابة دراسة دقيقة للمكونات البرمجية التي تسهم في بناء الإضافة، موضحًا كيفية عمل كل مكون على حدة، علاوة على العلاقة التفاعلية بين هذه المكونات لتحقيق فحص أمني دقيق وموثوق. سيتم مناقشة أهمية كل مكون وظيفيًا، بالإضافة إلى تبرير اختيار الأدوات واللغات البرمجية التي تم استخدامها، مع التركيز على تعزيز الأمان وخصوصية المستخدمين أثناء تصفحهم لمواقع الإنترنت.

أولًا يُعتبر ملف manifest.json العنصر الأساسي في بناء الإضافة البرمجية، حيث يُحدد الخصائص الرئيسية للإضافة، مثل الإصدار، الأذونات التي تحتاجها الإضافة، ونقطة البداية للإضافة، وغيرها من المعلومات التعريفية المهمة. في الواقع، لا يمكن لأي إضافة متصفح أن تعمل بشكل صحيح بدون هذا الملف، الذي يشكل الأساس الذي يُمكّن المتصفح من تحميل الإضافة وتفعيلها بشكل سليم. يعتمد هذا الملف على مواصفات Manifest V3، الذي يُعتبر أحدث إصدار من مواصفات بناء الإضافات على متصفحات Chromium، مثل Google Chrome و Brave.

من خلال هذا الملف، يتم تحديد الأذونات التي يحتاجها المطور للوصول إلى بعض البيانات الحساسة للموقع مثل الكوكيز والمحتوى النشط في الصفحات. كما يتم تحديد نقطة البداية للإضافة (مثل واجهة المستخدم المنبثقة scanner.html)، بالإضافة إلى تحديد الإعدادات الخاصة بتحميل الإضافات غير المعبأة (unpacked extensions) كما هوا موضح في الشكل(4).

تم اختيار manifest.json كأداة أساسية لأن هذا الملف هو المكون الوحيد الذي يُمكّن المتصفح من التعرف على الإضافة وتحميلها، وتحديد الوظائف التي يجب أن تؤديها بناءً على الأذونات المصرح بها. علاوة على ذلك، يضمن استخدام Manifest V3 توافق الإضافة مع أحدث المعايير الأمنية على المتصفحات المدعومة، مما يسهم بشكل كبير في تعزيز حماية خصوصية المستخدم.

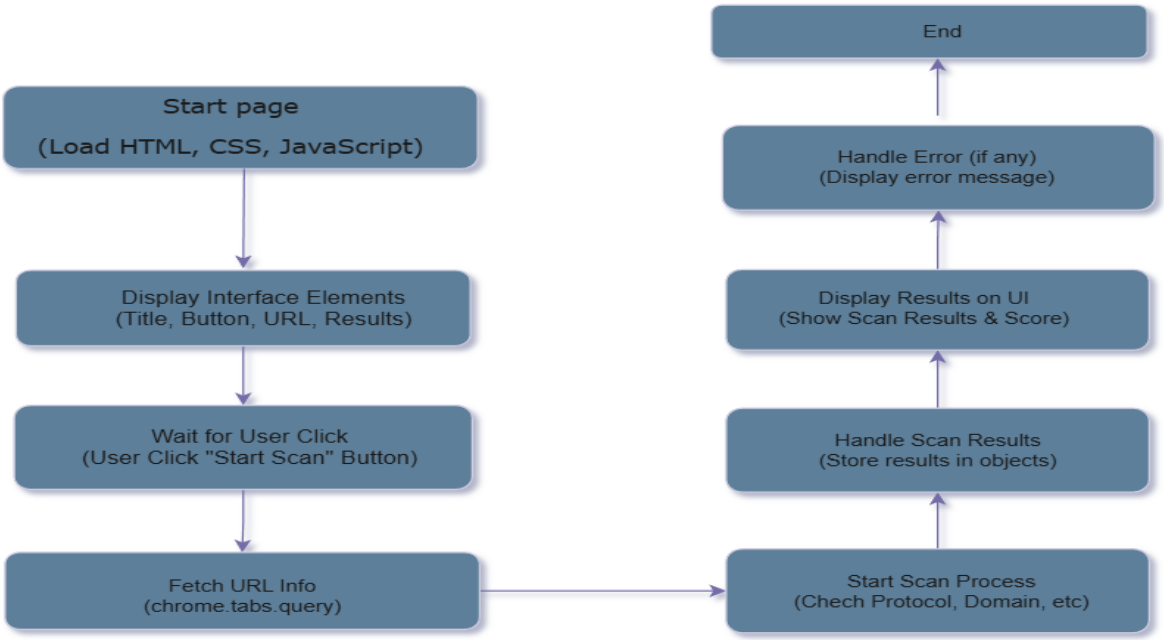


الشكل 4: مخطط هيكل ملف manifest.json

ثانيًا ملف scanner.html يُعتبر واجهة المستخدم التفاعلية التي يتفاعل من خلالها المستخدم مع الإضافة. يتمثل دور هذا الملف في تقديم تجربة مستخدم واضحة وفعّالة، حيث يتيح للمستخدم بدء فحص الأمان لموقع الويب الذي يتصفحه، وعرض نتائج الفحص بشكل مرن. يحتوي الملف على هيكل HTML يضم الأزرار اللازمة لبدء الفحص، إضافة إلى الحقول التي تعرض URL الموقع الذي يتم فحصه، فضلاً عن النتيجة التي تُعرض للمستخدم بعد انتهاء الفحص.

يتفاعل scanner.html مع JavaScript في scanner.js لضمان تنفيذ الإجراءات المطلوبة عند الضغط على الأزرار، كما يُستخدم CSS لتنسيق واجهة المستخدم. تتضمن واجهة المستخدم أيضًا عناصر لعرض نتائج الفحص بشكل مرئي، مما يسهل على

المستخدم فهم درجة أمان الموقع.تم اختيار هذا الملف لأنه يضمن للمستخدم تجربة استخدام مرنة وسهلة. من خلال هذا الملف، يتمكن المستخدم من التفاعل مع الإضافة في وقت حقيقي أثناء فحص الأمان، حيث تُعرض النتائج بشكل دقيق ومباشر. يعتمد هذا التصميم على التقنيات القياسية لـ HTML وCSS ، مما يسهل التنفيذ عبر متصفحات Brave و Chrome على حد سواء كم هوا موضح في الشكل(5).



الشكل 5: مخطط هيكل ملف scanner.html

ثالثًا يُعد ملف scanner.js هو المكون البرمجي الرئيسي الذي ينفذ جميع العمليات الأمنية اللازمة لفحص الموقع الإلكتروني. يتضمن هذا الملف مجموعة من الدوال البرمجية المسؤولة عن فحص جوانب متعددة من الأمان، مثل البروتوكول (HTTP/HTTPS)، الدومين، الكوكيز، المنافذ، الشهادات الأمنية (SSL/TLS)، ورؤوس الأمان. يتكامل scanner.js مع scanner.html ليعرض النتائج بطريقة مرئية للمستخدم بعد تنفيذ عمليات الفحص.

أثناء تنفيذ هذه العمليات، يقوم scanner.js بالتحقق من الأمان باستخدام مجموعة من واجهات برمجة التطبيقات الخاصة بـ Chrome مثل Cookies API و Tabs API، بحيث يتمكن من الوصول إلى البيانات المختلفة للموقع في الوقت الفعلي. على سبيل المثال، يتم فحص HTTP/HTTPS للتحقق من أن الاتصال آمن، ويتم فحص الكوكيز للتأكد من عدم وجود أي كوكيز غير آمنة، كما يتم فحص الشهادة الأمنية لضمان أن الموقع يدعم SSL/TLS بشكل صحيح. تم اختيار JavaScript في هذا الملف نظرًا لكونها اللغة المثالية لتطوير الإضافات في بيئة Chromium. من خلال هذه اللغة، يمكن إجراء العمليات الأمنية بشكل سريع ودقيق، حيث أنها تتكامل بسلاسة مع واجهات برمجة التطبيقات الخاصة بالمتصفح.

```
// 1. Function to check security headers for a URL
Function checkHeaders(url):
  If URL is trusted:
    Return "Trusted Site" with passed = true, status = safe
  Else:
    Return "Scan Skipped" with passed = true, status = info

// 2. Function to display results
Function displayResults(checks, score):
  For each check in checks:
    Display check name and message
  If score >= 80:
    Set score color to "safe"
  Else If score >= 60:
    Set score color to "warning"
  Else:
    Set score color to "danger"
  Display final score with color

// 3. Function to display error message
Function showError(message):
  Display error message with danger status

// 4. Function to load current URL from the active tab
Function loadCurrentURL():
  Get active tab URL
  If URL exists:
    Display current URL in the interface
```

رابعًا فحص البروتوكول (HTTPS) تعد عملية فحص البروتوكول أحد الفحوصات الأساسية لضمان أمان الموقع الذي يتم تصفحه. يتم التحقق من البروتوكول المستخدم في الاتصال بين المتصفح والخادم، وفي حال كانت البروتوكولات المستخدمة هي HTTPS أو WSS (WebSocket Secure)، يتم اعتبار الموقع آمنًا. إذا كان الموقع يستخدم HTTP بدلاً من HTTPS، يُعتبر الموقع غير آمن، حيث أن البيانات التي يتم تبادلها بين المتصفح والخادم يمكن أن تكون عرضة للاعتراض. تم اختيار فحص البروتوكول لأن HTTPS هو المعيار الأساسي لضمان تشفير البيانات بين المستخدم والخادم. من دون هذا البروتوكول الآمن، يمكن أن يكون المستخدم عرضة لهجمات Man-in-the-middle أو سرقة البيانات. هذا الفحص يمثل حجر الزاوية في تقييم الأمان للموقع.

خامسًا فحص الدومين في فحص الدومين، يتم التحقق من ما إذا كان اسم الموقع يحتوي على أي مؤشرات تدل على مواقع مشبوهة أو مزورة. يتضمن هذا الفحص تحديد إذا كان الدومين يحتوي على كلمات مشبوهة مثل faceb00k أو tw1tter أو استخدام نطاقات مجانية مثل . tk أو .ml. يتم أيضًا التحقق من أن الدومين يتبع ممارسات التسجيل الموثوقة. يعد هذا الفحص خطوة أساسية في كشف مواقع التصيد، حيث تستخدم المواقع الاحتيالية أسماء نطاقات مشابهة للمواقع الأصلية بهدف خداع المستخدمين. من خلال التحقق من الدومين، نضمن أن الموقع الذي يزوره المستخدم موثوق.

سادسًا فحص الكوكيز في فحص الكوكيز، يتم تحليل الكوكيز التي يستخدمها الموقع لتخزين المعلومات حول الجلسات، مثل بيانات المستخدم أو التفضيلات. يتم فحص ما إذا كانت الكوكيز آمنة، أي إذا كانت تُرسل عبر HTTPS وإذا كانت HttpOnly (أي لا يمكن الوصول إليها عبر JavaScript). تُعتبر الكوكيز غير الآمنة تهديدًا محتملاً لخصوصية المستخدم. يهدف هذا الفحص إلى حماية المستخدم من هجمات Cross-Site Scripting (XSS) والتتبع غير المصرح به. عبر فحص الكوكيز، يتم ضمان أن الموقع لا يستخدم آليات غير آمنة لتخزين البيانات.

سابعًا فحص المنفذ فحص المنفذ يتأكد من أن الموقع يستخدم المنافذ القياسية مثل 443 (لـ HTTPS) أو 80 (لـ HTTP). المنافذ غير القياسية قد تشير إلى وجود هجوم أو محاولة للوصول غير المشروع إلى الخوادم. يعد فحص المنفذ خطوة مهمة للكشف عن التهديدات الأمنية المتعلقة بالبنية التحتية للموقع، وتضمن الإضافة أمان الموقع من خلال هذه العملية.

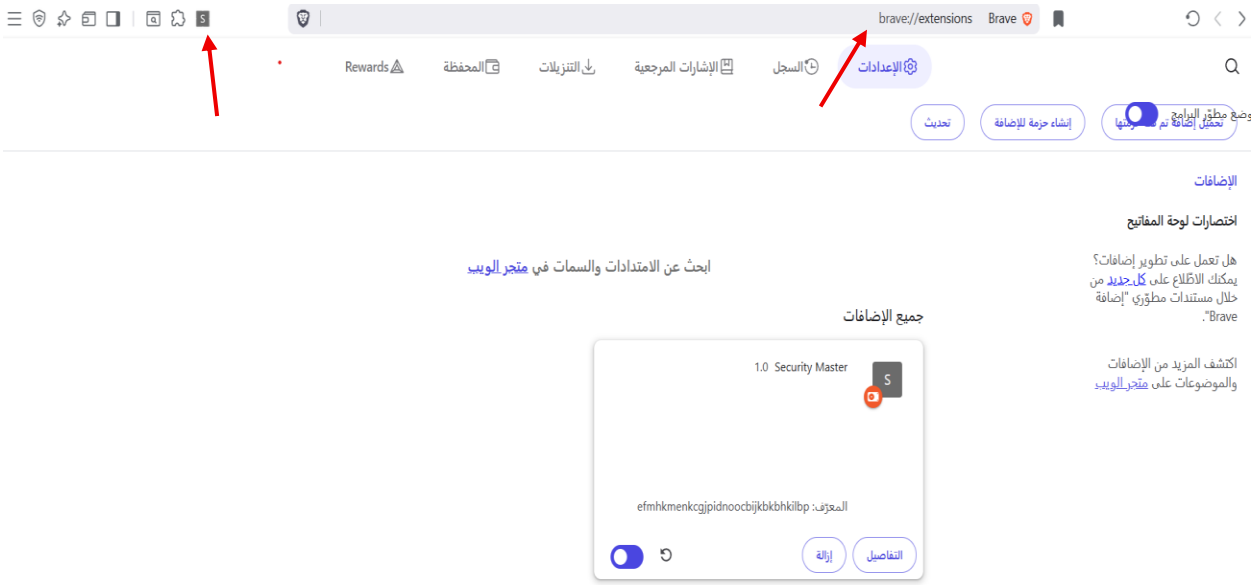
ثامنًا فحص شهادة SSL يتم في فحص شهادة SSL التأكد من أن الموقع يستخدم شهادة SSL/TLS لتشفير البيانات بين المستخدم والخادم. يُعد هذا الفحص ضروريًا لحماية بيانات المستخدمين، خاصة عند نقل المعلومات الحساسة مثل كلمات المرور أو تفاصيل الدفع. تم اختيار هذا الفحص نظرًا لأنه من أكثر الطرق أمانًا لضمان أن الموقع آمن من حيث التشفير.

تاسعًا فحص رؤوس الأمان في فحص رؤوس الأمان، يتم التحقق من وجود رؤوس أمان مثل X-Content-Type-Options و X-XSS-Protection، التي تحمي من بعض الهجمات الشائعة مثل Cross-Site Scripting

(XSS) و Clickjacking. تعد هذه الرؤوس من أهم وسائل الحماية للمواقع الحديثة. تم اختيار هذا الفحص لضمان أن الموقع يطبق أحدث تقنيات الأمان لحماية المستخدمين من الهجمات المتقدمة.

4.3 خطوات التثبيت والتفعيل

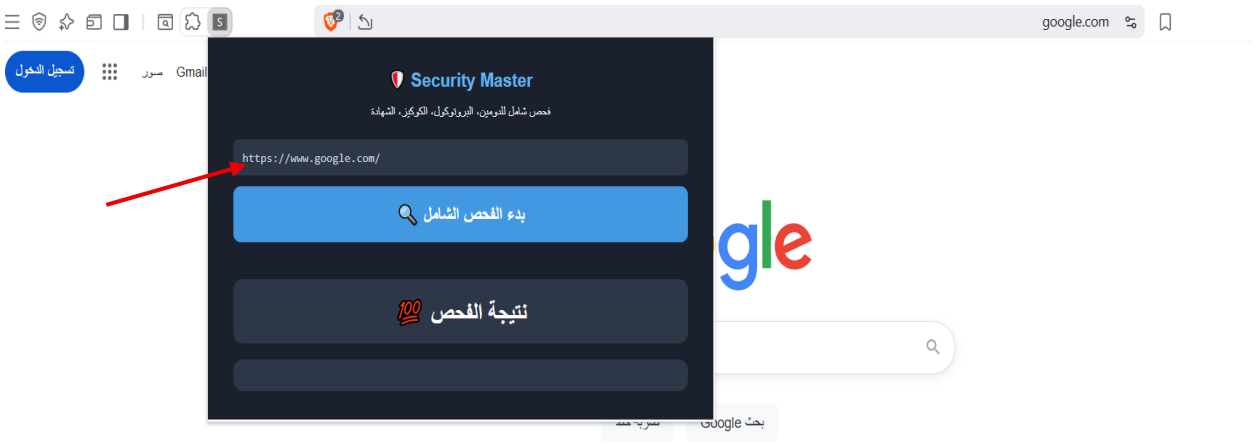
في هذه الخطوة، تم تثبيت الإضافة على متصفح Brave باستخدام خيار الإضافات غير المعبأة (unpacked extensions). بدايةً، تم تنزيل ملفات الإضافة وتثبيتها محليًا على المتصفح. ثم، تم تمكين الإضافة من خلال التوجه إلى صفحة الإضافات في المتصفح (chrome://extensions) وتفعيل خيار تحميل الإضافة غير المعبأة يظهر الشكل (6) تثبيت الإضافة على متصفح Brave.



الشكل 6 : توضيح تثبيت الإضافة على المتصفح

4.4 طريقة إجراء الفحص

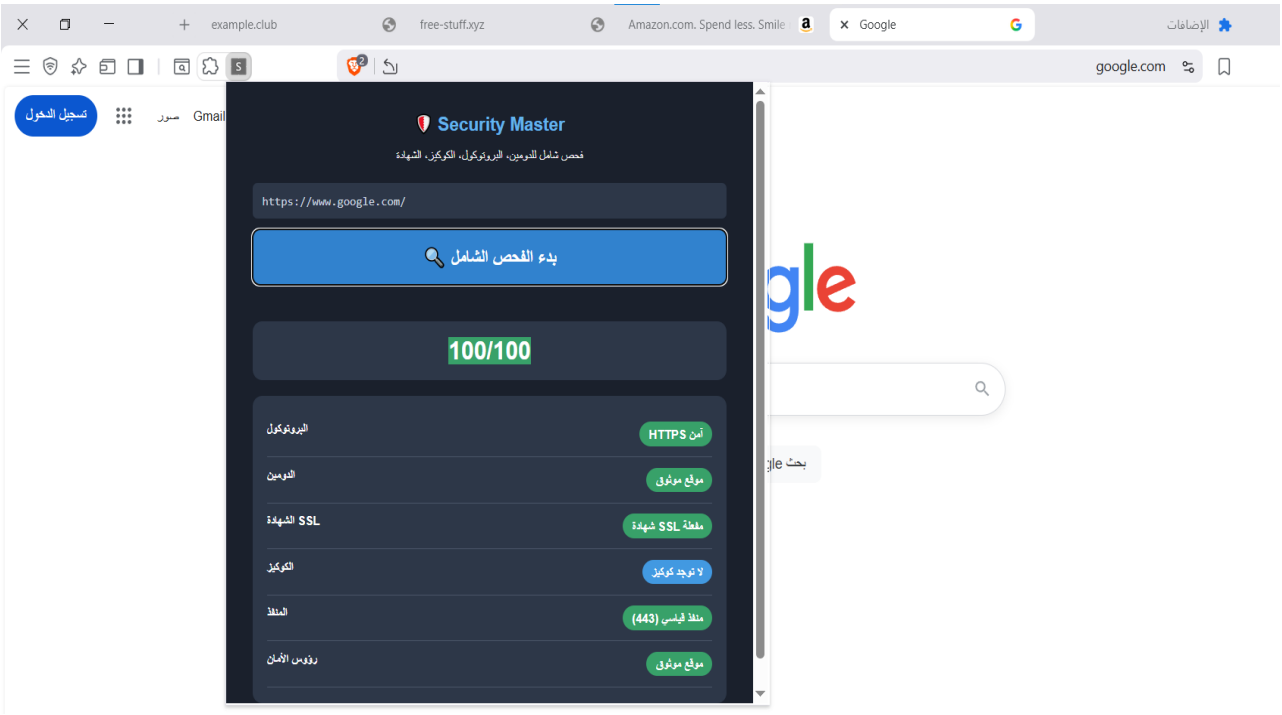
بعد تثبيت الإضافة بنجاح، تم فتح الموقع الإلكتروني المطلوب فحصه. تم الضغط على زر "بدء الفحص الشامل" داخل واجهة الإضافة لبدء عملية الفحص كما يظهر في الشكل (7), زر "بدء الفحص" والذي يتم النقر عليه لبدء فحص الموقع الحالي.



الشكل 7 : زر بدء الفحص في الإضافة

4.5 عرض النتائج وتفسيرها

بعد النقر على زر "بدء الفحص" في الإضافة، تبدأ العملية في تحليل الموقع المدخل. لنأخذ موقع Google كمثال على الفحص كما هوا موضح في الشكل (8). عند إتمام الفحص، تظهر النتائج في واجهة الإضافة بشكل مرتب وواضح. يتم فحص خمسة مجالات أساسية للموقع، وتظهر كل واحدة منها مع نتيجة مرفقة تبيّن ما إذا كان الموقع آمنًا أو يحتوي على بعض المشكلات الأمنية.



الشكل8: عرض نتائج الفحص

يظهر الشكل التالي نتائج الفحص التي تعرض تفاصيل الفحوصات المختلفة على الموقع، مع توضيح حالة كل فحص بشكل دقيق، مثل: (آمن، تحذير، خطر)، بالإضافة إلى تمثيل مرئي للحالة الأمنية لكل من البروتوكول، الدومين، الشهادة الأمنية، المنافذ، ورؤوس الأمان.

4.6 تحليل النتائج

بعد النقر على زر "بدء الفحص"، يقوم النظام بإجراء سلسلة من الفحوصات الأمنية على الموقع المدخل. باستخدام موقع Google كمثال، تبدأ عملية الفحص بتحديد البروتوكول المستخدم من قبل الموقع. حيث يتم التحقق مما إذا كان الموقع يستخدم بروتوكول HTTPS بشكل آمن، وفي حالة Google يظهر الفحص النتيجة "آمن" نظرًا لاستخدامه بروتوكول HTTPS المشفر. بعد ذلك، يتم فحص الدومين (النطاق) المستخدم في الموقع، حيث يتم التحقق من مصداقيته وما إذا كان يتبع موقعًا موثوقًا. في حالة Google، يتم التأكد من أن النطاق يعود إلى موقع موثوق عالميًا، فتظهر النتيجة "آمن". كما يتم فحص الشهادة الأمنية (SSL/TLS) للموقع للتحقق من تفعيلها بشكل صحيح. في Google، يتم تفعيل شهادة SSL بشكل سليم، مما يوفر حماية

قوية للبيانات بين المستخدم والخوادم، وتظهر النتيجة "آمن". في الخطوة التالية، يتم التحقق من المنافذ المستخدمة في الموقع، حيث يتم فحص ما إذا كانت المنافذ القياسية مثل 443 مُعتمدة، وهو ما يظهر أيضًا في موقع Google حيث يتم استخدام المنفذ الآمن 443، وبالتالي تظهر النتيجة "آمن". وأخيرًا، يتم فحص رؤوس الأمان الخاصة بالموقع، مثل Content Security Policy و X-Content-Type-Options، لضمان الحماية ضد الهجمات مثل Cross-Site Scripting (XSS) و Clickjacking. في Google، جميع رؤوس الأمان المطلوبة مفعلة بشكل صحيح، مما يعكس مستوى عالٍ من الحماية. عند جمع نتائج هذه الفحوصات، يتم عرض النتيجة النهائية التي تشير إلى أن الموقع آمن في جميع الجوانب المدروسة. في النهاية، يساهم هذا الفحص الشامل في ضمان أمان الموقع وحماية خصوصية المستخدم، مما يُظهر أهمية استخدام هذه الفحوصات في تطوير بيئة تصفح آمنة.

4.7 نتائج اختبار الإضافة على مواقع (أمنة وغير أمنة)

تم اختبار الإضافة على مجموعة متنوعة من المواقع الإلكترونية لتقييم كفاءتها في اكتشاف تقنيات التصيد وتحديد مستوى الأمان. شملت هذه التجارب مواقع تُعد آمنة وموثوقة، مثل Google و Amazon، حيث أظهرت النتائج قدرة الإضافة على تحديد البروتوكولات الآمنة (HTTPS)، وكذلك فحص الدومين والشهادات بطريقة دقيقة. في المقابل، تم اختبار الإضافة على مواقع تم تصميمها خصيصًا لمحاكاة تقنيات التصيد، حيث كشفت النتائج عن تصنيفات تحذيرية أو "خطر"، مما يعكس وجود بروتوكولات غير آمنة أو دومينات مشبوهة. على سبيل المثال، تم اختبار الموقع http://faceb00k-ss، الذي هو نسخة غير موثوقة ومزورة من موقع Facebook، وأظهرت الإضافة تحذيرًا من وجود دومين مشبوه يحتوي على كلمات مشبوهة في عنوانه. بالإضافة إلى ذلك، تم تحليل مواقع تحتوي على ثغرات أمان تتعلق بالكوكيز أو المنافذ غير القياسية، والتي تم تصنيفها كمواقع ذات مخاطر أمنية. نتائج هذه التجارب ساعدت في تقييم فاعلية الإضافة في تصنيف المواقع الآمنة والغير آمنة بناءً على مجموعة من معايير الأمان المعتمدة.

جدول3: مقارنة بين المواقع

العامل	الموقع الأمن	الموقع غير الأمن
البروتوكول	يستخدم HTTPS, الاتصال مشفر وأمن	يستخدم HTTP,الاتصال غير مشفر.
الدومين	دومين موثوق ومعروف	دومين مشبوه أو مزيف
الشهادة الأمنية(ssl)	شهادة ssl فعالة ومعتمدة	لا توجد شهادة ssl او الشهادة غير صالحة
الكوكيز	الكوكيز محمية وأمنة.	لا يحتوي على كوكيز أو لا يوجد حماية لها
المنافذ	استخدام منافذ القياسية (443,80)	استخدام منافذ غير قياسية أو خطيرة
رؤوس الأمان	يحتوي على رؤوس أمان	يفتقر إلى رؤوس الأمان أو يحتوي على رؤوس ضعيفة
الفحص الأمني	تم اجتياز جميع اختبارات الأمان بنجاح	يوجد تحذيرات أو مخاطر أمنية

Reference

1.Ali, N. S. M., Abdel-Wahab, H. A. S., & Eltoweissy, S. M. M. (2016). Phishing and its detection methods: A survey. International Journal of Computer Science and Network Security (IJCSNS), 16(7), 1-14.

2. Yalcin, B. G. (2018). Web scraping detection and prevention: A survey. In Proceedings of the 2018 IEEE 8th International Conference on Cloud Computing and Intelligence Systems (CCIS), 125-130.

3.Goethals, P. L. J. S., Suh, P. G. L. L., & Chang, C. C. (2014). Improving phishing detection using HTTP headers and URL features. In Proceedings of the 7th International Conference on Security of Information and Networks (SIN), 48-55.

4.Venkatesh, S. S., & Saha, S. K. (2020). Content-based web cloning detection and mitigation. In 0Proceedings of the 2020 International Conference on Artificial Intelligence and Computer Engineering (ICAICE), 178-184.

5.Ahmed, M. A. R., AlZain, M. A., & Khan, M. K. (2020). Phishing website detection using AI techniques. Computers, Materials & Continua, 65(3), 2771-2790.

6.Zhang, X., Wang, Z., & Liu, F. (2017). Detecting phishing websites using visual content comparison. In Proceedings of the IEEE International Conference on Computational Intelligence and Security (CIS), 116-123.

7.Wang, D. Z., He, Q., & Zhang, J. (2022). Web scraping detection: Techniques and challenges. IEEE Transactions on Knowledge and Data Engineering, 34(6), 1256-1270.

8.Iqbal, M. M. A. R., Shah, S. A., & Khan, A. H. (2018). Clickjacking: The hidden threat of web security. Journal of Computer Science and Technology, 23(5), 1026-1036.

9.Suresh, J. B. D. R. K., & Raj, K. R. (2020). Web security and phishing protection techniques: A survey. International Journal of Computer Applications (IJCA), 38(5), 23-29.

10.Pradeep, A. K., Sinha, R. K., & Raj, R. (2019). Phishing detection techniques using URL and web content analysis. In Proceedings of the International Conference on Advanced Computing and Software Engineering (ICACSE), 72-80.

11.Maheswari, A. R., & Arshad, T. A. (2021). Machine learning algorithms for detecting phishing websites: A comprehensive review. Journal of King Saud University-Computer and Information Sciences, 33, 1712-1720.

12.Patel, P., & Patel, M. L. (2017). A review of phishing detection techniques using machine learning. International Journal of Advanced Research in Computer Science and Software Engineering, 7(2), 123-130.