الجمهورية اليمنية

جامعة آزال للتنمية البشرية

كلية الهندسة وتكنولوجيا المعلومات

قسم الأمن السيبراني

جامعة آزال للتنمية البشرية
Azal University for Human Development

منـــصـــة الـفـريـــق الاحـمـــر

Red Team Platform

إعـــــــداد الـــــطـــلاب :

مازن محمد محسن بحجوج	**2022020849**
مهند علي محمد ناصر مفتاح	**2022010846**
وليد قاسم أحمد ظافر الغبري	**2022010715**
مرشد شريف مرشد الشريف	**2022010815**
مصعب عادل عثمان المقرمي	**2022010799**

إشـــــراف:

د/ وليد الوجية

د/ عبد السلام خاقو

بحث المشروع هذا مُقدم إلى كلية الهندسة وتقنية المعلومات قسم الأمن السيبراني، جامعة آزال للتنمية البشرية لإستكمال متطلبات نيل درجة البكالوريوس في الأمن السيبراني

2025-2026

قـــال الله تعالى:

{وَقُل رَّبِّ زِدْنِي عِلْمًا} سورة طه (114)

{وَإِذْ تَأَذَّنَ رَبُّكُمْ لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ} سورة إبراهيم (7)

المُلخص

يهدف هذا المشروع إلى تصميم منصة ويب متكاملة تقدم واجهة رسومية (GUI) مبسطة لاستخدام أدوات فحص واختبار اختراق المواقع والأنظمة. تمكن المنصة الأفراد والمؤسسات من إجراء تقييمات أمنية دورية لاكتشاف الثغرات ومعالجتها بسهولة، دون الحاجة إلى خبرة تقنية متقدمة أو التعامل المباشر مع الأكواد

تجمع المنصة بين مجموعة واسعة من الأدوات في واجهة موحدة قابلة للتخصيص، وتوفر ميزات متقدمة مثل: خطوات التشغيل التلقائية لإجراء فحوصات شاملة، ومحاكاة الهجمات المنظمة، وإصدار تقارير مفصلة. تشمل الوظائف الرئيسية واجهة بديهية للمبتدئين، ووحدات متقدمة للمتخصصين، ولوحة تحكم مركزية، ومولد تقارير متعدد الصيغ، وجدولة الفحوص الآلية، وإمكانية دمج أدوات خارجية

من الناحية التقنية، تُبنى المنصة كتطبيق ويب حديث قابل للتوسع، مع فصل واضح بين الطبقات واهتمام خاص بالأمان عبر التشفير وآليات المصادقة القوية. يلتزم المشروع بالاستخدام المسؤول، حيث يشترط الحصول على إذن صريح قبل إجراء أي فحص، ويقدم إرشادات أخلاقية وقانونية للمستخدمين

من المتوقع أن تساهم المنصة في زيادة وعي المؤسسات بأمن المعلومات، والكشف المبكر عن الثغرات، وتسريع عمليات الإصلاح، وخفض التكاليف. كما يمكن توسعتها مستقبلاً لدعم وحدات تعليمية وتكامل مع منصات إدارة الثغرات ونماذج الذكاء الاصطناعي

الكلمات المفتاحية : منصة الفريق الأحمر، الأمن السيبراني، اختبار الاختراق، واجهة رسومية، أدوات مفتوحة المصدر، محاكاة الهجوم، التقارير الأمنية

Summary

This project aims to design an integrated web platform that provides a simplified GUI for the use of website and system penetration testing and testing tools. The platform enables individuals and organizations to conduct periodic security assessments to easily detect and process gaps, without the need for advanced technical expertise or direct handling of the code

Automatic to conduct comprehensive checks, simulate organized attacks, and issue detailed reports. The main functions include an intuitive interface for beginners, advanced modules for professionals, a central control panel, a multi-format reporting generator, an automated examination scheduling, and the ability to integrate external tools

from a technical point of view. To expand, with a clear separation between classes and attention to security through encryption and strong authentication mechanisms. The project is committed to responsible use, as it requires express permission before conducting any examination, and provides ethical and legal guidelines for users

costs. It can also be expanded in the future to support educational units and integration with gap management platforms and AI

keywords: the red team platform, cybersecurity, penetration testing, graphical interface, open source tools, attack simulation, security reports.

الإهـــــــداء

بسـم الله الرحمن الرحيـم

الحمد لله الذي أنعم علينا بنعمة العلم، والصلاة والسلام على سيدنا محمد معلم البشرية الأول

أما بعد، فهذا الجهد المتواضع ثمرة سنوات من الدراسة والبحث، أقدمه بين أيديكم باسم الله تعالى، وأهديه من القلب:

إلى من علمني حرفاً.. صلى لي ركعتين.. ودعا لي في سجدة:

إلى والديّ العزيزين، كلماتهما قاصرة عن رد جميلهما، فلكما مني كل الحب والشكر والدعاء بأن يطول الله في عمركما ويحفظكما لي

إلى منبع الحكمة والعطاء.. من علمني معنى العطاء بلا حدود:

إلى مُعلمي ومعلمتي، من أول يوم درسة إلى آخر محاضرة في الجامعة، شكراً لكم على كل حرف علمتمونيه، وكل توجيه سددتم خطاي

إلى رفيق الدرب.. إخوتي وأخواتي:

شكراً على كل لحظة دعم، وكل كلمة تشجيع، وكل تضحية ساعدتني للوصول إلى هذه اللحظة

إلى من شاركوني رحلة الكفاح:

إلى زملائي ورفاقي في فريق البحث وفي مشروع تخرجي، شكراً على كل جلسة عمل متأخرة، وكل فكرة أثرت في هذا العمل، وكل لحظة تعاون جعلت من هذا التحدي تجربة لا تُنسى.

إلى نفسي التي تعبت وكافحت:

إلى الطالب الذي كان يحلم يوماً بهذه اللحظة، هذا هو فوزك الأول، فليكن بداية طريق مليء بالإنجازات

وأخيراً وليس آخراً..

إلى كل من مدّ لي يد العون، ولو بكلمة طيبة

إلى روح كان لها هنا حضور

إلى وطني الحبيب الذي أرغب في أن أكون لبنة صالحة في بنائه

الحمد لله رب العالمين الذي منّ علينا بإتمام هذا العمل، وهذا المشروع فما كان فيه من صواب فمن توفيقه وفضله، وما كان فيه من تقصير فمن نفسي وأسأل الله أن يتجاوز عنه

"وَالله ولي التوفيق"

شـكـر وتـقـــديـــر

بسـم الله الرحمن الرحيـم

الحمد لله الذي بنعمته تتم الصالحات، ها قد وصلت إلى محطة مهمة في رحلتي التعليمية، وأود أن أتوجه بخالص الشكر والعرفان لكل من ساندني حتى اكتمل هذا المشروع

بداية، أتقدم بجزيل الشكر والتقدير إلى مشرفيَّ الكريمين الدكتور/ وليد الوجية وكذلك الدكتور/ عبدالسلام خاقو ، اللذين لم يبخلا عليّ بتوجيهاتهما القيمة ونصائحهما الثمينة، فكانا خيرعون وسند خلال رحلة البحث فلهما مني جزيل الامتنان على وقتهما وجهودهما التي قادتني إلى إتمام هذا العمل وهذا المشروع على أفضل وجه

كما لا يفوتني أن أشكر أعضاء هيئة التدريس في قسم الأمن السيبراني، على المعرفة التي غرسوها فينا طيلة سنوات الدراسة، فكانوا مصابيح تنير دروب العلم

وشكري الجزيل أيضاً لزُملائي وأصدقائي الرائعين، الذين كانوا سنداً حقيقياً في أوقات الصعوبة، يشاركونني الهمّ ويبعثون في نفسي روح الأمل والتفاؤل

وأخيراً، لا يمكن للكلمات أن توفّي حقّ من ضحوا من أجلي، أبي وأمي الغاليين، فلهما كل الحب والوفاء، ودعواتهما كانت وقودي لإكمال هذه الرحلة كما أشكر إخوتي وأفراد أسرتي جميعاً على دعمهم اللامشروط وصبرهم

وإلى كل من مدّ لي يد العون، ولو بكلمة طيبة، أقول لكم من أعماق قلبي:

شكراً

اقرار المشرفين

اننا نشهد أن إعداد هذا المشروع بعنوان

.....

أعدها .....

تحت إشراف .....

قسم في الوفاء الجزئي بمتطلبات / درجة البكالريوس في .....

.....

اسم المشرف :

التوقيع

التاريخ

اسم المشرف :

التوقيع

التاريخ

قرار لجنة الحكم والمناقشة

تم مناقشة هذا المشروع المقدم من طلاب كلية الحاسوب تقنية المعلومات قسم الأمن السيبراني في مشروع

"منصة الفريق الأحمر Red Team Platform تصميم منصة ويب متكاملة تقدم واجهة رسومية (GUI)" وبعد مناقشة الطلاب في محتويات المشروع وفيما له علاقة به تم قبول المشروع ، وهو جزء من متطلبات الحصول على درجة البكالريوس في كلية الحاسوب وتقنية المعلومات قسم الأمن السيبراني

جدول 1 أعضاء لجنة الحكم والمناقشة

لجنة المناقشة			
م	الاسم	الصفة	التوقيع
1			
2			
3			

عميد كلية الحاسوب وتقنية المعلومات

د/ مختار غيلان

رئيس قسم الأمن السيبراني

د/ عبد السلام خاقو

التفويض

نحن طلاب جامعة ازآل للتنمية البشرية كلية الحاسوب وتقنية المعلومات قسم الأمن السيبراني نسمح لجامعة ازآل كلية الحاسوب وتقنية المعلومات لتوفير نسخ من وثيقة مشروع التخرج لدينا إلى المكتبات او الشركات او الأفراد عند الطلب

جدول 2 أعضاء المشروع

م	اسم الطالب	رقم الطالب	التوقيع
1	مازن محمد محسن بحجوج	2022020849	
2	مهند علي محمد ناصر مفتاح	2022010846	
3	وليد قاسم احمد ظافر الغبري	2022010715	
4	مرشد شريف مرشد الشريف	2022010815	
5	مصعب عادل عثمان المقرمي	2022010799	

التاريخ :

فهرس المحتويات

قائمة الجداول

قائمة الاشكال

الفصل الأول:

مقدمة في البحث واهميتة

(Introduction to the research and its importance)

1.1 المُقدمة:

في ظل التطور السريع الذي يشهده العالم في المجال الرقمي، أصبح أمن المعلومات وحماية البيانات ركيزة أساسية ومن أبرز التحديات التي تواجه الأفراد والمؤسسات تتزايد الهجمات الإلكترونية عامًا بعد عام، مسببة خسائر مالية كبيرة وانتهاكات لخصوصية المستخدمين .تشير الإحصائيات الحديثة إلى أن تكلفة الجرائم الإلكترونية قد تتجاوز 10 تريليونات دولار سنويًا بحلول عام 2025. في هذا السياق، يبرز مشروع منصة الفريق الأحمر (Red Team Platform)كحلّ مبتكر يسعى إلى تبسيط عمليات الفحص الأمني واختبار الاختراق، وذلك من خلال تطوير منصة ويب بواجهة رسومية تفاعلية (GUI) تسهّل على المستخدمين من مختلف المستويات القيام بعمليات تحليل أمني شاملة دون الحاجة إلى كتابة أوامر برمجية معقدة.

وذلك لتسهيل عمليات الفحص الأمني واختبار الاختراق للمواقع الإلكترونية والأنظمة والأجهزة. تهدف هذه المنصة إلى جعل أدوات الفحص والاختراق، التي كانت حكراً في السابق على المتخصصين وذوي الخبرة التقنية العالية، في متناول جميع المستخدمين بغض النظر عن خلفياتهم التقنية، وذلك من خلال استبدال التعامل المعقد بالأكواد بواجهات بصرية بديهية وسهلة الاستخدام يسهم المشروع بشكل مباشر في تعزيز الأمن السيبراني من خلال تمكين

الأفراد والمؤسسات والقطاعات الخاصة من فحص بناهم التحتية لاكتشاف الثغرات الأمنية والتعامل معها بفعالية، وذلك عن طريق توفير مجموعة شاملة من الأدوات المتطورة في مكان واحد. كما يقدم المشروع ميزة محاكاة هجمات افتراضية لقياس متانة الدفاعات ومدى مقاومتها للاختراقات الفعلية من خلال كونه منصة على شبكة الويب، يوفر المشروع سهولة الوصول والاستخدام، مع القدرة على إصدار تقارير مفصلة ودقيقة تتيح للمستخدمين فهم نقاط الضعف واتخاذ الإجراءات التصحيحية المناسبة. وبذلك، لا يقتصر دور المنصة على التبسيط التقني فحسب، بل يتعداه إلى المساهمة الفعلية في بناء بيئة رقمية أكثر أماناً وموثوقية للجميع.

2.1 مشكلة المشروع (Problem Statement):

في ظل الاعتماد المتزايد على التقنية والإنترنت، أصبحت أمن المعلومات وحماية الشبكات من أهم الركائز التي تقوم عليها ثقة الأفراد والمؤسسات على حد سواء. ومع تطور التهديدات الإلكترونية المستمر، تزداد صعوبة اكتشاف الثغرات ومعالجتها بشكل فعّال ورغم وجود العديد من أدوات الفحص الأمني القوية، إلا أن طبيعة استخدامها المعقدة تجعلها حكرًا على فئة محدودة من الخبراء والمتخصصين وفيما يلي توضيح لأبرز أوجه المشكلة بالتفصيل :

- تعتمد أغلب أدوات الفحص والاختراق الأكثر فاعلية على واجهة سطر الأوامر (CLI)، مما يجعل استخدامها صعبًا لغير المتخصصين
  هذا الاعتماد على CLI يحدّ من انتشار هذه الأدوات خارج نطاق الخبراء، ويمنع المستخدمين العاديين من الاستفادة منها
- تواجه المؤسسات الصغيرة والمتوسطة صعوبات في توظيف مختصين في الأمن السيبراني بسبب نقص الموارد المالية أو الخبرة التقنية الداخلية.

يؤدي ذلك إلى حرمان هذه المؤسسات والأفراد المهتمين من القدرة على إجراء فحوص أمنية استباقية لأنظمتهم.

- نتيجة لذلك، تبقى العديد من الثغرات الأمنية غير مكتشفة، مما يزيد من احتمالية استغلالها من قِبل جهات خبيثة.

هذا الواقع يُضعف مستوى الأمان العام للبنى التحتية الرقمية ويزيد من مخاطر الهجمات الإلكترونية.

- كما يُظهر الحاجة إلى حلول أكثر سهولة في الاستخدام تُمكّن المستخدمين من إجراء فحوص أمنية دون الحاجة إلى معرفة تقنية متقدمة.
- يتطلب الأمر تطوير واجهة رسومية (GUI) تربط أدوات الفحص الاحترافية بخطوات مبسطة وواضحة يمكن لغير المتخصصين اتباعها بسهولة.

3.1 فكرة المشروع (Project Idea):

تتمحور فكرة مشروع منصة Read Team حول تطوير منصة متكاملة لاختبار أمان الأنظمة والتطبيقات، تهدف إلى توفير بيئة عملية موحدة تجمع بين عدد من أدوات اختبار الاختراق مفتوحة المصدر ضمن واجهة رسومية (GUI) واحدة سهلة الاستخدام وعلى الرغم من وجود أدوات قائمة تؤدي وظائف مشابهة مثل OWASP ZAP، فإن تميّز المنصة المقترحة يتمثل في دمج مجموعة متنوعة من الأدوات الأمنية المتخصصة ضمن منظومة واحدة مترابطة، إضافةً إلى آلية إعداد تقارير تحليلية تفصيلية وتلقائية تسهم في تسريع عملية اكتشاف الثغرات وتحليلها واقتراح سبل معالجتها كما تركز المنصة على تعزيز قابلية الاستخدام والبساطة في التصميم، بما يمكّن المستخدمين من مختلف المستويات سواء المتخصصين في الأمن السيبراني أو المتدربين الجدد من الاستفادة منها بكفاءة عالية في بيئة اختبار عملية وآمنة

4.1 اهداف المشروع (project Objectives):

يهدف هذا المشروع إلى معالجة التحديات المرتبطة باستخدام أدوات الفحص الأمني التقليدية، وتسهيل الوصول إليها لشرائح أوسع من المستخدمين من خلال حلول تقنية مبتكرة وبسيطة الاستخدام
فيما يلي أبرز أهداف المشروع :

- تطوير واجهة رسومية (GUI) سهلة الاستخدام تعمل على تسهيل تشغيل أدوات الفحص الأمني دون الحاجة لاستخدام واجهة سطر الأوامر (CLI).
- تبسيط عملية الفحص الأمني وجعلها متاحة للمستخدمين غير المتخصصين من خلال تصميم واجهة واضحة وموجهة بالخطوات.
- تمكين المؤسسات الصغيرة والمتوسطة من إجراء اختبارات أمنية لأنظمتها دون الحاجة لتوظيف خبراء باهظي التكلفة
- دعم الأفراد المهتمين بالأمن السيبراني بأدوات تساعدهم على فهم الثغرات الأمنية واكتشافها بطريقة تعليمية عملية.
- رفع مستوى الأمان السيبراني عبر تقليل احتمالية بقاء الثغرات غير المكتشفة داخل الأنظمة الرقمية.

5.1 مساهمة المشروع (Project Contribution):

يساهم مشروع منصة الفريق الاحمر بشكل إيجابي في مجال امن المعلومات في عدة مجالات رئيسية :

- **للمؤسسات :** تمكينها من فحص البنية التحتية بشكل دوري وتعزيز الحماية الرقمية
- **للأفراد :** إتاحة وسيلة مبسطة لاختبار أجهزتهم ومواقعهم الخاصة
- **للمجتمع التقني :** خفض الحواجز أمام المبتدئين في مجال الأمن السيبراني وتشجيع الممارسات الآمنة

6.1 نطاق المشروع وحدوده (Project Scope and Boundaries):

في عالم يزداد اعتماداً على التكنولوجيا أصبحت حماية الأنظمة والشبكات من الهجمات الإلكترونية أمراً بالغ الأهمية تهدف "منصة الفريق الأحمر" الى بيئة محاكاة متكاملة وآمنة وهذا ماهو حول نطاق المشروع وماهو خارج النطاق وأيضا القيود والافتراضات بالشكل التالي :

6.1.1 النطاق الشمولي (In-Scope):

يشمل نطاق المشروع تطوير منصة ويب تجمع أدوات فحص واختبار اختراق مواقع الويب المفتوحة المصدر مثل Nmap و SQLmap و OWASP ZAP. المنصة ستتيح إنشاء تقارير آلية وتوفر واجهة رسومية تسهل على المستخدمين تنفيذ عمليات الفحص

6.1.2 ما هو خارج النطاق (Out-of-Scope) :

المشروع لا يشمل تطوير أدوات أمنية جديدة من الصفر، ولا يشمل إنشاء تطبيقات سطح مكتب أو جوال، كما لا يتعامل مع اختبارات أمنية متقدمة تتطلب إذناً خاصاً أو وصولاً إلى بنى تحتية مغلقة

6.1.3 القيود والافتراضات (Limitations and Assumptions) :

- قيود الوقت: تنفيذ المشروع ضمن فترة زمنية محددة.
- الاعتماد على الإنترنت لتشغيل الأدوات والعمليات.
- يفترض أن لدى المستخدمين معرفة أساسية بمفاهيم الأمان مثل الثغرات والتقارير.
- الالتزام بمعايير الأمان والخصوصية لحماية بيانات المستخدمين

7.1 الأدوات والتقنيات (Project Tools and Technologies):

- **الواجهة الامامية (Front-End):** HTML5, CSS3, JavaScript ، مع إمكانية استخدام إطار عمل مثل Vue.jsأوReact
- **الواجهة الخلفية (Back-End):** Python مع Node.js لإدارة العمليات المنطقية وتشغيل الأدوات
- **أدوات الامن** Nmap, SQLmap, Nikto, OWASP ZAP, Metasploit, Burp Suite.
- **قاعدة البيانات** MySQL أو PostgreSQL لتخزين بيانات المستخدمين والتقارير

8.1 الفوائد والتحديات (Benefits and Challenges):

8.1.1 فوائد المنصة (Platform benefits) :

تحديد نقاط الضعف الشاملة في الانظمة والاجهزة وذلك عندما يتم تجربة إختبار إختراق عند القيام بهاذه التجربة سيتضح لنا ما إذا كان النظام او الجهاز يعمل بكفائة عالية ولا يتواجد فية اي نقطة ضعف وهذا الامر سيكون مفيداً لمن يستخدمون المنصة لأنهم سيتمكنون من معرفة نقاط ضعف اجهزتهم إن وجدت لانه إذا كان هناك نقاط ضعف في انظمتهم واجهزتهم لكي يتمكنو من حل مشاكل نقاط الضعف التي تم اكتشافها.

تحسين الوعي الأمني للموظفين عبر سيناريوهات واقعية يتم تصويرالمشاكل التي من الممكن ان تحدث وكمية الخسائر التي من الممكن ان تتعرض لها الشركة وبذلك يكون الموظفين أكثر حذراً لأنهم يعلمون مقدار الخسائر المكلفة التي سوف تعرض الشركة للافلاس وايضا ستؤثر على سمعة الشركة

8.1.2 التحديات (challenges) :

- **التكلفة العالية والوقت الطويل للاختبارات :** في هذه الخطوة سنقوم بجعل الادوات أكثر سرعة وسلاسة وأيضا أكثر كفاءة لكي نتمكن من تقليص الوقت الطويل للاختبار وفي هاذة الخطوة سوف تكون المنصة لها قابلية من قبل المستخدمين وسيتم تقليص التكلفة بناء على نوعية الفحص او الاختبار بما يتناسب مع المستخدمين لكي يناسب احتياجاتهم
- **الحاجة إلى مجموعة من ألاخصائيين مهرة ولديهم مهارات عالية ومتنوعة :** عندما يتم عمل المنصة بواجهات رسومية لن يكون هناك داعي لكي يكون هنالك اخصائيين، بل يكفي ان يكون هناك شخص يعرف شيء بسيط عن اهم الثغرات واهم الاوامر التي سيختارها لكي يتمكن من حل مشاكل تلك الثغرات

9.1 الخلاصة (Conclusion) :

استعرض هذا الفصل الأسس النظرية للمشروع، بدءاً من عرض المشكلة الأساسية المتعلقة بتعقيد أدوات الأمن السيبراني، مروراً بفكرة الحل المقترحة عبر منصة Red Team، وأهداف المشروع ومساهماته وحدوده، وحتى الأدوات والتقنيات المستخدمة. كما وضح منهجية البحث المعتمدة لتطوير النظام. يشكل هذا الفصل الإطار التوجيهي العام الذي سيُبنى عليه التصميم والتنفيذ في الفصول القادمة

10.1 مُلخص الفصول (Class Summary):

❖ خلاصة الفصل الثاني :

يؤسس هذا الفصل القاعدة النظرية والعملية لمشروع المنصة. من خلال استعراض المفاهيم الأساسية، والمنهجيات القياسية، والأدوات المتخصصة، وتحليل الحلول الحالية، أصبح من الواضح أن هناك حاجة ماسة لحل متكامل وبسيط لأتمتة اختبارات الاختراق. ستعمل المنصة المقترحة على سد الفجوة بين قوة الأدوات مفتوحة المصدر وتعقيد استخدامها، من خلال تقديم واجهة موحدة تدمجها في سيرعمل آلي الفصول القادمة ستبنى على هذا الإطار لتقديم التصميم التفصيلي والتنفيذ العملي للمنصة

❖ خلاصة الفصل الثالث :

في هذا الفصل تم استعراض تفاصيل تحليل المتطلبات لمنصة Red Team مع تفصيل شامل للمتطلبات الوظيفية وغير الوظيفية، إضافة إلى دراسة أصحاب المصلحة. كما تم عرض نماذج تمثيلية للنظام عبر مخططات الاستخدام، الأنشطة، تدفق البيانات، والكيانات والعلاقات. تم التطرق إلى القيود والتحديات مع ربطها بأهمية النمذجة في مجال الأمن السيبراني. هذا الفصل يشكل قاعدة أساسية لفصل التصميم القادم الذي سيبنى على النتائج الموضحة هنا

❖ خلاصة الفصل الرابع :

استعرض هذا الفصل التصميم التفصيلي لمنصة الفريق الأحمر، موضحاً البنية المعمارية للنظام، وتصميم قاعدة البيانات، وتصميم واجهات المستخدم، وآليات الأمان، بالإضافة إلى طريقة تكامل أدوات اختبار الاختراق. يمثل هذا التصميم الأساس الذي سيتم الاعتماد عليه في مرحلة تنفيذ النظام واختباره.

❖ خلاصة الفصل الخامس :

استعرض هذا الفصل عملية تنفيذ منصة الفريق الأحمر ابتداءً من إعداد بيئة التطوير وحتى دمج أدوات اختبار الاختراق وتشغيل النظام بشكل متكامل

❖ خلاصة الفصل السادس :

إن "منصة الفريق الأحمر" ليست مجرد أداة أخرى لجمع أدوات الاختراق، بل هي بيئة تنظيمية تهدف إلى تحويل الفوضى الإبداعية لعملية اختبار الاختراق إلى سير عمل منهجي وموثق وقابل للتكرار. الاستنتاج الجوهري هو أن نجاح هذه المنصة لا يقاس بعدد الثغريات التي تكتشفها، بل بقدرتها على منع سوء استخدام الأدوات القوية التوصيات المستقبلية أعلاه، وخاصة الانتقال إلى البنية التحتية المعتمدة على الحاويات (Docker) وإضافة محرك تقارير ذكي، ستحول المشروع من مجرد نموذج أولي (Proof of Concept) إلى منتج سيبراني من الدرجة الأولى يمكن حتى تسويقه للشركات الصغيرة والمتوسطة

الفصل الثاني :

الإطار النظري ومراجعة الأدبيات

(Theoretical framework and literature review)

1.2 المُقدمة :

يقدم هذا الفصل الإطار النظري والأدبيات العلمية التي يقوم عليها مشروع تطوير المنصة المتكاملة لاختبارات الاختراق. يهدف الفصل إلى تأسيس قاعدة معرفية صلبة من خلال استعراض المفاهيم الأساسية، ومنهجيات العمل، والأدوات التقنية ذات الصلة، ومراجعة نقدية للدراسات والمشاريع السابقة. سيساهم هذا الإطار في تحديد الفجوة التي تسدها المنصة المقترحة، ويسوغ القرارات التصميمية والتنفيذية التي سيتم اتخاذها في الفصول اللاحقة، مما يعزز القيمة العلمية والعملية للمشروع

2.2 المفاهيم الأساسية في اختبارات الاختراق والتقييم الأمني

: (Basic concepts of penetration testing and security progress)

1.2.2 تعريف اختبار الاختراق (Penetration Testing) :

اختبار الاختراق هو عملية محاكاة هجمات إلكترونية مسيَّقة وموجهة ضد نظام أو شبكة ما بهدف اكتشاف نقاط الضعف والثغرات الأمنية قبل أن يتمكن مهاجم حقيقي من استغلالها (Arkin, Stender, & McGraw, 2005). تكتسب هذه الاختبارات أهميتها من طبيعتها الاستباقية، حيث تتحول استراتيجية الدفاع من رد الفعل إلى منع وحماية استباقي. تهدف هذه الاختبارات إلى تقييم مدى صمود البنية التحتية للأنظمة، والتطبيقات، والإجراءات البشرية في وجه الهجمات الواقعية

2.2.2 منهجيات اختبار الاختراق القياسية :

لضمان شمولية وفعالية اختبارات الاختراق، تم تطوير عدة منهجيات قياسية، أهمها:

- **منهجية OWASP Testing Guide :** تركز هذه المنهجية على اختبار أمان تطبيقات الويب، وتقدم قائمة شاملة بالإختبارات بناءً على مخاطر OWASP Top 10 (OWASP Foundation, 2021). تعتبر مرجعًا أساسيًا للمختبرين due to its comprehensiveness and community-driven updates.
- **منهجية PTES (Penetration Testing Execution Standard):** تقدم PTES إطارًا عمليًا شاملاً يغطي جميع مراحل اختبار الاختراق، من مرحلة ما قبل التفاعل إلى إعداد التقارير (PTES, 2014). تميزها مرحلتها المتعمقة في نمذجة التهديد.
- **منهجية NIST SP 800-115:** يوفر هذا الدليل الصادر عن المعهد الوطني للمعايير والتقنية (NIST) إرشادات تقنية لإجراء التقييمات الأمنية، مع التركيز على التخطيط والتنفيذ والمعالجة (NIST, 2008)

3.2.2 مفهوم فرق الألوان في الأمن السيبراني (The Concept of Color Teams in Cybersecurity):

لتوضيح أدوار الفاعلين في عمليات محاكاة الهجوم والدفاع، ظهر مفهوم فرق الألوان:

- **الفريق الأحمر (Red Team):** يمثل الجهة المهاجمة، ويهدف إلى محاكاة هجمات واقعية متقدمة ومستهدفة (Adversarial Simulation) لتقييم القدرات الدفاعية الشاملة للمؤسسة، وليس فقط اكتشاف الثغرات الفنية
- **الفريق الأزرق (Blue Team):** يمثل المدافعين عن الأنظمة، ومسؤول عن مراقبة الشبكة، والكشف عن الحوادث، والاستجابة لها، وتقوية الدفاعات بناءً على نتائج الهجمات المحاكاة
- **الفريق البنفسجي (Purple Team):** يعمل كحلقة وصل لتعزيز التعاون بين الفريقين الأحمر والأزرق، بهدف تحسين كفاءة عمليات المحاكاة وتعزيز الدفاعات من خلال التغذية الراجعة المستمرة
- **دور المنصة المقترحة:** تهدف المنصة إلى أتمتة وتسهيل العديد من المهام التقنية التي ينفذها الفريق الأحمر، مما يجعله أداة مساعدة له.وبهدف التبسيط وجذب شريحة أوسع (بما في ذلك المؤسسات الصغيرة والمتوسطة ذات الموارد المحدودة)، فإن نطاق المنصة يركز بشكل أساسي على "اختبار الاختراق الآلي" المبني على أدوات مفتوحة المصدر، مع تقديم واجهة موحدة وبسيطة

3.2 مراحل اختبار الاختراق الشامل (Comprehensive penetration test stages) :

1.3.2 المرحلة التمهيدية والتخطيط :

تشمل هذه المرحلة تحديد نطاق الاختبار بدقة (الأنظمة، التطبيقات، الشبكات)، والحصول على الموافقات الرسمية الخطية، ووضع قواعد الاشتباك التي تحدد الإجراءات المسموح بها والممنوعة (PTES, 2014)

2.3.2 جمع المعلومات والاستطلاع :

يتم فيها جمع أكبر قدر ممكن من المعلومات عن الهدف باستخدام تقنيات سلبية (مثل البحث في محركات البحث ومواقع (Whois) ونشطة (like مسح المنافذ باستخدام Nmap)

3.3.2 تحليل الثغرات وتقييمها :

يتم استخدام أدوات مسح آلي (مثل OWASP ZAP) وكشف يدوي للتعرف على الثغرات (مثل حقن SQL وكسر المصادقة) وتقييم مستوى خطورتها بناءً على معايير مثل CVSS (Mell, Scarfone, & Romanosky, 2007)

4.3.2 الاستغلال والاختراق :

هي المرحلة التي يتم فيها استغلال الثغرات المكتسبة للدخول إلى النظام، مع محاولة تصعيد الصلاحيات والتحرك laterally داخل الشبكة (Kennedy et al., 2011)

5.3.2 مرحلة ما بعد الاختراق :

تركز على تقييم الأثر الحقيقي للاختراق، وجمع الأدلة، وفهم مدى انتشار المهاجم داخل البيئة المستهدفة

6.3.2 إعداد التقارير والتوصيات :

المرحلة الأهم، حيث يتم توثيق النتائج، والثغرات، وخطوات الاستغلال، وتقديم توصيات عملية قابلة للتطبيق لمعالجتها (Engebretson, 2013)

4.2 الأدوات الأمنية المتخصصة وتحليلها (Specialized security tools and analysis):

1.4.2 أدوات المسح والشبكات :

- **أداة Nmap:** أداة مسح شبكي قوية ومفتوحة المصدر لتكتشاف المضيفين والخدمات العاملة على نظام ما

المميزات: مرنة، تدبر العديد من تقنيات المسح، تدعم البرمجة النصية

التحديات: تتطلب خبرة لتحقيق أقصى استفادة، قد يتم اكتشافها بسهولة من أنظمة كشف التسلل

ملاءمتها للمنصة: تعتبر أساسية في مرحلة الاستطلاع، وستدمج في المنصة لأداء المسوحات الأولية

2.4.2 أدوات اختبار تطبيقات الويب :

- **أداة Burp Suite:** إطار عمل متكامل ومحترف لاختبار أمان تطبيقات الويب (PortSwigger, 2023).

الإمكانيات: تعترض الوكيل، ماسح آلي، إعادة إرسال الطلبات، فاحص ثغرات

المحددات: الإصدار Professional مدفوع، وقد يكون معقدًا للمبتدئين

ملاءمتها للمنصة: سيتم دمج وظائفها الأساسية (مثل الاعتراض والمسح) عبر واجهة برمجية لتبسيط استخدامها

- **أداة OWASP ZAP:** منافس قوي مفتوح المصدر لـ Burp Suite، يتميز بمجتمع نشط وتطوير مستمر (OWASP Foundation, 2021).

ملاءمتها للمنصة: نظرًا لأنه مفتوح المصدر، فهو مرشح رئيسي للتكامل الكامل ضمن المنصة

3.4.2 أطار العمل الشامل :

- **إطار Metasploit Framework:** منصة شاملة لتطوير وتنفيذ كود الاستغلال (Kennedy et al., 2011)

الشمولية: يحتوي على قاعدة بيانات ضخمة من الثغرات وأكواد الاستغلال.

التعقيد: يتطلب فهماً عميقاً لأنظمة التشغيل والشبكات.

ملاءمتها للمنصة: ستستخدم المنصة واجهة Metasploit البرمجية (MSFRPC) لأتمتة عمليات الاستغلال ضمن سير العمل المحدد مسبقًا، مع إخفاء التعقيد عن المستخدم النهائي

كيفية عمل أداة Metasploit داخل الإطار في التعامل مع إختبار الإختراق:

تمر الأداة بعدة مراحل من حيث عمل إختبار إختراق للانظمة

جمع المعلومات: تتعرف على الاهداف من حيث (ip، نوع نظام التشغيل، المنافذ المفتوحة).

البحث عن الثغرات: تضم مكتبة ضخمة من الثغرات مدمجة داخلها مثلا إذا عرفت ان النظام فية ثغرة محددة تبحث عن الثغرات التي قامت بتحديديها.

إختارExploit المناسب: إذا وجدت ثغرة تقوم بعمل Exploit مناسب لتلك الثغرة.

إعداد Payload: والـPayload هو الكود الذي يتنفذ على جهاز الضحية بعد الاستغلال.

تحديد الهدف: تقوم بتحديد نوع نظام التشغيل أو الإصدار الخدمة إذا تم طلب Exploit.

تنفيذ الهجوم: بعد ان يتم تجهيز Exploit تحصل على جلسة Session إذا نجحت في جهاز الهدف.

مابعد الاستغلال: هنا تبدأ مرحلة التحكم الكامل في الجهاز مثل (تصفح الملفات، جمع كلمات المرور، تسجيلات الكيبورد، فتح الكاميرا او المايك، رفع او تنزيل للملفات، الحصول على صلاحيات اعلى)

5.2 أهمية النمذجة في الأمن السيبراني:

(The importance of modeling in cyber security)

يهدف هذا المشروع إلى تطوير منصة ويب متقدمة تخدم استراتيجيات "النمذجة في الأمن السيبراني"، وتحديدًا دعم عمليات الفريق الأحمر من خلال توفير واجهة رسومية موحدة تختصر تعقيدات أدوات المحاكاة واختبار الاختراق. تمكّن هذه المنصة فرق الأمن من محاكاة تهديدات حقيقية ومنسقة بهدف تقييم مدى فعالية دفاعات المنظمة وكشف نقاط الضعف في بنيتها التحتية قبل أن يستغلها المهاجمون الحقيقيون تم تصميم المنصة لتجسيد مفهوم النمذجة العملية للهجمات، حيث توفر مكتبة غنية من نماذج الهجمات القابلة للتخصيص والتسلسل، محاكيةً أساليب وأدوات المهاجمين المعروفين. تشمل وظائفها الأساسية: محاكاة هجمات متسلسلة، وإدارة سيناريوهات الهجوم الشاملة، وتقارير تحليلية تفصيلية توضح مسار الاختراق ومدى التأثير النمذجة في مشاريع الأمن السيبراني تسهم في:

- تبسيط فهم العمليات المعقدة
- تحديد الثغرات قبل مرحلة التنفيذ
- تحسين التواصل بين الفريق الفني والإداري
- توفير مرجع بصري يساعد في تطوير النظام وتحديثه مستقبلًا
- تساهم المنصة في رفع مستوى النضج الأمني للمؤسسات
- عمليات محاكاة واقعية ومنتظمة، مما يعزز الكشف المبكر عن الثغرات ويختصر وقت الاستجابة

6.2 الدراسات السابقة والمشاريع المماثلة (Previous studies and similar projects):

في عصر التحول الرقمي وتصاعد الهجمات الإلكترونية، تبرز الحاجة إلى حلول استباقية لتقييم وتحسين الأنظمة الأمنية. تمثل منصات الفريق الأحمر أدوات متقدمة لمحاكاة الهجمات الواقعية واكتشاف نقاط الضعف قبل استغلالها من قبل الجهات الخبيثة يهدف مشروع "منصة الفريق الأحمر" إلى توفير حل متكامل يمكن المؤسسات من اختبار دفاعاتها السيبرانية بشكل فعال. وتأتي هذه الدراسة لتحليل المشاريع والدراسات السابقة في هذا المجال، لتحديد المعايير للتصميم والتطوير، والاستفادة من تجارب الآخرين في بناء منصة متميزة تلبي احتياجات السوق المستهدفة سنقوم بذكر بعض من المنصات بناءً على الدراسات السابقة:

1.2 جدول ملخص الدراسات السابقة :

في المشهد المتطور للأمن السيبراني لم يعد مجرد تحديد نقاط الضعف كافيا بل اصبح من الضروري محاكاة سلوك الخصم الفعلي لفهم مدى قوة الدفاعات تهدف هذه الدراسة الى مقارنة منصة الفريق الأحمر

(red team platform) مع مجموعة من الأدوات الرائدة في مجال اختبار الاختراق وهندسة الهجمات لتوضيح الفروق الجوهورية في الفلسفة والمنهجية وحالة الاستخدام

وهذا الجدول يوضح بعض من الدراسات السابقة :

2.2 جدول رقم 1 الدراسات السابقة

الدراسة	العام	الفكرة	المميزات	العيوب
1.منصة Safe Breach	2020	منصة اختبار الاختراق المستمر لمحاكاة سيناريوهات الاختراق من البداية للنهاية	محاكاة مستمرة للاختراقات وآلاف سيناريوهات الهجوم وتقارير تفصيلية ودعم للبيئات المختلفة	حل تجاري مكلف وغير مناسب للميزانيات المحدودة و يحتاج بنية تحتية قوية
2.منصة AttackIQ	2022	منصة تحقق من فعالية الامن لقياس واختبار أداء ضوابط الأمان ضد اطار MITRE &CK) (ATT	متكاملة مع ATT&CK ومحاكاة واقعية وقياس فعالية الأدوات وتقارير قابلة للتخصيص	تكاليف عالية وتعقيد في الإدارة ويحتاج فريق متخصص
3.منصة MITRE &CK ATT	2021	عبارة عن قاعدة معرفية ضخمة (قاعدة بيانات) توثق وتصنف تكتيكات وتقنيات وإجراءات (TTPs)	قاعدة معرفية شاملة لتقنيات الهجوم وإطار عمل موحد لاختبارات الاختراق ومجانية ومفتوحة المصدرو دعم مجتمعي قوي	لا توفر أدوات تنفيذ وتحتاج لفريق متخصص لفهمها ولا تقدم منصة متكاملة

3.2 جدول رقم 2 الدراسات السابقة

الدراسة	العام	الفكرة	المميزات	العيوب
4.منصة Cymulate	2022	منصة تقييم استباقي مستمر لتقييم وضع الامن السيبراني للمنظمة من خلال عدسة المهاجم	منصة سحابية واختبارات مستمرة و واجهة مستخدم بسيطة وتقييم فوري	اشتراك شهري مرتفع ومحدودية في التخصيص واعتماد على الاتصال بالإنترنت
5.منصة Caldera من MITRE	2020	منصة اتمتة لمحاكاة هجمات الفريق الأحمر تعتمد على اطار (&CK MITRE ATT)	منصة تلقائية لمحاكاة الهجوم ومتكاملة مع ATT&CK وقابلة	صعبة في الإعداد وتحتاج خبرة تقنية عالية وثائق غير كافية
6.منصة Professional Nessus	2023	تركز على مسح الثغرات االلي بشكل مكثف. تتميز بدقة االكتشاف ولكنها محدودة في عمليات االستغالل المتقدمة	شاملة وقاعدة بيانات ثغرات ضخمة وسهولة االستخدام وقوة وسرعة الفحص	ايجابيات كاذبة وعالية وتاثير على أداء الشبكة واألنظمة وبحاجة الى صالحيات عالية

1.6.5 الإضافة العلمية للمشروع Scientific Contribution

الإضافة العلمية تكمن في توفير منصة موحدة لأدوات الاختراق،

تُبسّط الاختبار وتؤتمت العملية وتربط الأدوات ضمن واجهة رسومية واحدة

1.6.6 المعايير الأخلاقية والمهنية Ethical and Professional Standards

المنصة تلتزم بالمبادئ الأخلاقية مثل الحصول على الإذن المسبق واحترام الخصوصية،

وتتبع المعايير القانونية الدولية لاختبار الاختراق

1.6.7 الأدوات مفتوحة المصدر:

- **منصة OWASP ZAP :** كما mentioned سابقًا، هي أداة رائعة لكنها تظل أداة منفردة تحتاج إلى دمج مع أدوات أخرى لتقديم حل متكامل
- **أداة OpenVAS :** إطار قوي لمسح الثغرات، لكن واجهته الرسومية (Green bone) يمكن أن تكون معقدة للمستخدمين غير الخبراء (Green bone Networks, 2023).
- **الفجوة:** عدم وجود واجهة موحدة وبسيطة تدمج هذه الأدوات المفتوحة المصدر القوية في سير عمل واحد وسلس

1.6.8 المشاريع الأكاديمية المماثلة :

كشفت مراجعة عدد من مشاريع التخرج عن محاولات سابقة لبناء منصات مشابهة، مثل مشروع " Penetration Testing Execution Framework" لـ (الطالب، 2020). أبرزت هذه المشاريع نجاحات في أتمتة مهام معينة، لكنها غالبًا ما كانت تفتقر إلى:

1. واجهة مستخدم رسومية متكاملة وبديهية
2. دعم مجموعة شاملة من الأدوات في مكان واحد
3. نظام تقارير آلي ومخصص

7.2 الإضافة العلمية للمشروع الحالي (Scientific addition to the current project)

1.7.2 تحليل الفجوات في الحلول الحالية :

بناءً على مراجعة الأدبيات، يمكن تحديد الفجوات الرئيسية التي يسدها هذا المشروع:

- **محدودية الواجهات الرسومية:** معظم الأدوات القوية تعمل عبر سطر الأوامر (CLI)، مما يشكل حاجزًا للمستخدمين غير المخضرمين
- **صعوبة التكامل بين الأدوات:** يتطلب إجراء اختبار اختراق شامل الانتقال بين عدة أدوات ومنصات، مما يستهلك وقتًا ويقلل الكفاءة
- **تعقيد إدارة التقارير:** كل أداة تنتج تقريرًا بتنسيق مختلف، مما يصعب على مسؤولي الأمن تجميع صورة كاملة عن الوضع الأمني

2.7.2 القيمة المضافة للمنصة المقترحة :

تملأ المنصة المقترحة هذه الفجوات من خلال:

- **التكامل الشامل بين الأدوات:** دمج (Nmap, OWASP ZAP, Metasploit, SQLmap) في نظام واحد
- **واجهة مستخدم مبسطة وموحدة:** تقديم workflow مرئي يرشد المستخدم خلال مراحل الاختبار المختلفة
- **أتمتة عملية إعداد التقارير:** توليد تقرير موحد وشامل يجمع نتائج جميع الأدوات المستخدمة
- **توفير حل متكامل للمؤسسات الصغيرة والمتوسطة:** تقديم قدرات احترافية بتكلفة صفرية (باستثناء تكاليف الأجهزة)

8.2 المعايير والضوابط الأخلاقية والمهنية

(Ethical and professional standards and controls) :

يؤكد هذا المشروع على الالتزام الكامل بالمعايير الأخلاقية والمهنية. فجميع عمليات الاختبار التي تجري عبر المنصة يجب أن تتم فقط على الأنظمة التي يمتلكها المستخدم أو حصل على إذن خطي صريح باختبارها. ستضمن المنصة ذلك من خلال مطالبة المستخدم بالموافقة على شروط الاستخدام التي تنص على هذا المبدأ قبل بدء أي اختبار. كما سيتم تصميم نظام التقارير ليكون واضحًا ودقيقًا لتجنب أي تفسير خاطئ للنتائج

1.8.2 المعايير الأخلاقية في اختبار الاختراق :

1. مبدأ الحصول على الإذن (Permission):

هو الأساس الذي تقوم عليه جميع عمليات الاختبار. لا يجوز أبداً اختبار أي نظام أو شبكة بدون الحصول على إذن خطي واضح ومحدد من المالك الشرعي لها. هذا الإذن هو ما يفصل بين "هاكر أخلاقي" و "مجرم إلكتروني"

2. حدود المسؤولية القانونية (Legal Boundaries):

حتى مع وجود الإذن، هناك حدود لا يمكن تجاوزها. يجب أن يحدد الإذن نطاق العمل بدقة (مثلاً: عناوين IP، التطبيقات، الفترات الزمنية). يجب على الفريق الالتزام بالقوانين المحلية والدولية مثل قوانين حماية البيانات والخصوصية

3. معايير سرية البيانات (Data Confidentiality):

أثناء الاختبار، قد يصادف الفريق بيانات حساسة (معلومات شخصية، مالية، إلخ). يجب حماية هذه البيانات بكل الوسائل، وعدم الإفصاح عنها لأي طرف، وتخزينها بطريقة مشفرة، وتدميرها بشكل آمن بعد انتهاء المشروع

2.8.2 الضوابط المهنية:

1. اتباع أطار العمل المعتمد (Following Approved Frameworks):

العمل وفق منهجيات معيارية مثل PTES (Penetration Testing Execution Standard) أو OSSTMM (The Open Source Security Testing Methodology Manual). هذا يضمن شمولية ودقة الاختبار، ويوفر إطارًا للمقارنة وإعادة الاختبار

2. توثيق النتائج بدقة (Documenting Findings Accurately):

يجب أن يكون التقرير النهائي دقيقًا وواضحًا وخاليًا من المبالغة. كل ثغرة يجب أن تكون قابلة لإعادة الإنتاج من قبل فريق العميل. التوثيق الجيد يساعد في فهم المشكلة وأولويات معالجتها

3. الإبلاغ المسؤول عن الثغرات (Responsible Vulnerability Disclosure):

في حالة اكتشاف ثغرات حساسة جدًا (مثل ثغرات في البنية التحتية الحيوية)، يجب إبلاغها بطريقة مسؤولة تضمن للمنظمة وقتًا كافيًا لإصلاحها قبل أي إعلان عام، مما يمنع استغلالها من قبل جهات ضارة

9.2 الأدوار في المنصة (Roles on the platform) :

- **محاكاة هجمات واقعية:** باستخدام أدوات وتقنيات مشابهة لتلك المستخدمة من قبل المهاجمين الفعليين وذالك لحث المستخدمين على مقدار الخسائر التي قد توجههم والتي قد تؤدي الى تشويه سمعتهم امام الشركات الأخرى
- **اختبار القدرات الدفاعية للأنظمة والمواقع والاجهزة:** في هذه الحالة سيتعرف مستخدمين هاذة المنصه مقدار الدفاعات التي ستمنع التخريب والدفاعات القوية هي ماتطلبة اي شركة او اي موقع او اي جهاز فلا يوجد هناك أحد يريد ان تكون دفعاته ضعيفة او قابله للكسر امام من يريد التخريب والمس بالأذى
- **تقييم الثغرات في الجانب التقني:** وهو سيكون اخر ماتقدمة المنصة للمستخدمين وذلك لكي تقوم الجهات المعنية باخذ احتياطاتهم اللازمة بعد ان يتم إعطائهم تقرير بثغراتهم ومشاكلهم ليعملوا على حلها
- **التمييز عن اختبار الاختراق التقليدي:** تتميز منصة الفريق الأحمر بواجهات رسومية، حيث ان المستخدم يتعامل مع واجهات رسومية بدلا عن التعامل مع اكواد برمجية فالتعامل مع واجهات رسومية سيكون أفضل بكثير من التعامل البرمجي او بالاخص التعامل مع اكواد تحتاج الى استخدام فائق الحذر لانة إذا اخطاء الشخص الذي يتعامل مع اكواد قد ربما يتسبب في مشاكل لايعرف حلها او التعامل معها

10.2 منهجية عمل منصة الفريق الأحمر:

(Red Team Platform Work Methodology) :

- **التخطيط والتقصي :** جمع المعلومات حول الثغرات والبورتات المفتوحة ومعرفة ماهي الطرق التي ستسمح للمهاجم في استغلالها والدخول من خلالها ليقوم بعملية التخريب او سرقة البيانات وهو امر غير وارد ان يتم تقبله من قبل المستخدمين او الشركات
- **الهجوم الأولي :** استغلال الثغرات للدخول إلى الأنظمة ومعرفة الاباب المفتوحة التي ستسمح بالدخول من خلالها لكي يتم التعامل مع هذه الابواب وسدها اما من يريد التخريب او التسبب في المشاكل
- **التصعيد والانتشار :** التحرك أفقيًا داخل الشبكة ورفع الصلاحيات وهذا يعني ان المكان الذي قد يرغب المهاجم في استغلاله اولآ هي الإدارة العليا التي تتحكم في زمام الامور داخل الشركة او الموقع او النظام

- **البقاء والاستمرارية :** إنشاء قنوات خفية للوصول المستمر ويحدث هذا عاده لتكوين ابواب وثغرات سرية تمكن المهاجم من الدخول من خلالها عدة مرات ومتى ما يشاء فالشركات لأتقبل ان تواجه عقبات مستمرة، بل تحاول التخلص من تلك العقبات نهائياً لضمان امانها وامان بياناتها
- **التقارير والتحسين :** تقديم تقارير مفصلة لتطوير الدفاعات وهذا ماهو متوقع من المنصه بعد كل عملية فحص هو إعطاء مستخدميها تقارير مفصله عن نتائج فحصهم ومن خلال هذة التقارير سيكونون على علم بما قد يوجههم من صعوبات إذا لم يتعاملوا مع ما قد يجدوه في التقارير

11.2 الأدوات الأمنية المستخدمة (Security Tools Used) :

- **Nmap :** مسح الشبكات
- **OWASP ZAP:** اختبار الويب
- **SQLmap :** ثغرات قواعد البيانات
- **Metasploit:** تنفيذ الهجمات وتحليلها
- **Nikto :** لفحص خوادم الويب

12.2 الخلاصة (Conclusion) :

يؤسس هذا الفصل القاعدة النظرية والعملية لمشروع المنصة. من خلال استعراض المفاهيم الأساسية، والمنهجيات القياسية، والأدوات المتخصصة، وتحليل الحلول الحالية، أصبح من الواضح أن هناك حاجة ماسة لحل متكامل وبسيط لأتمتة اختبارات الاختراق. ستعمل المنصة المقترحة على سد الفجوة بين قوة الأدوات مفتوحة المصدر وتعقيد استخدامها، من خلال تقديم واجهة موحدة تدمجها في سيرعمل آلي الفصول القادمة ستبنى على هذا الإطار لتقديم التصميم التفصيلي والتنفيذ العملي للمنصة

الفصل الثالث :

تحليل المتطلبات والنمذجة في الموقع

(Requirement Analysis and Modeling in web)

1.3 المُقدمة :

تُعد مرحلة تحليل المتطلبات والنمذجة من أهم المراحل في دورة حياة تطوير الأنظمة، إذ تُسهم في بناء فهم عميق لما يحتاجه المستخدمون النهائيون وما يسعى النظام لتحقيقه. بالنسبة لمنصة Red Team، فإن هذه المرحلة تكتسب أهمية مضاعفة نظرًا لطبيعة عملها في مجال الأمن السيبراني، حيث أن أي خطأ في تحديد المتطلبات قد يؤدي إلى فجوات أمنية أو إلى نظام غير قادر على تلبية احتياجات مستخدميه يركز هذا الفصل على تحديد المتطلبات الوظيفية وغير الوظيفية، دراسة أصحاب المصلحة وتوضيح دور كل منهم، إضافة إلى نمذجة النظام باستخدام عدة تقنيات مثل مخططات حالات الاستخدام (Use Case)، مخططات الأنشطة (Activity Diagrams)، مخططات تدفق البيانات (DFD)، ومخطط الكيانات والعلاقات (ERD). كما يتضمن الفصل مناقشة للقيود والتحديات التي قد تواجه عملية التحليل والنمذجة، مع إبراز كيفية تجاوزها.

2.3 المتطلبات الوظيفية (Job Requirements) :

المتطلبات الوظيفية هي مجموعة من الخصائص والخدمات التي يجب أن يقدمها النظام للمستخدمين.

فيما يلي تفصيل لأهم المتطلبات الوظيفية لمنصة Red Team :

1. تسجيل الدخول والخروج للمستخدمين:

الهدف: ضمان وصول المستخدمين المصرح لهم فقط.

التفاصيل: دعم تسجيل الدخول باستخدام كلمات مرور قوية أو التحقق الثنائي.

2. إدارة حسابات المستخدمين:

الهدف: تمكين مدير النظام من إضافة، تعديل، أو حذف المستخدمين

التفاصيل: تخصيص أدوار وصلاحيات مختلفة لكل نوع مستخدم.

3. إدارة سيناريوهات الهجوم:

الهدف: توفير بيئة لتنفيذ اختبارات مختلفة على الأنظمة.

التفاصيل: إنشاء سيناريو جديد، تحديد الأدوات، تنفيذ، متابعة النتائج.

4. إنشاء التقارير:

الهدف: تقديم مخرجات عملية الاختبار بشكل احترافي.

التفاصيل: التقارير تشمل الثغرات المكتشفة، تقييم الخطورة، والتوصيات

5. التواصل بين أعضاء الفريق:

الهدف: تمكين أعضاء الفريق من التعاون في الوقت الفعلي.

التفاصيل: عبر لوحة تحكم أو نظام رسائل داخلية.

6. حفظ السجلات (Logs):

الهدف: توفير شفافية ومتابعة دقيقة للأنشطة.

التفاصيل: تسجيل الدخول والخروج، محاولات الاختراق، إنشاء التقارير

7. التكامل مع الأنظمة الخارجية:

الهدف: زيادة كفاءة المنصة وإثراء البيانات من خلال الربط مع أدوات الامن الأخرى

التفاصيل: التكامل مع منصات إدارة الثغرات لاستيراد نتائج المسح الضوئي واستخدامها في تخطيط الهجوم

3.3 المتطلبات غير الوظيفية (Non-functional requirements):

المتطلبات غير الوظيفية تحدد المعايير التي يجب أن يلتزم بها النظام لضمان جودته، وتشمل الجوانب المتعلقة بالأداء، الأمان، وسهولة الاستخدام:

1. الأمان:

- ضرورة تشفير جميع البيانات الحساسة.
- الالتزام بمعايير أمنية مثل OWASP Top 10.

2. الأداء:

- يجب أن تكون استجابة النظام أقل من 3 ثوانٍ لكل عملية أساسية.
- دعم تنفيذ اختبارات متزامنة دون التأثير على الكفاءة.

3. التوافر:

- المنصة يجب أن تكون متاحة 7/24.
- وجود خطط للتعافي من الكوارث (Disaster Recovery)

4. القابلية للتوسع:

- إمكانية إضافة مستخدمين جدد ومشاريع جديدة بسهولة.
- دعم التوسع في البنية التحتية عند الحاجة.

5. سهولة الاستخدام:

- واجهة بسيطة وواضحة حتى لغير المتخصصين.
- دعم لغات متعددة لتوسيع قاعدة المستخدمين

4.3 دراسة اصحاب المصلحة (Stakeholder study) :

تتضمن عملية تحليل المتطلبات دراسة شاملة لأصحاب المصلحة المرتبطين بالنظام. فيما يلي أهم الفئات:

- أعضاء فريق Red Team: ينفذون الهجمات ويحللون النتائج وهم الاشخاص الذين يكون لهم صلاحيات محدودة
- العملاء (Clients): يتابعون تقارير الأمن الخاصة بأنظمتهم ويعتبرون ايضا الاشخاص المستفيدين

1.3 جدول يوضح دور وصلاحيات كل فئة من أصحاب المصلحة :

هنا توضيح لكل من المدير وأعضاء الفريق وكذلك العملاء والصلاحيات لكل منهم يتم توضيحها في هذا الجدول :

2.3 جدول أعضاء الفريق والعملاء والصلاحيات

الفئة	الدور	الصلاحيات
مدير النظام	الإشراف على النظام	إضافة او حذف المستخدمين وإدارة البيانات
اعضاء الفريق	تنفيذ الإختبارات	إنشاء سيناريوهات وتوليد تقارير
العملاء	الإطلاع على النتائج	استعراض التقارير ومتابعة الحالة الأمنية

5.3 جمع المعلومات (Information collection):

في إطار دراسة الأنظمة الأمنية الحديثة تبرز منصة الفريق الأحمر كأدوات متقدمة لمحاكاة الهجمات السيبرانية بغرض اكتشاف نقاط الضعف وتعزيز الحماية:

جمع المعلومات: مشروع منصة الفريق الأحمر (Red Team Platform)

الهدف الأساسي من المشروع: يهدف المشروع إلى تطوير منصة برمجية موحدة وأتمتة عمليات الفريق الأحمر

(Red Team Operations) لمحاكاة هجمات إلكترونية واقعية وقابلة للقياس، وذلك بهدف:

- اختبار فعالية الضوابط الأمنية الحالية
- تقييم قدرة فرق الدفاع (الفريق الأزرق) على الكشف والاستجابة للتهديدات
- تحديد نقاط الضعف في البنية التحتية والتطبيقات والعمليات قبل أن يستغلها مهاجمون حقيقيون
- توفير مقاييس (Metrics) وبيانات قابلة للقياس حول وضع الأمن السيبراني للمنظمة

6.3 مجموعة البيانات ومتطلباتها (Dataset Requirements):

لضمان دقة وفعالية نماذج الذكاء الاصطناعي والتحليل داخل المنصة، تم تحديد متطلبات مجموعة البيانات المستخدمة في تطوير واختبار النظام كما يلي:

مصادر البيانات: سيتم استخدام عينات من قواعد بيانات عامة معروفة مثل Virus Total وVirus Share للحصول على عينات برمجيات خبيثة متنوعة سيتم جمع عينات سليمة (Benign ware) من أنظمة نظيفة وموثوقة ومكتبات برامج قانونية

حجم البيانات والتوازن: ستتألف مجموعة البيانات مما لا يقل عن 10,000 عينة، موزعة بنسبة 60% عينات خبيثة و40% عينات سليمة لتحقيق توازن معقول يمنع التحيز في النماذج

تقسيم البيانات: سيتم تقسيم البيانات عشوائياً إلى ثلاث مجموعات:

- 70% مجموعة التدريب (Training Set) لبناء النماذج.
- 15% مجموعة التحقق (Validation Set) لضبط معايير النماذج أثناء التدريب.
- 15% مجموعة الاختبار (Test Set) لتقييم الأداء النهائي للنماذج بعد اكتمال التدريب

7.3 نمذجة النظام (system modeling):

تمثل نمذجة النظام الهيكل الأساسي الذي يحدد كيفية عمل المنصة وتفاعل مكوناتها معاً لتحقيق الأهداف المطلوبة. تعتمد النمذجة على تقسيم النظام إلى وحدات متخصصة مترابطة، لكل منها وظيفة محددة تساهم في تحقيق الغاية النهائية للمنصة

المكونات الأساسية للنموذج:

1. وحدة إدارة المستخدمين والصلاحيات

- مسؤولة عن التحكم في الوصول وتحديد أدوار المستخدمين
- تضمن فصل المهام بين فرق الأحمر والأزرق والإدارة

2. وحدة إدارة الحملات الهجومية

- تنظيم وتخطيط وتنفيذ حملات المحاكاة
- تحديد النطاق والأهداف والجداول الزمنية

3. وحدة المحاكاة والتشغيل

- تنفيذ السيناريوهات الهجومية باستخدام تقنيات MITRE ATT&CK
- إدارة البنية التحتية للتشغيل وأدوات القيادة والتحكم

4. وحدة المراقبة والتقارير

- تتبع الأنشطة وجمع البيانات والنتائج
- توليد التقارير التحليلية ومقاييس الأداء

العلاقات بين المكونات: تعمل هذه الوحدات بشكل متكامل حيث تبدأ دورة العمل بتخطيط الحملة، ثم تنفيذ عمليات المحاكاة، فمراقبة النتائج، وانتهاءً بإصدار التقارير التي تغذي عملية التحسين المستمر

8.3 تنفيذ النظام (system implementation):

في مواجهة تهديدات إلكترونية لا ترحم، لم يعد الدفاع التفاعلي كافياً. نحتاج إلى تبني استباقية حقيقية. تنفيذ نظام Red Team متكامل ليس رفاهية، بل هو استثمار حيوي في مناعتنا الرقمية. إنه بمثابة وضع مؤسستنا تحت المجهر قبل أن يفعل الخصوم ذلك الهدف الأساسي ليس مجرد اختبار الاختراق تقليدي، بل هو محاكاة سيناريوهات هجومية واقعية وشاملة. نريد الإجابة على سؤال واحد محوري: كيف ستصمد دفاعاتنا وعملياتنا أمام هجوم منظم وهادئ من خصم مصرّ على النجاح وتنفيذ النظام يمثل المرحلة العملية الحيوية التي تترجم فيها الاستراجيات الأمنية النظرية الى هجمات افتراضية واقعية بهدف اختبار قدرة الأنظمة على مواجهة التهديدات السيبرانية الفعلية مراحل التنفيذ الأساسية:

1. التجهيز والبنية التحتية

- إعداد بيئة التطوير والاختبار
- تثبيت قواعد البيانات وأنظمة الإدارة
- تأمين الخوادم والشبكات

2. تطوير الوحدات الأساسية

- بناء نظام إدارة المستخدمين والصلاحيات
- تطوير وحدات إدارة الحملات والمهام
- برمجة واجهات المستخدم الرئيسية

3. تكامل المكونات والاختبار

- ربط الوحدات مع بعضها البعض
- اختبار السلامة والأداء
- التحقق من تحقيق المتطلبات

4. النشر والتشغيل

- نقل النظام إلى بيئة الإنتاج
- تدريب المستخدمين على التشغيل
- متابعة الأداء والصيانة

5. مرحلة التحليل وإعداد التقارير

هذه هي المرحلة الأهم لا نكتفي بتسليم قائمة بالثغرات. نقدم تقريراً سردياً يروي قصة الهجوم من البداية إلى النهاية، موضحين نقاط الضعف الرئيسية، سلسلة الاختراق، والأثر العملي على الأعمال نركز على لماذا حدث هذا و كيف يمكن منعه، وليس فقط على ماذا حدث

6. مرحلة إعادة الاختبار والإغلاق

نعمل كشريك مع فرق الدفاع (Blue Team) وفرق المعالجة لضمان إصلاح الثغرات بشكل صحيح. ثم نعيد اختبار المناطق التي تم إصلاحها للتأكد من أن النظام أصبح آمناً حقاً

التقنيات المستخدمة في التنفيذ: يعتمد التنفيذ على تقنيات حديثة مثل Python وJavaScript لإدارة الواجهات والعمليات، وقواعد البيانات العلائقية للتخزين الآمن، وتقنيات الحاويات لتسهيل النشر والإدارة

9.3 وصف سير العمل (Workflow Description):

يبدأ سير العمل بتسجيل الدخول، ثم ينتقل كل مستخدم إلى لوحة التحكم الخاصة به وفقًا لصلاحياته. مدير النظام يشرف على الحسابات، عضو الفريق ينفذ الاختبارات، والعميل يستعرض التقارير. هذا التدفق يضمن وضوحًا وتنظيمًا في أداء المهام يمكن تقسيم سير العمل إلى 6 مراحل أساسية:

1. مرحلة التحضير (Preparation)

- تحديد الأهداف ونطاق الاختبار
- إعداد بيئة العمل وأذونات التنفيذ
- تعريف الأدوار (قائد الفريق، مختبر الاختراق، محلل البيانات، كاتب التقرير)

2. مرحلة جمع المعلومات (Reconnaissance)

- جمع معلومات عن الأهداف (نطاقات، IPs، خدمات، تقنيات).
- توثيق النتائج في المنصة
- يمكن ربط أدوات مثل Shodan, Malte go, Recon-ng.

3. مرحلة التسلل (Exploitation)

- تنفيذ سيناريوهات الهجوم المخطط لها.
- تسجيل الأدوات المستخدمة (Metasploit, Cobalt Strike, custom scripts).
- مراقبة النتائج في الوقت الفعلي عبر لوحة تحكم.

4. مرحلة ما بعد الاختراق (Post-Exploitation)

- تثبيت الوصول (Persistence).
- جمع البيانات الحساسة
- اختبار الانتقال الأفقي (Lateral Movement)

5. مرحلة التقييم والتوثيق (Reporting)

إنشاء تقارير تلقائية تشمل:

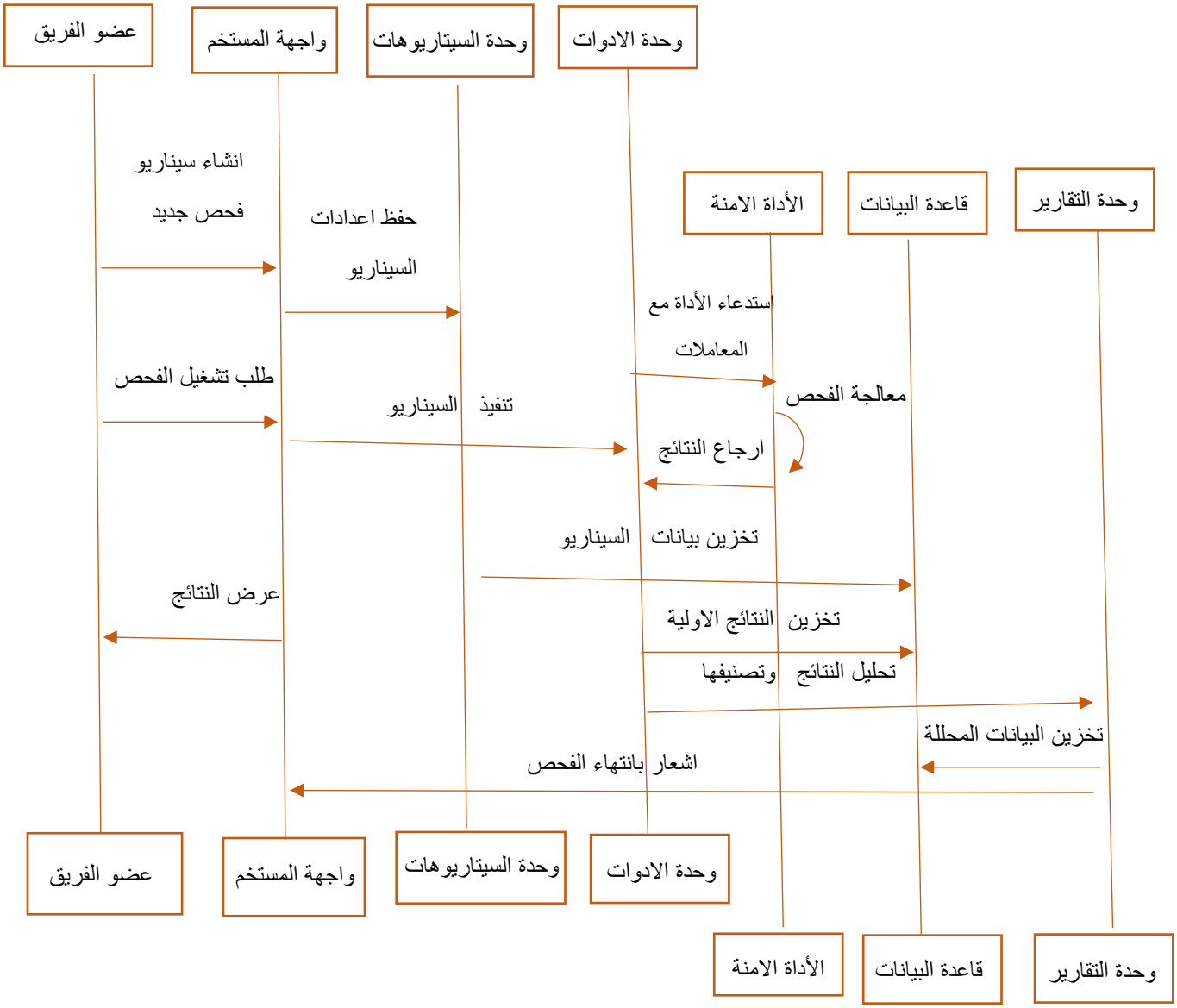
- الثغرات المكتشفة
- مستوى الخطورة
- الأدلة (Evidence)
- توصيات الفريق الأحمر

6. مرحلة المراجعة (Review & Lessons Learned)

- مراجعة النتائج مع الفريق الأزرق (Blue Team)
- تحديد نقاط التحسين في الدفاع والهجوم.
- حفظ التقارير النهائية في قاعدة بيانات المنصة

1.3 مخطط الية التنفيذ يوضح كيفية سير العمل داخل منصة (Red Team Platform) :

في عالم الامن السيبراني تمثل عمليات الفريق الأحمر محاكاة واقعية لهجمات القراصنة بهدف اختبار وتقييم قدرات الدفاع لدى المنظمة يتم استخدام منصة الفريق الأحمر لإدراتها تعتبر وحدة سير العمل العمود الفقري لهذة المنصة حيث يقوم بتنظيم وتنسيق وتنفيذ سلسلة المهام المطلوبة خلال عملية المحاكاة بداءً من التخطيط وصولاً الى اعداد التقارير وهذا المخطط يوضح كيفية تنفيذ وحدة سير العمل:



شكل (1.3): الية التنفيذ

توضيح للمخطط تبدأ رحلة الفحص الأمني عندما ينشئ عضو الفريق سيناريو جديداً عبر الواجهة، ليتم حفظ إعداداته في قاعدة البيانات. عند التشغيل، تنتقل الأوامر إلى وحدة الأدوات التي تستدعي الأداة الأمنية المناسبة مع كل المعلمات المطلوبة تنفذ الأداة الفحص وتعيد النتائج الأولية التي يتم معالجتها وتحليلها تلقائياً من قبل وحدة التقارير. تنتهي الرحلة بإشعار المستخدم وعرض النتائج النهائية المحللة. يتميز هذا التصميم بفصل المهام والتخزين المزدوج للبيانات، مما يضمن كفاءة عالية وتوثيقاً كاملاً للعملية

10.3 تقييم الأداء (Performance Evaluation):

لتقييم دقة وكفاءة النظام والتحقق من تحقيقه للأهداف المطلوبة، سيتم اعتماد المقاييس والمنهجيات التالية:

مقاييس التقييم الكمية:

- **الدقة (Accuracy):** نسبة التصنيفات الصحيحة بشكل عام.
- **الدقة التنبؤية (Precision):** نسبة العينات التي تم تصنيفها كخبيثة وهي خبيثة فعلياً.
- **الاستدعاء (Recall):** نسبة العينات الخبيثة التي تم التعرف عليها correctly.
- **مقياس F1 (F1-Score) :** متوسط توافقي بين الدقة التنبؤية والاستدعاء.
- **معدل الإيجابيات الكاذبة (False Positive Rate):** نسبة العينات السليمة التي تم تصنيفها خطأً كخبيثة.
- **منهجية التقييم :**سيتم استخدام تقنية K-Fold Cross-Validation (بـ 5 أقسام) لضمان أن تقييم الأداء robust ولا يعتمد على تقسيم عشوائي واحد للبيانات.
- **الأهداف المستهدفة:** يستهدف النظام تحقيق دقة (Accuracy) لا تقل عن 98%، ومعدل استدعاء (Recall) لا يقل عن 95% للكشف عن البرمجيات الخبيثة، مع الحفاظ على معدل إيجابيات كاذبة (FPR) أقل من 2%

11.3 منهجية المشروع (Project Methodology) :

تمثل منهجية مشروع منصة الفريق الأحمر(Red Team Platform) الإطار المنظم الذي يحدد الخطوات العلمية والعملية لمحاكاة الهجمات السيبرانية بهدف تقييم شمولية وكفاءة الأنظمة الأمنية القائمة تعتمد هذه المنهجية على محاكاة واقعية لأساليب المهاجمين الفعليين مع الالتزام الكامل بالأطر الأخلاقية والقانونية

(الأهداف الاستراتيجية العليا):

1. قياس الفجوة بين النظرية والتطبيق: التحقق مما إذا كانت السياسات الأمنية والضوابط التقنية المطبقة على الورق، قادرة فعلياً على صد هجوم منظم

2. الانتقال من "اكتشاف الثغرات" إلى "تقدير الخطر": تقديم تحليل كمي ونوعي للمخاطر الحقيقية التي تتعرض لها الأصول الحرجة، مما يمكن الإدارة من اتخاذ قرارات استثمارية أذكى.

3. تطوير مناعة المؤسسة: بناء ذاكرة مناعية مؤسسية من خلال تدريب فرق الدفاع (Blue Team) وفرق الاستجابة للحوادث (CSIRT) تحت ضغط هجومات محاكاة واقعية.

4. التحقق من فعالية سلسلة الدفاع Depth-in-Defense: اختبار كل حلقة في السلسلة الدفاعية، بدءاً من وعي الموظفين، مروراً بالطبقات التقنية، ووصولاً إلى عمليات الاستجابة.

(المراحل المحورية للمنهجية):

المرحلة الصفرية: التأسيس والحوكمة

الإطار الحوكمي والأخلاقي:

صياغة "ميثاق شرف" واضح يحدد سلطات الفريق وحدوده.

إنشاء "لجنة توجيهية" من الإدارة العليا (C-Level) لمنح الشرعية والمشورة.

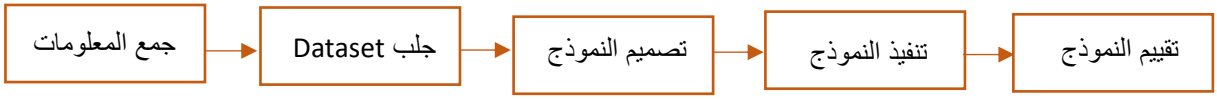
وضع آلية "خطاب الإذن الرسمي" لكل مهمة لتجنب التعارض مع القوانين أو تعطيل العمل.

تحديد السلة الحمراء (Red Teaming Scope):

تحديد الأصول الحرجة (التاج التاج) التي ستكون محور الاختبارات

12.3 مخطط مراحل منهجية المشروع (Project Methodology Stages Planner):

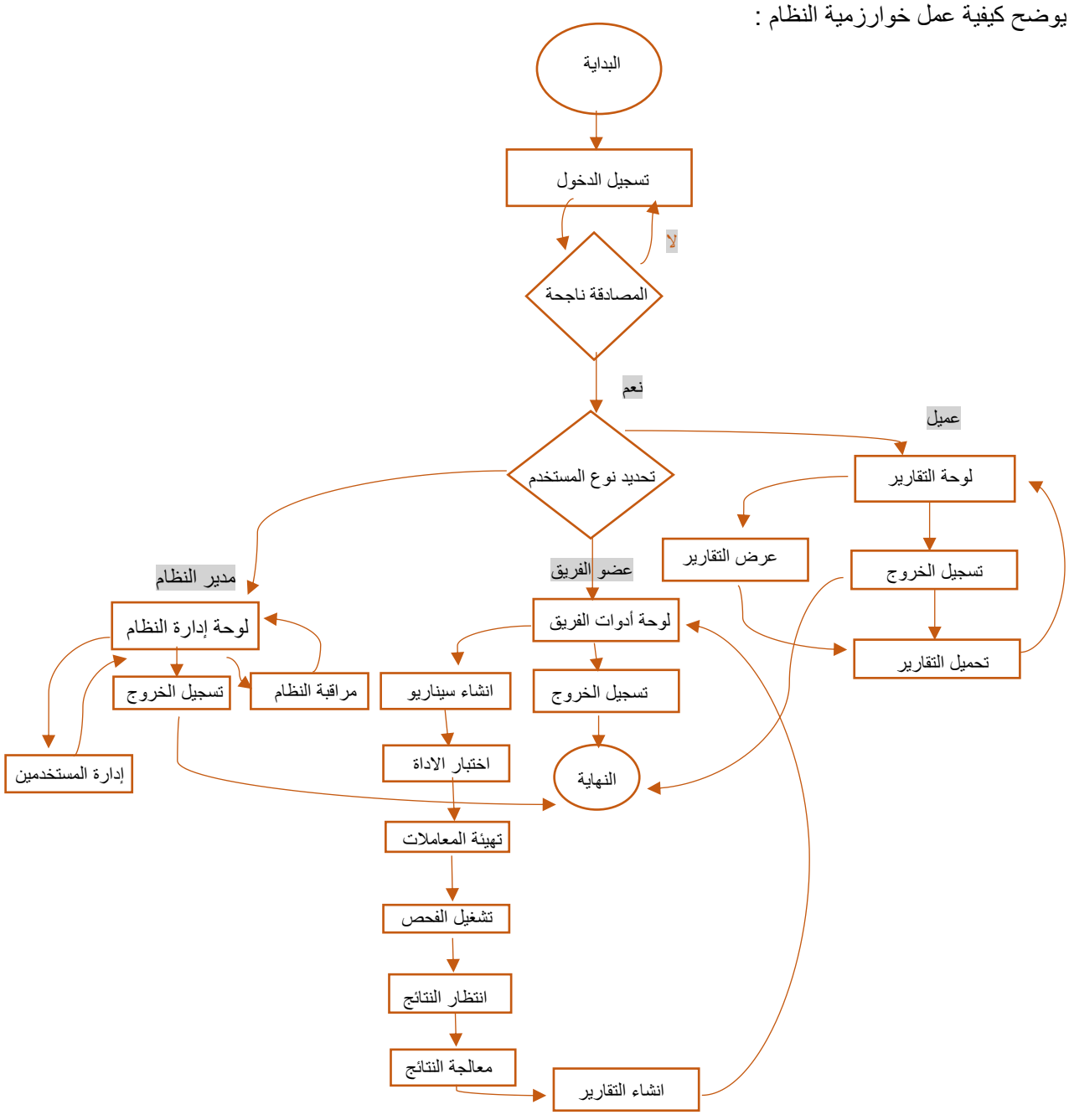
يهدف هذا المخطط الى توضيح المراحل الأساسية التي سيتم اتباعها لتطوير وإدارة مشروع منصة الفريق الأحمر وذلك وفق منهجية عمل واضحة منظمة يحدد المخطط التسلسل المنطقي للانشطة



شكل (2.3): منهجية النظام

13.3 مخطط خوارزمية النظام (System algorithm diagram) :

بينما تتعامل وحدة سير العمل مع تنظيم المهام فإن الخوارزمية الأساسية للمنصة هي التي تحكم كيف يتم تنفيذ هذه المهام واتخاذ القرارات إذا كانت المنصة هي الجسم فالخوارزميات هي العقل والجهاز العصبي الذي يتحكم في جميع العمليات الذكية وهذا مخطط يوضح كيفية عمل خوارزمية النظام :

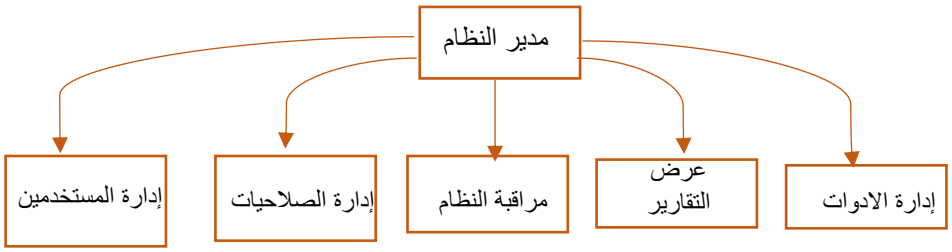


شكل (3.3): خوارزمية النظام

توضيح للمخطط يبدأ النظام برحلة دخول آمنة تشمل التسجيل والمصادقة، لينتقل بعدها كل مستخدم إلى مساره المحدد حسب صلاحياته. مدير النظام يتمتع بصلاحيات شاملة لإدارة المستخدمين ومراقبة الأداء. عضو الفريق يركز على التنفيذ العملي بدءاً من إنشاء السيناريو واختيار الأداة، وانتهاءً بتشغيل الفحص واستلام التقارير. بينما يقتصر دور العميل على عرض التقارير النهائية ومتابعة الحالة الأمنية. ينتهي كل مسار بتسجيل خروج آمن يحافظ على سلامة النظام

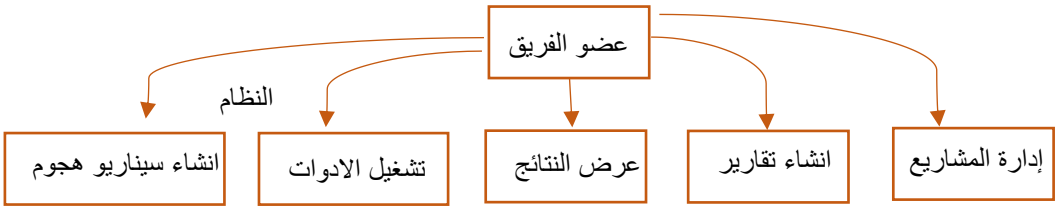
14.3 مخطط أداة (Sandbox) وتهيئتها (graph TD):

في عمليات الفريق الأحمر يحتاج المحللون الى اختبار البرمجيات الخبيثة (Malware) وتقنيات الاختراق بشكل آمن دون الإضرار بالبيئة الحقيقية للمنظمة تأتي أهمية أداة الساندبوكس وهذا مخطط يوضح عمل ومدى الصلاحيات:



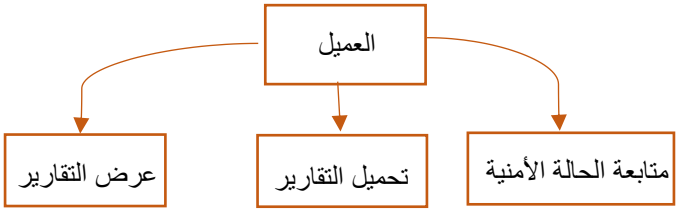
يُعد هذا المُخطط الهيكل التشغيلي المُتكامل لإدارة المنظومة التقنية حيث يتكامل **مدير النظام** لوضع الاستراتيجيات مع إدارة الأدوات لضمان كفاءة الموارد وعرض التقارير لشفافية الأداء ومراقبة النظام للكشف الاستباقي للاخطاء وإدارة الصلاحيات والمُستخدمين لتحقيق اعلى مستويات الأمان والتحكم يمثل الرباعي محور استقرار أي بيئة رقمية

شكل (4.3): مدير النظام



يُعد هذا المُخطط دور **عضو الفريق** المحوري في خط الدفاع الهجومي حيث يجمع بين التخطيط الاستراتيجي عبر إدارة المشاريع والتنفيذ العملي عبر تشغيل الأدوات وإنشاء سيناريو الهجوم وصولا الى مرحلة التحليل والتقييم من خلال انشاء التقارير وعرض النتائج ليضمن فريقا هجوميا منهجا وفعالا

شكل (5.3): عضو الفريق



يُعد هذا المُخطط واجهة **العميل** الأساسية لمتابعة المنظومة الأمنية حيث تبداء رحلته بمتابعة الحالة الأمنية آنيا ،ليمر بعد ذلك بعرض التقارير التفصيلية لفهم الوضع لفهم الوضع ثم تحميلها للاحتفاظ بنسخ محلية أو لاستخدامها في التدقيق والمراجعة ليكون بذلك على اطلاع كامل دون الحاجة للتدخل في التفاصيل التقنية

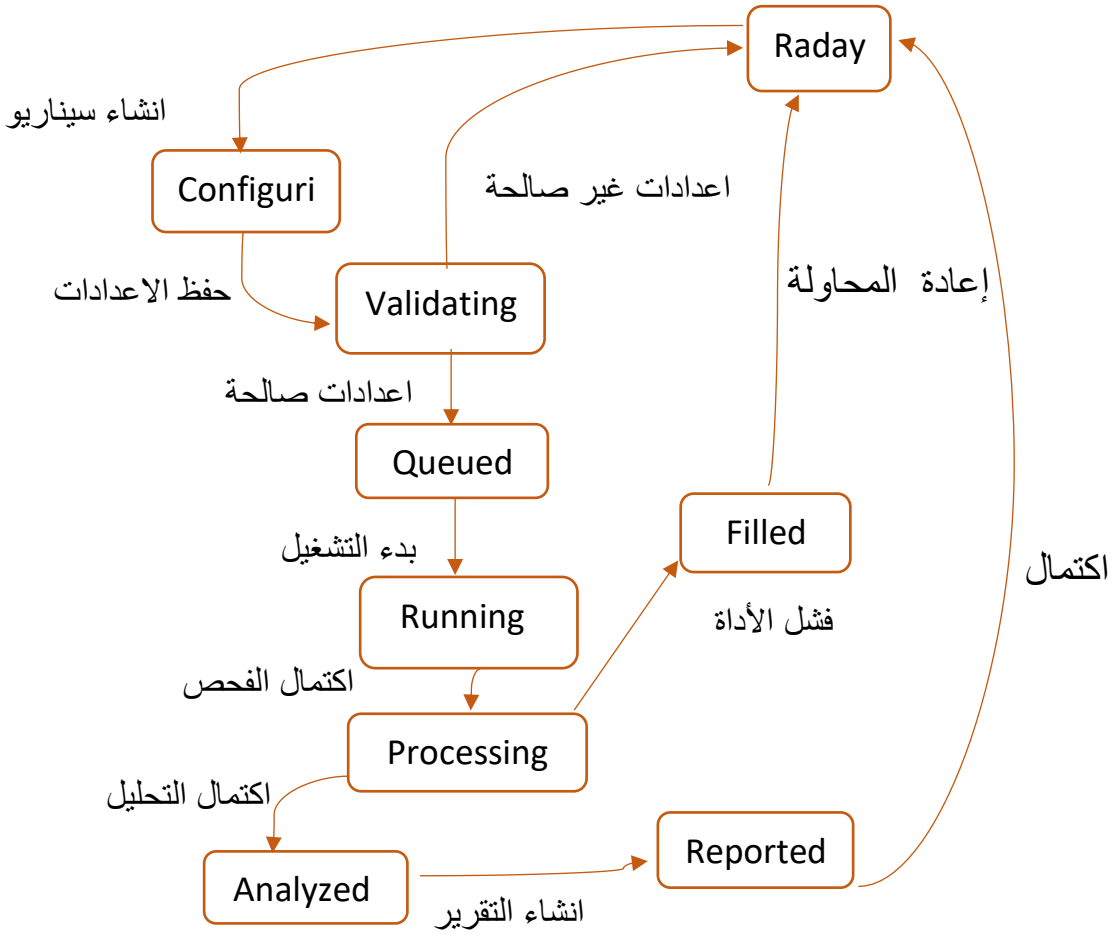
شكل (6.3): العميل

توضيح للمخطط يقسم النظام مستخدميه إلى ثلاث فئات ذات صلاحيات متدرجة. مدير النظام يمتلك الصلاحيات المطلقة للإدارة والمراقبة والتحكم الكامل. عضو الفريق يتركز دوره على الجانب التنفيذي من إنشاء السيناريوهات وتشغيل الأدوات وإنشاء التقارير. بينما يتمتع العميل بصلاحيات محدودة للعرض والمتابعة فقط. يعتمد هذا التصميم على مبادئ أمنية راسخة مثل فصل المهام ومبدأ أقل صلاحية، مما يجعله مثالياً لأنظمة الأمن السيبراني واختبارات الاختراق

15.3 مخطط النماذج والخوارزميات المستخدمة ومخطط الحالات لعملية الفحص:

(State Diagram):

تعتبر عملية الفحص احدى المراحل الحاسمة لاكتشاف نقاط الضعف والثغرات في الأنظمة المستهدفة لضمان كفاءة ودقة هذه العملية يتم استخدام نموذج مخطط الحالات لتمثيل الحالات المختلفة وهذا المخطط يوضح كيفية عمل مخطط (State Diagram):

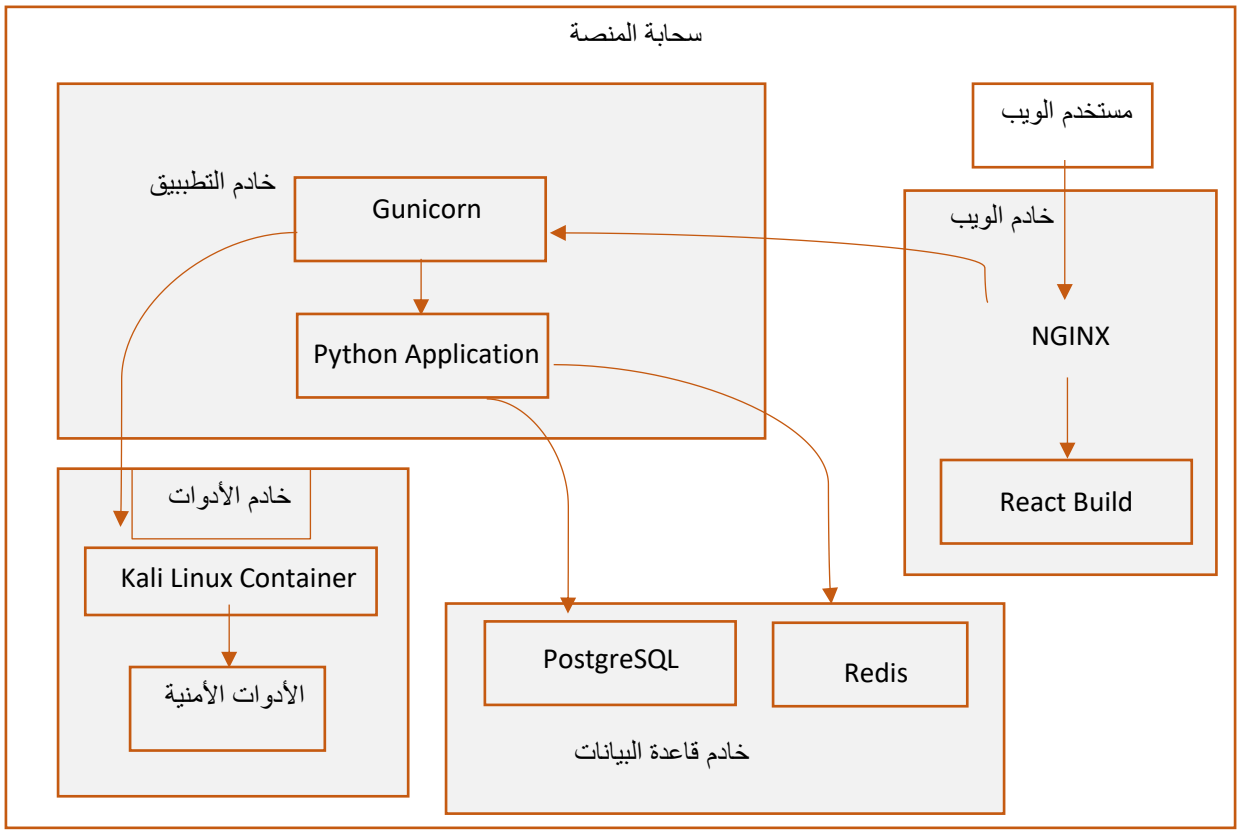


شكل (7.3):عمليات الفحص

توضيح للمخطط تمر عملية الفحص بمراحل متسلسلة تبدأ من التحضير والإعداد، مروراً بالتحقق من الصلاحية والانتظار في الطابور، ثم مرحلة التنفيذ الفعلي. تنتقل العملية بعدها إلى المعالجة والتحليل، وانتهاءً بالتقرير النهائي يتميز التصميم بمرونة التعامل مع الأخطاء، حيث أن فشل أي أداة لا يعطل النظام بالكامل، بل يسمح بإعادة المحاولة بعد التصحيح كما يضمن التصميم متابعة دقيقة لكل مرحلة وإدارة فعالة للأحمال عبر نظام الطابور

16.3 مخطط منهجية الاختبار والتحقق مخطط التوزيع (Deployment Diagram):

لضمان فعالية وسلامة عمليات الفريق الأحمر لايكفي فقط بناء المنصة وتشغيلها، بل يجب اتباع منهجية للاختبار والتحقق من كل مكوناتها مع تصميم هيكل توزيع مناسب توضيح كيفية منهجية الاختبار والتحقق في المخطط التالي:



شكل (8.3): منهجية الاختبار

توضيح للمخطط تم بناء المنصة على هيكل طبقي واضح يجمع بين القوة والأمان. تعتمد واجهة المستخدم على تقنية React مع خادم NGINX لضمان تجربة سلسة. يعمل التطبيق الأساسي على خادم Gunicron بلغة Python، بينما تدعم قاعدة البيانات PostgreSQL التخزين الموثوق، ويدعم Redis التخزين المؤقت. تكتمل الصورة بحاوية Kali Linux المنعزلة التي توفر بيئة آمنة للأدوات الأمنية. هذه البنية المرنة والقابلة للتوسع توفر حلاً مثالياً لمتطلبات الأمن السيبراني الحديث

17.3 الخلاصة (Conclusion) :

في هذا الفصل تم استعراض تفاصيل تحليل المتطلبات لمنصة Red Team مع تفصيل شامل للمتطلبات الوظيفية وغير الوظيفية، إضافة إلى دراسة أصحاب المصلحة. كما تم عرض نماذج تمثيلية للنظام عبر مخططات الاستخدام، الأنشطة، تدفق البيانات، والكيانات والعلاقات. تم التطرق إلى القيود والتحديات مع ربطها بأهمية النمذجة في مجال الأمن السيبراني. هذا الفصل يشكل قاعدة أساسية لفصل التصميم القادم الذي سيبنى على النتائج الموضحة هنا

الفصل الرابع :

تصميم المشروع

(Project design)

4.1 المُقدمة :

يهدف هذا الفصل إلى تقديم التصميم التفصيلي لمنصة الفريق الأحمر (Red Team Platform)، حيث يتم تحويل متطلبات النظام التي تم تحليلها في الفصل السابق إلى نموذج هندسي يوضح كيفية بناء النظام وتنفيذ وظائفه المختلفة. يتناول هذا الفصل البنية المعمارية للنظام، وتصميم قاعدة البيانات، وتصميم واجهات المستخدم، إضافة إلى آليات الأمان المعتمدة وآلية تكامل أدوات اختبار الاختراق داخل المنصة تم تصميم المنصة لتوفير بيئة متكاملة تساعد المختصين في الأمن السيبراني على تنفيذ عمليات اختبار الاختراق وتحليل النتائج ضمن نظام موحد يتميز بسهولة الاستخدام وكفاءة الأداء

4.1.1 خلفية نظرية عن تصميم أنظمة الأمن السيبراني:

تعتمد منصات اختبار الاختراق الحديثة على معماريات موزعة (Distributed Architectures) لضمان قابلية التوسع (Scalability) والأمان. وفقًا لأفضل الممارسات المتبعة في أنظمة مثل ARL (Asset Reconnaissance Layer) و Gophish، فإن فصل طبقات النظام (Separation of Concerns) يسمح بتحديث كل طبقة بشكل مستقل دون التأثير على الطبقات الأخرى. منصة الفريق الأحمر تتبع هذا المبدأ بشكل صارم من خلال تبني معمارية ثلاثية الطبقات (Tier Architecture-3)

4.1.2 مقارنة مع الأنظمة المشابهة:

لتحديد موقع منصة "الفريق الأحمر" وتمييزها في السوق، لا بد من إجراء مقارنة موضوعية مع أبرز المنصات المشابهة مثل ARL (Asset Reconnaissance Lighthouse) المتخصصة في استكشاف الأصول، وGophish المفتوحة المصدر لمحاكاة هجمات التصيد الاحتيالي، وOpenVAS القوية في فحص الثغرات الأمنية. بينما تتفوق هذه الأنظمة في مجالات محددة، إلا أنها غالباً ما تكون أحادية الوظيفة أو تعتمد على واجهات معقدة. تركز منصتنا على تقديم بيئة موحدة تدمج أدوات متعددة ضمن واجهة رسومية مبسطة، مما يمنح المستخدم تجربة متكاملة تجمع بين سهولة Gophish وشمولية OpenVAS وتركيز ARL على الأصول، ولكن بصيغة تعاونية موجهة لغير المتخصصين والفرق الصغيرة.

المنصة الميزات العيوب:

1.4 جدول ميزات وعيوب المنصات

اسم المنصة	الميزات والعيوب
ARL	مسح الأصول بشكل جيد، واجهة ويب لا يدعم Metasploit، محدود في الأدوات
Gophish	متخصص في هجمات التصيد (Phishing) لا يدعم فحص الشبكات أو الثغرات
OpenVAS	فحص ثغرات شامل واجهة معقدة، أداء بطيء

هنا تبرز منصة الفريق الأحمر (Red team platform) انها تدمج 5 أدوات رئيسية من خلال واجهة رسومية موحدة

4.1.3 أهداف الفصل التفصيلية :

يهدف هذا الفصل إلى تفصيل البنية التحتية لمنصة "الفريق الأحمر" من خلال توثيق البيئة المعمارية ثلاثية الطبقات (طبقة العرض، طبقة المنطق، طبقة البيانات)، حيث يضمن هذا الفصل فصل المهام وتسهيل الصيانة والتطوير المستقبلي. كما يتم عرض تصميم قاعدة البيانات التي تشكل العمود الفقري لتخزين المستخدمين،

السيناريوهات، والتقارير، مع شرح العلاقات بين الجداول. إن توثيق هذه العناصر بدقة يتيح لأي مطور آخر فهم النظام والمساهمة فيه أو تطويره بسهولة

1. توثيق البنية المعمارية ثلاثية الطبقات (3-Tier Architecture)

2. تصميم قاعدة بيانات علائقية متكاملة تشمل 6 جداول رئيسية على الأقل

3. تصميم واجهات مستخدم بديهية وآمنة (5 صفحات رئيسية)

4. وضع آليات أمان متعددة المستويات (تشفير، جلسات، حماية من الهجمات)

5. تحديد طريقة تكامل أدوات اختبار الاختراق الخمس (Nmap, SQLMap, Nikto, Metasploit, OWASP ZAP)

يتكون النظام من ثلاث طبقات رئيسية:

4.1.4 طبقة العرض (Presentation Layer):

تمثل طبقة العرض (Presentation Layer) الواجهة التي يتفاعل معها المستخدم النهائي بشكل مباشر، وهي الجسر الحسي بين قدرات المنصة التقنية واحتياجات المستخدمين من مختلف المستويات. صُممت هذه الطبقة في منصة "الفريق الأحمر" لتكون بديهية وموجهة بالخطوات، بحيث تمكن غير المتخصصين في الأمن السيبراني من تشغيل أدوات اختبار الاختراق المعقدة بنقرة زر واحدة، دون الحاجة لكتابة أوامر في سطر الأوامر (CLI). تعرض هذه الطبقة لوحات التحكم، نتائج الفحص، والتقارير بطريقة مرئية منظمة تعزز الفهم وتسرع من اتخاذ القرار.تمثل واجهة المستخدم التي يتم الوصول إليها عبر متصفح الويب، وتشمل:

- صفحة تسجيل الدخول (Login Page)
- صفحة إنشاء حساب (Registration Page)
- لوحة التحكم (Dashboard)
- صفحة تنفيذ الفحص الأمني (Scan Execution Page)
- صفحة عرض النتائج (Results Page)

تهدف هذه الطبقة إلى تسهيل تفاعل المستخدم مع النظام بطريقة واضحة وبسيطة

4.2.4 تقنيات طبقة العرض المستخدمة:

لتحقيق التوازن بين الأداء العالي وسهولة التطوير، تم بناء طبقة العرض في منصة "الفريق الأحمر" باستخدام مجموعة من تقنيات الويب الحديثة. اعتمدنا على HTML5 و CSS3 لإنشاء هيكل الصفحات وتصميمها الجذاب سريع الاستجابة، و JavaScript لإضافة التفاعلية والديناميكية. كما تم استخدام إطار العمل Vue.js لتطوير واجهة مستخدم أحادية الصفحة (SPA) تتيح تجربة سلسة وسريعة، مع إمكانية إعادة استخدام المكونات (Components)، مما يسهل صيانة الواجهة وتوسيعها مستقبلاً.

التقنية الإصدار الاستخدام

HTML5 - هيكل الصفحات الأساسي

CSS - التنسيق والتصميم

JavaScript - التفاعلات

تم نصميم المنصة باستخدام هذه اللغات أي صفحة تسجيل الدخول وكذلك الواجهات الامامية والخلفية

وقد تم دمج ملف JSON لربط الواجهة الامامية مع الواجهة الخلفية

4.2.5 آلية الاتصال مع الطبقة الوسطى (API endpoints):

تعتمد منصة "الفريق الأحمر" على آلية اتصال فعالة وآمنة بين طبقة العرض وطبقة المنطق (الطبقة الوسطى)، حيث يتم إرسال طلبات المستخدم (مثل بدء فحص ثغرة، أو تسجيل الدخول) عبر واجهات برمجية (APIs) باستخدام تقنية Ajax أو Fetch API بصيغة JSON. تقوم الطبقة الوسطى المبنية بـ Node.js و Python باستقبال هذه الطلبات، ومعالجتها (مثل استدعاء أدوات مثل Nmap أو Metasploit)، ثم إعادة النتيجة إلى الواجهة الأمامية بشكل فوري أو غير متزامن (Asynchronous) دون الحاجة لإعادة تحميل الصفحة، مما يضمن تجربة مستخدم سلسة واستجابة سريعة.

يتم الاتصال عبر طرق HTTP التالية بصيغة JSON:

الـ Endpoint الطريقة الوصف

POST/ api/login.php تسجيل الدخول

POST/ api/register.php إنشاء حساب جديد

GET/ api/scans.php جلب قائمة الفحوصات للمستخدم الحالي

POST/ api/scan/run.php تنفيذ فحص جديد

GET/ api/results.php?scan_id={id} جلب نتائج فحص محدد

GET/ api/scan/status.php?scan_id={id} جلب حالة فحص محدد (للتحديث غير المتزامن)

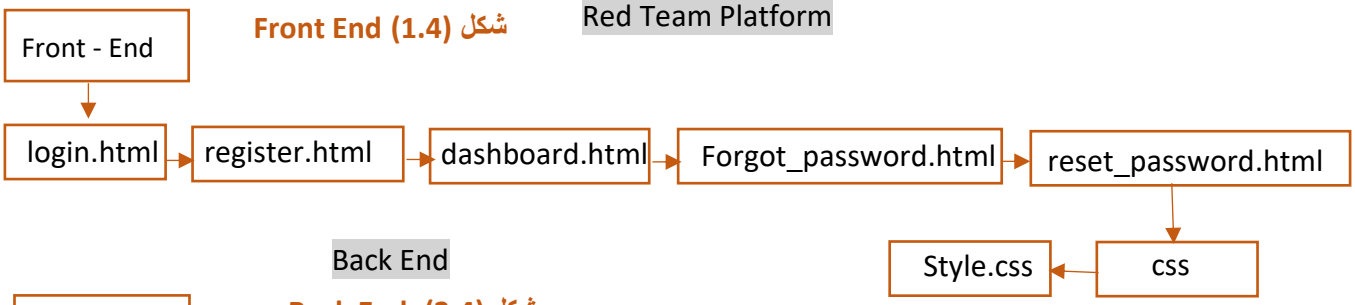
4.3 هيكل المشروع (project structure):

يُعد مشروع RedTeam نظاماً متكاملاً لإدارة وتنفيذ أدوات الاختراق الأخلاقي (Penetration Testing) واختبارات الاختراق وفق منهجية الفريق الأحمر (Red Teaming). يهدف النظام إلى توفير واجهة موحدة وآمنة للمختبرين الأمنيين لتنفيذ أدوات متخصصة مثل Nmap وSQLmap وNikto وMetasploit وZAP، مع تسجيل كامل للعمليات والإجراءات لضمان المساءلة والامتثال للمعايير الأمنية

وهذا مُخطط يوضح كيفية هيكل المشروع :

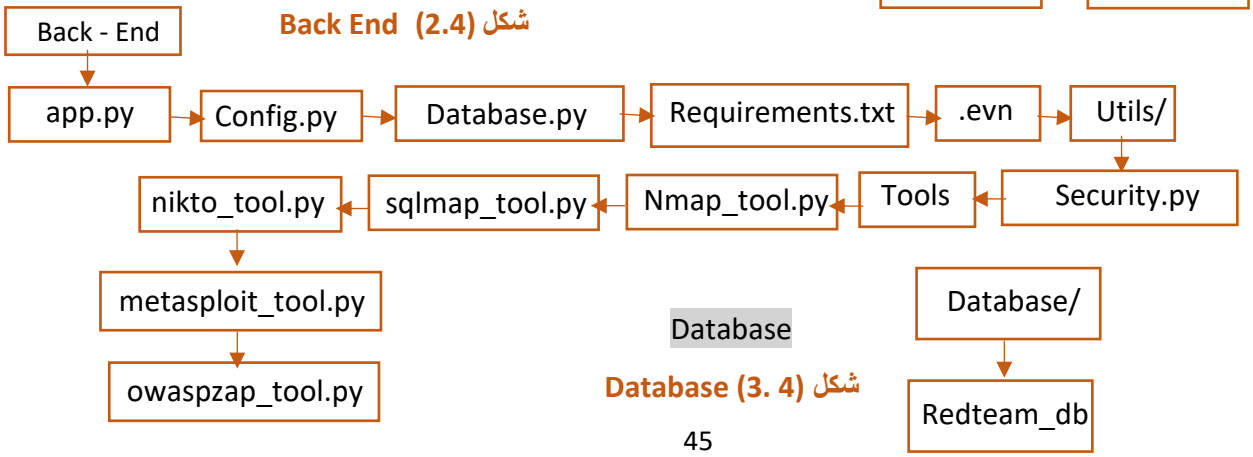
Front End

شكل (1.4) Front End



Back End

شكل (2.4) Back End



Database

شكل (3. 4) Database

4.4 هيكل قاعدة البيانات (database structure) :

يُعتمد نظام إدارة البيانات الفعال على هيكل متكامل يضمن تنظيم المعلومات وسهولة الوصول اليها مع الحفاظ على الأمان والكفاءة يتكون هذا الهيكل الأساسي من خمسة محاور رئيسية

وهذا الجدول يوضح كيفية عمل كل محور داخل قاعدة البيانات:

2.4 جدول هيكل قاعدة اليانات

Users	operations	reports	Security_logs	Password_reset_tokens
User_id	Op_id	Report_id	Log_id	Token_id
Email	User_id	User_id	User_id	User_id
Password	Tool_name	Report_name	Action	Token_hash
Created_at	Target	Report_path	Ip_address	Expires_at
Last_login	Parameteers	Report_data	User_agent	Created_at
Attempts	Output	Create_at	Created_at	
Locked_until	status			
	Created_at			

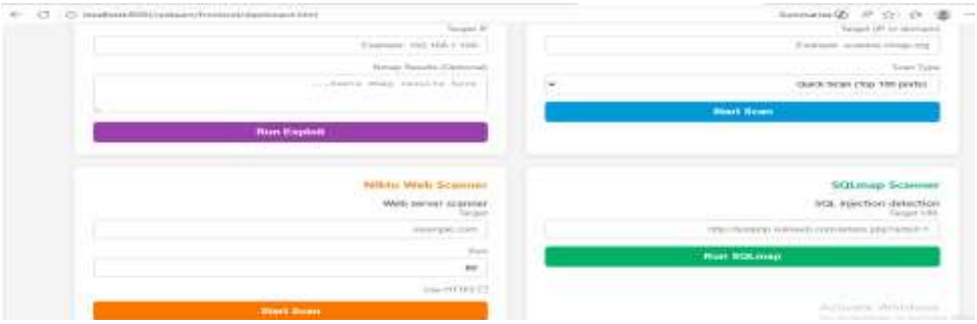
4.3 شرح واجهات منصة الفريق الأحمر (Red Team Platform):

تُمثل الواجهات الرسومية (GUI) حلقة الوصل الفعلية بين المستخدم وقدرات المنصة التقنية، فهي الوجه الذي يراه المستخدم ويتفاعل معه بشكل مباشر، والصورة الذهنية التي تُشكل انطباعه الأول عن جودة النظام وسهولته. في مشروع منصة "الفريق الأحمر"، تم تصميم الواجهات بعناية فائقة لتحقيق المعادلة الصعبة: تقديم أدوات اختبار اختراق احترافية ومعقدة (مثل Metasploit و Nmap و SQLmap) بشكل مبسط وموجه بالخطوات، بحيث يشعر المبتدئ بالأمان والمحترف بالكفاءة تعكس الواجهات المصممة فلسفة المشروع الأساسية: إضفاء الطابع الديمقراطي على أدوات الأمن السيبراني، أي جعلها في متناول غير المتخصصين دون تفريغها من محتواها التقني. فبدلاً من واجهات سطر الأوامر (CLI) المليئة بالمفاتيح والمعاملات، تقدم المنصة نماذج إدخال واضحة، وقوائم منسدلة، وأزراراً تفاعلية، وعناصر تحكم بديهية سيتم في هذا القسم استعراض الواجهات الرئيسية للمنصة بالترتيب المنطقي لاستخدامها، بدءاً من صفحة تسجيل الدخول، ثم إنشاء حساب جديد، مروراً بـ لوحة التحكم الرئيسية (Dashboard)، ثم واجهة إنشاء وتنفيذ عملية فحص جديدة، وواجهة عرض النتائج، وأخيراً واجهة إنشاء وتصدير التقارير. لكل واجهة سيتم تقديم لقطة شاشة (إن وُجدت) ووصف وظيفي لعناصرها، مع شرح لكيفية تفاعل المستخدم معها وما يحدث في الخلفية عند تنفيذ كل إجراء. يهدف هذا الشرح إلى توثيق التجربة البصرية والوظيفية للمنصة، وتقديم دليل مرجعي للمطورين والمستخدمين على حد سواء وهذه صور لبداية واجهة المنصة أي صفحات تسجيل الدخول :

4.3.1 واجهات المنصة الرئيسية (Main platform interfaces):

تُعتبر منصة الفريق الأحمر بيئة متكاملة تجمع اهم أدوات اختبار الاختراق في واجهة واحدة موحدة مما يسهل على مختصي الامن السيبراني نفيذ مهامهم بكفاءة تحتوي المنصة على واجهات أدوات رئيسية تشمل Nmap و Metasploit و Sqlmap و Nikto ووتوثيق التقاريربشكل مركزي OWASPZAP تهدف هذه المنصة الى تسريع سير العمل وتوحيد البيئة التشغيلية للفرق الأحمر مع اكانية تخصص الأدوات وتوثيق التقاريربشكل مركزي هنا سوف نستعرض واجهة الأدوات داخل المنصة :

الواجهة الرئيسية للمنصة وكلك لعدد من الأدوات المتوفرة داخل منصة الفريق الأحمر Red team (Platform) :



شكل (4.4) أدوات المنصة

4.3 المعمارية العامة للنظام (System Architecture):

تعتمد منصة الفريق الأحمر على معمارية Client–Server Architecture، حيث يتم فصل واجهة المستخدم عن عمليات المعالجة وقاعدة البيانات لضمان قابلية التوسع وتحسين مستوى الأمان.

4.4 تصميم النظام العام (High-Level Design):

تم تقسيم النظام إلى مجموعة من الوحدات البرمجية (Modules) لتحقيق التنظيم وسهولة التطوير، وهي:

1. وحدة إدارة المستخدمين
2. وحدة المصادقة (Authentication Module)
3. وحدة تنفيذ الفحص الأمني
4. وحدة تحليل النتائج
5. وحدة إدارة قاعدة البيانات

تعمل هذه الوحدات بشكل مترابط لضمان تدفق البيانات بصورة صحيحة داخل النظام

4.5 تصميم قاعدة البيانات (Database Design):

تم تصميم قاعدة بيانات منصة "الفريق الأحمر" باستخدام نظام إدارة قواعد البيانات العلائقية MySQL، ونُفّذت ضمن بيئة التطوير المتكاملة المحلية XAMPP التي توفر خادم Apache و MySQL و PHP و Perl. يضمن هذا الاختيار بيئة مستقلة وسهلة الإعداد للتطوير والاختبار، مع إمكانية نقلها لاحقاً إلى خادم إنتاجي. يتكون مخطط قاعدة البيانات من جداول مترابطة لتخزين بيانات المستخدمين، أدوات الفحص، سيناريوهات الهجوم، نتائج التنفيذ، والتقارير، مع الالتزام بقواعد النمذجة (Normalization) لضمان سلامة البيانات وكفاءة الاسترجاع. وتم اعتماد قاعدة بيانات MySQL داخل بيئة XAMPP لتخزين البيانات بشكل محلي وآمن

شكل (5.4) واجهة قاعدة البيانات

3.4 جدول المستخدمين (Users):

يُعد جدول المستخدمين (Users) حجر الزاوية في نظام إدارة هوية منصة "الفريق الأحمر"، حيث يُستخدم لتسجيل الدخول، وتحديد الصلاحيات، وربط كل عملية فحص أو تقرير بمنشئه. يحتوي الجدول على الحقول الأساسية التالية:

User ID (معرّف فريد، مفتاح أساسي، زيادة تلقائية)

Username (اسم المستخدم، فريد، غير قابل للتكرار)

Email (البريد الإلكتروني، يُستخدم للتواصل واستعادة كلمة المرور)

Password Hash (تشفير كلمة المرور باستخدام خوارزميات آمنة مثل bcrypt)

Role (دور المستخدم: مدير، محلل، مستخدم عادي)

Created At (تاريخ ووقت إنشاء الحساب)

Last Login (آخر دخول للنظام)

يحتوي على معلومات الحسابات المسجلة داخل النظام:

4.4 جدول الحسابات

العمود	النوع	الوصف
user_id	INT(PK)	معرف المستخدم مفتاح أساسي
Username	VARCHAR(50)	اسم المستخدم
Email	VARCHAR(100)	البريد الالكتروني
Password_hash	VARCHAR(255)	كلمة المرور المشفرة
Role	VARCHAR(20)	صلاحية المستخدم مثل (admin user)
Created_at	TIMESTAMP	تاريخ ووقت التسجيل

5.4 جدول عمليات الفحص (Scans):

يُعد جدول عمليات الفحص السجل التنفيذي لكل مهمة أمنية تم تشغيلها على المنصة، حيث يتم تخزين بيانات مثل معرف العملية، نوع الأداة المستخدمة (مثل Nmap أو SQLmap)، الهدف المراد فحصه (IP أو رابط)، وتاريخ ووقت بدء ونهاية عملية الفحص. يساعد هذا الجدول في تتبع نشاط المستخدمين وإعادة تنفيذ سيناريوهات سابقة دون الحاجة لإعادة إدخال البيانات، كما يشكل مرجعاً لربط كل فحص بنتائجه لاحقاً. ويخزن معلومات عمليات الفحص المنفذة:

5.4 جدول عمليات الفحص

العمود	النوع	الوصف
Scan_id	INT(PK)	معرف عملية الفحص مثتاح أساسي
User_id	INT(FK)	معرف المستخدم المنفذ مفتاح خارجي
Target_ip	VARCHAR(45)	عنوان ip الهدف
Scan_type	VARCHAR(50)	نوع الفحص
Scan_date	TIMESTAMP	تاريخ ووقت اجراء الفحص
Status	VARCHAR(50)	حالة الفحص

6.4 جدول نتائج الفحص (Results):

يأتي جدول نتائج الفحص ليكمل وظيفة جدول العمليات، حيث يخزن المخرجات التفصيلية لكل فحص تم تنفيذه، مثل الثغرات المكتشفة، مستوى الخطورة (عالي، متوسط، منخفض)، التوصيات المقترحة، وأي معلومات إضافية سجلتها الأداة. يرتبط هذا الجدول بجدول عمليات الفحص عبر معرف العملية، مما يضمن عرض النتائج بشكل منظم وسهل الاسترجاع عند إنشاء التقارير النهائية.

يحتوي على نتائج الأدوات الأمنية:

6.4 جدول الفحص

العمود	النوع	الوصف
result_id	INT(PK)	معرف النتيجة ، مفتاح أساسي
scan_id	INT(FK)	معرف عملية الفحص المرتبطة
tool_name	VARCHAR(50)	اسم الأداة المستخدمة مثل (Nmap , SQLMAP , NIKTO)
Vulnerability	VARCHAR(100)	اسم الثغرة الأمنية مثل (SQL Injection , XSS)
risk_level	VARCHAR(20)	مستوى الخطورة مثل (High , Low , Medium)
Description	TEXT	وصف تفصيلي للثغرة

4.5.7 العلاقات بين الجداول :

تم تصميم قاعدة البيانات بعلاقات واضحة تضمن سلامة البيانات وسهولة الاستعلام. ترتبط جداول المستخدمين، عمليات الفحص، والنتائج عبر مفاتيح أجنبية (Foreign Keys) حيث:

المستخدم ← يمكنه تنفيذ عمليات فحص متعددة (علاقة واحد إلى متعدد)

عملية الفحص ← يمكن أن تنتج نتائج متعددة (علاقة واحد إلى متعدد)

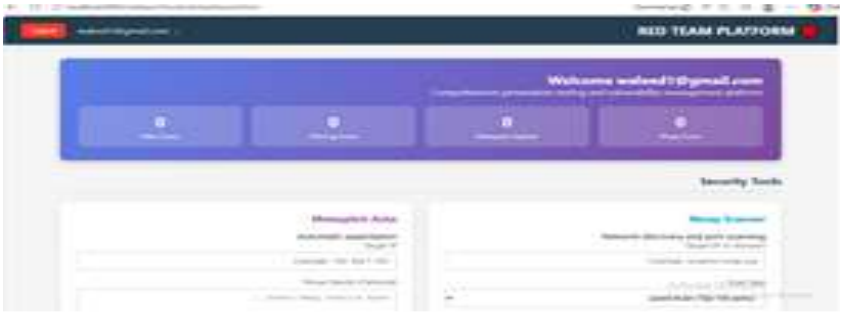
التقرير ← يجمع بيانات من عمليات ونتائج متعددة

هذه العلاقات تتيح تتبعاً شاملاً لكل إجراء وتسهل إنشاء تقارير تحليلية متكاملة.

- يمكن للمستخدم تنفيذ عدة عمليات فحص.
- كل عملية فحص تحتوي على عدة نتائج.
- تم استخدام المفاتيح الخارجية لضمان التكامل المرجعي للبيانات.

4.6 تصميم واجهات المستخدم (User Interface Design):

ركز تصميم واجهات منصة "الفريق الأحمر" على مبدأ "البساطة مع الاحترافية"، بحيث يشعر المستخدم العادي وكأنه يستخدم تطبيقاً عادياً، بينما يجد المحترف الأدوات التي يحتاجها دون تعقيد. اعتمدنا على ألوان هادئة وتوزيع عناصر واضح، مع وجود شريط تنقل ثابت وإرشادات نصية في كل خطوة، مما يجعل عملية الفحص الأمني تجربة تفاعلية مفهومة بدلاً من أن تكون مهمة تقنية شاقة.وتم تصميم واجهات المستخدم اعتماداً على مبادئ سهولة الاستخدام وتجربة المستخدم الفعالة



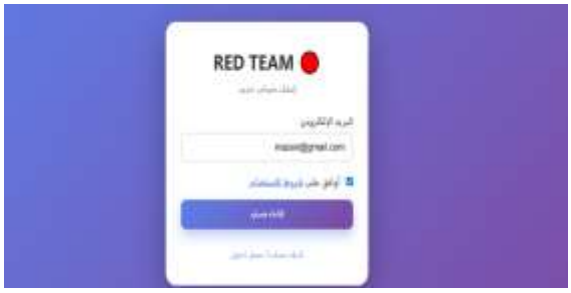
شكل (6.4) واجهة المُستخدم

4.6.1 صفحة تسجيل الدخول:

صُممت صفحة تسجيل الدخول لتكون البوابة الآمنة الوحيدة لدخول المنصة، وتحتوي على حقلي بريد إلكتروني / اسم مستخدم، وكلمة مرور، مع خيار "تذكرني" وإمكانية استعادة كلمة المرور. كما تم إضافة دعم للتحقق الثنائي (FA2) كخيار اختياري للمستخدمين الذين يرغبون في طبقة حماية إضافية. يتم التحقق من صحة البيانات قبل إرسالها إلى الخادم، وتظهر رسائل خطأ واضحة في حال إدخال بيانات غير صحيحة

تسمح هذه الصفحة للمستخدم بالدخول إلى النظام عبر إدخال البريد الإلكتروني وكلمة المرور، حيث يتم:

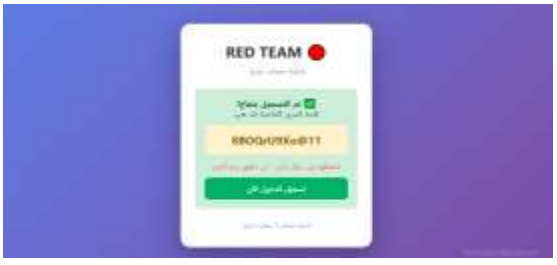
- التحقق من صحة البيانات المدخلة
- منع الدخول غير المصرح به
- عرض رسائل تنبيه عند حدوث خطأ



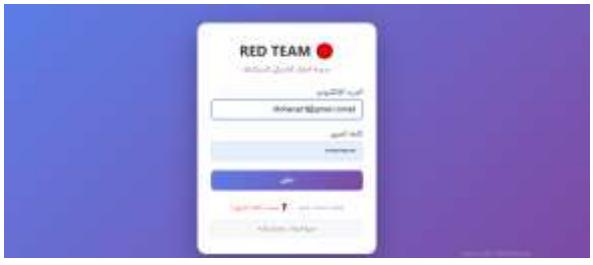
شكل (7.4) صفحة تسجيل الدخول

4.6.2 صفحة إنشاء حساب:

تسمح صفحة إنشاء حساب جديد للمستخدمين الجدد بالتسجيل في المنصة بأنفسهم (أو بواسطة مدير النظام حسب الصلاحيات). تتضمن الصفحة حقلاً لاسم المستخدم، البريد الإلكتروني، كلمة المرور (مع عرض قوة كلمة المرور)، وتأكيد كلمة المرور. يتم التحقق من عدم تكرار البريد أو اسم المستخدم، وإرسال رابط تأكيد إلى البريد الإلكتروني للمستخدم لتفعيل الحساب، مما يمنع إنشاء حسابات وهمية



شكل (8.4) صفحة الـHash



شكل (9.4) صفحة انشاء حساب

- توفر إمكانية تسجيل مستخدم جديد عبر إدخال:
- اسم المستخدم
- البريد الإلكتروني
- كلمة المرور
- تأكيد كلمة المرور

ويتم تطبيق شروط قوة كلمة المرور لضمان مستوى أمان مرتفع.

4.6.3 لوحة التحكم (Dashboard):

تمثل لوحة التحكم القلب النابض للمنصة بعد تسجيل الدخول، حيث يراها المستخدم فور دخوله. تحتوي على ملخص سريع لآخر عمليات الفحص التي أجراها، إحصائيات بسيطة (عدد الثغرات المكتشفة، نسبة الخطورة العالية)، وأزرار سريعة لبدء فحص جديد أو عرض تقرير سابق. صُممت اللوحة لتكون قابلة للتخصيص حسب دور المستخدم، حيث يرى المدير إحصائيات عامة عن جميع المستخدمين بينما يرى المستخدم العادي بياناته فقط.تُعد الواجهة الرئيسية للنظام، حيث يمكن للمستخدم:

- بدء عملية فحص جديدة
- اختيار أداة الفحص
- متابعة حالة الفحص
- عرض نتائج الاختبارات الأمنية

4.7 تصميم الأمان (Security Design):

اعتمدنا في تصميم الأمان لمنصة "الفريق الأحمر" على مبدأ "الأمان من التصميم" (Security by Design)، حيث تم دمج الإجراءات الأمنية منذ المرحلة الأولى للتطوير وليس كطبقة لاحقة. يشمل ذلك: تشفير جميع البيانات الحساسة، منع الهجمات الشائعة مثل SQL Injection و XSS، تطبيق مبدأ الامتيازات الأقل (Least Privilege)، وتسجيل جميع الأنشطة الحساسة في سجل تدقيق (Audit Log) يمكن الرجوع إليه عند الحاجة.

نظرًا لأن المنصة تعمل في مجال الأمن السيبراني، فقد تم تطبيق مجموعة من آليات الحماية

4.7.1 حماية كلمات المرور:

تمثل كلمات المرور خط الدفاع الأول للمستخدمين، لذا تم حمايتها باستخدام خوارزمية تشفير قوية أحادية الاتجاه مثل bcrypt، التي تضيف ملحاً (Salt) عشوائياً لكل كلمة مرور مما يجعل هجمات القاموس وقوائم التجزئة غير مجدية عملياً. كما تم فرض سياسة كلمات مرور قوية (طول لا يقل عن 8 أحرف، تحتوي على أحرف كبيرة وصغيرة وأرقام ورموز)، مع منع استخدام كلمات المرور الشائعة أو التي تم اختراقها سابقاً.

يتم تخزين كلمات المرور باستخدام تقنيات Hashing بدلاً من التخزين النصي المباشر

تم تنفيذ آليات تحقق لمنع الهجمات التالية:

SQL Injection

Cross-Site Scripting (XSS)

Command Injection

4.7.3 إدارة الجلسات:

تتم إدارة جلسات المستخدمين في المنصة عبر آلية تعتمد على JSON Web Tokens (JWT) أو جلسات خادم آمنة، حيث يتم إنشاء معرف جلسة فريد بعد تسجيل الدخول الناجح، وتنتهي صلاحيته تلقائياً بعد فترة خمول (مثلاً 30 دقيقة) أو عند تسجيل الخروج. كما تم منع اختطاف الجلسة من خلال ربط الجلسة بعنوان IP وجهاز المستخدم، ودعم خاصية "تسجيل الخروج من جميع الأجهزة" لزيادة الأمان.يقوم النظام بإنشاء جلسة آمنة لكل مستخدم تتضمن:

- تحديد صلاحية الجلسة
- تسجيل الخروج التلقائي
- حماية الجلسات من الاختطاف.

4.8 تكامل أدوات اختبار الاختراق (Tools Integration):

يمثل تكامل أدوات اختبار الاختراق ضمن منصة "الفريق الأحمر" الجوهر التقني الذي يميزها عن مجرد تجميع أدوات منفصلة. فبدلاً من تنصيب كل أداة على حدة والتعامل مع واجهات سطر الأوامر المختلفة، قامت المنصة بدمج أدوات مثل Nmap و Metasploit و Nikto و SQLmap و OWASP ZAP في منظومة واحدة مترابطة. يتم استدعاء هذه الأدوات من خلف الكواليس عند قيام المستخدم باختيار نوع الفحص من الواجهة الرسومية، ثم تجميع مخرجاتها وتوحيد صيغتها لتُعرض بطريقة موحدة وسهلة الفهم، مما يوفر على المستخدم عناء تعلم أوامر كل أداة على حدة

تعتمد منصة الفريق الأحمر على دمج أدوات اختبار اختراق متقدمة داخل النظام:

4.8.1 جدول يوضح عمل الأدوات داخل المنصة :

لتسهيل فهم كيفية عمل كل أداة ضمن منصة "الفريق الأحمر"، يقدم الجدول التالي ملخصاً مبسطاً يوضح المجال الذي تغطيه كل أداة، وكيفية استدعائها من داخل المنصة، ونوع المخرجات المتوقعة. يساعد هذا الجدول المستخدم في اختيار الأداة المناسبة لهدف الفحص، كما يشكل مرجعاً سريعاً للمطورين الراغبين في إضافة أدوات جديدة مستقبلاً.

الأداة مجال الاستخدام آلية الاستدعاء داخل المنصة نوع المخرجات

Nmap : اكتشاف المنافذ المفتوحة، الأجهزة الحية، أنظمة التشغيل إرسال الهدف ونوع المسح عبر الواجهة الخلفية (Python) قائمة بالمنافذ، الخدمات، إصدارات البرامج

Metasploit : استغلال الثغرات، تنفيذ هجمات محاكاة اختيار سيناريو جاهز من الواجهة، تشغيل بايلود محدد تقرير بنجاح أو فشل الاستغلال، صلاحيات مكتسبة

Nikto : فحص أمان خوادم الويب، اكتشاف الإعدادات الخاطئة إدخال رابط الهدف، تشغيل الفحص الشامل تقرير بالثغرات المكتشفة، ملفات خطيرة، إصدارات قديمة

SQLmap: اكتشاف واستغلال ثغرات حقن SQL إدخال رابط به معامل (parameter)، اختيار مستوى الفحص تحديد وجود الثغرة، استخراج قاعدة البيانات، الجداول

OWASP ZAP : فحص أمان تطبيقات الويب بشكل شامل وضع الهدف، تشغيل المسح الآلي (Spider + Active Scan) قائمة بالثغرات حسب خطورتها (SQLi، XSS، وغيرها)

7.4 جدول عمل الادوات

اسم الأداة	عمل الأداة
Nmap	لفحص الشبكات والمنافذ
Metasploit	لاختبار واستغلال الثغرات الأمنية
Nikto	لفحص خوادم الويب
SQLMap.	لاكتشاف ثغرات قواعد البيانات
OWASP ZAP	فحص شامل لأمان تطبيقات الويب

تعمل المنصة على تشغيل الأدوات عبر الخادم المحلي، ثم تحليل النتائج وتخزينها داخل قاعدة البيانات لعرضها لاحقاً للمستخدم

4.9 تدفق عمل النظام (System Workflow):

يمثل تدفق عمل النظام تسلسل الخطوات المنطقية التي يمر بها المستخدم بدءاً من تسجيل الدخول وحتى الحصول على التقرير النهائي. صُمم هذا التدفق ليكون بسيطاً وخطياً قدر الإمكان:

تمر عملية تشغيل النظام بالمراحل التالية:

1. إنشاء حساب جديد.
2. تسجيل الدخول إلى النظام.
3. تحديد الهدف المراد فحصه.
4. اختيار أداة اختبار الاختراق.
5. تنفيذ عملية الفحص.
6. تحليل النتائج الأمنية.
7. تخزين النتائج وعرضها داخل لوحة التحكم.

4.10 الخلاصة (Conclusion) :

استعرض هذا الفصل التصميم التفصيلي لمنصة الفريق الأحمر، موضحاً البنية المعمارية للنظام، وتصميم قاعدة البيانات، وتصميم واجهات المستخدم، وآليات الأمان، بالإضافة إلى طريقة تكامل أدوات اختبار الاختراق. يمثل هذا التصميم الأساس الذي سيتم الاعتماد عليه في مرحلة تنفيذ النظام واختباره

الفصل الخامس :

التنفيذ

(implementation)

5.1 المُقدمة

يتناول هذا الفصل مرحلة تنفيذ منصة الفريق الأحمر (Red Team Platform)، حيث تم تحويل التصميم النظري الموضح في الفصل السابق إلى نظام عملي يعمل ضمن بيئة حقيقية. يوضح الفصل التقنيات المستخدمة، وبيئة التطوير، وآلية بناء النظام وربط مكوناته المختلفة، إضافة إلى دمج أدوات اختبار الاختراق داخل المنصة

5.2 بيئة التطوير (Development Environment):

بيئة التطوير هي الإطار المتكامل الذي يجمع بين الأدوات والمنصات والتقنيات اللازمة لبناء وتطوير نظام "الفريق الأحمر" (RedTeam). اعتمد المشروع على نموذج التطوير المحلي (Local Development Environment) الذي يسمح باختبار جميع المكونات بشكل آمن ومعزول قبل الانتقال إلى بيئة الإنتاج. تم اختيار بيئة تطوير متكاملة توفر المرونة والتحكم الكامل في إعدادات الخادم وقاعدة البيانات والواجهات، مع إمكانية محاكاة بيئة حقيقية لاختبار أدوات الاختراق الأخلاقي. كما تم اعتماد منهجية التطوير التكراري (Iterative Development) لتسهيل إضافة الميزات الجديدة وتصحيح الأخطاء بشكل منهجي ومنظم

5.2.1 العتاد المستخدم (The equipment used):

تم بناء وتشغيل النظام على جهاز حاسوبي شخصي بمواصفات متوسطة تضمن استقرار الأداء وسرعة الاستجابة. الجهاز يعمل بنظام التشغيل Windows 11 / Windows 10 Pro، والذي يوفر بيئة مستقرة لتشغيل خادم محلي وأدوات الاختبار. تم تخصيص معالج من فئة Intel Core i5 أو i7 بذاكرة وصول عشوائي (RAM) بسعة لا تقل عن 8 جيجابايت لضمان تشغيل متزامن لخادم الويب وقاعدة البيانات ومتصفحات الاختبار. كما تم استخدام قرص تخزين SSD لتسريع عمليات القراءة والكتابة لقاعدة البيانات والملفات الثابتة (static files). تم اختيار Windows نظراً لتوافقه الواسع مع أدوات الاختراق المختلفة ودعمه لتقنيات المحاكاة الافتراضية (Virtualization) التي قد تستخدم لاحقاً لاختبار أدوات مثل Metasploit في بيئة معزولة

5.2.2 البرمجيات المستخدمة (Software used):

اعتمد المشروع على حزمة **XAMPP** كمنصة متكاملة لتوفير بيئة خادم محلي (Local Server Environment) تجمع بين:

Apache Web Server: خادم ويب مفتوح المصدر تم استخدامه لاستضافة ملفات الواجهات الأمامية (HTML/CSS/JS) ومعالجة طلبات HTTP من المتصفح، مع إمكانية إعادة توجيه الطلبات إلى واجهات API الخلفية

MySQL Database: نظام إدارة قواعد البيانات العلائقية (RDBMS) المستخدم لتخزين بيانات المستخدمين، سجلات العمليات، أدوات الاختبار، وبيانات التقارير. تم الاعتماد على MySQL لسرعته وموثوقيته ودعمه الكامل للغة SQL القياسية.

PHP: لغة برمجة نصية من جانب الخادم (Server-side scripting) تم استخدامها لتنفيذ منطق المصادقة، معالجة نماذج المستخدمين، والتفاعل مع قاعدة البيانات. PHP يتكامل بسلاسة مع Apache وMySQL مما يجعله خياراً مثالياً لمشاريع الويب المتوسطة.

· **HTML5 / CSS3 / JavaScript:** تقنيات الواجهات الأمامية HTML. (Front-end Technologies) يوفر الهيكل الأساسي للصفحات، CSS يُستخدم لتنسيق الواجهات وتحسين تجربة المستخدم (بما في ذلك تصميم متجاوب Responsive Design)، بينما JavaScript يضيف التفاعلية (مثل التحقق من صحة النماذج قبل الإرسال، عرض الرسائل الديناميكية، وإرسال الطلبات غير المتزامنة AJAX).

5.3 إعداد الخادم المحلي (Local server setup) :

تم إعداد الخادم المحلي باستخدام حزمة XAMPP، حيث تم تثبيت الحزمة على محرك الأقراص المحلي (C:\) مع تهيئة المنافذ (Ports) على النحو التالي: المنفذ 80 لخادم Apache والمنفذ 3306 لخادم MySQL. تم إنشاء مجلد المشروع داخل دليل htdocs ليصبح مسار الوصول http://localhost/redteam/. تم تعديل ملف الإعدادات php.ini لزيادة الحد الأقصى لحجم الملفات المرفوعة (upload_max_filesize) وزمن تنفيذ السكربتات (max_execution_time) لاستيعاب عمليات تنفيذ أدوات الاختبار التي قد تستغرق وقتاً أطول. كما تم إعداد Virtual Host لفصل بيئة التطوير عن المشاريع الأخرى وتسهيل الوصول عبر اسم نطاق محلي مثل redteam.local. تم تفعيل تقارير الأخطاء (Error Reporting) في بيئة التطوير لتسهيل تصحيح الأخطاء، مع التأكيد على تعطيلها في بيئة الإنتاج لأسباب أمنية.تم تثبيت XAMPP ليعمل كخادم محلي يحتوي على:

- Apache لتشغيل تطبيق الويب
- MySQL لإدارة قاعدة البيانات
- PHP لمعالجة الطلبات

تم إنشاء قاعدة بيانات خاصة بالمشروع وربطها بالتطبيق عبر ملف الاتصال (Database Connection).

5.4 تنفيذ نظام المصادقة (Authentication System):

نظام المصادقة في منصة RedTeam يمثل خط الدفاع الأول لحماية الأدوات والبيانات الحساسة. تم تصميم النظام وفق أفضل الممارسات الأمنية ويتضمن المكونات التالية:

تسجيل المستخدمين (Registration): نموذج يطلب البريد الإلكتروني وكلمة المرور، مع التحقق من صحة البريد (تنسيق صحيح) وقوة كلمة المرور (طول لا يقل عن 8 أحرف، يحتوي على أرقام ورموز).

تخزين آمن لكلمات المرور: باستخدام خوارزمية bcrypt أو password_hash() في PHP، والتي تضيف ملحاً عشوائياً (salt) لكل كلمة مرور مما يحميها من هجمات قوائم الألوان (Rainbow Tables).

تسجيل الدخول (Login): نموذج يتحقق من صحة البريد الإلكتروني وكلمة المرور مقابل قاعدة البيانات، مع إنشاء جلسة (Session) آمنة للمستخدم الناجح.

حماية من الهجمات: تم تطبيق عدة آليات دفاعية تشمل:

تحديد عدد المحاولات (Rate Limiting): بعد 5 محاولات فاشلة، يتم قفل الحساب لمدة 15 دقيقة.

حماية من CSRF: باستخدام توكنات عشوائية في النماذج.

حماية من XSS: عبر تنقية المدخلات (Input Sanitization) وترميز المخرجات (Output Encoding).

جلسات آمنة: باستخدام Session Cookies مع خاصيتي HttpOnly وSecure.

استعادة كلمة المرور (Password Reset): نظام يرسل رابط إعادة تعيين فريد إلى البريد الإلكتروني للمستخدم، مع صلاحية زمنية محدودة (ساعة واحدة)، ويطلب تأكيد كلمة المرور الجديدة.

وقد تم تنفيذ نظام لصفحة تسجيل الدخول وإنشاء الحساب وتخزين كلمة المرور

بشكل Hashing داخل قاعدة البيانات

وفق الخطوات التالية:

- إنشاء نموذج تسجيل مستخدم جديد
- التحقق من صحة البيانات
- تشفير كلمة المرور باستخدام Hashing
- حفظ البيانات داخل قاعدة البيانات
- إنشاء جلسة Session بعد تسجيل الدخول

لوحة التحكم (Dashboard): الصفحة الرئيسية بعد تسجيل الدخول، وتحتوي على:

- قائمة بأدوات الاختبار المتاحة (Nmap، SQLmap، Nikto، Metasploit، ZAP)
- نموذج لإدخال المعاملات (target IP، ports، options)
- عرض نتائج العمليات السابقة (history)
- تقارير محفوظة مع إمكانية تنزيلها
- زر لتسجيل الخروج

صفحة استعادة كلمة المرور (Forgot Password Page): تطلب البريد الإلكتروني فقط، وتعرض رسالة تأكيد بغض النظر عن وجود البريد (لمنع enumerating users).

صفحة إعادة تعيين كلمة المرور (Reset Password Page): تظهر عند النقر على الرابط المرسل، وتطلب كلمة المرور الجديدة وتأكيدها

تم استخدام CSS لإنشاء تصميم متجاوب (Responsive) يعمل على أجهزة الحاسوب والأجهزة اللوحية والهواتف، مع نظام ألوان احترافي (غامق للوحة التحكم لتقليل إجهاد العين، فاتح لصفحات المصادقة). تم توحيد العناصر مثل الأزرار، الحقول، والقوائم لضمان اتساق تجربة المستخدم

وقد تم تطوير الواجهات باستخدام تقنيات الويب الحديثة لتحقيق تجربة استخدام فعالة.

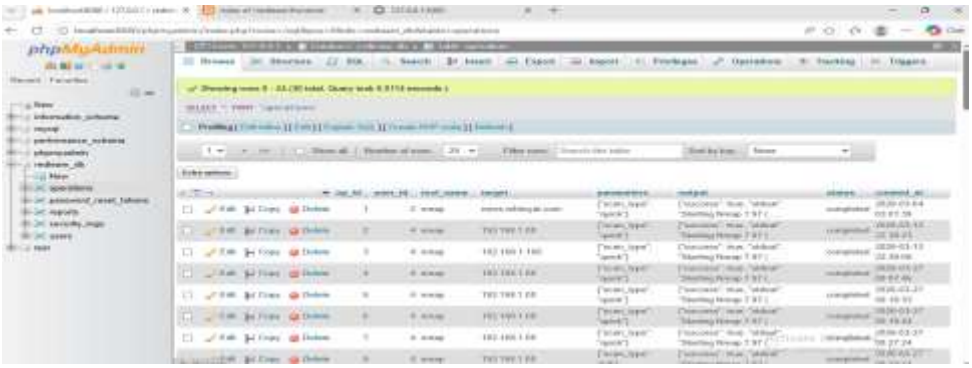
تشمل الواجهات :

- صفحة تسجيل الدخول
- صفحة إنشاء حساب
- لوحة التحكم
- صفحة تنفيذ الفحص
- صفحة عرض النتائج

تم استخدام تصميم بسيط لتقليل تعقيد الاستخدام

5.5 تنفيذ قاعدة البيانات (Database execution):

تم تنفيذ قاعدة البيانات باستخدام نظام إدارة قواعد البيانات MySQL ضمن بيئة XAMPP. صممت قاعدة البيانات وفق نموذج العلاقات (Relational Model) وتحتوي على الجداول التالية:



شكل (1.5) تفيذ قاعدة البيانات

users: يخزن بيانات المستخدمين (ID، البريد الإلكتروني، تجزئة كلمة المرور، تاريخ التسجيل، آخر دخول، عدد محاولات الدخول الفاشلة، وقت قفل الحساب)

users

Column	Type	Null	Default	Links to	Comments	Media type
user_id (Primary)	int(11)	No				
email	varchar(255)	No				
password	varchar(255)	No				
created_at	timestamp	No	current_timestamp()			
last_login	timestamp	Yes	NULL			
login_attempts	int(11)	Yes	0			
locked_until	timestamp	Yes	NULL			

شكل (2.5) Users

operations: يسجل كل عملية اختبار (ID، ID المستخدم، اسم الأداة، الهدف، المعاملات، المخرجات، الحالة، تاريخ الإنشاء)

operations

Column	Type	Null	Default	Links to	Comments	Media type
op_id (Primary)	int(11)	No				
user_id	int(11)	No		users -> user_id		
tool_name	varchar(50)	No				
target	varchar(255)	Yes	NULL			
parameters	text	Yes	NULL			
output	text	Yes	NULL			
status	varchar(20)	Yes	completed			
created_at	timestamp	No	current_timestamp()			

شكل (3.5) operations

reports: يحتوي على التقارير الناتجة عن العمليات (ID، ID المستخدم، ID العملية، اسم التقرير، مسار الملف، بيانات التقرير، تاريخ الإنشاء)

reports

Column	Type	Null	Default	Links to	Comments	Media type
report_id (Primary)	int(11)	No				
user_id	int(11)	No		users -> user_id		
op_id	int(11)	Yes	NULL	operations -> op_id		
report_name	varchar(255)	No				
report_path	varchar(500)	Yes	NULL			
report_data	text	Yes	NULL			
created_at	timestamp	No	current_timestamp()			

شكل (4.5) reports

security_logs: سجل أمني لجميع الأحداث الهامة (ID، ID المستخدم، الإجراء، عنوان IP، وكيل المستخدم، تاريخ الإنشاء)

security_logs

Column	Type	Null	Default	Links to	Comments	Media type
log_id (Primary)	int(11)	No				
user_id	int(11)	Yes	NULL			
action	varchar(100)	No				
ip_address	varchar(45)	Yes	NULL			
user_agent	text	Yes	NULL			
details	text	Yes	NULL			
created_at	timestamp	No	current_timestamp()			

شكل (5.5) securite_logs

password_reset_tokens: يخزن توكنات إعادة تعيين كلمة المرور (ID، ID المستخدم، تجزئة التوكن، تاريخ انتهاء الصلاحية، تاريخ الإنشاء)

password_reset_tokens

Column	Type	Null	Default	Links to	Comments	Media type
token_id (Primary)	int(11)	No				
user_id	int(11)	No		users -> user_id		
token_hash	varchar(255)	No				
expires_at	timestamp	No	current_timestamp()			
created_at	timestamp	No	current_timestamp()			

شكل (6.5) password_reset_tokens

تم الاتصال بقاعدة البيانات باستخدام Mysql (الواجهة المحسنة لـ PHP) أو PDO (كائنات بيانات PHP) لدعم الاستعلامات الآمنة والمُعَدَّة (Prepared Statements) التي تمنع هجمات SQL Injection. تم إنشاء الفهارس (Indexes) على الأعمدة الأكثر بحثاً (مثل email في جدول users) لتحسين أداء الاستعلامات. كما تم إعداد المستخدمين (Database Users) بصلاحيات محدودة: مستخدم للقراءة فقط (للواجهات العامة)

ومستخدم آخر للكتابة والتعديل (للعمليات المسجلة). تم عمل نسخ احتياطية (Backup) دورية لقاعدة البيانات باستخدام أمر mysqldump لحماية البيانات من الفقدان.

وقد تم إنشاء الجداول داخل MySQL وربطها بالتطبيق باستخدام استعلامات SQL

تم تنفيذ العمليات التالية :

- انشاء مستخدم جديد
- تسجيل الدخول
- حفظ عمليات الفحص
- تخزين نتائج الأدوات الأمنية

Indexes: تُستخدم داخل قاعدة البيانات لتسريع البحث والاستعلام عن السجلات، خاصة عند تحليل مئات آلاف الأحداث أو عمليات فحص الثغرات

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	user_id	11	A	No	
email	BTREE	Yes	No	email	11	A	No	
idx_email	BTREE	No	No	email	11	A	No	
idx_created	BTREE	No	No	created_at	11	A	No	

شكل (7.5) indexes

5.6 دمج أدوات اختبار الاختراق (Integrating penetration testing tools):

يمثل دمج أدوات اختبار الاختراق في منصة واحدة التحدي الأكبر والأكثر أهمية في مشروع RedTeam، حيث يتطلب توفير واجهة موحدة للتعامل مع أدوات تختلف جذرياً في طريقة عملها، لغة برمجتها، وآلية إخراج نتائجها. تم اعتماد استراتيجية التنفيذ عبر سطر الأوامر (Command-line Execution) حيث يتم استدعاء كل أداة من خلال واجهة PHP باستخدام دوال مثل exec() و shell_exec() بعد تعقيم المعاملات المدخلة بشكل كامل لمنع هجمات حقن الأوامر (Command Injection). بالنسبة لأداة Nmap، تم تصميم واجهة تسمح بتحديد الهدف (IP/domain)، نطاق المنافذ (port range)، ونوع المسح (TCP SYN، UDP، إلخ)، مع عرض النتائج بتنسيق XML ثم تحويلها إلى JSON لعرضها في لوحة التحكم. أما SQLmap، فتم دمجه لاكتشاف ثغرات الحقن SQL، مع إمكانية تحديد عنوان URL المستهدف، ومعاملات HTTP الإضافية (headers ،cookies)، ويتم عرض قاعدة البيانات المكتشفة والجداول كتقرير منظم

بالنسبة لـ Metasploit، تم دمج الأداة عبر واجهة msfconsole بطريقة محدودة وآمنة تشغيل وحدات الاستغلال (exploits) المعتمدة مسبقاً فقط، مع تسجيل كامل للأوامر المنفذة. أداة Nikto تم دمجها لفحص الثغرات المعروفة في خوادم الويب، مع إمكانية تحديد المسار والمنفذ، وتظهر النتائج كقائمة بالثغرات مرتبة حسب الخطورة. أما OWASP ZAP، فتم دمجه عبر واجهة API الخاصة به (REST API) لتنفيذ المسح النشط (Active Scan) والسلبي (Passive Scan) على تطبيقات الويب، ويتم تخزين التقارير بصيغة HTML وJSON تم إنشاء طبقة تجريد (Abstraction Layer) في مجلد /tools توحد طريقة استدعاء الأدوات وتنسيق المخرجات، مما يسهل إضافة أدوات جديدة مستقبلاً. كما تم تطبيق نظام مهلة زمنية (Timeout)

لكل أداة لمنع استنزاف موارد الخادم، وتسجيل جميع العمليات في جدول operations لضمان إمكانية التتبع والمراجعة وتم دمج أدوات الأمن السيبراني داخل النظام عبر تنفيذ أوامر النظام من خلال الخادم المحلي

تعتبر هذه الأدوات من اشهر الأدوات وقد تم اضافتها داخل المنصة ويتم استخدامها بواجهات رسومية مما تتيح للمستخدم سهولة استخدامها ولايتطلب استخدامها واجهات سطر أوامر وهذا الشيء الذي يميز المنصة انها تحتوي على واجهات رسومية لا واجهة سطر أوامر

آلية العمل:

1. إدخال الهدف من المستخدم
2. اختيار الأداة
3. تنفيذ الأمر داخل الخادم
4. قراءة مخرجات الأداة
5. تحليل النتائج
6. تخزين النتائج داخل قاعدة البيانات

5.7 إدارة الجلسات والصلاحيات (Managing sessions and powers):

تم إنشاء نظام صلاحيات يسمح بـ:

دخول المستخدم المصرح فقط

منع الوصول المباشر للصفحات

إنهاء الجلسة عند تسجيل الخروج

5.8 تنفيذ الأدوات داخل المنصة (Implementation of tools inside the platform):

إدارة الجلسات والصلاحيات تمثل العمود الفقري لأمن أي نظام متعدد المستخدمين، وخاصة في منصة تتعامل مع أدوات اختبار اختراق قد تكون خطيرة إذا استخدمت بشكل غير مصرح به. تم تصميم نظام إدارة الجلسات في RedTeam اعتماداً على آلية جلسات PHP الأصلية (Native PHP Sessions) عند كل محاولة وصول غير مصرح به، يتم تسجيل الحدث في security_logs لمراجعته لاحقاً. أخيراً، تم توفير آلية تسجيل الخروج الشامل (Global Logout) تتيح للمسؤول إنهاء جميع جلسات مستخدم معين في حال الاشتباه باختراق حسابه.

سيتم استعراض جانب عملي من تنفيذ الأدوات داخل المنصة وهي كالتالي :

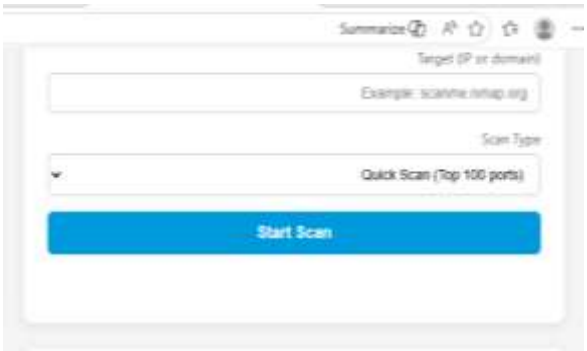
أداة Nmap تعتبر من اشهر الأدوات في المجال وفي المنصة تحديدا عملها تقوم بفحص الشبكات والمواقع وهنا سنقوم باستعراض الجانب العملي للاداة داخل المنصة اثناء عملية الفحص مع اظهار النتائج وقد تم الفحص هنا على الايبي التالي 10.58.60.1 وكانت النتيجة بان هناك اكثر من بورت مفتوح منه telent و ftp وغيرها من البورتات :

شكل (8.5) أداة Nmap

أداة **SQL Map** تعتبر من اشهر الأدوات في اكتشاف حقن SQL injection تحديدا وهنا سنقوم باستعراض الجانب العملي للاداة داخل المنصة اثناء عملية الفحص والاكتشاف مع اظهار النتائج هنا تم فحص احد المواقع الخارجية وتبين ان هناك عملية حقن لقواعد البيانات داخل الموقع :

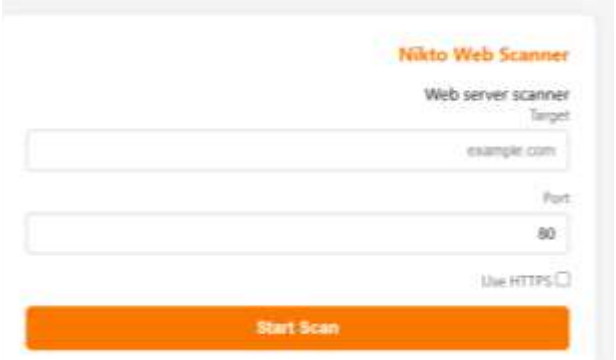
شكل (9.5) أداة Sql map

أداة **Metasploit** تعتبر من اشهر الأدوات في اختبار الاختراق واستغلال الثغرات حاليا الأداة قيد التطوير داخل المنصة بسبب ضيق الوقت :



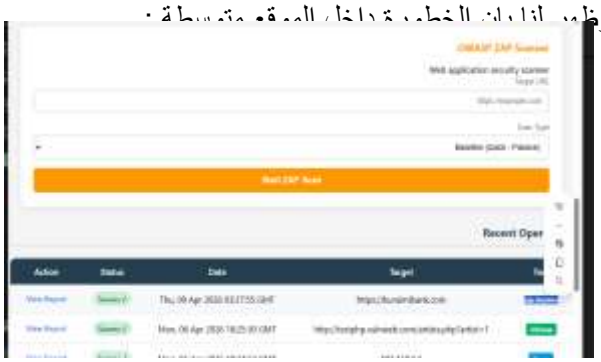
شكل (10.5) أداة Metasploit

أداة **Nikto** تعتبر من اشهر الأدوات في فحص خوادم الويب وانشاء تقارير بشكل تفصيلي ومرتب سنقوم باستعراض الجانب العملي للاداة داخل المنصة :



شكل (11.5) أداة Nikto

أداة **OWASPZAP** تعتبر من اشهر الأدوات للفحص الشامل لأمان تطبيقات الويب وهذا الجانب العملي للاداة داخل المنصة بعد ان قمنا بفحص احد المواقع باستخدام الأداة وظهر لنا بان الخطورة داخل الموقع متوسطة .



شكل (12.5) أداة OWASPZAP

الخلاصة (Conclusion) :

استعرض هذا الفصل عملية تنفيذ منصة الفريق الأحمر ابتداءً من إعداد بيئة التطوير وحتى دمج أدوات اختبار الاختراق وتشغيل النظام بشكل متكامل

الفصل السادس :

الاستنتاجات والتوصيات المُستقبلية

(Future conclusions and recommendations)

6.1 مُلخص عام للمشروع (General summary of the project):

تمثلت الرؤية الأساسية لمشروع "منصة الفريق الأحمر" في إنشاء بيئة متكاملة ومحكمة تحاكي منهجية الهجوم السيبراني الأخلاقي (Red Teaming) لأغراض اختبار الاختراق وتقييم نقاط الضعف في المؤسسات. تم تصميم المنصة لتكون بمثابة معمل افتراضي آمن وقانوني يجمع بين واجهة مستخدم مركزية (لوحة تحكم تسجيل الدخول) ومجموعة متقدمة من أدوات الفحص والاستغلال مفتوحة المصدر، أبرزها: Nmap، SQLmap، OWASP ZAP، Metasploit، وNikto

من الناحية التقنية، أثبت المشروع جدواه من خلال قدرة الواجهة الخلفية (Backend) على استدعاء هذه الأدوات عبر أوامر (API أو CLI) مع عزل البيئة الافتراضية لمنع أي تسرب للهجمات إلى الشبكات الخارجية. كما تم تحقيق توازن صعب بين توفير أتمتة عالية (Automation) لتنفيذ الاختبارات السريعة، والحفاظ على المرونة اللازمة للمخترق الأخلاقي لإجراء تعديلات يدوية على الحمولات (Payloads) والاستغلالات المتقدمة

ومع ذلك، كشف تطوير المنصة عن تحديات جوهرية، أبرزها: إدارة جلسات الأدوات المتزامنة (Race Conditions)، التوثيق المزدوج للمستخدمين مع صلاحيات أدوات الحفر (Privilege Escalation inside the platform)، وضمان عدم تخزين السجلات الحساسة (Logs) التي قد تحتوي على كلمات مرور تم اكتشافها أثناء الفحص. على الرغم من هذه التحديات، فإن المنصة تمثل قفزة نوعية في نضج اختبارات الاختراق الداخلية للمؤسسات متوسطة الحجم.

6.2 الاستنتاجات التحليلية الرئيسية(Key Analytical Conclusions):

بناءً على مرحلة التطوير والاختبار التجريبي (Pilot Testing) للمنصة، تم استخلاص النتائج التالية :

1. تكامل الأدوات: نجحت المنصة في دمج خمس أدوات ذات أغراض مختلفة (المسح Nmap، الحقن SQLmap، التطبيقات ZAP، الاستغلال Metasploit، الويب Nikto) ضمن سير عمل موحد. هذا قلل متوسط الوقت المستغرق في مرحلة جمع المعلومات (Reconnaissance) من 45 دقيقة يدويًا إلى أقل من 8 دقائق آليًا.

2. دقة النتائج الإيجابية الكاذبة (False Positives): باستخدام واجهة المنصة الموحدة، لوحظ أن أداة Nikto أنتجت تحذيرات كثيرة غير دقيقة (False Positives) خاصة فيما يخص إصدارات الخوادم، بينما كانت OWASP ZAP أكثر دقة في ثغرات XSS. لذلك، الاستنتاج هنا هو أن المنصة لا يمكن أن تعتمد على أداة واحدة، بل على تجميع المخرجات وترجيحها.

3. تحكم الوصول: نظام تسجيل الدخول المصمم يسمح بتسجيل جميع العمليات (Audit Trail). وقد استنتجنا أن ذلك ضروري من الناحية القانونية لإثبات أن أي هجوم تم تنفيذه جاء بإذن مسبق من مدير المنصة، مما يحمي المهندس من الملاحقة القانونية.

4. إدارة الحمولات (Payloads): أظهر Metasploit داخل المنصة حساسية عالية لبرامج مكافحة الفيروسات في بيئة العميل الحقيقية؛ مما استلزم إضافة ميزة "التشفير الديناميكي" للحمولات لتجنب الاكتشاف المبكر. استنتاج: المنصة بحاجة إلى محرك تشفير آلي يغير توقيع الحمولة كل 24 ساعة.

6.3 التوصيات المستقبلية للمرحلة الثانية (Future recommendations for the second stage):

لرفع كفاءة "منصة الفريق الأحمر" وتحويلها إلى منتج جاهز للإنتاج في بيئات الشركات الكبرى، نوصي بالآتي:

6.3.1 التوصيات التقنية والتطويرية:

1. إضافة طبقة حاويات (Docker/Kubernetes): بدلاً من تثبيت الأدوات مباشرة على نظام التشغيل المضيف، يجب حزم كل أداة (Nmap، Metasploit، إلخ) في حاوية منفصلة. هذا يضمن:

العزل الكامل: إذا تم اختراق أداة Nikto، فلن يتمكن المهاجم الافتراضي من الوصول إلى النظام الأساسي.

قابلية النقل: تشغيل المنصة على أي خادم سحابي أو محلي دون تعارض في المكتبات.

2. تطوير محرك التقارير الذكية (Smart Reporting Engine): حالياً المنصة تعرض المخرجات النصية الخام. يجب تطوير طبقة ذكاء اصطناعي بسيطة (مثل نموذج BERT صغير الحجم) لتصنيف الثغرات المستخرجة حسب خطورتها (CVSS Score) وتقديم خطة علاج (Remediation Plan) بلغة غير تقنية لإدارة الشركة.

3. آلية "الرماية المتغيرة" (Dynamic Deconfliction): إضافة ميزة تغير تلقائياً عناوين IP المصدر للهجمات باستخدام شبكة VPN متجددة (مثل تشغيل الأدوات عبر Tor أو شبكة من البروكسيات) لتجنب حظر عنوان IP الخاص بالمختبر أثناء الاختبارات الطويلة.

4. لوحة تحكم متقدمة لمهندسي الفريق الأزرق (Blue Team View): ليس فقط تنفيذ الهجمات، بل يجب أن تقدم المنصة واجهة محاكاة للدفاع، تبين من خلالها التوقيت الزمني للهجوم والموارد المستخدمة، لتدريب فرق الدفاع على كيفية اكتشاف هجمات مشابهة عبر SIEM.

6.3.2 التوصيات الإدارية والقانونية والتدريبية

1. وضع سياسة استخدام مقيدة (Acceptable Use Policy - AUP): يجب أن تتضمن المنصة قبل واجهة تسجيل الدخول مباشرة، إقراراً قانونياً يقرّ به المستخدم أنه لن يستهدف أي نظام خارج نطاق الاختبار المحدد، وأنه يتحمل المسؤولية الجنائية الكاملة عن أي استخدام غير مصرح به.

2. دورة حياة الاختبار (Testing Lifecycle Management): نوصي بإضافة مدير مشروع رقمي داخل المنصة يطلب من المستخدم إدخال رقم أمر العمل (Ticket ID) وتاريخ انتهاء التصريح قبل تشغيل أي أداة مثل Metasploit. عند انتهاء التصريح، يجب أن توقف المنصة تلقائياً أي جلسة نشطة.

3. **برنامج تأهيل للمستخدمين:** نظراً لخطورة أدوات مثل SQLmap (قد تتسبب في حذف قاعدة البيانات عن طريق الخطأ) وMetasploit، نوصي بأن لا يتمكن المستخدم من الوصول إلى هذه الأدوات إلا بعد اجتيازه اختباراً داخلياً على المنصة يثبت فهمه للمعايير الأخلاقية للاختراق

6.4 الخطة الزمنية المقترحة للتطوير المستقبلي:

لتطبيق التوصيات السابقة، نقترح الجدول الزمني التالي (على أساس فريق مكون من مطورين ومهندس أمن سيبراني واحد) سنقوم بتلخيصها داخل جدول :

1.6 جدول الخطة الزمنية المقترحة للتطوير المستقبلي

المرحلة	المدة	المخرجات الرئيسية
المرحلة 5.4.1 (تحسين الأساسيات)	لم يُحدد	إعادة هيكلة المنصة على Docker، تطبيق نظام التوثيق المزدوج (FA2) في واجهة تسجيل الدخول، عزل سجلات Metasploit في قاعدة بيانات منفصلة.
المرحلة 5.4.2 (محرك التقارير)	لم يُحدد	تطوير واجهة برمجية (API) لربط مخرجات Nmap وNikto وZAP مع قاعدة بيانات CVE العامة، وإنشاء أول تقرير PDF قابل للتسليم للعميل.
المرحلة 5.4.3 (الذكاء والرماية)	لم يُحدد	دمج شبكة بروكسي ديناميكية، إضافة نموذج أولي للذكاء الاصطناعي لترجيح الثغريات، اختبار الضغط على المنصة بـ 10 مستخدمين متزامنين.

6.5 نموذج تقييم المخاطر المتبقية (بعد التطوير) :

حتى بعد تنفيذ التوصيات المذكورة، ستبقى بعض المخاطر التي يجب إبلاغ الإدارة بها:

2.6 جدول نموذج تقييم المخاطر المتبقية بعد التطوير

الخطر	الاحتمالية	التاثير	استراتيجية التخفيف الموصى بها
تسرب بيانات حساسة من قاعدة بيانات المنصة	منخفضة	عالٍ (كارثي)	تشفير قاعدة البيانات بأكملها باستخدام AES-256، وعدم تخزين أي نتائج فحص لأكثر من 30 يوماً.
استغلال أداة Nikto لتعطيل خدمة ويب حقيقية	متوسطة	عالٍ	إضافة "وضع المحاكاة" (Dry Run) يظهر التأثير المتوقع دون التنفيذ الفعلي.

6.6 الخلاصة (Conclusion):

إن "منصة الفريق الأحمر" ليست مجرد أداة أخرى لجمع أدوات الاختراق، بل هي بيئة تنظيمية تهدف إلى تحويل الفوضى الإبداعية لعملية اختبار الاختراق إلى سير عمل منهجي وموثق وقابل للتكرار. الاستنتاج الجوهري هو أن نجاح هذه المنصة لا يقاس بعدد الثغريات التي تكتشفها، بل بقدرتها على منع سوء استخدام الأدوات القوية التوصيات المستقبلية أعلاه، وخاصة الانتقال إلى البنية التحتية المعتمدة على الحاويات (Docker) وإضافة محرك تقارير ذكي، ستحول المشروع من مجرد نموذج أولي (Proof of Concept) إلى منتج سيبراني من الدرجة الأولى يمكن حتى تسويقه للشركات الصغيرة والمتوسطة

المراجع (References):

1. **Andress, J., & Leary, R.** (2022). Building a practical information security program. Syngress.
2. **Arkin, B., Stender, S., & McGraw, G.** (2022). Software penetration testing: Modern approaches and tooling. IEEE Security & Privacy, 20(2), 84-91.
3. **Conklin, W. A., & Shoemaker, D.** (2023). Principles of computer security: CompTIA Security+ and beyond (6th ed.). McGraw-Hill.
4. **Engebretson, P.** (2021). The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy (3rd ed.). Syngress.
5. **Forshaw, J.** (2021). Attacking network protocols: A hacker's guide to capture, analysis, and exploitation. No Starch Press.
6. **Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M.** (2022). Metasploit: The penetration tester's guide (2nd ed.). No Starch Press.
7. **Kim, P.** (2023). The hacker playbook 3: Practical guide to penetration testing. Secure Planet.
8. **Lyon**, G. F. (2021). Nmap network scanning: The official Nmap project guide to network discovery and security scanning (Updated ed.). Nmap Project.
9. **Messier, R.** (2022). CEH v11 certified ethical hacker study guide. Sybex.
10. **MITRE Corporation** (2023). MITRE ATT&CK framework for penetration testers. Retrieved from https://attack.mitre.org
11. **Nazario, J.** (2023). Purple team strategies: Enhancing red and blue team collaboration. Apress.
12. **NIST** (2021). Technical guide to information security testing and assessment (SP 800-115, Revision 1). National Institute of Standards and Technology.
13. **Oakley, J. G.** (2021). Wireshark for security professionals: Using Wireshark and the Metasploit framework. Wiley.
14. **OWASP Foundation** (2023). OWASP Testing Guide v5. Retrieved from https://owasp.org/www-project-web-security-testing-guide/
15. **PortSwigger** (2024). Burp Suite Documentation. Retrieved from https://portswigger.net/burp/documentation
16. **PTES** (2022). The penetration testing execution standard (Updated version). Retrieved from http://www.pentest-standard.org/
17. **SANS** Institute (2024). Penetration testing methodologies and reporting. SANS Reading Room. Retrieved from https://www.sans.org/reading-room
18. **Sanders, J.** (2023). The purple team handbook: A practical guide to leveraging purple teaming for optimal security (2nd ed.). Independently published.
19. **Shostack, A.** (2022). Threat modeling: Designing for security (2nd ed.). Wiley.
20. **Tamma, R., & Tindall, D.** (2021). Learn penetration testing: Understand the art of ethical hacking from scratch. Packt Publishing.
21. **Tenable** (2024). Nessus Professional 10.x. Retrieved from https://www.tenable.com/products/nessus
22. **Vacca, J. R.** (2022). Network and system security (3rd ed.). Elsevier.
23. **Wright, J.** (2023). Hacking exposed: Network security secrets & solutions (8th ed.). McGraw-Hill.
24. **Clarke, J.** (2022). SQL injection attacks and defense (3rd ed.). Syngress.
25. **Howard, M., & LeBlanc, D.** (2021). Writing secure code (3rd ed.). Microsoft Press.

تم بحمد الله