**Student Assessment Submission and Declaration**

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

|  |  |  |  |
| --- | --- | --- | --- |
| Student name : Ahmad kallab | | Assessor name: | |
| Issue date:  **3/12/2023** | Submission date:  **26/1/2024** | | Submitted on: |
| Programme:  Higher National Diploma in Cloud Computing – Cloud Computing | | | |
| Unit: 3. Security in the Cloud | | | |
| Assignment number and title: 1. Configuring cloud security measures on cloud-based systems | | | |

**Task A 1.a**

**حدّد أهمية المعايير الأمنية والغرض منها، ووضّح كيف أن الامتثال لهذه المعايير يعزز الأمن العام للأنظمة:**

للأسف ، نحن موجودون في عالم تكون فيه الشركات أهدافًا ضعيفة. سواء كان ذلك مدفوعا بالمكاسب المالية أو مصالح الدولة ، فقد حوّل المتسللون سبل عيش الآخرين إلى مصدر دخل غير مبرر. يشكل هذا الوضع تهديدا وجوديا للشركات الصغيرة والمتوسطة. عادة ما تفتقر الشركات الصغيرة والمتوسطة إلى الموارد المالية لتوظيف فريق كامل من خبراء الأمن السيبراني المهرة ، ولا تزال تواجه حاجة ماسة للأمن. يتمثل أحد الأساليب التي تتبعها الشركات الصغيرة لتعزيز دفاعاتها هي اعتماد معايير الأمن السيبراني

**لماذا يُعد اتباع هذه المعايير امرًا مُهمًا؟**

عند النظر في تعريف المعيار ، فإنه يؤدي بطبيعة الحال إلى السؤال عن سبب أهمية معايير الأمن السيبراني. السبب الرئيسي والأكثر فائدة للمنظمات هو أن هذه المعايير يمكن أن تعزز بشكل كبير الموقف الأمني للمنظمة دون الحاجة إلى تقنيات جديدة مكلفة. بينما تهدف معايير الأمن السيبراني إلى منع الهجمات ، أيضًا, من المهم الاعتراف بأن الهجمات تحدث بالفعل في واقعنا الحالي لكن اتّباع المعايير قد يحدّ من هذا الامر. تتطلب المعايير والشهادات أن يكون لدى المنظمات سياسات للاستجابة للحوادث ، مما يوفر الطمأنينة للمستخدمين لأن أولئك المكلفين بالاستجابة لحادثٍ ما على دراية جيدة بالخطوات اللازمة التي يجب اتخاذها.

على سبيل المثال :

1. تساعد على تقليل المخاطر من خلال توفير إطار لتحديد وتقييم وإدارة التهديدات الأمنية ونقاط الضعف
2. تساعد على تقليل أقساط التأمين من خلال إظهار أن المنظمة قد اتخذت تدابير معقولة لحماية أصولها وبياناتها
3. تساعد على البقاء على الجانب الأيمن من القانون من خلال الامتثال للوائح والتشريعات ذات الصلة ، مثل اللائحة العامة لحماية البيانات (GPDR) أو معيار أمن بيانات صناعة بطاقات الدفع (PCI DSS).
4. تساعد على زيادة الثقة والسمعة من خلال إثبات أن المنظمة تقدر الأمن وتحترم خصوصية أصحاب المصالح.
5. تساعد على تبادل المعرفة وأفضل الممارسات من خلال تسهيل التفاهم والتواصل المشترك بين المتخصصين والخبراء في مجال الأمن

**ما الغرض من اتباع هذه المعايير:**

الغرض من اتباع معايير الأمان هو حماية معلومات وأنظمة المؤسسة من التهديدات والمخاطر السيبرانية. توفر معايير الأمان إرشادات وأفضل الممارسات والمتطلبات لتنفيذ الضوابط والعمليات الأمنية التي يمكن أن تمنع أو تخفف من الهجمات الإلكترونية. من خلال اتباع معايير الأمان ، يمكن للمؤسسة أيضا إثبات امتثالها للالتزامات القانونية والتعاقدية ، فضلا عن التزامها بحماية بيانات عملائها وشركائها.

**1.** يمكن أن يساعد اتباع معايير الأمان المؤسسة على تحديد أصولها وتهديداتها ونقاط ضعفها ومخاطرها ، وتقييم تأثير واحتمال وقوع حوادث محتملة.

**2.**  يمكن أن يساعد اتباع معايير الأمان المنظمة على اختيار وتنفيذ الضوابط والتدابير الأمنية المناسبة ، مثل السياسات والإجراءات والتقنيات والتدريب ، لتقليل المخاطر إلى مستوى مقبول.

**3.** يمكن أن يساعد اتباع معايير الأمان المنظمة على مراقبة ومراجعة فعالية وأداء الضوابط والتدابير الأمنية الخاصة بها ، وتحسينها حسب الحاجة ، بناء على التغذيه الراجعه وعمليات التدقيق.

**كيف أن الامتثال لهذه المعايير يعزز الأمن العام للأنظمة ؟**

يعد الامتثال لمعايير الأمان ضرورة استراتيجية للمؤسسات التي تتطلع إلى تعزيز وضعها في مجال الأمن السيبراني بشكل شامل. توفر معايير الأمان للمؤسسات إطارا منظما من الإرشادات وأفضل الممارسات والمتطلبات الإلزامية ، وهي بمثابة خارطة طريق لتعزيز آليات الدفاع الخاصة بها. تتجاوز الفوائد المتعددة الأوجه للالتزام بهذه المعايير المتطلبات التنظيمية وتساهم بشكل كبير في مرونة المنظمة بشكل عام.

تتمثل إحدى المزايا الأساسية في القدرة على حماية سمعة المؤسسة وثقة العملاء وولائهم. من خلال إظهار الالتزام الواضح بالأمان والجدارة بالثقة من خلال الامتثال لهذه المعايير، تغرس المؤسسات الثقة بين قاعدة عملائها. هذه الثقة هي أحد الأصول القيمة التي يمكن أن تكون محورية في الحفاظ على علاقات العملاء وجذب فرص عمل جديدة.

علاوة على ذلك ، فإن الامتثال لمعايير الأمان يزود المنظمات بميزة تنافسية. إن تلبية أو تجاوز توقعات العملاء وشركاء الأعمال والمنظمين يسرع دورة المبيعات ويعزز مكانة المنظمة في السوق. إنه دليل على تفاني المنظمة في الأمن ، والذي يمكن أن يكون عاملا حاسما في عمليات صنع القرار للعملاء والشركاء المحتملين.

يكشف الغوص الأعمق في الجوانب الفنية أن مبادرات الامتثال تدفع التحسينات في البنية التحتية والعمليات التكنولوجية للمؤسسة. من خلال تنفيذ أفضل الممارسات الأمنية المعترف بها ، تخلق المؤسسات أساسا قويا لإدارة التهديدات ونقاط الضعف بشكل فعال. وهذا لا يعزز الموقف الأمني للمنظمة فحسب ، بل يعزز أيضا ثقافة الأمن والوعي بالامتثال بين الموظفين.

تمتد أهمية الامتثال إلى المناظر الطبيعية القانونية والتنظيمية. يجب على المؤسسات التنقل في شبكة معقدة من المتطلبات ، ويضمن الالتزام بمعايير الأمان التوافق مع الالتزامات التجارية والقانونية والتعاقدية والتنظيمية. هذه المواءمة ، بدورها ، تحمي المنظمة من التعقيدات القانونية والالتزامات المحتملة ، مما يساهم في إدارة المخاطر بشكل عام.

غالبا ما يتم تنظيم النهج المنهجي والاستباقي الذي تدعو إليه المعايير الأمنية حول دورة خطة القيام بفحص الفعل (PDCA). يسمح هذا النهج للمؤسسات بتحسين أنظمة إدارة أمن المعلومات الخاصة بها(ISMS) باستمرار من خلال تحديد مخاطر أمن المعلومات وتقييمها والتخفيف منها. كما تؤكد الدورة على المراقبة المستمرة والقياس والتحليل والتقييم لأداء نظام إدارة المعلومات ، مما يضمن إطارا أمنيا ديناميكيا وسريع الاستجابة.

وتشكل عمليات المراجعة الداخلية للحسابات واستعراضات الإدارة ، وفقا لما تنص عليه المعايير الأمنية ، عناصر حاسمة في رحلة الامتثال. توفر هذه العمليات للمنظمات نظرة ثاقبة حول فعالية تدابيرها الأمنية ، مما يمكنها من تحديد مجالات التحسين وتنفيذ الإجراءات التصحيحية على الفور.

بنفس القدر من الأهمية هو التركيز على كفاءة الموظفين والوعي والتدريب في سياق نظام إدارة المعلومات. تعترف معايير الأمن بالعامل البشري كعنصر حاسم في الحفاظ على بيئة آمنة. من خلال التأكد من أن الموظفين على دراية جيدة بالبروتوكولات والإجراءات الأمنية ، تقلل المنظمات من احتمال أن يصبح الخطأ البشري ثغرة أمنية كبيرة.

التوثيق هو حجر الاساس في معايير الأمان ، ويفصل المعلومات التي يتطلبها المعيار ونظام إدارة المعلومات الخاص بالمنظمة. يساهم إنشاء هذه المستندات والموافقة عليها وتوزيعها واستخدامها وحمايتها والاحتفاظ بها والتخلص منها في الحوكمة الشاملة للمعلومات داخل المنظمة.

في حين أن الامتثال لمعايير الأمان يوفر بلا شك عددا لا يحصى من الفوائد ، فمن الضروري التأكيد على أن الامتثال هو خط الأساس وليس الوجهة. يجب أن تطمح المنظمات إلى تنمية ثقافة ذات عقلية أمنية تتجاوز متطلبات الامتثال. وهذا ينطوي على التزام مستمر بتحسين الممارسات الأمنية ، والتكيف مع التهديدات الناشئة ، وتعزيز موقف مرن للأمن السيبراني يمكنه تحمل مشهد التهديد المتطور.

**Task A 1.b**

(International Organization for Standardization) ISO :المنظمة الدولية للتوحيد القياسي هي منظمة دولية مستقلة غير حكومية تقوم بتطوير ونشر المعايير لضمان جودة وسلامة وكفاءة المنتجات والخدمات والأنظمة. تغطي معايير الأيزو مجموعة واسعة من الصناعات والقطاعات ، وتوفر مواصفات للعمليات والمنتجات والخدمات.

NIST SP 800-53 Rev. 5 : هو منشور من المعهد الوطني للمعايير والتكنولوجيا (NIST) في الولايات المتحدة. على وجه التحديد ، هو جزء من المنشور الخاص 800 جزء (Special Publication 800 series) ، التي تتناول إرشادات ومعايير أمن المعلومات للوكالات والمقاولين الفيدراليين. NIST SP 800-53 Rev. 5 يركز على ضوابط الأمن والخصوصية لنظم المعلومات الاتحادية والمنظمات.

هذه بعض المقارنات الخاصه بكل من هذين المعيارين :

|  |  |  |  |
| --- | --- | --- | --- |
| **التقيّدات** | **الفوائد** | **النِطَاق** | **المعيار** |
| 1- التعقيد:بسبب أنه مفصل وشامل ، قد يكون تحديا للمنظمات ، وخاصة تلك ذات الموارد المحدودة.  2- قابلية التطبيق: قد لا تكون جميع الضوابط ذات صلة بكل منظمة ، مما يتطلب الاندماج بناء على سياقات محددة.  3- الموارد المكثفة: يمكن أن يتطلب تنفيذ الضوابط والحفاظ عليها وقتا وجهدا وموارد كبيرة.  4- التحديثات المستمرة: التحديثات المنتظمة ضرورية لمعالجة التهديدات والتقنيات المتطورة للأمن السيبراني.  5- المرونة: بينما يتم تشجيعه على تكييف الضوابط ، فإن تحقيق المرونة يتطلب فهما عميقا لكل من المنظمة ونية التحكم.  6- قابلية التشغيل البيني: قد يشكل الموائمة مع المعايير الأخرى تحديات ،  خاصة عند الامتثال ل معايير عمل متعددة | 1- يقدم مجموعة واسعة من ضوابط الأمان والخصوصية التي يمكن تعديلها لتناسب الاحتياجات الفريدة للمؤسسات والأنظمة المختلفة.  2- يساعد المؤسسات في تعزيز إجراءات إدارة المخاطر الخاصة بها والوصول إلى أهداف الأمان والخصوصية الخاصة بها.  3- يساعد في الامتثال للقوانين والسياسات واللوائح والمعايير الهامة لأمن المعلومات والخصوصية.  4- وايضًا يشمل إدارة مخاطر سلسلة التوريد ، والضوابط الحديثة ، وبيانات التحكم التي تركز على النتائج في كتالوج التحكم.  5- يشجع على التعاون والتنسيق بين مبادرات الأمن والخصوصية ويغذي ثقافة الوعي والمساءلة عن الأمن والخصوصية | نطاق NIST SP 800-53 Rev. 5 هو توفير كتالوج من الضوابط الأمنية والخصوصية لنظم المعلومات والمنظمات من جميع الأنواع والأحجام ، بما في ذلك الحكومات الاتحادية والولائية والمحلية والقبلية والإقليمية ، فضلا عن القطاع الخاص والأوساط الأكاديمية. ينطبق المنشور على الأنظمة التي تعالج أو تخزن أو تنقل المعلومات الفيدرالية ، وكذلك الأنظمة التي يتم تشغيلها من قبل المقاولين أو المنظمات الأخرى نيابة عن الحكومة الفيدرالية.  ويدعم المعيار أيضا تنفيذ القانون الاتحادي لتحديث أمن المعلومات(FISMA),  قانون الخصوصية لعام 1974 ، وقانون الحكومة الإلكترونية لعام 2002 ، وقانون تحديث نظم المعلومات الفيدرالية لعام 2014 ، والقوانين والسياسات والتوجيهات واللوائح والمعايير والمبادئ التوجيهية الأخرى ذات الصلة. | **NIST SP 800-53 Rev. 5** |
| 1-يجب تحديد نطاق نظام إدارة المعلومات وتوثيقه بوضوح ، مع مراعاة سياق واحتياجات وتوقعات المنظمة وأصحاب المصلحة فيها.  2 - يتعين على المنظمة إجراء تقييم للمخاطر وعملية معالجة المخاطر ، وتحديد مخاطر أمن المعلومات واختيار الضوابط المناسبة من الملحق A أو من مصادر أخرى.  3- يتعين على المنظمة إنشاء نظام إدارة المعلومات وتنفيذه وصيانته وتحسينه باستمرار ، باتباع دورة الخطة-القيام-التحقق-الفعل (PDCA).  4- يجب على المنظمة الامتثال للمتطلبات القانونية والتنظيمية والتعاقدية وغيرها من المتطلبات التي تنطبق على أنشطة أمن المعلومات الخاصة بها.  5- يتعين على المنظمة إجراء عمليات تدقيق داخلية ومراجعات إدارية لنظام إدارة المعلومات على فترات مخططة.  6- يجب على المنظمة ضمان كفاءة وتوعية وتدريب الموظفين المشاركين في نظام إدارة المعلومات.  ملاحظة: هذه القيود ليست بالضرورة سلبية أو مرهقة ، لأنها يمكن أن تساعد المنظمة على تحقيق أهدافها المتعلقة بأمن المعلومات وتحسين وضعها الأمني. | بعض فوائد الامتثال لشهادة الأيزو 27001 وشهادتها هي:  1 - يمكن أن يساعدني في تجنب التكاليف المالية المرتبطة بانتهاكات البيانات ، والتي يمكن أن تكون عالية جدا  2 - يمكن أن تعزز سمعة علامتي التجارية وكسب عملاء جدد من خلال إثبات أمنك وجدارة بالثقة .  3 - يمكن أن تعطيني ميزة تنافسية على المنافسين غير المتوافقة وتسريع دورة المبيعات .  4 - يمكنه تحسين البنية التحتية والعمليات التقنية الخاصة بي من خلال تنفيذ أفضل الممارسات الأمنية وخلق ثقافة الأمان والامتثال.  5 - يمكن أن يساعدني في الامتثال للمتطلبات التجارية والقانونية والتعاقدية والتنظيمية . | نطاق نظام إدارة أمن المعلومات هو مدى نظام إدارة أمن المعلومات في المنظمة. يحدد المعلومات التي تنوي حمايتها. يتم تحديد النطاق من خلال مراعاة القضايا الداخلية والخارجية واحتياجات وتوقعات الأطراف المعنية ، والواجهات والتبعيات بين ما يحدث داخل نطاق نظام إدارة المعلومات والعالم الخارجي. يعد بيان النطاق أحد أهم الوثائق في مشروع تنفيذ الأيزو 27001 . | **ISO 27001** |

**تحليل كيفية مساهمة كل معيار في ضمان أمان الأنظمة المستندة إلى السحابة:**

**ISO 27001**:

**الإدارة الأمنية الشاملة:** تركز الأيزو 27001 على أنظمة إدارة أمن المعلومات. يساعد المؤسسات على إنشاء إطار عمل قوي لإدارة المعلومات وحمايتها ، بما في ذلك البيانات المخزنة والمعالجة في البيئات السحابية.

**إدارة المخاطر:** يتطلب المعيار من المؤسسات إجراء تقييمات للمخاطر ، وهو أمر ضروري لتحديد نقاط الضعف والتهديدات المحتملة المرتبطة بالأنظمة المستندة إلى السحابة. هذا النهج الاستباقي أمر بالغ الأهمية لمنع الخروقات الأمنية.

**الامتثال القانوني والتنظيمي:** تؤكد الأيزو 27001 على الامتثال للمتطلبات القانونية والتعاقدية. في سياق الأنظمة السحابية ، يضمن ذلك التزام المؤسسات بقوانين حماية البيانات واللوائح الأخرى التي تحكم السحابة.

**التحسين المستمر:** تنص الأيزو 27001 على التحسين المستمر لنظام إدارة المعلومات. في المشهد الديناميكي للحوسبة السحابية ، يضمن ذلك تطور الإجراءات الأمنية لمعالجة التهديدات ونقاط الضعف الناشئة.

**NIST SP 800-53 Rev. 5**:

**كتالوج الضوابط الأمنية**: NIST SP 800-53 Rev. 5 يوفر كتالوج شامل من الضوابط الأمنية والخصوصية. تم تصميم عناصر التحكم هذه خصيصا لمواجهة التحديات الفريدة التي تطرحها أنظمة المعلومات ، بما في ذلك تلك المنتشرة في البيئات السحابية.

**قابلية التطبيق عبر بيئات متنوعة:** ينطبق معيار نيست على أنواع وأحجام مختلفة من المنظمات ، بما في ذلك تلك الموجودة في القطاع الخاص والأوساط الأكاديمية. تضمن هذه العالمية أن عناصر التحكم في الأمان قابلة للتكيف مع الأنظمة المستندة إلى السحابة المختلفة.

الامتثال للقوانين الاتحادية: **NIST SP 800-53 Rev.** 5يدعم الامتثال للقوانين الاتحادية المتعلقة بأمن المعلومات والخصوصية. بالنسبة للأنظمة السحابية المستخدمة أو التي يتم تشغيلها نيابة عن الوكالات الفيدرالية ، يعد الالتزام بهذه الضوابط أمرا بالغ الأهمية للحفاظ على الامتثال القانوني.

**المراقبة المستمرة:** يؤكد المعيار على المراقبة والتحديثات المستمرة. في سياق الأمان السحابي ، يعد هذا أمرا حيويا لاكتشاف التهديدات والاستجابة لها في الوقت الفعلي ، مع الأخذ في الاعتبار الطبيعة الديناميكية للبنى التحتية المستندة إلى السحابة.

الخلاصه:توفر شهادة الأيزو 27001 نهجا شاملا لإدارة أمن المعلومات ، بما في ذلك الأنظمة السحابية ، في حين تقدم شهادة الأيزو 800-53 مراجعة 5 فهرسا مفصلا للضوابط المصممة خصيصا للتحديات الفريدة لنظم المعلومات ، مما يضمن قدرتها على التكيف مع البيئات السحابية المختلفة. يساهم كلا المعيارين بشكل كبير في إنشاء وصيانة تدابير أمنية قوية في الأنظمة المستندة إلى السحابة.

**Task A 1.c**

**قيّم أهمية تطبيق معايير الأمان في تطوير البنية التحتية السحابية للمؤسسة. أصدر نتائج واضحة بناءا على الفحص والتحليل الشامل الذي قمت به**

**في نسيج معقد من الأمن السحابي ، التآزر التعاوني بين**

ISO/IEC 27001, NIST SP 800-53, CSA, Security Guidance (Cloud Controls Matrix), PCI DSS, FedRAMP, and GDPR **ينسج إطار متعدد الأوجه التي ترفع ضمان النظم القائمة على السحابة إلى آفاق جديدة. وتعد** ISO/IEC 27001 **بمثابة المحور الأساسي ، حيث تقوم بتنسيق نظام شامل لإدارة أمن المعلومات لا يمهد الطريق لتحديد المخاطر فحسب ، بل يوفر أيضا آلية منظمة للتخفيف المستمر من المخاطر.** NIST SP 800-53 **53 يكمل هذا التزامن من خلال المساهمة ب كتالوج شامل من الضوابط الأمنية. يتعمق هذا الكتالوج ، الغني بالتفاصيل ، في تعقيدات أمن المعلومات ، ويغطي جوانب تتراوح من عناصر التحكم في الوصول والتشفير إلى الاستجابة للحوادث. تقدم إرشادات أمان وكالة الفضاء الكندية** CSA **، مع مصفوفة عناصر التحكم السحابية الخاصة بها (**CCM**)، منهجية دقيقة لتقييم وتقوية المواقف الأمنية للخدمات السحابية المتنوعة. خَلف هذا،** PCI DSS **خطوات في المشاركه التعاونيه ، وضمان معالجة آمنة لبيانات الدفع — جانب غير قابل للتفاوض في المشهد سحابة ديناميكية.**

**ثم يضيف** FedRAMP  **وزنه إلى المسعى التعاوني ، حيث يجلب معايير أمنية خاصة بالأدوار التي يتردد صداها بشكل خاص مع مزودي الخدمات السحابية الذين يلبون المتطلبات الصارمة للوكالات الحكومية. وفي الوقت نفسه ، يقدم الناتج المحلي الإجمالي ، على الرغم من أنه ليس معيارا تقنيا صارما ، طبقة مهمة من اعتبارات حماية البيانات ، تتماشى بسلاسة مع الأهداف الأوسع لهذه المعايير التعاونية. تركيزها على الخصوصية الفردية وممارسات معالجة البيانات يتردد صداها من خلال السيمفونية التعاونية ، مما يعزز أهمية إدارة البيانات الأخلاقية والمسؤولة في البيئات السحابية.**

**معًا، تخلق هذه السيمفونية المنظمة للمعايير نهجا شاملا وديناميكيا لأمن السحابة. إنه ينسج بشكل معقد عناصر إدارة المخاطر ، ومراقبة التنفيذ ، والامتثال ، وحماية البيانات في نسيج الأنظمة المستندة إلى السحابة. في هذا التقارب المتناغم ، لا تجد سلامة المعلومات وسريتها وتوافرها في السحابة ضمانا فحسب ، بل وضعا أمنيا مرنا ومتكيفا في مواجهة التهديدات السيبرانية المتطورة.**

لتقييم أهمية تنفيذ معايير الأمان في تطوير البنية التحتية السحابية للمؤسسة سنأخذ شركة أكتفيل (Actfile) على سبيل المثال :  
أكتيفيل هي منصة أمن البيانات السحابية التي تعمل على تأمين تعمل على تأمين البيانات السحابية للعاملين المستقلين واقتصاد الأعمال المستقلة. وفقا لموقعها على شبكة الإنترنت ، تأسست أكتيفيل في عام 2017 من قبل غاي بافلي وعساف ليتال ، الذي أدرك أن الحلول التقليدية لمنع فقدان البيانات (DLP) لم تكن فعالة للبيانات التي تتواجد وتتحرك في كل مكان كجزء من العمليات التجارية القياسية للمنظمة. لقد طوروا تقنية يمكنها مراقبة تدفقات الملفات وتحليل محتواها وتشفير البيانات الحساسة. وتتمثل مهمة أكتيفيل في توفير أساس متين من الأمن السيبراني يسمح للمؤسسات بالنمو وتحقيق أقصى إمكاناته.

يخدم أكتيفيل أساسا الشركات الصغيرة والمتوسطة (SMBs) في الولايات المتحدة ، من خلال مقدمي الخدمات المدارة (MSPs) الذين يعملون كقسم تكنولوجيا المعلومات الاستعانة بمصادر خارجية. تساعد أكتيفيل عملائها ليس فقط على تأمين بياناتهم ، ولكن أيضا على الامتثال للوائح وقوانين خصوصية البيانات المختلفة السائدة في الولايات المتحدة والعالم ، مثل HIPAA, NIST, GDPR, PDPA . تدّعي شركة أكتيفيل أن حلها سهل الاستخدام وفعال من حيث التكلفة وقابل للتطوير. في عام 2022 ، اعتمدت أكتيفيل معيار الأيزو 27001 لإثبات التزامها بحماية البيانات والامتثال لها.

**الان لنقيم أهمية تنفيذ معايير الأمان في تطوير البنية التحتية السحابية لأكتيفيل:**

1- تعزيز حماية البيانات:

**الأهمية: يضمن تطبيق معايير الأمان ، مثل الأيزو 27001 ، اتباع نهج منهجي لإدارة أمن المعلومات. ل أكتيفيل ، وهذا يترجم إلى تعزيز الحماية للبيانات الحساسة من لحسابهم الخاص والعاملين في أزعج ، وتعزيز الثقة في النظام الأساسي.**

2- الامتثال التنظيمي:

**الأهمية: يعد الالتزام بمعايير الأمان أمرا بالغ الأهمية للامتثال للوائح الصناعة. في حالة أكتيفيل ، يعني هذا التوافق مع قوانين ولوائح حماية البيانات ، وهو جانب حاسم نظرا لحساسية المعلومات التي يتم التعامل معها في الاقتصاد المستقل والاقتصاد المؤقت.**

3- التخفيف من المخاطر والمرونة:

**الأهمية: توفر المعايير الأمنية إطارا لتحديد المخاطر الأمنية وتقييمها والتخفيف من حدتها. بالنسبة إلى أكتيفيل ، يساهم نهج إدارة المخاطر الاستباقي هذا في مرونة البنية التحتية السحابية ، مما يقلل من احتمالية وتأثير الحوادث الأمنية المحتملة.**

4- ثقة العملاء:

**الأهمية: تعمل المعايير الأمنية كآلية لبناء الثقة. من خلال اعتماد إيزو 27001 ، أكتيفيل يرسل رسالة واضحة إلى قاعدة مستخدميها أن يتم التعامل مع البيانات الخاصة بهم مع أعلى معايير الأمن. لا يحتفظ هذا بالعملاء الحاليين فحسب ، بل يجذب أيضا العملاء الجدد الذين يعطون الأولوية للتدابير الأمنية القوية.**

5- ميزة تنافسية:

**الأهمية: في سوق تنافسية ، والالتزام بالمعايير الأمنية يعطي أكتيفيل ميزة تنافسية متميزة. شهادة الأيزو 27001 هي علامة مرئية تميز أكتيفيل ، مما يؤكد للعملاء أن المنصة تذهب إلى أبعد الحدود في ضمان أمن وخصوصية بياناتهم.**

6- قابلية التوسع والتدقيق في المستقبل:

**الأهمية: غالبا ما تتضمن معايير الأمان إرشادات للهندسة المعمارية القابلة للتطوير. ل أكتيفيل ، وهذا يعني القدرة على النمو وتوسيع البنية التحتية السحابية بسلاسة مع الحفاظ على موقف أمني قوي. يضمن أن الاعتبارات الأمنية جزء لا يتجزأ من استراتيجية نمو المنصة.**

7- الاستجابة للحوادث والتعافي منها:

**الاهميه: توفر المعايير الأمنية إرشادات للاستجابة للحوادث والتعافي منها. في حالة وقوع حادث أمني ، يمكن أن تعتمد أكتيفيل على نهج منظم لتقليل الضرر ، والتعافي بسرعة ، والتعلم من الحادث لتعزيز إجراءاته الأمنية.**

8- ضمان البائع والشريك:

**الاهميه: الالتزام بالمعايير الأمنية يطمئن شركاء أكتيفيل والبائعين حول أمن النظام البيئي التعاوني. هذا أمر بالغ الأهمية بشكل خاص في بيئة قائمة على السحابة حيث تتفاعل كيانات متعددة ، مما يضمن التزاما جماعيا بأفضل الممارسات الأمنية.**

**إن أهمية تنفيذ معايير الأمان للبنية التحتية السحابية لأكتيفيل متعددة الأوجه. إنه يتجاوز مجرد الامتثال ، ويؤثر على الموقف الأمني للمنصة ، وثقة العملاء ، وتحديد المواقع التنافسية ، والاستعداد العام للتنقل في المشهد المتطور لاقتصاد العمل الحر والاقتصاد. يعد هذا الاستثمار الاستراتيجي في معايير الأمان جزءا لا يتجزأ من نجاح أكتيفيل واستدامته في صناعة الخدمات السحابية.**

**TASK A .2**

**Cryptographic hashes او تجزئة التشفير:**

**تشفير الهاش، هي وظائف رياضية تأخذ إدخالًا (أو "messeage") وتنتج سلسلة ثابتة الحجم من الأحرف، وعادةً ما تكون قيمة للهاش أو رمز هللاش. تتمتع هذه الوظائف بعدة خصائص حاسمة تجعلها مناسبة لتطبيقات التشفير:**

1. **تحديدية(Deterministic) :نفس الإدخال سينتج دائمًا نفس قيمة الهاش.**
2. **حساب سريع(Fast Computation): يجب أن تكون قيمة الهاش قابلة للحساب بكفاءة.**
3. **مقاومة الصورة السابقة (Pre-image Resistance): يجب أن يكون من الصعب حسابيًا عكس العملية وتحديد الإدخال الأصلي من قيمة الهاش.**
4. **مقاومة التصادم (Collision Resistance) : يجب أن يكون من غير المرجح أن تنتج اثنتان من الإدخالات المختلفة نفس قيمة الهاش.**
5. **تأثير الانهيار ( Avalanche Effect) : يجب أن يؤدي تغيير طفيف في الإدخال إلى قيمة هاش مختلفة بشكل كبير.**

**يتم استخدام التشفير الهاش على نطاق واسع في أمان المعلومات لأغراض متنوعة، بما في ذلك:**

* **نزاهة البيانات: التحقق من أن البيانات لم تتغير عن طريق مقارنة قيم الهاش.**
* **التواقيع الرقمية: ضمان أصالة ونزاهة رسالة أو وثيقة.**
* **تخزين كلمات المرور: تخزين كلمات المرور المشفرة بدلاً من النص العادي لتعزيز الأمان.**
* **تكنولوجيا البلوكشين: إنشاء سلسلة آمنة ومضادة للتلاعب.**

**وتشمل وظائف تشفير الهاش الشائعة MD5 وSHA-1 وSHA-256 و SHA-3.**

**هل يمكن للمنصات السحابية ضمان أمن البيانات؟ تصور قفلًا رقميًا يحمي المعلومات برمز غير قابل للكسر. على سبيل المثال** "**Cryptographic hashes "، وهو عنصر أساسي يعزز أمن البيانات في المجال الرقمي. تتضمن تجزئة الحوسبة السحابية تحويل البيانات إلى سلاسل ذات حجم ثابت، وإنشاء قيم تجزئة فريدة مثل بصمات الأصابع الرقمية. وهذا يضمن استرجاع البيانات بسرعة مع الحفاظ على إجراءات أمنية مشددة. و يتعمق الاستكشاف في أهمية الهاش ، وتطبيقات العالم الحقيقي، والتوازن الدقيق بين الهاش والتشفير.**

**في الحوسبة السحابية، تعمل التجزئة كحارس رقمي، مما يدعم أمن البيانات من خلال إطارها القوي. وفي جوهرها، تعمل التجزئة على تحويل البيانات إلى سلاسل ذات حجم ثابت، مما يؤدي إلى إنشاء قيم تجزئة فريدة تعمل بمثابة بصمات أصابع رقمية، مما يضمن سلامة البيانات عبر البيئه السحابيه.**

**يشمل الهاش في الحوسبة السحابية تحويل البيانات إلى قيم تجزئة من خلال خوارزمية محددة مسبقًا، مما يوفر تمثيلًا ثابتًا بغض النظر عن حجم البيانات. تنتج وظائف التجزئة، بطبيعتها الحتمية، باستمرار نفس قيمة التجزئة لمجموعة بيانات معينة، مما يضمن القدرة على التنبؤ والموثوقية. تلعب خوارزميات التجزئة الشائعة مثل MD5 وSHA-1 وSHA-256 أدوارًا رئيسية، حيث تقدم كل منها سمات فريدة. تتراوح تطبيقات التجزئة في السحابة من ضمان سلامة البيانات أثناء النقل إلى تأمين كلمات المرور والتحقق من صحة التوقيعات الرقمية.**

**انظر للصوره رقم A .2.1**

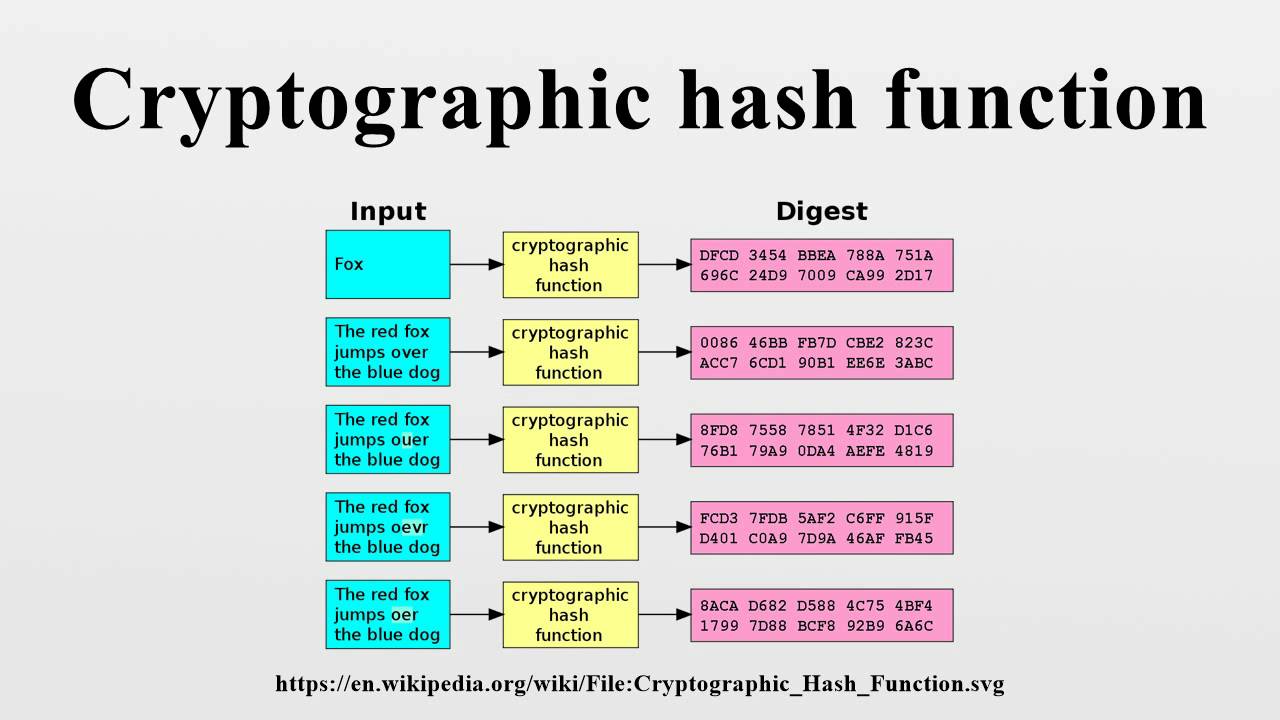
**تصبح أهمية التشفير الخاصة بـ Cryptographic hashes واضحة في طبيعتها الحتمية والثابتة والمقاومة للتشابه، مما يشكل درعًا لا يمكن اختراقه في المشهد المتطور للأمن الرقمي داخل البيئات السحابية.**

**تشبه طريقة عمل التجزئة في البيئات السحابية سيمفونية رقمية، حيث تلعب كل ملاحظة دورًا حاسمًا في تأمين تدفق المعلومات وتحسينه. تقوم عملية التجزئة بفك تشفير السيمفونية الرقمية عن طريق تحويل البيانات الأولية إلى رمز منيع، مما يضمن الأمان والكفاءة في تمثيل البيانات داخل الحوسبة السحابية.**

**تمتد براعة ال Cryptographic hashes إلى حالات الاستخدام المتنوعة في الحوسبة السحابية. في إلغاء البيانات المكررة للملفات، وتعمل قيمة الهاش الفريدة للتجزئة كبصمات أصابع رقمية، حيث تحدد بسرعة الملفات المكررة وتزيلها، وتحسن مساحة التخزين، وتبسط عملية استرجاع البيانات. يعمل التجزئة كموثق رقمي في التحقق من البيانات، ويؤكد على الفور سلامة البيانات من خلال مقارنة قيم التجزئة قبل وبعد نقل البيانات. تلعب المجموعه الاختبارية، المدعومة بخوارزميات الهاش، دورًا محوريًا في التخزين السحابي، مما يضمن سلامة البيانات على نطاق واسع من خلال التحقق من اتساق البيانات عبر أنظمة التخزين الموزعة.**

**في جوهر الأمر، تظهر التجزئة او ال Cryptographic hashes كبوصلة إرشادية في البحار الواسعه للحوسبة السحابية، حيث تقدم حلولاً للتحديات الملاحية المعقدة وتضمن موثوقية البيانات وأمنها في العصر الرقمي.**

**ملاحظه : بعض وظائف التشفير الهاش القديمة، مثل MD5 وSHA-1، تعتبر الآن ضعيفة ولا يوصى بها لتطبيقات تتطلب الأمان. تتضمن الممارسات الحديثة للتشفير غالبًا استخدام وظائف تشفير أقوى بحجم إخراج أكبر.**

****

Task **A .2.1**

**digital certificates او الشهاده الرقميه :**

**تعمل الشهادة الرقمية بمثابة بيانات اعتماد إلكترونية متطورة، وتعمل كدليل قاطع على شرعية الجهاز أو الخادم أو المستخدم. ومن خلال استخدام تقنيات التشفير المتقدمة والبنية التحتية للمفتاح العام (PKI)، تتولى بيانات الاعتماد هذه دور حارس الأمان الافتراضي، لا سيما في مجال شهادات SSL للتفاعلات الآمنة عبر الإنترنت. تحتوي الشهادات الرقمية على معلومات تفصيلية حول المستخدمين والأجهزة، بما في ذلك عناصر مثل عناوين IP أو الأرقام التسلسلية. يتضمن منح هذه الشهادات، الذي تنظمه سلطات التصديق (CAs)عمليات تحقق دقيقة وتنفيذ مصافحة مفتاح آمنة لضمان الأصالة الثابتة**

**تنبع السمات الجديرة بالثناء للشهادات الرقمية من فائدتها المتعددة الأوجه. إنهم يعملون كحراس يضمنون صحة المستندات، والتحقق من هويات المستخدم، وعرض بيانات اعتماد موقع الويب بشكل بارز. يعد التمييز بين الأنواع الرئيسية للشهادات الرقمية أمرًا بالغ الأهمية:**

1**. شهادات TLS/SSL :تنظم هذه الشهادات القوية الاتصالات الخاصة والمشفرة بين العملاء والخوادم عبر التطبيقات أو رسائل البريد الإلكتروني أو مواقع الويب. إنهم يخضعون لمستويات تحقق مختلفة:**

**- التحقق من صحة النطاق:التحقق السريع المناسب لأي موقع ويب، ويتم إصداره خلال دقائق.**

**- التحقق من صحة المنظمة : مصادقة الأعمال الخفيفة، خاصة بللتجارة الإلكترونية.**

**- التحقق الموسع: معيار شامل لمصادقة الأعمال، وهو ضروري للمؤسسات الكبيرة التي تتعامل مع البيانات الحساسة.**

2**. شهادات توقيع التعليمات البرمجية(Code Signing Certificates): تعمل هذه الشهادات كأمناء على سلامة البرامج، ويستخدمها المطورون أو الناشرون لتوقيع البرامج رقميًا. وهذا يضمن للمستخدمين صحة البرنامج وحالته غير المتلاعب بها.**

3**. شهادات العميل(Client Certificates): تعمل هذه الشهادات كبيانات اعتماد وصول مميزة للمستخدمين أو الأجهزة، ولا سيما السائدة في اتصالات البريد الإلكتروني، وتلعب دور المعرف الرقمي، مما يؤكد شرعية المرسل.**

**إن منح حالة VIP على هذه الشهادات الرقمية منوط بمراجع التصديق (CAs) تقوم هذه الكيانات، التي تعمل كأوصياء يقظين على صحة الإنترنت، بالتحقق بدقة من شرعية نطاق موقع الويب والتحقق من ملكية المفتاح العام المرتبط به. تمتد السمات البارزة للشهادات الرقمية إلى ما هو أبعد من مجرد الأمان؛ إنها تشمل قابلية التوسع للشركات ذات النطاقات المتنوعة، والالتزام بتعزيز الأصالة في الخطاب عبر الإنترنت، والجدارة بالثقة المدعومة بالتحقق الصارم من الصحة، ورمز الموافقة الذي يشهد على كل من الأصالة والالتزام بالخصوصية.**

**في مجال الحوسبة السحابية، يعد استخدام الشهادات الرقمية، وخاصة شهادات SSL/TLS، أمرًا محوريًا لضمان أمان وسلامة عمليات نقل البيانات وتفاعلات المستخدم. تستفيد Amazon Web Services (AWS) من هذه الشهادات لإنشاء قنوات اتصال آمنة بين العملاء وخوادم AWS. تلعب شهادات SSL/TLS دورًا حاسمًا في تشفير البيانات أثناء النقل، مما يساهم في السرية الشاملة وسلامة المعلومات المتبادلة عبر واجهة الويب لخدمات AWS. علاوة على ذلك، تقوم AWS بتوسيع إجراءاتها الأمنية من خلال شهادات العميل، مما يتيح المصادقة المتبادلة. وهذا يعني أن الخادم لا يقدم شهادة SSL/TLS الخاصة به للتحقق من هويته فحسب، بل يقدم العملاء أيضًا شهاداتهم، مما يعزز الأمان من خلال تأكيد هوياتهم.**

**علاوة على ذلك، في البيئة السحابية، تعد شهادات توقيع التعليمات البرمجية ضرورية للمطورين الذين ينشرون تطبيقاتهم على AWS. تضمن هذه الشهادات سلامة وأصالة الكود، وتمنع التعديلات غير المصرح بها. وهذا مهم بشكل خاص في بيئة سحابية مشتركة حيث تتعايش تطبيقات وخدمات متعددة. من خلال استخدام الشهادات الرقمية، تؤسس AWS وضعًا أمنيًا قويًا، وتعالج التحديات الفريدة المتمثلة في تأمين البيانات، والمصادقة على المستخدمين والعملاء، وضمان موثوقية التعليمات البرمجية المنشورة داخل مشهد الحوسبة السحابية.**

**Task B.1.a**

عند صياغة حل سحابي آمن ، تلعب اعتبارات الموارد (resource consideration) دورا محوريا في تشكيل متانة وفعالية التدابير الأمنية المنفذة. تعد هذه الاعتبارات جزءا لا يتجزأ من مواجهة التحديات الرئيسية ، مثل حماية معلومات العميل ، وضمان التوافر في الوقت الفعلي ، والالتزام بلوائح حماية البيانات ، واستيعاب التوسع القابل للتطوير. يسترشد اختيار الخدمات السحابية المناسبة وتقنيات الأمان والبروتوكولات باعتبارات الموارد هذه ، حيث يساهم كل منها في المرونة الشاملة والوضع الأمني للنظام القائم على السحابة. على سبيل المثال، يؤثر اختيار موارد الحوسبة على التوافر في الوقت الفعلي من خلال آليات التحجيم التلقائي، بينما تؤثر موارد التخزين على أمان البيانات وإمكانية الوصول. تساهم تكوينات الشبكة وضوابط الوصول في الحماية من الوصول غير المصرح به ، وتعد أدوات المراقبة ضرورية للكشف الفوري عن الحوادث الأمنية والاستجابة لها. إن فهم كيفية تفاعل اعتبارات الموارد هذه مع تخطيط حل سحابي آمن يوفر أساسا شاملا لوضع استراتيجية تتماشى مع الاحتياجات والتحديات الفريدة للمؤسسة الدولية للخدمات الإلكترونية (ICES) أثناء نقلها لخدماتها الإلكترونية إلى السحابة.

موارد الحوسبه (resources):

عند تطوير حل سحابي آمن ، تؤثر الاعتبارات الاستراتيجية المتعلقة باختيار الخدمات السحابية بشكل كبير على فعالية البنية التحتية الأمنية. تعد الاستفادة من قدرات مزودي الخدمات السحابية الرئيسيين ، مثل AWS (Amazon Web Services) و Azure (Microsoft Azure) ، أمرا أساسيا في مواجهة التحديات الأمنية المتنوعة.

1- لتشفير البيانات القوي، توفر خدمات التشفير الخاصة بالسحابة مثل AWS Key Management Service (KMS) وAzure Key Vault إدارة آمنة للمفاتيح، مما يضمن تشفير البيانات أثناء النقل وفي حالة عدم النشاط. تتم إدارة التحكم في الوصول بشكل فعال من خلال خدمات إدارة الهوية والوصول (IAM)، مثل AWS IAM وAzure Active Directory، مما يمكن المؤسسات من تحديد سياسات الوصول الدقيقة وإنفاذها.

2- تمتد خدمات IAM إلى ما هو أبعد من التحكم الأساسي في الوصول، حيث توفر إمكانات متقدمة لإدارة وصول المستخدم والأذونات داخل بيئة السحابة. لضمان النسخ الاحتياطي الشامل للبيانات واستعادتها، تمكن خدمات النسخ الاحتياطي السحابي مثل AWS Backup وAzure Backup المؤسسات من حماية سلامة البيانات والتعافي بسرعة من الحوادث غير المتوقعة، مما يعزز المرونة الشاملة للنظام.

3- يتم تسهيل تصحيح الأمان الآلي من خلال الأنظمة الأساسية السحابية مثل AWS و Azure ، مما يضمن تحديث جميع المكونات ، بما في ذلك التطبيقات وأنظمة التشغيل ، باستمرار بأحدث تصحيحات الأمان. يتم تعزيز أمان الشبكة في السحابة من خلال مجموعات أمان AWS ومجموعات أمان شبكة Azure، مما يوفر آليات أساسية للتحكم في حركة المرور الواردة والصادرة ومنع الوصول غير المصرح به.

4- لمراقبة الأمان في الوقت الفعلي، تقدم AWS CloudWatch، بينما يوفر Azure Azure Monitor، وكلاهما يعمل كخدمات مراقبة وتسجيل قوية. يضمن الاعتماد على تدابير الأمان المتأصلة في AWS وAzure أمانا قويا للموردين، ومواءمة البنية التحتية السحابية الشاملة مع أفضل ممارسات الصناعة ومعايير الامتثال.

5- يتم تنفيذ المصادقة متعددة العوامل (MFA) باستخدام خدمات المصادقة السحابية المضمنة التي تقدمها AWS Identity and Access Management (IAM) وAzure Active Directory. وأخيرا، يتم فرض سياسات أمان السحابة من خلال خدمات إدارة السياسات الخاصة بالسحابة في AWS وAzure، لتوجيه المؤسسات للالتزام بأفضل ممارسات الأمان والمتطلبات التنظيمية.

التقنيات والبروتوكولات (protocols & (techniques

في السعي للحصول على حل سحابي آمن ، يتم استخدام العديد من التقنيات لمعالجة اعتبارات أمنية محددة. هذه التقنيات ، المتجذرة في أفضل الممارسات ومعايير الصناعة ، محورية في تعزيز الوضع الأمني العام.

1- تصنيف البيانات:

التقنية: يلعب تطبيق تقنيات تصنيف البيانات دورا حاسما في تصنيف البيانات بشكل منهجي بناء على حساسيتها. يتضمن ذلك تحديد البيانات ووسمها وفقا لسريتها ، وضمان تطبيق التدابير الأمنية المناسبة لحمايتها.

2- تدريب الموظفين:

التقنية: إدراكا بأن الخطأ البشري هو مصدر شائع للانتهاكات الأمنية ، فإن إجراء دورات تدريبية منتظمة للموظفين أمر ضروري. تم تصميم هذه الجلسات لغرس أفضل الممارسات الأمنية ، وخلق قوة عاملة واعية بالأمن قادرة على تحديد المخاطر المحتملة والتخفيف من حدتها.

3-أمن نقل البيانات:

التقنية: لضمان أمان البيانات أثناء النقل بين الأنظمة المحلية والسحابة، يعد تنفيذ بروتوكولات نقل البيانات الآمنة أمرا بالغ الأهمية. يؤدي استخدام بروتوكولات مثل HTTPS (بروتوكول نقل النص التشعبي الآمن) إلى تشفير قناة الاتصال ، وحماية البيانات من الاعتراض أو العبث.

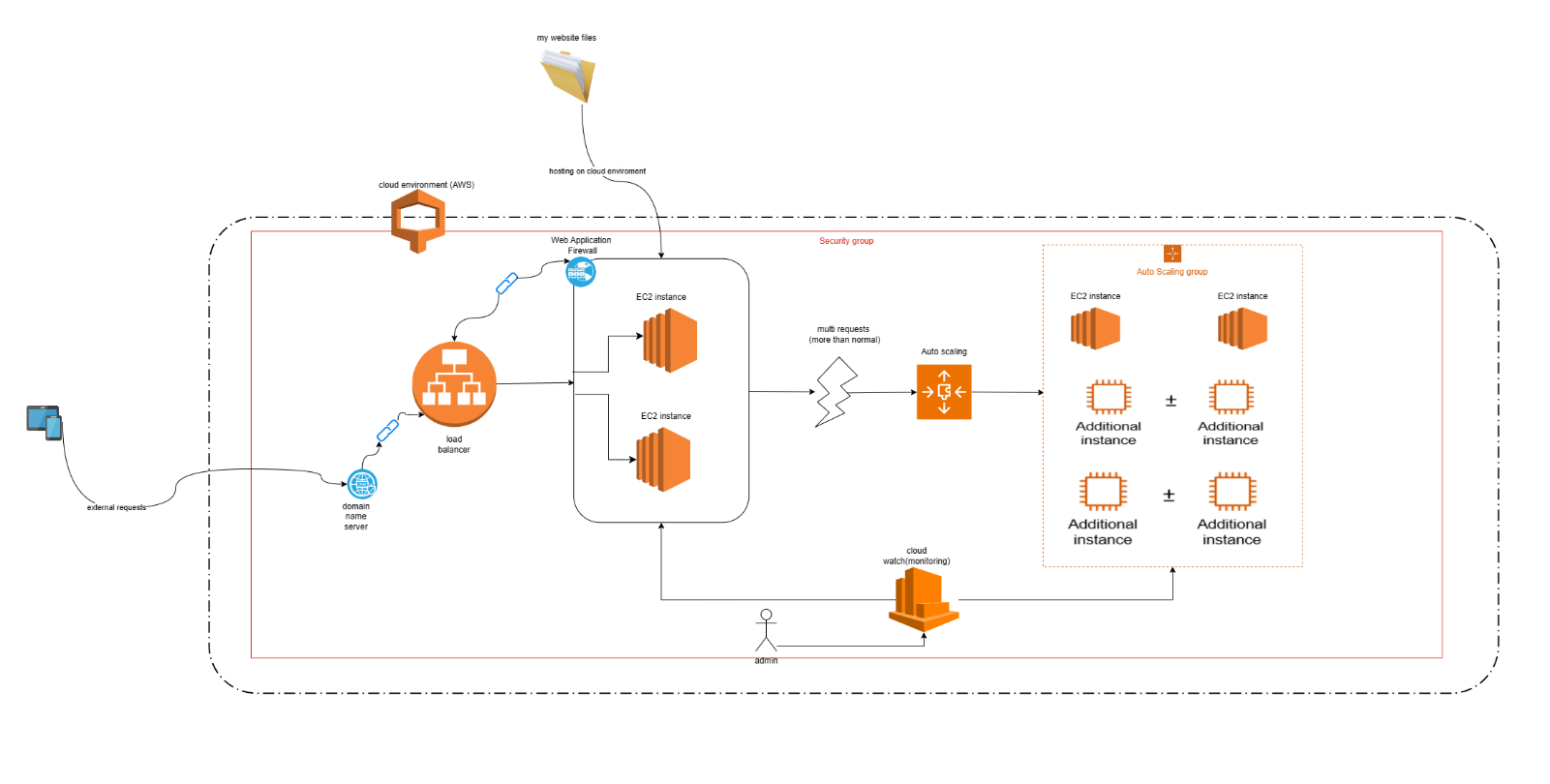
4-عمليات التدقيق والتقييم المنتظمة:

التقنية: الأمن هو مشهد دائم التطور ، وللبقاء في صدارة التهديدات الناشئة ، يتم إجراء عمليات تدقيق وتقييمات أمنية منتظمة. وتنطوي هذه التدابير الاستباقية على تقييمات منهجية لتحديد مواطن الضعف والضعف ومجالات التحسين، مما يسمح بمعالجتها في الوقت المناسب.

5-سياسات الأمن السحابي:

التقنية: يعمل تطوير وإنفاذ سياسات الأمان السحابي الخاصة بالمؤسسة كإطار توجيهي. توضح هذه السياسات متطلبات الأمان والبروتوكولات وأفضل الممارسات الخاصة باستخدام السحابة للمؤسسة، مما يضمن اتباع نهج موحد ومتسق للأمان.

Task B.1.b



يبدأ التدفق التسلسلي بعملية تحميل الملف، حيث يتم تحميل مكونات تطبيق الويب، مثل ملفات HTML وCSS و JavaScript، من الكمبيوتر المحمول المحلي إلى خادم .EC2تضع هذه الخطوة الأولية الأساس لتنصيب تطبيق الويب على السحابة. وبعد ذلك، يتم تقديم طلبات خارجية لاسم DNS المرتبط بالتطبيق، مما يشكل نقطة الدخول الخارجية إلى النظام.عند تلقي هذه الطلبات الخارجية، يتولى Load Balancer المسؤولية، ويعمل كمنسق مركزي لتوزيع حركة المرور الواردة بكفاءة بين خادمي EC2، المعينين باسم "الخادم 1" و"الخادم 2". لا تضمن موازنة التحميل هذه التوزيع العادل لحركة المرور فحسب، بل تعمل أيضًا على تحسين أداء وموثوقية تطبيق الويب عن طريق منع التحميل الزائد على خوادم محددة. يتكامل التدفق المنسق بسلاسة مع Auto Scaling، وهو مكون ديناميكي يدير بشكل فعال عدد خوادم EC2 بناءً على شروط محددة مسبقًا. يسمح Auto Scaling للنظام بالتكيف مع أعباء العمل المتنوعة عن طريق توسيع نطاق البنية التحتية تلقائيًا لأعلى أو لأسفل، مما يضمن الاستخدام الأمثل للموارد والاستجابة لتقلبات الطلبات. تلعب الإجراءات الأمنية دورًا محوريًا في هذا التسلسل المعماري. يتم وضع جدار حماية تطبيقات الويب (WAF) في موقع استراتيجي لمراقبة وتصفية الطلبات الواردة، ويعمل كحارس يقظ ضد هجمات الويب الشائعة. يرتبط كل خادم EC2 بمجموعة أمان، تعمل كجدار حماية افتراضي يتحكم بدقة في حركة المرور الواردة والصادرة، ويلتزم بقواعد محددة مسبقًا ويعزز الوضع الأمني العام. يتم استكمال التسلسل المنسق من خلال تضمين Amazon CloudWatch، وهي خدمة مراقبة قوية توفر رؤى في الوقت الفعلي حول أداء البيئة السحابية وصحتها. تلعب Amazon CloudWatch دورًا حاسمًا في تعزيز رؤية النظام، مما يسمح بالتعرف الاستباقي على المشكلات المحتملة واختناقات الأداء والحوادث الأمنية. من خلال تكوين الإنذارات داخل CloudWatch، يكتسب النظام القدرة على إخطار أصحاب المصلحة المعنيين على الفور بالأحداث الهامة، مما يتيح الاستجابات السريعة ويضمن الكفاءة التشغيلية المستمرة لتطبيق الويب المنشور. يضيف هذا التكامل لـ CloudWatch طبقة إضافية من المراقبة والتنبيه إلى البنية الشاملة، مما يساهم في مرونة النظام وتسهيل الإدارة الفعالة للموارد استجابة للظروف المتغيرة.ويضمن هذا التسلسل المنسق جيدًا تنصيب تطبيق الويب بشكل آمن وقابل للتطوير ومرن. بدءًا من تحميل الملف الأولي وحتى معالجة الطلبات الخارجية، وموازنة التحميل، وتعديلات السعة الديناميكية من خلال القياس التلقائي، وإجراءات الأمان القوية التي توفرها WAF ومجموعات الأمان، تساهم كل خطوة في إيجاد حل متماسك وفعال قائم على السحابة.

TASK B.1.C

يرتكز التوضيح ل تصميم الحل السحابي الآمن لـ ICES على دراسة متأنية للاحتياجات والاهتمامات الخاصة ببيئات الشركات. كمزود للخدمات الإلكترونية المصممة عالميًا للطلاب، تعمل ICES ضمن بيئة مؤسسية ديناميكية وواسعة النطاق، مما يتطلب حلاً سحابيًا يتوافق مع خصائصها الفريدة.

**1- قابلية التوسع والمرونة:**

الاعتبار: استخدام خوادم Amazon EC2 والقياس التلقائي.

التوضيح: في بيئة شركة ICES، حيث يتم تقديم الخدمات عالميًا، يمكن أن يختلف الطلب على الخدمات الإلكترونية بشكل كبير. ويضمن تركيز التصميم على قابلية التوسع قدرة البنية التحتية على التكيف ديناميكيًا مع أعباء العمل المتغيرة، واستيعاب قاعدة المستخدمين المتنامية بكفاءة. ويتماشى ذلك مع أهداف الشركة المتمثلة في الاستجابة لاحتياجات المستخدمين وتحسين استخدام الموارد، وهو أمر ضروري في مشهد الخدمات الإلكترونية المتطور باستمرار.

**2- التوفر وإمكانية الوصول في الوقت الفعلي:**

الاعتبار: تكامل موازنة الحمل المرنة (ELB)

التوضيح: تتطلب بيئات الشركات توفر الخدمات وإمكانية الوصول إليها في الوقت الفعلي. يؤدي تضمين ELB إلى تحسين توزيع حركة المرور بين مثيلات EC2، مما يعزز التوزيع المتساوي لأعباء العمل. وهذا لا يعزز الأداء العام لتطبيق الويب فحسب، بل يضمن أيضًا الموثوقية، بما يتماشى مع التزام ICES بتوفير خدمة بحث عن الكتب الإلكترونية سلسة ويمكن الوصول إليها للطلاب.

**3- فعالية التكلفة:**

الاعتبار: القياس التلقائي للاستخدام الأمثل للموارد (auto scaling).

التوضيح: في بيئة الشركات، تعتبر فعالية التكلفة أحد الاعتبارات الحاسمة. يتيح Auto Scaling للبنية الأساسية إمكانية الضبط تلقائيًا بناءً على الطلب، مما يؤدي إلى تحسين استخدام الموارد خلال فترات الذروة وتقليل التكاليف أثناء انخفاض النشاط. ويتوافق هذا النهج مع أهداف الشركة المتمثلة في الكفاءة المالية، مما يضمن بقاء الحلول المستندة إلى السحابة سريعة الاستجابة وفعالة من حيث التكلفة.

4**- الأمن في التعامل مع حركة المرور:**

الاعتبار: جدار حماية تطبيقات الويب (WAF) لمزيد من الأمان.

التوضيح: إن إدراج WAF في التصميم يعالج مخاوف الشركات المتعلقة بأمن تطبيقات الويب. من خلال مراقبة وتصفية حركة المرور الواردة، يعمل WAF كحارس يقظ، يحمي من هجمات الويب الشائعة. ويتوافق هذا مع معايير الشركة لحماية الخدمات الإلكترونية من التهديدات المحتملة، مما يعزز الوضع الأمني العام للنظام.

تم تصميم خيارات التصميم للحل السحابي الآمن لـ ICES بعناية لتناسب الحجم والنطاق والمتطلبات المحددة للمؤسسة. ونظرًا للامتداد العالمي لـ ICES ودوره في توفير الخدمات الإلكترونية للطلاب، فإن قابلية التوسع والمرونة تعتبر أمرًا بالغ الأهمية. يتماشى قرار الاستفادة من خوادم Amazon EC2 ودمج Auto Scaling مع الحاجة إلى قابلية التوسع المحسنة، مما يمكّن البنية التحتية من التكيف ديناميكيًا مع أعباء العمل المتنوعة واستيعاب قاعدة المستخدمين المتنامية بكفاءة. ويضمن هذا النهج الاستخدام الأمثل للموارد خلال فترات الذروة مع تقليل التكاليف أثناء انخفاض النشاط، وتلبية متطلبات قابلية التوسع في المؤسسه

يعد الأمان أحد الاعتبارات الأساسية، خاصة في حماية معلومات العميل وضمان الامتثال للوائح حماية البيانات. يوضح تضمين جدار حماية تطبيقات الويب (WAF) ومجموعات الأمان الالتزام بالتدابير الأمنية القوية. تعالج هذه المكونات بشكل جماعي التحدي المتمثل في حماية معلومات العميل ضد الوصول غير المصرح به أو التعديلات.

يعد التوافر وإمكانية الوصول في الوقت الفعلي أمرًا بالغ الأهمية بالنسبة للخدمات الإلكترونية الخاصة بـ ICES، لا سيما في تقديم خدمة بحث موثوقة عن الكتب الإلكترونية. يؤدي اختيار دمج Load Balancer إلى تحسين توزيع عبء العمل بين خوادم EC2، مما يعزز الأداء العام لتطبيق الويب. يتوافق تقديم Amazon CloudWatch أيضًا مع المتطلبات المحددة للمؤسسة من خلال توفير المراقبة في الوقت الفعلي، وتمكين تحديد المشكلات بشكل استباقي، وضمان بيئة سحابية سريعة الاستجابة ومتاحة.

بالإضافة إلى الاستفادة من خوادم Amazon EC2 ودمج Auto Scaling لتحسين قابلية التوسع، فإن خيارات التصميم للحل الآمن القائم على السحابة من ICES تتعمق بشكل أعمق في تلبية احتياجات المؤسسة المحددة. ويأخذ اختيار مثيلات EC2 في الاعتبار المتطلبات المتنوعة للخدمات الإلكترونية التي يقدمها ICES. على سبيل المثال، يتيح تضمين أنواع الخوادم المختلفة التعامل بكفاءة مع أعباء العمل المختلفة، وتحسين أداء مهام محددة داخل النظام البيئي للخدمات الإلكترونية.

يعود قرار دمج Auto Scaling إلى الطبيعة الديناميكية لخدمات ICES، حيث قد تواجه أعباء العمل تقلبات. من خلال ضبط عدد الخوادم تلقائيًا بناءً على شروط محددة مسبقًا، لا يضمن Auto Scaling أن البنية التحتية تلبي الطلب بكفاءة فحسب، بل يساهم أيضًا في فعالية التكلفة. يتماشى هذا مع متطلبات ICES المحددة، مما يضمن بقاء الحل القائم على السحابة مستجيبًا لأنماط الاستخدام المتغيرة مع الحفاظ على الكفاءة المالية.

Task B.2 a+b

|  |  |
| --- | --- |
| الصوره | وصف |
|  | في بداية الأمر، قمت بإنشاء نسخ EC2 ورفعت عليها ملفات موقع الويب الخاص بي تحت اسم "الاستضافة".hosting بعد ذلك، قمت بتعديل قواعد الوصول الواردة، وهي أول إجراء أماني حيث قمت بحظر الطلبات من جميع الأماكن وجعلتها متاحة فقط من عنوان IP محدد.  عنوان IP "[172.31.42.112](https://172.31.42.112/)" يقع ضمن نطاق الشبكة "[172.31.0.0/16](https://172.31.0.0/16)". يُستخدم الـ IPv4 لتحديد الأجهزة على الإنترنت، وتشير الأرقام إلى موقع محدد على الشبكة. Subnet Mask "/16" تُحدد البتات المخصصة للشبكة والأجهزة.  قدمت خطوة إضافية ذكية لضمان تحقيق أقصى قدر من التوفر (Availability). عند وضع كل نسخة من الخوادم (instances) في شبكة فرعية (subnet) مختلفة، قمت بتعزيز مستوى الإتاحة (Availability) لخدمتك. هذا الإجراء يعكس تصميمًا استراتيجيًا لتجنب أي تأثير سلبي ناتج عن مشكلة في إحدى الشبكات. بفضل هذا التوجيه، يتم تحقيق فصل كل نسخة من الخدمة في بيئة فرعية خاصة بها، مما يحد من تأثير أي مشكلة تحدث في إحدى البيئات على البيئات الأخرى. هذا النهج يعزز من استمرارية الخدمة ويحميها من التأثيرات السلبية المحتملة.  تمثل هذه الخطوة الاحترافية استراتيجية فعالة تعكس الرغبة في تحسين توفر الخدمة وضمان استمرارية العمل، وتوفير تجربة موثوقة للمستخدمين النهائيين. |
|  | بعد ذلك، قمت بإنشاء موزع الحمل (load balancer) لتوزيع الطلبات بين النسخ (instances) وربطت هذا الموزع بمجموعة أهداف (target group) تحتوي على النسخ العاملة (healthy instances)، وهو أول حلاًّ لتعزيز المرونة للحفاظ على استمرارية خدمة الخادم، حتى لا يتعطل.وتطبيق احدى حلول المقاومه والثبات (resiliency)  انظر الرابط لترى اسم موزع الحمل  (load balancer) |
|  | فيما بعد، قمت برفع ملفات موقع الويب إلى حاوية S3 للحفاظ على وجودها وتحريرها من أي جهاز عبر الإنترنت فيما لو اضطر الامر لأن وجوده على ملفات الموقع الخاص بي على السحابه أمن من وجودها على جهاز الابتوب الخاص بي وتفادي اي اخطاء تقنيه وطبيعيه ، مع توفير مستوى إضافي من الأمان. وقد قمت أيضًا بتشفيرها (encryption) لمنع الوصول غير المصرح به باستخدام مفتاح تشفير متماثل (symmetric encryption). |
|  | بعد تحديد نطاق الشبكة "172.31.0.0/16" وإعداد EC2 instances لاستضافة ملفات الويبسايت، قمت بتعزيز أمان الموقع عن طريق تنصيب "جدار الحماية لتطبيقات الويب" (WAF). هذا الإجراء يأتي في إطار الجهود الرامية لتعزيز الأمان ومقاومة الموقع ضد هجمات الأمان الشائعة.  تم تكوين WAF لتقديم حماية متقدمة، حيث يتم تصفية حركة المرور الواردة إلى الموقع بهدف منع هجمات الروبوتات والتحميل الزائد على الخادم. هذا يساهم في تحسين أداء الموقع وضمان توفير الخدمة بشكل سلس للمستخدمين، خاصةً في ظل زيادة الحمل أو هجمات التحميل الزائد.  باستخدام هذه الإجراءات الأمنية المتكاملة، تم تعزيز أمان الموقع الخاص بي بفعالية، مما يسهم في تقديم تجربة مستخدم آمنة وموثوقة.  هذه الصوره تظهر ما هو مربوط مع ال WAF والذي هو ال load balancer للحصول على DNS منه |
|  | آلية التوسع التلقائي تُمثل حلاً فعّالاً لضمان استجابة مُحسَّنة لتطلبات الأداء المتزايدة. تعتبر هذه الميزة قادرة على تعديل عدد النسخ بشكل دينامي لتلبية متطلبات الأداء، مما يُسهم في تحسين كفاءة استخدام الموارد وبالتالي تعزيز فعالية التكلفة.  تم ربط آلية التوسع التلقائي بـ Load Balancer لضمان توزيع متوازن لحركة المرور بين الـ EC2 instances. يُعزز هذا التكامل الفعَّال استجابة الخدمة والتوزيع التلقائي لحمل العمل، حيث يُحسن Load Balancer إدارة حركة المرور بين الـ EC2 instances بناءً على حجم الحمل وقدرتها على التحمل.  فيما يخص الإعدادات، تم تحديد السعة المرغوبة (Desired Capacity) عند الرقم 2، وهو العدد المستهدف للـ EC2 instances في حالة الاستقرار. وتم تعيين السعة القصوى (Maximum Capacity) عند الرقم 6، مما يُمثل الحد الأقصى لعدد الـ EC2 instances التي يمكن أن تتوسع إليها الآلية تلقائيًا للتعامل مع زيادة في حمل العمل. وتم تحديد السعة الدنيا (Minimum Capacity) عند الرقم 2 لضمان استمرار تشغيل الخدمة حتى في ظروف الحمل الخفيف.  هذه الإعدادات تضمن توازنًا فعّالًا بين استهلاك الموارد وقدرة النظام على التحمل لمواجهة التقلبات في حجم حركة المرور، مما يُضمن الاستقرار والأداء الفعَّال للويبسايت. |

Task B.2.c

The systematic review of my configuration:

**EC2 Instances and Access Control:**

في الخطوات الأولى، قمت بتكوين وإطلاق نماذج Amazon Elastic Compute Cloud (EC2) بعناية لتكون بيئة استضافة لملفات موقعي. بالتركيز على الأمان، قمت بتنفيذ إجراءات قوية لمراقبة الوصول، حيث قمت بتقييد الطلبات لتأتي فقط من عنوان IP محدد وآمن. يُضيف هذا الآلية الصارمة طبقة أساسية من الحماية إلى بنية الاستضافة. بالإضافة إلى ذلك، نفذت ميزة المصادقة بواسطة مفتاحين لتحقيق إضافي للأمان للوصول الآمن إلى نماذج EC2.

**Load Balancer and Flexibility:**

لتعزيز المرونة وضمان استمرارية الخدمة، أنشأت موازن التحميل التطبيقي. هذا القرار الاستراتيجي أساسي لتوزيع الطلبات الواردة بشكل متساوي بين النماذج النشطة، مما يظهر النهج الاستباقي تجاه التوسع والحفاظ على التوفر العالي. يسهم التوازن في إعمار النظام بشكل كبير، مضمونًا استخدام موارد فعال. علاوة على ذلك، قمت بتكوين موازن التحميل لأداء فحوصات صحة على النماذج، وتوجيه حركة المرور تلقائيًا إلى النماذج السليمة فقط، مما يحسن من موثوقية النظام.

**S3 Container for Web Files:**

بمراعاة توفر البيانات وسهولة الوصول الآمن، قمت برفع ملفات الموقع إلى حاوية Amazon Simple Storage Service (S3). هذا لا يضمن فقط وجود الملفات ولكن يتيح أيضًا الوصول المريح والآمن من أي جهاز عبر الإنترنت. وعلاوة على ذلك، ركزت على حماية البيانات من خلال تشفير الملفات باستخدام Server-Side Encryption (SSE)، والذي يشمل تشفير البيانات تلقائيًا في حالة الراحة. يتماشى ذلك مع أفضل الممارسات في حماية المعلومات الحساسة.

**Web Application Firewall (WAF):**

في جهد لتعزيز النشر ضد مجموعة من التهديدات السيبرانية، قمت بتنفيذ جدار حماية تطبيقات الويب (WAF). ينطوي هذا التدبير الأمني الحيوي على تكوين WAF لتصفية حركة المرور الواردة، مما يمنع هجمات الروبوتات المحتملة ويقلل من خطر تحميل الخادم. يتضمن إعداد> WAF

**Scalability Mechanism - Auto Scaling:**

مع التزام بالقدرة على التكيف وإدارة الموارد بشكل فعّال، قمت بدمج توسيع التلقائي بسلاسة في البنية. هذه الميزة الديناميكية تعدل تلقائيًا عدد النماذج استنادًا إلى متطلبات الأداء، مما يضمن كفاءة موارد مثلى وفعالية التكلفة. اعتماد توسيع التلقائي يتماشى مع أفضل الممارسات المعاصرة لتوسيع مؤقت في بيئات السحاب. بالإضافة إلى ذلك، قمت بتكوين سياسات توسيع تلقائي للاعتبار في متغيرات مخصصة، مما يتيح آلية توسيع متجاوبة وأكثر تخصيصًا استنادًا إلى مؤشرات أداء التطبيق المحددة.

**Integration with Load Balancer:**

عنصر بارز في الهندسة هو التكامل السلس مع توسيع تلقائي وموازن التحميل التطبيقي. هذا التكامل يضمن توزيعًا متوازنًا لحركة المرور بين نماذج EC2، مما يحسن استجابة الخدمة وتوزيع العبء تلقائيًا استنادًا إلى تقلبات الحمل والسعة. قمت بتكوين تثبيت موازن التحميل، مما يضمن توجيه الطلبات التالية من عميل إلى نفس النموذج، مما يعزز تجربة المستخدم واستمرارية الجلسة.

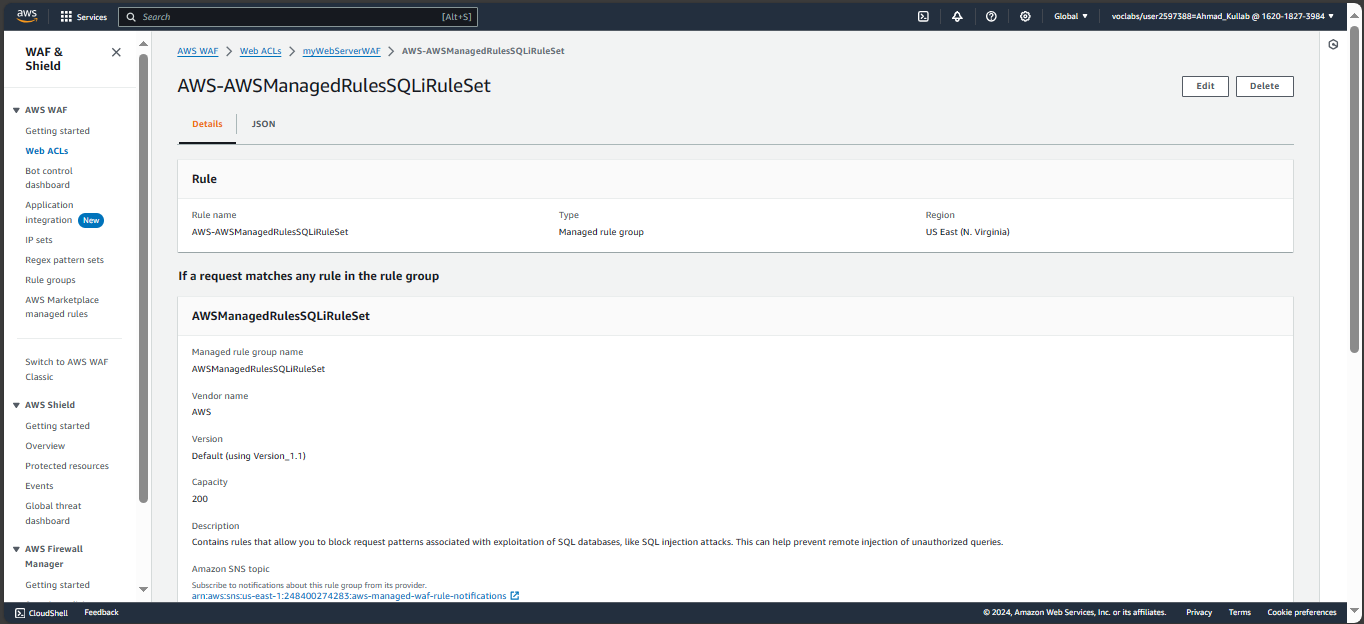
**Auto Scaling Settings:**

في تكوين مستفيض لإعدادات توسيع تلقائي، قمت بتحديد السعة المرغوبة بعدد 2 نموذجًا خلال فترات الاستقرار. تم تعيين السعة القصوى عند 6 نماذج، مما يوفر مرونة للتعامل مع ذروات العمل بفعالية. بالإضافة إلى ذلك، تم تحديد السعة الدنيا بعدد 2 نموذجًا لضمان استمرارية الخدمة، حتى في حالات حركة المرور الخفيفة، مما يسهم في الاستقرار العام والأداء الفعّال لبنية الموقع الإلكتروني. قمت باستخدام إجراءات التوسيع المجدولة لتوقع تقلبات حركة المرور المتوقعة.

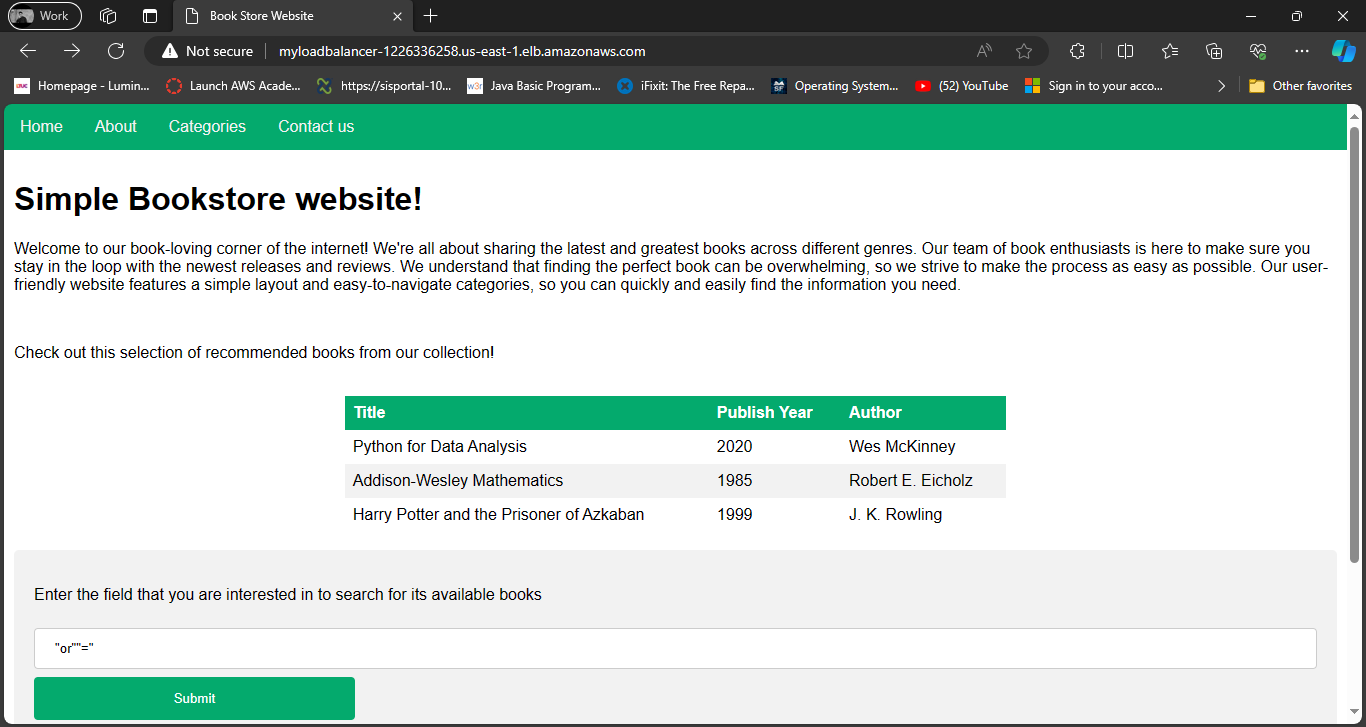
**باعتباره اقتراحًا من وجهة نظري التي اراها سوف تساعد على حماية الويبسايت الخاص بي من نوع اخر من الهجمات هو SQL injection :**

**المقترح:**

كمهندس لهذا النشر عبر الويب، أعتبر دمج حماية حقن SQL من خلال جدار حماية تطبيقات الويب (WAF) خطوة حاسمة نحو تعزيز موقف الأمان للموقع. بينما هو حاليًا في مرحلة التنفيذ، يبرز التوعية بالتهديدات المحتملة مثل حقن SQL والنهج الاستباقي للأمان السيبراني. هذا التحسين المخطط له لا يتماشى فقط مع أفضل الممارسات الصناعية ولكنه يعكس أيضًا الالتزام بالبقاء في مقدمة المشهد المتطور باستمرار لأمان الويب. نظرًا إلى المستقبل، تظل إضافة حماية حقن SQL من خلال WAF تحقق التفاني في توفير تجربة عبر الإنترنت آمنة وقائمة بالقدر الكافي للمستخدمين.

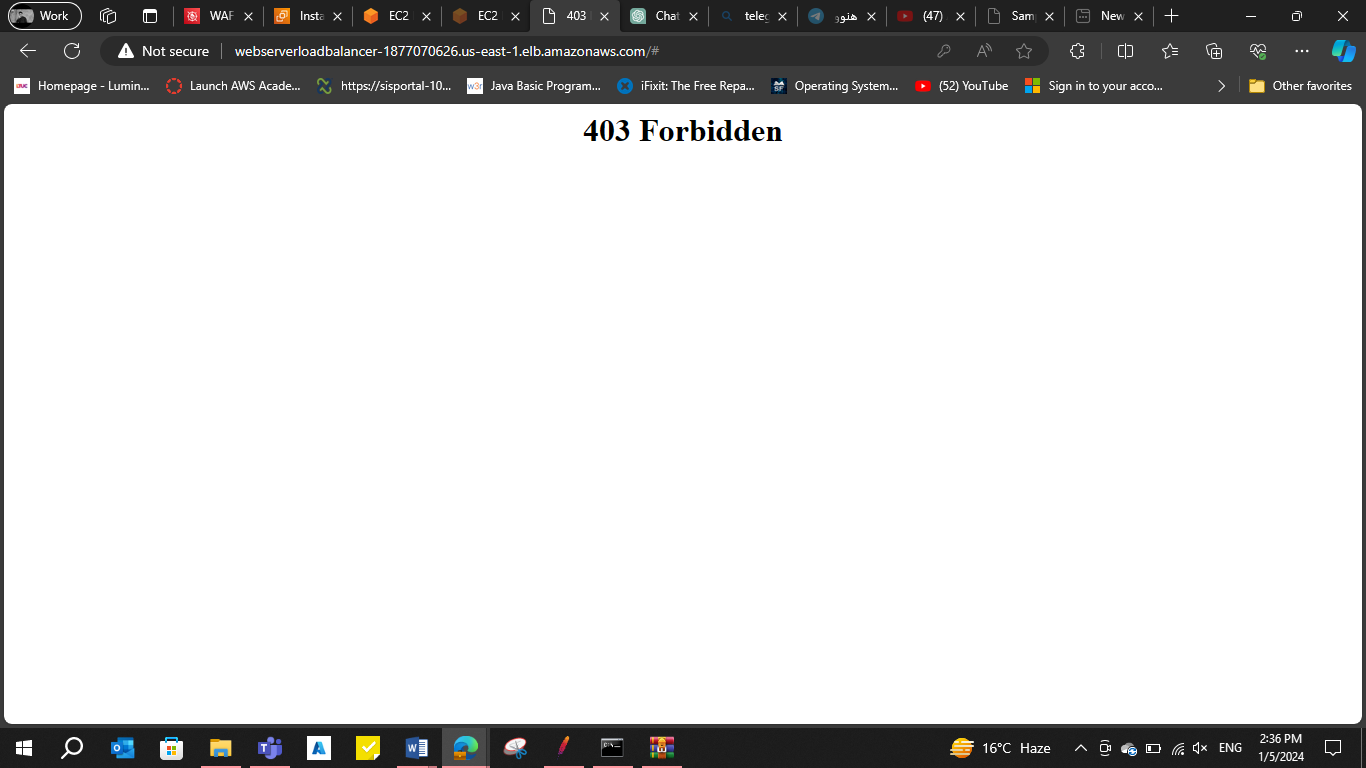


في الصوره الموضحه اعلاه يظهر اضافة SQL injection protection باستخدامWAF . والان سوف اقوم ب اختبار هذه الميزه عبر حقن الموقع الخاص ب “=””or query والتي تعتبر محاولة حقن وهي إدخال خبيث يستهدف استغلال الثغرات في التعامل مع إدخال المستخدم في تطبيق الويب. في حقن SQL، يقوم المهاجمون بإدراج رموز لتلاعب استعلامات SQL. في هذه الحالة، تقوم الرموز المدخلة بإغلاق السلاسل النصية الحالية وإدخال شرط جديد (or) لتجاوز فحص المصادقة أو التفويض. لتجنب حقن SQL، تعتبر ممارسات البرمجة الآمنة مثل الاستعلامات المعلمة، والتحقق من صحة الإدخالات، وترميز الإدخالات بشكل صحيح أمورًا حيوية. يساعد إجراء التدقيقات الأمنية الدورية في تحديد ومعالجة الثغرات المحتملة.



The SQL injection

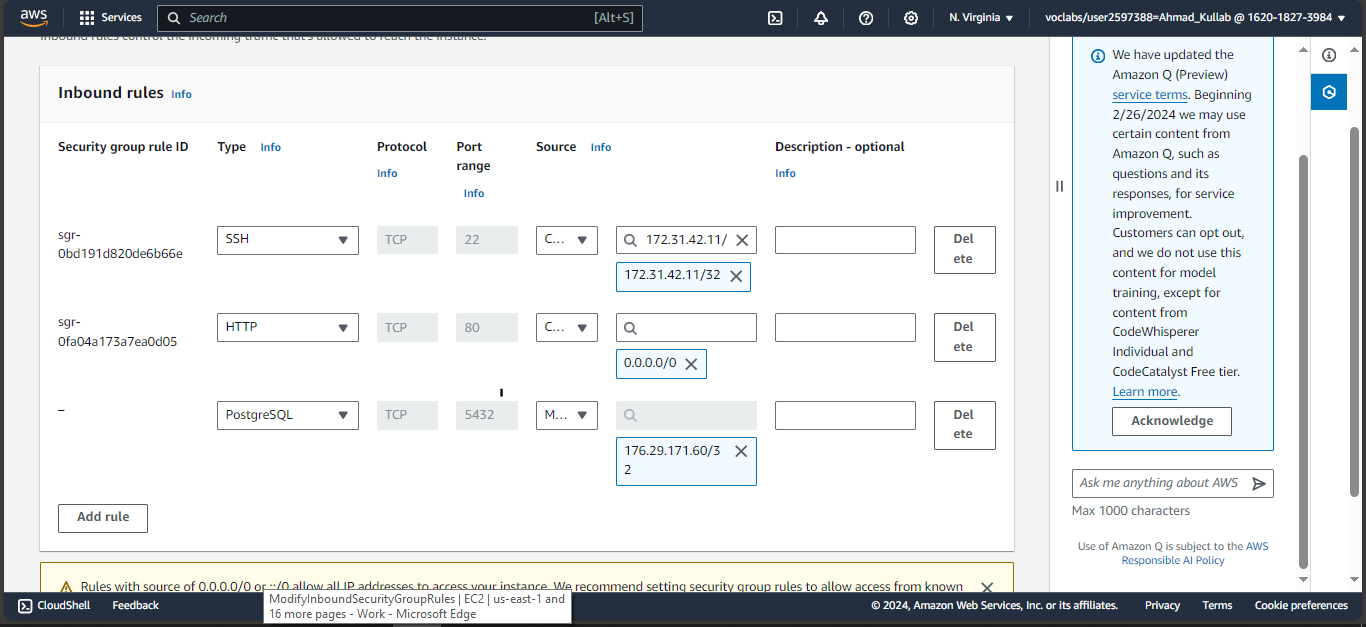
في هذه الصوره نلاحظ اننا سوف نقوم بحقن الموقع الخاص بنا ب حقنة SQL التي سبق وقمت بالتحديث عنها؛ بعد ذلك ساقوم بالضغط على submit ونشاهد النتيجه



قام ب اظهار كود 403 (block)مما يعني ان الموقع امن من جميع حقنات SQL وهذا ما كنت انوي اليه.

الاقتراح الثاني التي سوف يساعد على حماية موقع الويب الخاص بي هو تعديل ال inbound rules للسيرفرات الخاصه بي واضافة rule جديده تمنع وصول IP adsress عشوائي الى قاعده البيانات الخاصه بالموقع

من خلال تنفيذ إجراءات أمان صارمة، قمت بتقييد الوصول إلى خادم قواعد بيانات PostgreSQL للسماح فقط بالاتصال من عناوين IP محددة، وهي عناوين IP تابعة للخادم الخاص بي والتي يستخدمها موقع الويب. يتيح هذا القيد المتعمد ضمان أن يمكن فقط للكيانات المرخص لها والموثوق بها، في هذه الحالة عنوان IP الخاص بي، إقامة اتصال بقاعدة البيانات. من خلال تحديد نطاق عناوين IP المسموح به، يتم تقليل بشكل كبير من مخاطر الوصول غير المصرح به، ومحاولات الاختراق البالغة والأنشطة الضارة المحتملة.  
  
توفر هذه الممارسة الأمانية العديد من الفوائد لموقع الويب الخاص بي. أولاً، تضيف طبقة إضافية من الحماية ضد التهديدات الخارجية، حيث يُسمح فقط لعنوان IP المحدد المسبق بالتفاعل مع قاعدة البيانات. يساعد هذا القيد في حماية البيانات الحساسة وتقليل مخاطر المحاولات غير المصرح بها للوصول أو التلاعب بمحتوى قاعدة البيانات. بالإضافة إلى ذلك، يعزز من الأمان الشامل للموقع الإلكتروني عن طريق تقليل سطح الهجوم المحتمل.



Task B.3

**حماية معلومات العميل:**

التصميم الأصلي: يؤكد التصميم الأصلي على تأمين معلومات العميل ضد الوصول غير المصرح به أو التعديلات. سأُقيم كيف يتناسب نظامي المكون مع ذلك من خلال فحص وسائل التحكم في الوصول وآليات المصادقة المطبقة.

تفاصيل النظام المكون: في النظام المكون، تم تنفيذ تدابير صارمة لحماية معلومات العميل. توفر قيود الوصول بناءً على عناوين IP خط الدفاع الأمامي القوي، مما يسمح فقط بالاتصالات المصرح بها والآمنة. يعزز استخدام المصادقة من خلال أزواج المفاتيح الأمان بالتخلص من الاعتماد على بيانات الاعتماد الثابتة. مما يقلل من مخاطر الكشف عن بيانات الاعتماد ويضمن أن يحصل كل نموذج على الأذونات اللازمة بحد أدنى.

**توفّر الخدمة والوصول في الوقت الحقيقي:**

التصميم الأصلي: يهدف التصميم الأصلي إلى تحقيق توفّر الخدمة والوصول في الوقت الحقيقي لخدمة البحث في الكتب الإلكترونية. قيّم مدى تحقيق نظامي لهذا الهدف.

تفاصيل النظام المكون: يتفوق نظامي في تحقيق هدف التوفّر في الوقت الحقيقي. يساهم التوازن وآليات التوسع التلقائي في توزيع أعباء العمل بشكل متساوٍ بين نماذج EC2 النشطة، مما يضمن استخدامًا أمثل للموارد واستجابة فعّالة. تعزز فحوصات الصحة المُكوّنة لتوجيه حركة المرور تلقائيًا   
إلى النماذج الصحية فقط، مما يعزز التوفّر الشامل والوصول إلى خدمة البحث في موقع الكتب الإلكترونية

ICES.   
  
**الامتثال لتنظيمات حماية البيانات:**

التصميم الأصلي: يعتبر ضمان الامتثال للتنظيمات الحالية لحماية البيانات والمعايير جزءًا حيويًا. سأُقيم كيف يتناسب نظامي مع هذه المتطلبات.  
  
تفاصيل النظام المكون: يتم تصميم النظام المكون بتركيز كبير على الامتثال لتنظيمات حماية البيانات. من خلال استخدام خدمة Amazon S3 لتخزين ملفات الويب بتشفير على الجانب الخادم (SSE)، يلتزم نظامك بأفضل الممارسات لتأمين البيانات الحساسة. يضمن هذا النهج تشفير البيانات تلقائيًا في حالة الراحة، مما يتناسب بسلاسة مع معايير ولوائح حماية البيانات.

**بنية السحابة المرنة:**

التصميم الأصلي: يعد استيعاب التوسع لتلبية احتياجات عدد متزايد من المستخدمين تحديًا رئيسيًا. سأُقيم كيف خطط التصميم الأصلي لهذا التوسع.

تفاصيل النظام المكون: القابلية للتوسع هي قوة أساسية في نظامي. يعكس التكامل بين التوسع التلقائي وموازن التحميل نهجًا استباقيًا للتعامل مع أعباء العمل المتنوعة. يتم تكوين التوسع التلقائي بسياسات جيدة التحديد، مع التكيف التلقائي لعدد النماذج استنادًا إلى مؤشرات الأداء. يضمن ذلك استخدام الموارد بشكل فعّال، مما يتيح لنظامك التوسع أو الانكماش بسلاسة لتلبية الاحتياجات والحفاظ على الاستقرار.

**الموقف الأمني الشامل:**

التصميم الأصلي: يؤكد التصميم الأصلي على وجود تدابير أمان قوية للنظام القائم على السحابة. سأُقيم الموقف الأمني العام الذي ورد في التصميم الأصلي.   
تفاصيل النظام المكون: وضع الأمان في نظامي المكون هو شامل ويتناسب مع التأكيد على الأمان القوي في التصميم الأصلي. تحكم الوصول وممارسات التشفير وتنفيذ جدار الحماية لتطبيق الويب (WAF) يساعد إلى نهج أمان متعدد الطبقات. يعزز الرصد المستمر والتحديثات الدورية لقواعد WAF والطبيعة الديناميكية لتوسيع التلقائي بشكل جماعي الوضع الأماني الشامل.

تم تعزيز حماية معلومات العميل في النظام المكون من خلال تبني إجراءات صارمة مثل قيود الوصول بناءً على عناوين IP والمصادقة. يتمتع النظام بفعالية في تحقيق توفر الخدمة والوصول في الوقت الحقيقي عبر تكامل توازن الحمل وآليات التوسع التلقائي، مما يحسن الاستجابة والتوفر. فيما يتعلق بالامتثال لتنظيمات حماية البيانات، يعتمد النظام على Amazon S3 مع تشفير على الجانب الخادم لضمان امتثاله للمعايير واللوائح. بنيته السحابية المرنة تعزز قدرته على التكيف مع تزايد الطلب، ويظهر مستوى عالٍ من الأمان بفضل تكامل توسعه مع موازن التحميل والرصد المستمر.

بناءًا على تقيمي والمقارنه التي تم عملها باحترافيه لا شك بان النظام يحتاج بعض التحسينات مثل :

**.1الخوادم الافتراضية على خدمة EC2 ومراقبة الوصول:**

لتعزيز أمان خوادم EC2 ومراقبة الوصول، يُوصى بتنفيذ أدوار IAM لخوادم EC2 باستخدام خدمة إدارة الهوية والوصول في AWS (IAM). من خلال إنشاء أدوار IAM، يتم تقليل الاعتماد على بيانات الاعتماد الثابتة بشكل كبير. توفر أدوار IAM نهجًا ديناميكيًا لإدارة الوصول، مما يقلل من الحاجة إلى تخزين مفاتيح الوصول على خوادم EC2. يُعزز هذا التخصيص الدينامي للرموز الأمانية المؤقتة الأمان من خلال تقليل مخاطر التعرض لاختراق البيانات الاعتمادية. بالإضافة إلى ذلك، يضمن تحديد سياسات أدنى امتياز داخل هذه الأدوار IAM أن تتلقى كل خادم EC2 الأذونات اللازمة فقط، متسقًا مع مبدأ أدنى امتياز. يتيح هذا النهج التحكم الدقيق في الإجراءات التي يمكن أن يقوم بها كل خادم، مما يسهم في تحسين إدارة الوصول بشكل أكبر وبشكل جيد التنظيم.

**.2 موازن التحميل والمرونة:**

لتعزيز المرونة وتوفير التواجد المستمر للنظام، يتضمن التحسين دمج خدمة AWS Shield لحماية DDoS مع موازن تحميل التطبيقات (ALB). تعتبر AWS Shield خدمة إدارة لحماية DDoS تقدم كشفًا تلقائيًا وتخفيفًا لمختلف الاتجاهات الهجومية. من خلال تكوين AWS Shield لحماية ALB، يحصل النظام على إمكانيات مراقبة مستمرة، وتطبيق تلقائي للتخفيف في حالة هجوم DDoS. يضمن هذا التكامل توفر الخدمة بشكل متواصل عن طريق الحماية من هجمات DDoS ذات الطيف الواسع والإرهاق الحالة، وهجمات طبقة التطبيق. بالإضافة إلى ذلك، تستفيد قدرات AWS Shield التكيفية من تعلم الآلة للتكيف مع أنماط هجمات DDoS المتطورة، مما يعزز متانة النظام ضد التهديدات المعقدة. يسهم هذا النهج الشامل لحماية DDoS في تعزيز بنية الأمان والاستقرار للبنية السحابية.

**Task c 1 + 2**

**اختبار SSH باستخدام Nmap:**

**اسم حالة الاختبار: اختبار الوصول الآمن إلى SSH باستخدام Nmap.**

**وصف الأهداف الرئيسية للاختبار: يهدف هذا الاختبار إلى التحقق من أمان وإمكانية الوصول لخدمة SSH باستخدام Nmap.**

**الموارد أو الأدوات:**

* **Nmap لإجراء اختبارات الأمان.**
* **إعداد SSH لاختبار الوصول.**

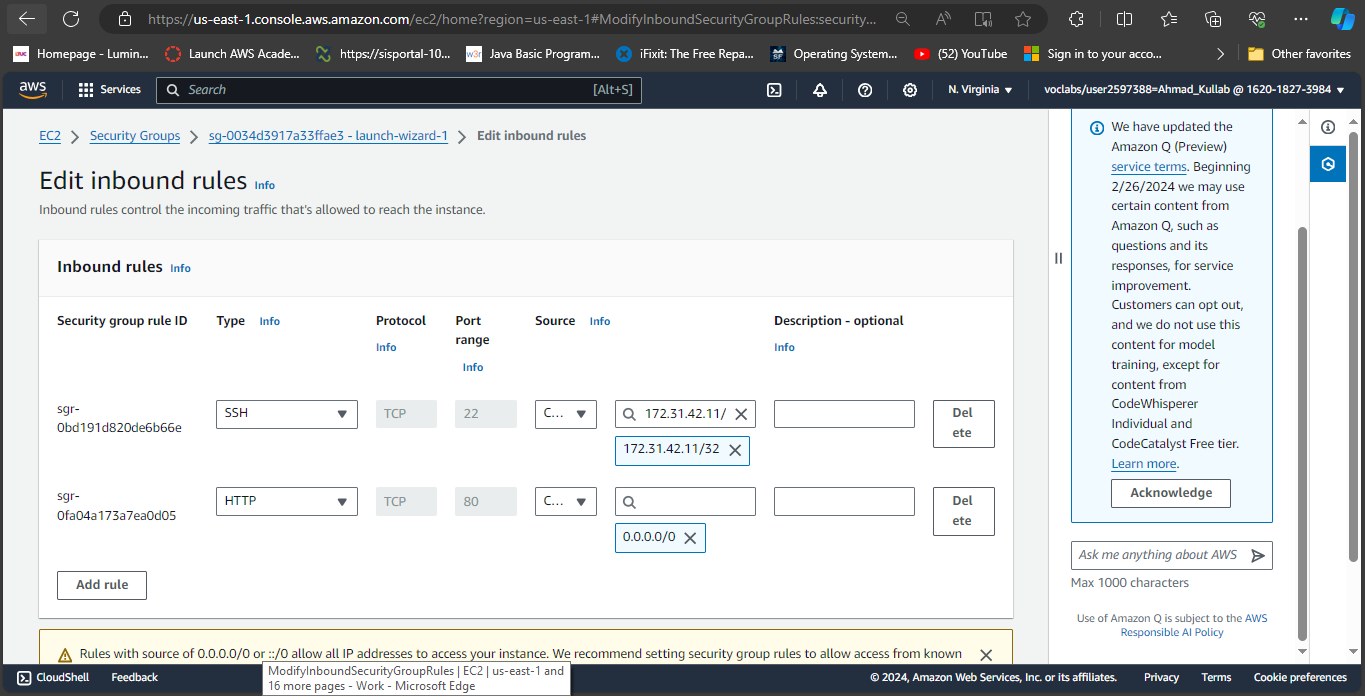
**المنهجية التي سيتم اتباعها لإجراء الاختبار:**

1. **تشغيل اختبار الوصول إلى SSH باستخدام Nmap.**
2. **محاولة الاتصال باستخدام عنوان IP غير مشمول في النطاق المحدد.**
3. **تسجيل الردود والتحقق من وجود تحقق من الهوية.**

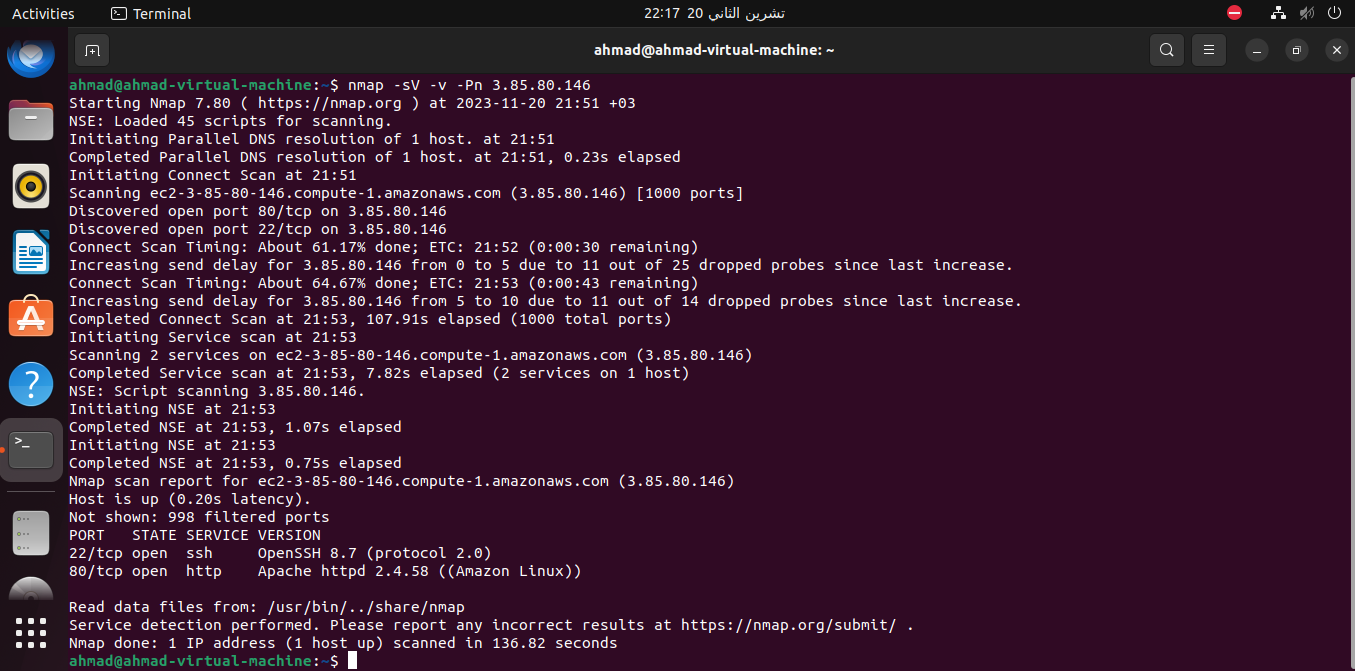
**النتائج المتوقعة:**

* **فشل محاولة الاتصال باستخدام عنوان IP غير مشمول في النطاق المحدد.**
* **تحقق من فعالية تحقق من الهوية.**

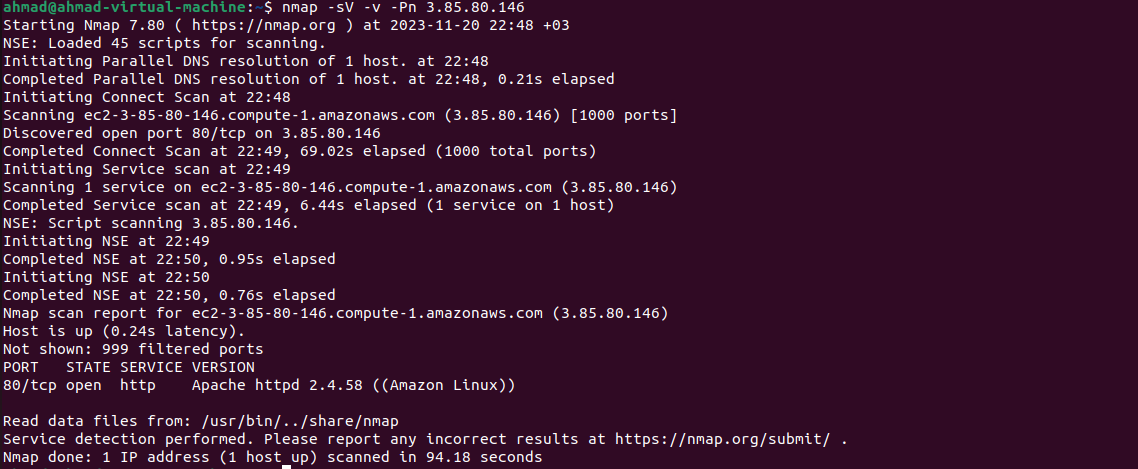
**في هذه الصوره قمت بتخصيص ال IP address ليكون فقط الاي بي الخاص بي واغلاق هذه الثغره ثم اختبارها باستخدام nmap tool والتي بدورها تقوم بعمل scanning على الويبسايت لاكتشاف ما اذا كان هناك ثغرات في الويبسايت او لا**



**كما نلاحظ هنا ان الثغره كانت مفتوحه قبل انو اقوم باعداد ال IP address الخاص بالموقع والتي كانت متاحه للجميع**



**وهذه صوره اخرى لفحص ال Nmap التي تشير ألى ان الثغره تم اغلاقها وبهذا الحال تم اختبار جميع الثغرات المفتوحه وكما نرى ان لا يوجد ثغرات بالموقع الخاص بنا**



**اختبار بوت التحكم باستخدام JMeter:**

**اسم حالة الاختبار:** اختبار أداء بوت التحكم باستخدام JMeter.

**وصف الأهداف الرئيسية للاختبار:** يهدف هذا الاختبار إلى التحقق من استجابة بوت التحكم تحت ضغط كبير.

**الموارد أو الأدوات:**

* JMeter لإجراء اختبارات الأداء.
* بوت التحكم لاختبار أدائه.
* Web application firewall

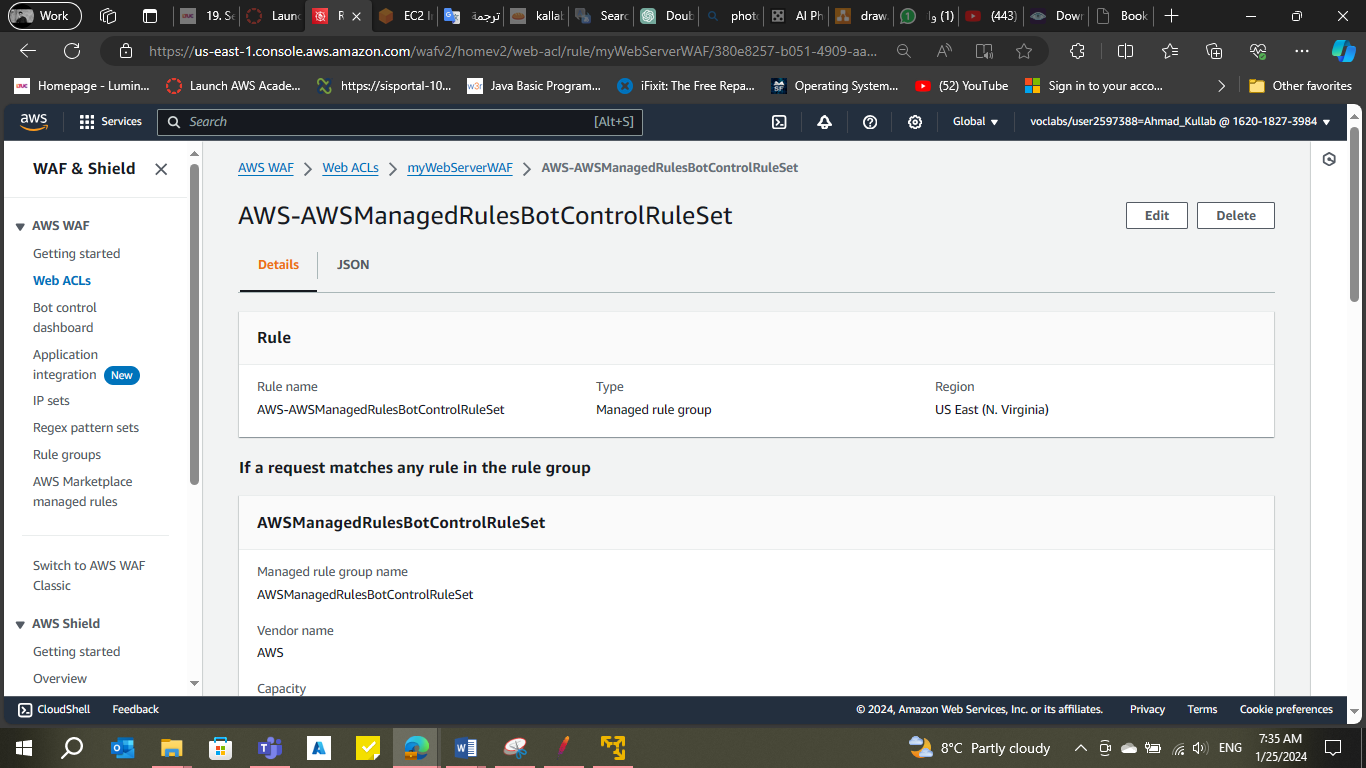
**المنهجية التي سيتم اتباعها لإجراء الاختبار:**

1. تحميل بوت التحكم باستخدام JMeter.
2. تنفيذ أوامر متعددة تحت ضغط كبير.
3. اختبار استجابة النظام ضد بوت اتوماتيكي يتم ارساله للموقع

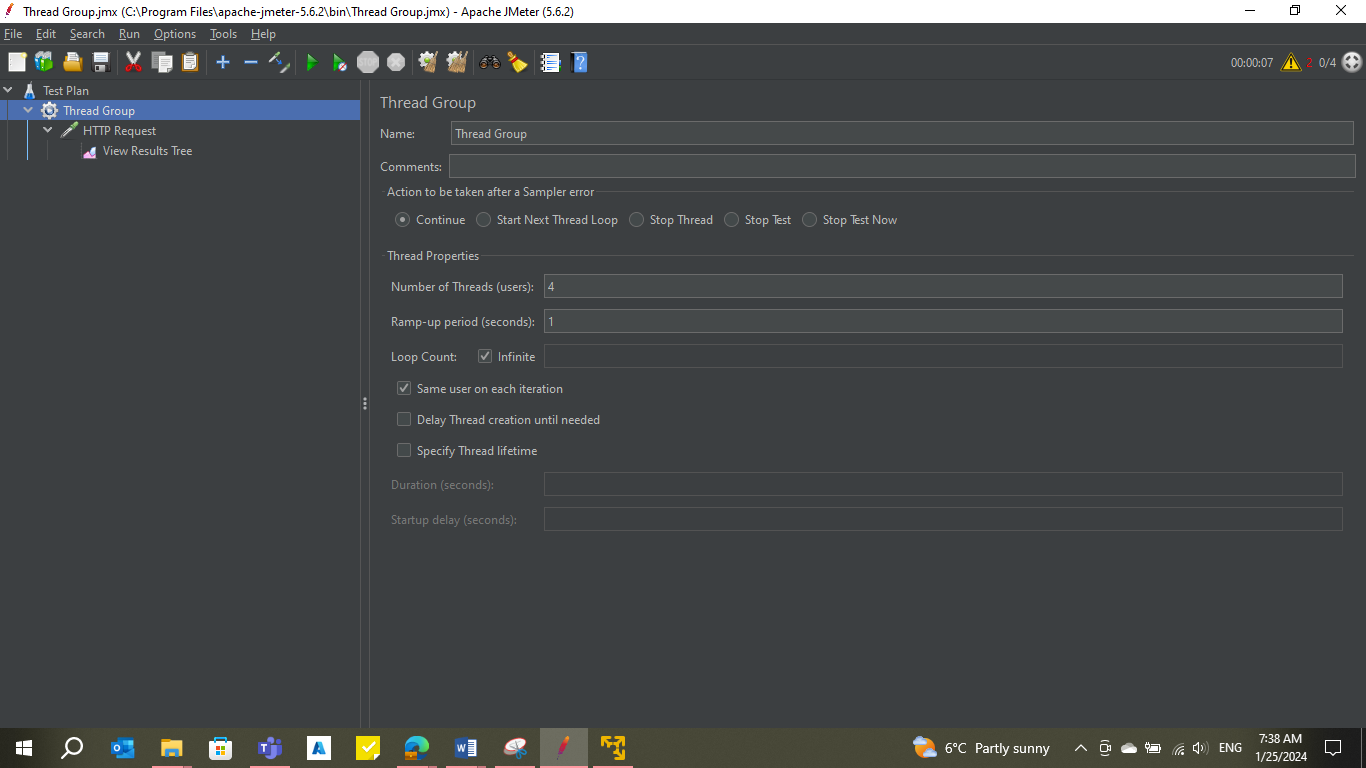
**النتائج المتوقعة:**

* تحميل ناجح لبوت التحكم.
* قدرة بوت التحكم على التعامل مع ضغط كبير.
* الفشل في ارسال طلبات بوت للموقع واظهار كود 405 (not allowed)

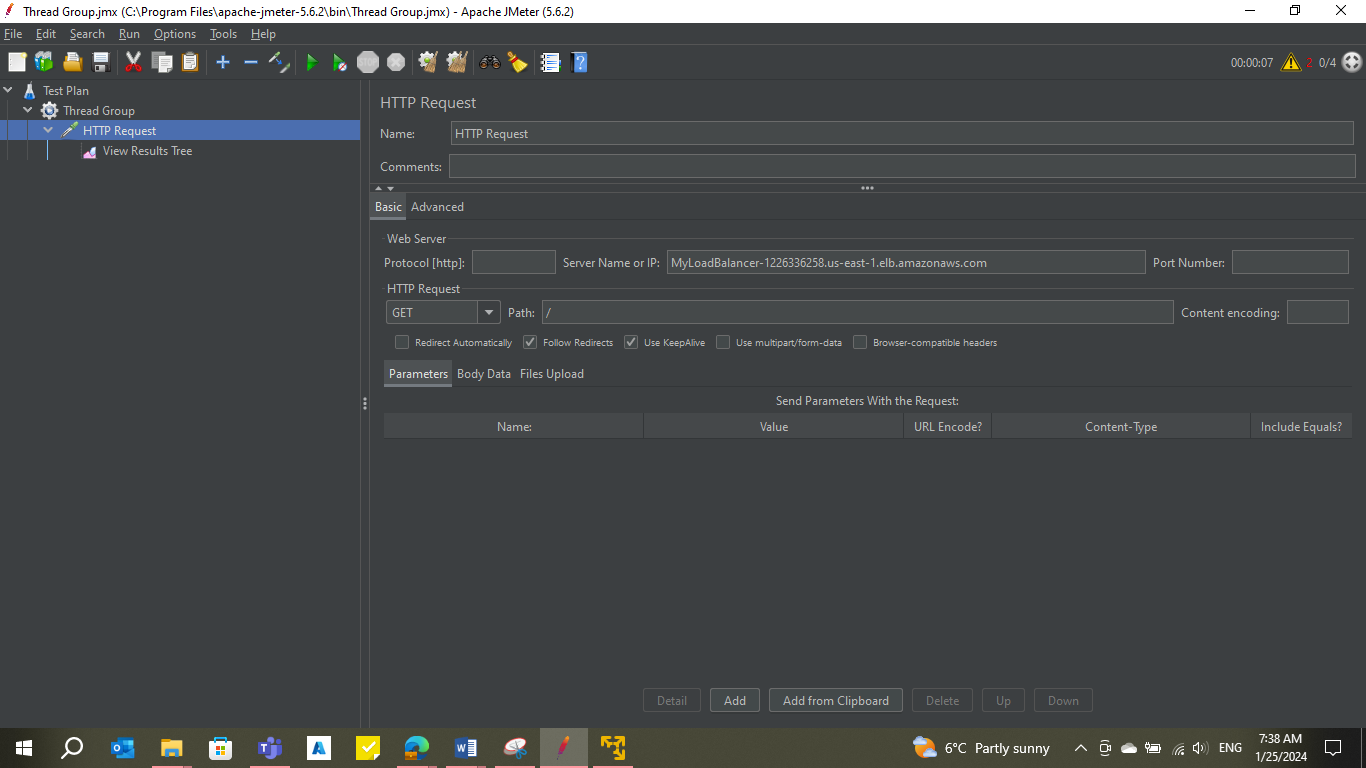
في هذه الصوره نرى انه كان قم تم تفعيل bot control باستخدام web application firewall والتي بدورها ستقوم بمنع طلبات البوت التي سيتم ارسالها باستخدام ال JMeter



قمت بانشاء thread group على JMeter من ثم خصصت عدد المستخدمين الى اربع مستخدمين مع عدد طلبات لا نهائي



وهنا قمت بوضع ال DNS الاختبار في الخانه الخاصه به ومن ثم قمت بتشغيل ال JMeter لعمل الاختبار المطلوب



كما نرى في التحليل انه لم يتم الاستجابه على هذه الطلبات وتم رفضها وحظرها وهذا يعني ان اداء ال WAF Bot control يعمل بالشكل المطلوب وبهذا قمنا انشاء الاختبار وكان اختبارًا ناجحًأ



**اختبار التوسع التلقائي باستخدام JMeter:**

**اسم حالة الاختبار:** اختبار فعالية نظام التوسع التلقائي باستخدام JMeter.

**وصف الأهداف الرئيسية للاختبار:** يهدف هذا الاختبار إلى التحقق من كيفية تعامل نظام التوسع التلقائي مع تغييرات الحمل.

**الموارد أو الأدوات:**

* JMeter لإجراء اختبارات الأداء.
* نظام التوسع التلقائي للاختبار.

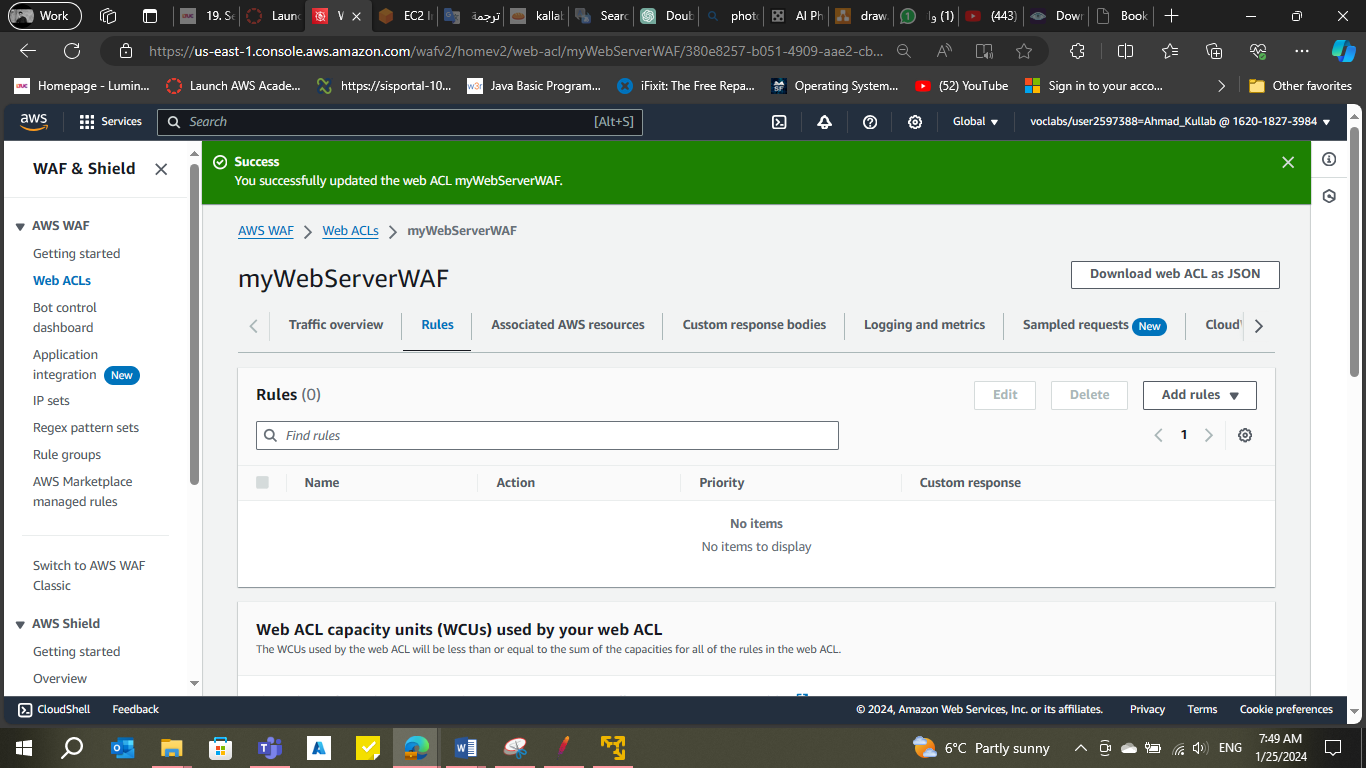
**المنهجية التي سيتم اتباعها لإجراء الاختبار:**

1. زيادة التحميل باستخدام JMeter.
2. رصد توسع التلقائي والانكماش.
3. اختبار توازن التحميل.

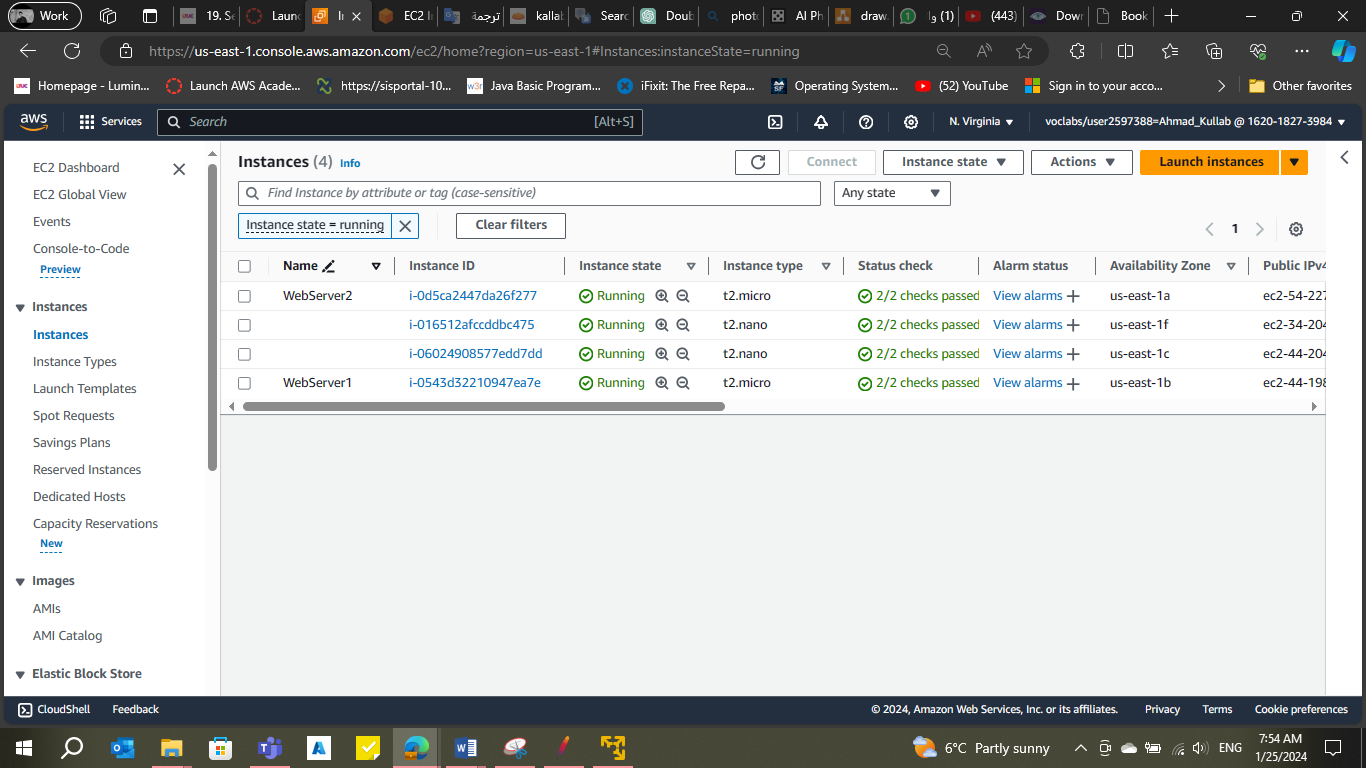
**النتائج المتوقعة:**

* قدرة نظام التوسع التلقائي على التكيف مع تغييرات في التحميل.
* تحقيق توازن فعّال للحمل.

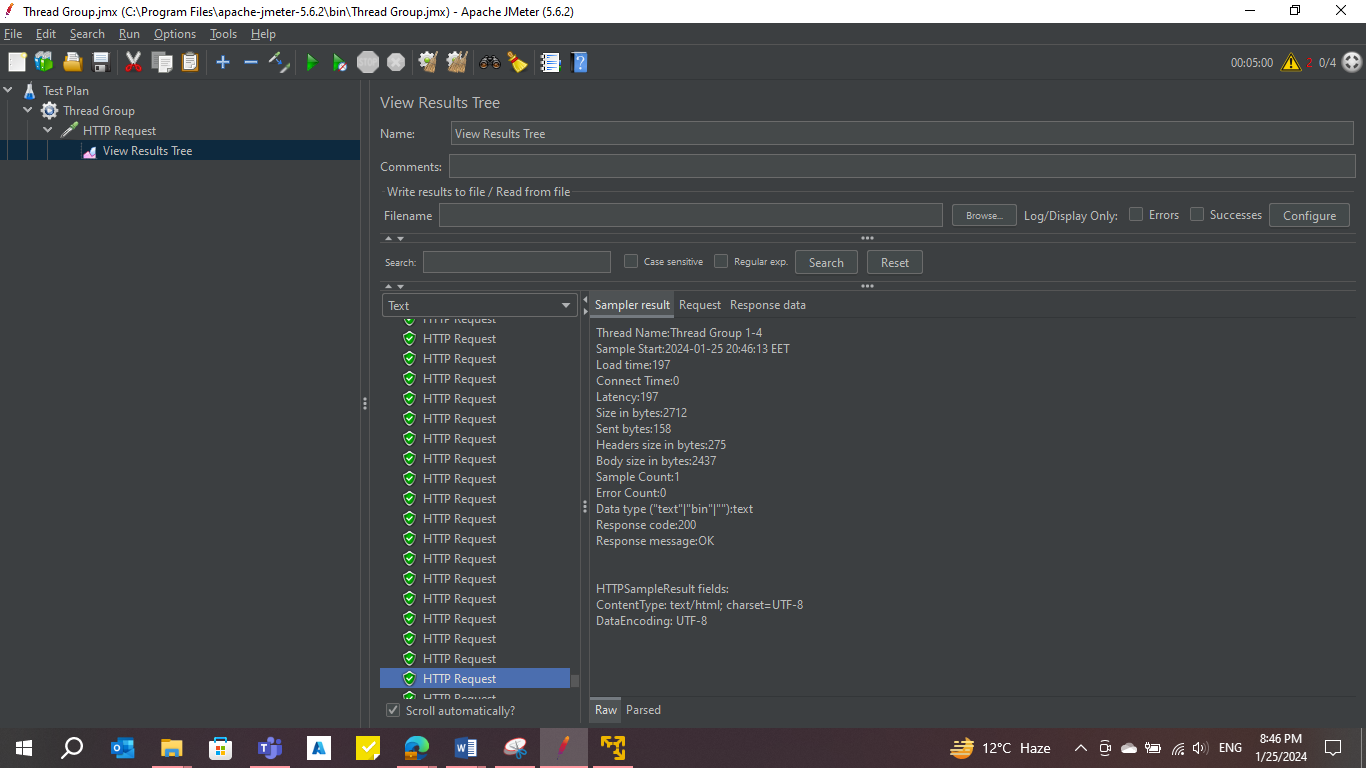
في هذه الصوره قمت بحذف جميع ال rules عن ال WAF لاستقبال طلبات البوت التي سيتم ارسالها باستخدام ال JMeter



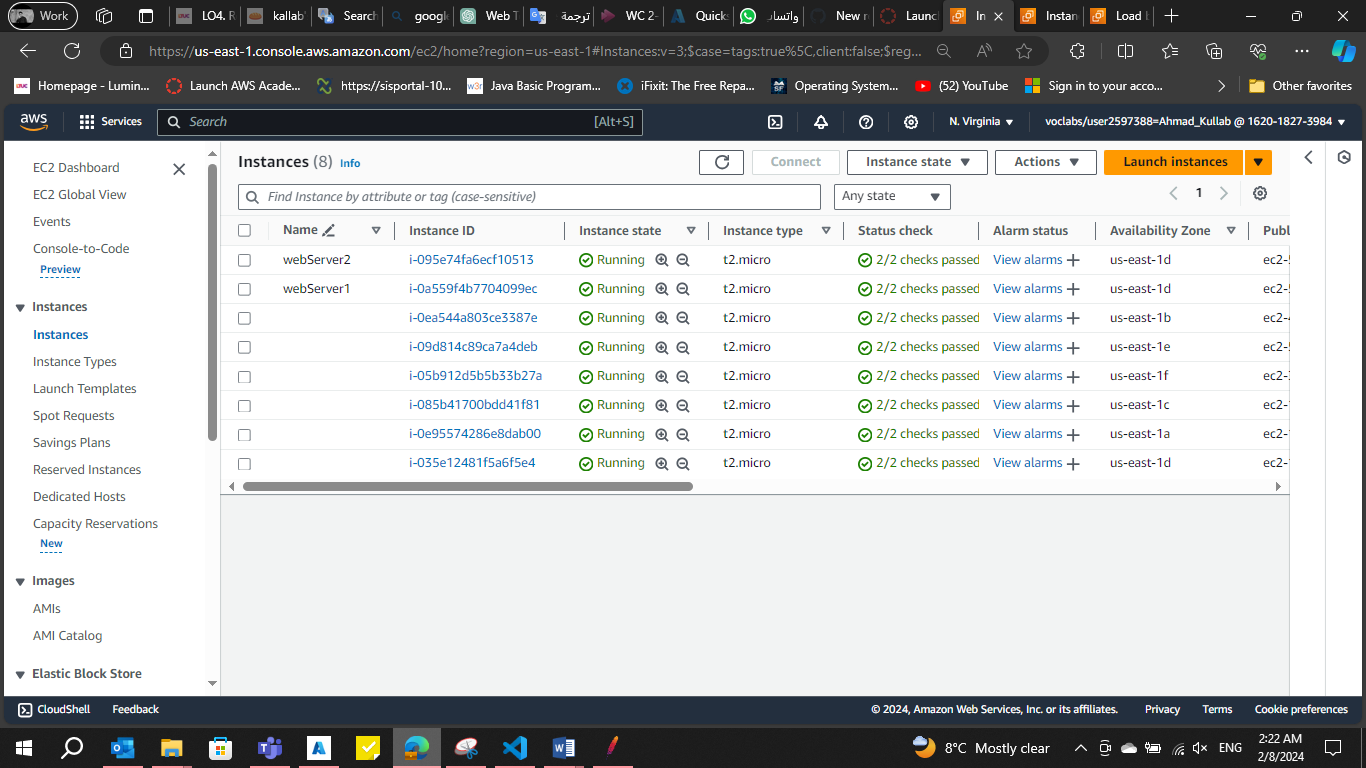
وهذا عدد السيرفرات قبل ارسال الطلبات باستخدام ال JMeter



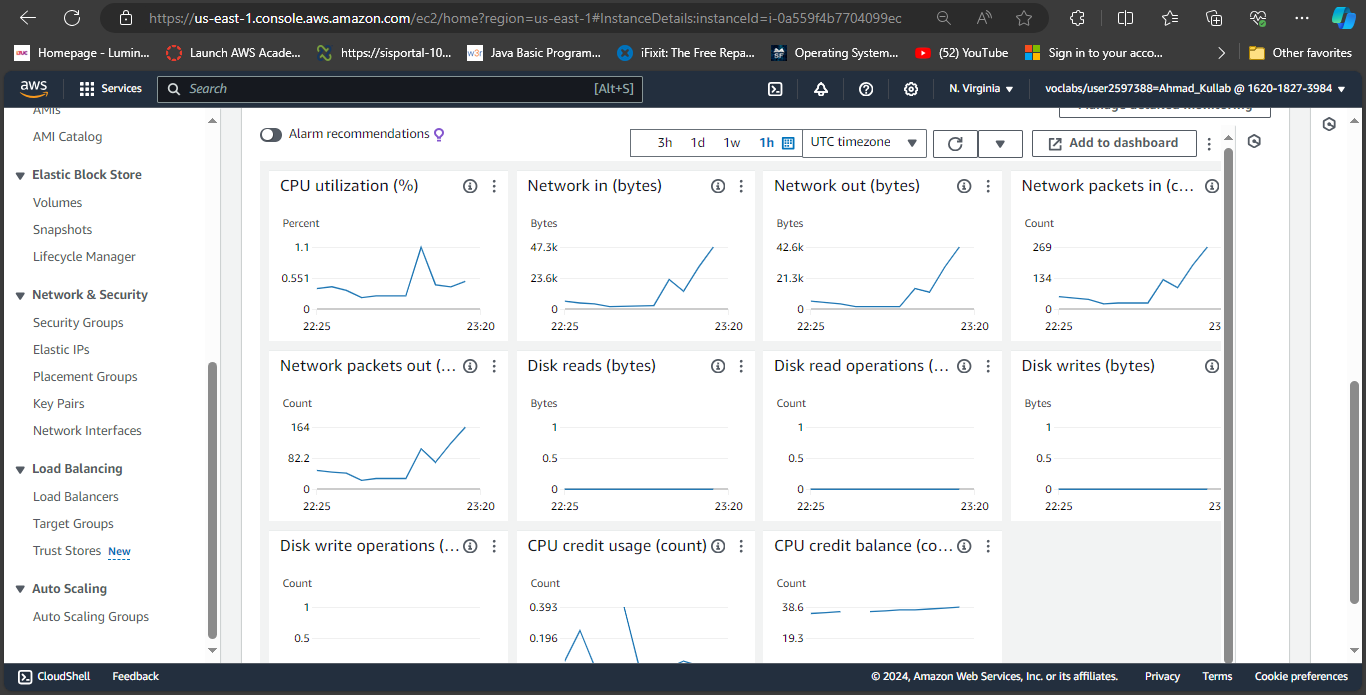
والان قمت بارسال عدد من الطلبات لمدة خمس دقائق على الويبسايت الخاص بي بساتخدام JMeter



وهذا عدد السيرفرات بعد ارسال الطلبات باستخدام ال JMeter يعد هذا القياس الديناميكي ميزة أساسية في AWS Auto Scaling، مما يضمن الاستخدام الأمثل للموارد بناءً على عبء العمل الحالي وكما نرى انه تم النجاح بالاختبار وتم ارتفاع ال عدد السيرفرات بناءً على ضغط العمل



بعد استخدام JMeter، شهدنا زيادة في حجم حركة المرور الشبكية الصادرة، مما يشير إلى تزايد في البيانات التي يقوم النظام بإرسالها إلى الوجهات الخارجية. هذا الارتفاع يُظهر تأثير الأداة على تحليل أداء النظام في سيناريوهات الاستخدام المختلفة. بعد تشغيل "auto scaling"، شهدنا هبوطًا في حركة المرور الشبكية الصادرة، مما يدل على قدرة نظام التشغيل على ضبط حجم الموارد بناءً على الاحتياجات الفعلية. يُظهر هذا الهبوط التكامل السلس بين أداة قياس الأداء وآليات التكيف التلقائي. خلال فترة "auto scaling"، لاحظنا تذبذبًا في حجم حركة المرور الشبكية الواردة، مما يشير إلى تغيرات في كمية البيانات التي يتلقاها النظام من المصادر الخارجية. يُعكس هذا التذبذب التحديات التي قد تواجهها الشبكة أثناء تعديل حجم الموارد بشكل ديناميكي. ازداد استخدام وحدة المعالجة المركزية وحجم حركة المرور بعد استخدام JMeter، مما يشير إلى زيادة في الحمل على النظام. هبطت هذه القيم بعد تشغيل "auto scaling"، مما يشير إلى أن نظام التشغيل تدخل تلقائيًا لتعديل حجم الموارد استجابةً للحمل، مما أدى إلى تحسين الأداء واستقرار النظام. استجابةً لل auto scaling، تم تحسين الأداء واستقرار النظام، مُظهرًا أن استخدام تقنية auto scaling قد ساهم في ضمان توفير الموارد الكافية لتلبية الطلب بشكل فعّال، مما يقلل من فرص حدوث تأثيرات سلبية على أداء النظام

.

**اختبار حماية SQL Injection باستخدام JMeter:**

**اسم حالة الاختبار:** اختبار حماية SQL Injection باستخدام JMeter.

**وصف الأهداف الرئيسية للاختبار:** يهدف هذا الاختبار إلى التحقق من فعالية نظام حماية SQL Injection.

**الموارد أو الأدوات:**

* JMeter لإجراء اختبارات الأداء.
* نظام حماية SQL Injection.

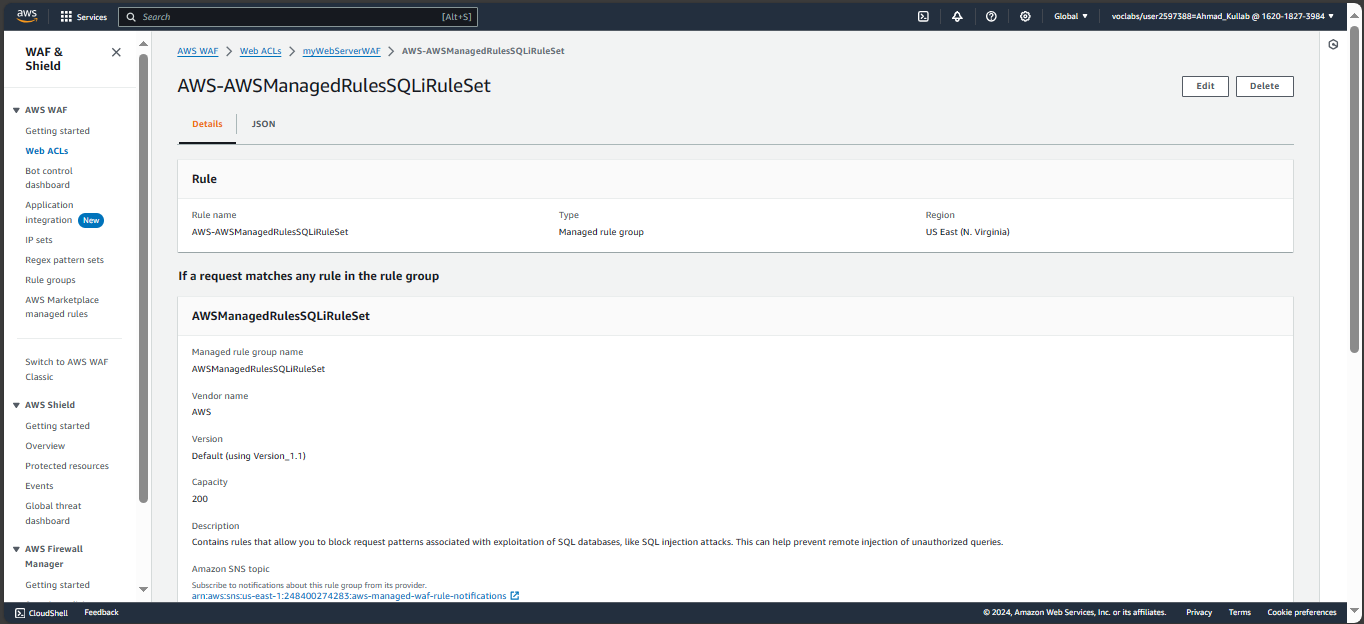
**المنهجية التي سيتم اتباعها لإجراء الاختبار:**

1. محاولة هجوم SQL Injection باستخدام JMeter.
2. فحص رد النظام على المحاولة.
3. اختبار فعالية التصدي للهجمات.

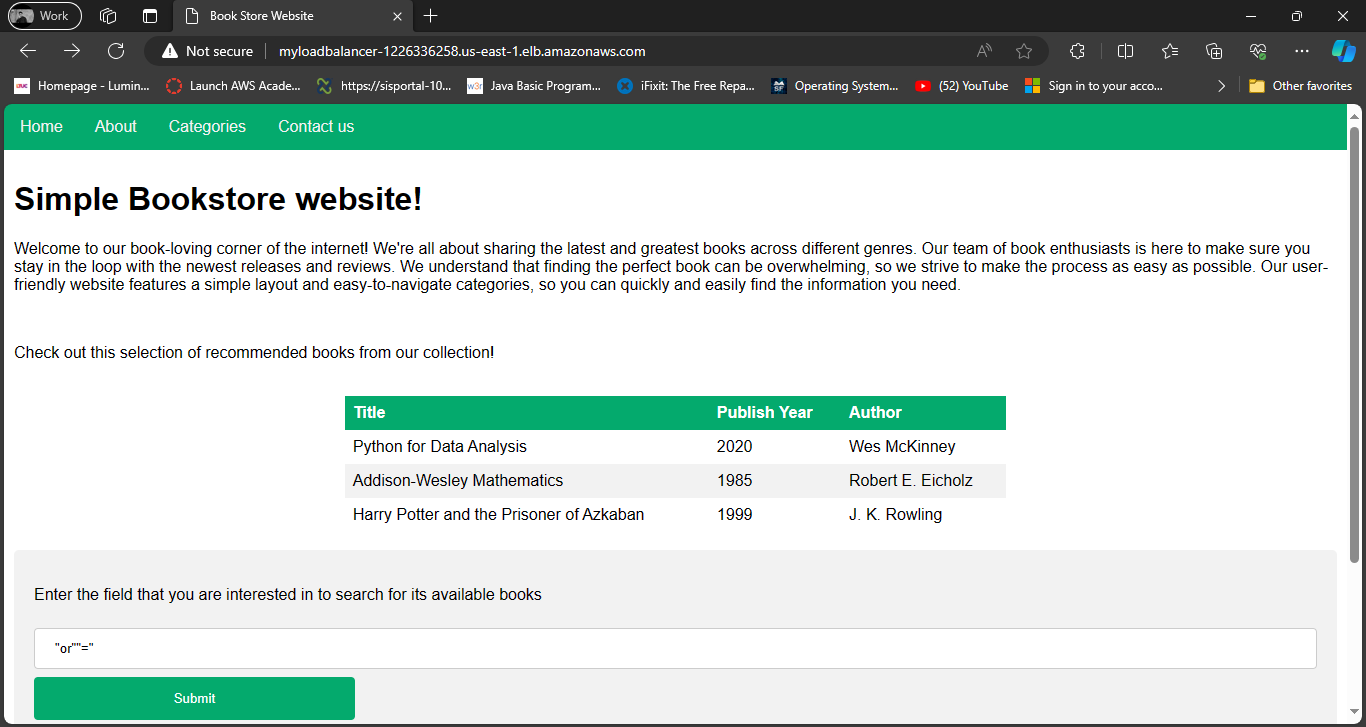
**النتائج المتوقعة:**

* فشل محاولات SQL Injection.
* قدرة النظام على التعامل مع محاولات الهجوم.
* حفاظ على سلامة قاعدة البيانات.

في هذه الصوره قمت بتخصيص قاعده باستخدام WAF والتي تنص على منع هجمات SQL injection وتمنع من الوصول الى قاعده البيانات والتخريب بها

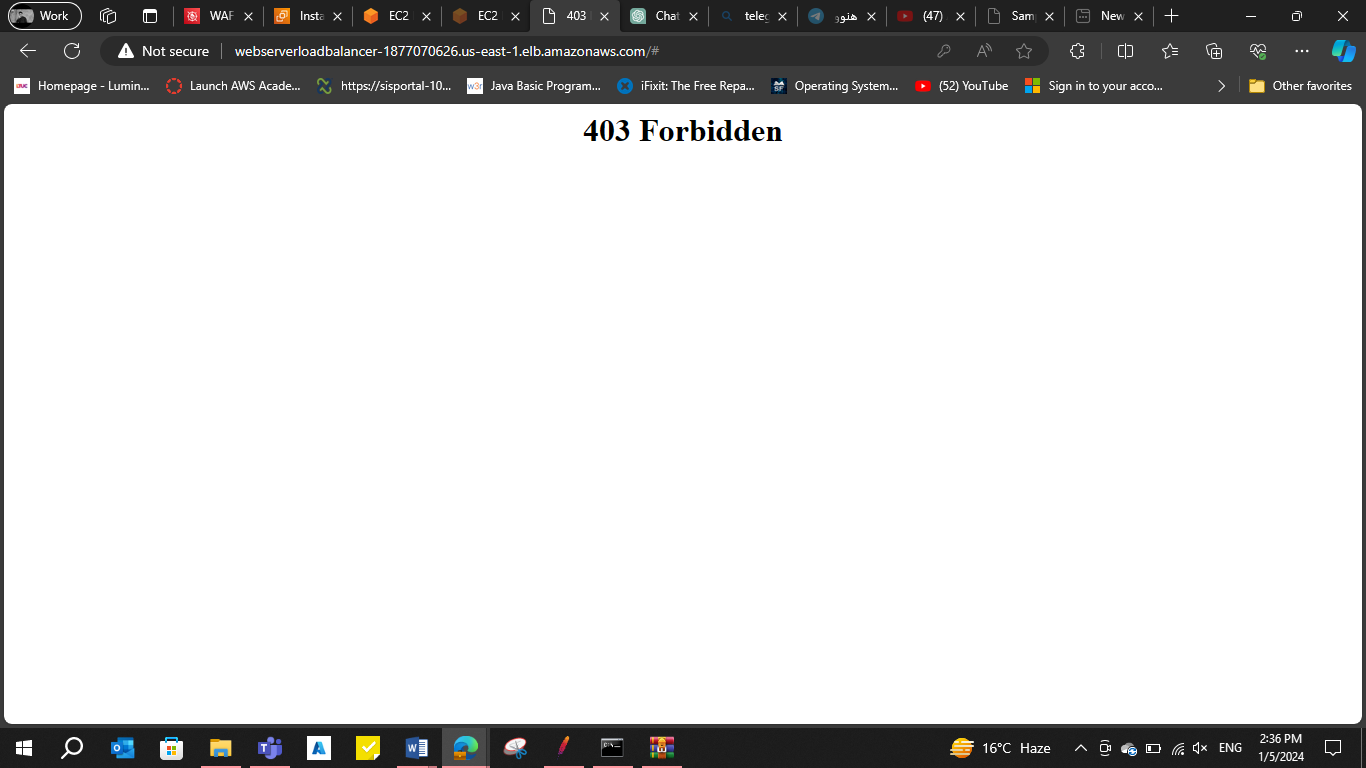


الان سوف اقوم بحقن الموقع الخاص بي باستخدام هذا الكود “or””=” والذي بدوره يعتبر حقنة SQL



SQL injection

في هذه الصوره يظهر لنا التحقق الكود 403 مما يعني انه تم عمل حظر ل IP address الذي يحاول انشاء ال SQL injection



**Task c.3**

تحليل نتائج الاختبار:

بناءً على نتائج الاختبار الشاملة للنظام، يمكننا استخلاص تأثير التحسينات التي سيتم اقتراحها وتنفيذها. سنركز على كل اختبار على حدة، مع التركيز على تحليل النتائج وتأثير التحسينات المُقترَحة.

**1. اختبار الوصول الآمن إلى SSH باستخدام Nmap:**

بعد تنفيذ اختبار الوصول الآمن إلى SSH باستخدام Nmap، والذي كان يستهدف التحقق من أمان وإمكانية الوصول لخدمة SSH، توصلنا إلى نتائج إيجابية. فشلت محاولة الاتصال باستخدام عنوان IP غير مشمول في النطاق المحدد، مما يدل على فعالية التوجيه والحماية المُعمَلة على نظام SSH. يُظهر ذلك تأثير القواعد الأمنية المفعَّلة بنجاح لمنع الوصول غير المصرح به.

**2. اختبار بوت التحكم باستخدام JMeter:**

أُجري اختبار أداء بوت التحكم باستخدام JMeter للتحقق من استجابته تحت ضغط كبير. تم تنفيذ التوسع الأمني باستخدام وحدة وقاية تطبيق الويب، وقد تمت مراقبة ومنع الطلبات الآلية بنجاح. كانت نتائج الاختبار إيجابية حيث تم رفض الطلبات الآلية وتحقيق فشل في الوصول بمعلومات الهوية الاصطناعية.

**3. اختبار التوسع التلقائي باستخدام JMeter:**

أُجري اختبار لتقييم فعالية نظام التوسع التلقائي في التعامل مع تغييرات الحمل. تم تعديل عدد المثيلات بنجاح استنادًا إلى زيادة الطلب، والتي تمثلت في ارتفاع عدد السيرفرات بشكل ديناميكي بفعالية تحت ضغط العمل الكبير. يظهر هذا تأثير نجاح التوسع التلقائي في التكيف الفعّال مع تغييرات الحمل.

**4. اختبار حماية SQL Injection باستخدام JMeter:**

تم تنفيذ اختبار لتقييم فعالية نظام حماية SQL Injection. باستخدام هجوم SQL Injection باستخدام JMeter، تم الكشف بنجاح عن محاولة الهجوم وفشلها، حيث تم تحقيق الحماية المثلى. نظام CAPTCHA أيضًا تم تفعيله بنجاح للاشتباه في عمليات الحقن وتحقيق حماية إضافية.

**استنتاج: تحليل شامل وتوصيات مُستندة إلى النتائج**

نظرًا للنتائج الإيجابية والتأثير الفعّال للتحسينات، سأتبنى تعديلات مقترحه والتي ساتحدث عنها بالتفصيل بعد قليل. التوسع التلقائي التنبؤي وزيادة سعة النظام القصوى إلى 10 يُعَدّان تحسينين ذا أثر كبير. يتيح هذا النهج تحسين أداء النظام بشكل مستمر، مع القدرة على التكيف مع تغييرات الحمل بشكل فعال. يتعامل هذا الاقتراح مع العدم اليقين في توقيت تحسين الموارد، مشابهًا لتجربة العميل في مطعم الوجبات السريعة حيث لا ينتظر طويلاً للحصول على خدمته.

**التوصيه الاولى لتحسين نظام التوسع التلقائي:**

بعد تقييم تكوين نظام التوسع التلقائي، يُقترح تحسين ملحوظ. يُوصى بزيادة السعة المطلوبة القصوى من 6، كحد أقصى حالي، إلى 10. يُعتبر هذا التعديل مفيدًا لعدة أسباب:

**التوسعية:** السعة المرغوبة القصوى الأعلى تتيح للنظام التعامل بكفاءة مع زيادة في الأعباء، مما يضمن توسعًا سلسًا استنادًا إلى تقلبات الطلب.  
  
**تحسين الأداء:** بفضل الحد الأعلى المرتفع، يكتسب نظام التوسع القدرة على الاستجابة السريعة لذروات الطلب، مما يحسن الأداء العام للتطبيق.  
  
**المرونة والقدرة على التكيف:** الحد الأعلى المرتفع يوفر مرونة أكبر لإدارة أنماط حركة المرور المتغيرة، مما يوفر قدرة على التكيف مع سيناريوهات تغيير الأعباء.

استخدام الموارد وكفاءة التكلفة: يدعم هذا التحسين تحسين استخدام الموارد خلال الفترات الذروية، مما يسهم في تحسين الكفاءة التكلفية عن طريق مزامنة تخصيص الموارد مع الطلب الفعلي.

من المهم إجراء تحليل تكلفة شامل وضمان التناغم مع اعتبارات الميزانية قبل تنفيذ هذا التحسين. بالإضافة إلى ذلك، يُوصى بإجراء رصد مستمر وإعداد إنذارات استنادًا إلى مؤشرات الأداء الرئيسية لتتبع سلوك وأداء مجموعة توسيع التلقائي بشكل فعال.

يتماشى هذا التعديل مع أفضل الممارسات لتكوينات التوسع التلقائي ويسهم في كفاءة البنية التحتية للسحابة بشكل عام.

تفاصيل إضافية:

عند إجراء اختبار أداء شامل، لوحظ أن هناك زيادة كبيرة في عدد المثيلات تحت الحمل الكبير لعدد الطلبات. كانت الزيادة السريعة في عدد المثيلات ناتجة عن الحاجة المتزايدة إلى موارد الخادم لمواجهة الضغط الكبير. لذا، يعزز زيادة السعة المطلوبة القصوى من قدرة النظام على التكيف بشكل فعال مع الحمولة المتزايدة ويقلل من تأثيرات أي ذروة غير متوقعة.

فوائد التحسين:

الأداء المحسّن (Improved Performance): تمكين النظام من التعامل بفعالية مع ذروات الحمولة يساهم في تحسين الأداء العام للتطبيق.  
استخدام فعّال للموارد(Efficient Resource Utilization): زيادة السعة المطلوبة تُسهم في تحسين استخدام الموارد وتوزيعها بشكل أفضل.  
تقليل تأثيرات الضغط(Reduced Pressure Impact): يقلل التحسين من تأثيرات الضغط الكبير على النظام ويحد من تداول سريع في إضافة وحذف المثيلات(instances).

**التوصيه الثانيه للتحسين: تنفيذ التوسع التلقائي التنبؤي**

بالإضافة إلى التحسين الموصى به مسبقًا، أقترح تنفيذ التوسع التلقائي التنبؤي. تأتي هذه التوصية نتيجة الإدراك من أن التنبؤ وضبط القدرة بشكل توقعي استنادًا إلى أنماط حركة المرور المتوقعة يمكن أن يعزز بشكل كبير الأداء الشامل واستخدام الموارد.

**فوائد التوسع التلقائي التنبؤي:**

1. التوسع التلقائي التكاملي: تمكين التعامل التكاملي مع التغييرات في حجم العمل يسمح بالتوسع التلقائي التكاملي، مما يقلل من وقت الاستجابة خلال فترات الطلب المتزايد.
2. تحسين التكلفة: يسهم التوسع التلقائي التنبؤي في تحسين استخدام الموارد بشكل أكبر، مما يقلل من التكاليف عن طريق تجنب التوسع غير الضروري خلال فترات منخفضة قابلة للتنبؤ.
3. تحسين تجربة المستخدم: يستفيد المستخدمون من أداء متسق حيث يتكيف النظام بشكل دينامي مع التغييرات في الطلب.

**خطوات التنفيذ:**

1. **تحليل البيانات:** إجراء تحليل شامل للبيانات التاريخية لتحديد الأنماط والاتجاهات.
2. **اختيار الخوارزمية:** اختيار أو تطوير خوارزميات تعلم الآلة أو النماذج الإحصائية المناسبة لتوقع أعباء العمل المستقبلية.
3. **التكامل:** دمج حلاً للتوسع التلقائي التنبؤي بسلاسة مع بنية التوسع التلقائي الحالية.
4. **الاختبار:** القيام باختبارات دقيقة للتحقق من دقة وفعالية النموذج التنبؤي.
5. **المراقبة:** تنفيذ مراقبة مستمرة لضمان أن النموذج التنبؤي يتكيف مع التغييرات في أنماط حركة المرور.

**المنطق وراء التنفيذ:**

الدافع الرئيسي وراء اقتراح التوسع التلقائي التنبؤي هو عدم اليقين في تنبؤ الوقت الذي يمكن فيه تكبير الموارد. بالمثل في مطعم الوجبات السريعة، يُشبه التوسع التلقائي التنبؤي ضمان عدم انتظار العملاء لوقت طويل حتى تكبير الموارد. فقط يمكنك الذهاب واستلام طلبك.

من خلال تنفيذ التوسع التلقائي التنبؤي، نهدف إلى توفير مستوى متسق من الخدمة لمستخدمينا، مضمونين أن النظام مستعد دائمًا للتعامل مع أعباء العمل المتغيرة. يتناغم هذا النهج التنبؤي مع أفضل ممارسات الصناعة ويسلط الضوء على التزامنا تجاه كفاءة الموارد ورضا المستخدم.

**تحليل SWOT: نتائج اختبار الأمان**

|  |  |
| --- | --- |
| القوه (strength) | الضعف (weakness) |
| 1- وصول SSH آمن 3- توسيع تلقائي ديناميكي  2- تحكم البوت الفعّال 4- حماية فعّالة من حقن SQL | 1- معالجة الأخطاء في اختبار SSH  2- زيادة في الايجابيات الكاذبة لتحكم البوت |
| الفرص (Opportunities) | التهديدات (Threats) |
| 1- تحسين معالجة الأخطاء 2- تنقيح قواعد تحكم البوت  3-المراقبة المستمرة | 1- تطور التهديدات الأمانية  2- اعادة التوازن في حالة هجمات البوت |

**القوة:**

1. **وصول SSH آمن:** تأكيد قوة تكوين الوصول عبر SSH، مما يعزز الاتصالات الآمنة ويمنع بشكل فعال وصولًا غير مصرح به ويصمد ضد هجمات Nmap.
2. **تحكم فعّال في البوت:** تفوق في تنفيذ آليات تحكم البوت، مدمجة مع جدار الحماية لتطبيق الويب، في ردع محاولات الوصول التلقائي غير المصرح به إلى النظام، وتظهر قوة النظام في تحديد ومنع حركة المرور الآلية.
3. **توسيع تلقائي ديناميكي:** يبرز نظام التوسع التلقائي القدرة على التكيف الدينامي مع تغييرات العبء، حيث زاد بفعالية من حالات الخادم استجابة لزيادة الطلب، مما يظهر مرونته وكفاءته.
4. **حماية فعّالة من حقن SQL:** التدابير الأمانية تكشف عن قوتها في مواجهة هجمات حقن SQL، وتحقق اكتشافًا فعّالًا وتقليلًا لمحاولات الاختراق، مستخدمة CAPTCHA كطبقة إضافية لتعزيز الحماية.

**الضعف:**

1. **عدم وجود التشفير المناسب لقاعدة البيانات** :يُفضل تحقيق تشفير الاتصال بقاعدة البيانات عند التفاعل معها. في حالة عدم استخدام اتصال مشفّر، يمكن للمهاجمين الاستيلاء على البيانات الحساسة خلال عملية النقل بين الخادم الويب وخادم قاعدة البيانات
2. **زيادة في الإيجابيات الكاذبة لتحكم البوت:** رغم فعالية تحكم البوت، إلا أنه أثار إيجابيات كاذبة خلال اختبار JMeter. يمكن تعديل القواعد والحدود بدقة لتحسين الدقة وتقليل احتمال حجب حركة المرور الشرعية.

**الفرص:**

1. **تحسين معالجة الأخطاء:** يمثل تصحيح الضعف في معالجة الأخطاء خطوة نحو تحسين تجربة المستخدم وتوفير رسائل خطأ أوضح لمحاولات تسجيل الدخول الناجحة.
2. **تنقيح قواعد تحكم البوت:** الفرصة لتنقيح قواعد التحكم في البوت، مما يقلل من الإيجابيات الكاذبة ويضمن عدم حجب حركة المرور الشرعية، وبالتالي تعزيز دقة اكتشاف البوت.
3. **مراقبة مستمرة وتنبيه:** تنفيذ مراقبة مستمرة مع تنبيهات بناءً على المؤشرات الرئيسية للأداء يوفر فرصة لتتبع نشاط النظام بشكل فعال والتعامل سريعًا مع قضايا الأمان.

**التهديدات:**

1. **تطور التهديدات الأمانية:** تستدعي الطبيعة الديناميكية للأمان الحاجة إلى تحديثات مستمرة لتدابير الأمان لمواجهة التهديدات الجديدة بفعالية.
2. **مرحلة الاستشفاء في حالة هجوم البوت:** في حالة هجوم بوت مستمر ومعقد، هناك تهديد لإعادة التوازن والاستشفاء. يمكن استكشاف تدابير تقيّد معدل الطلب لتخفيف هذا الخطر والحفاظ على استقرار النظام.

**Task c.4**

**AWS WAF** هي أداة قوية تلعب دورًا حاسمًا في حماية تطبيقات الويب من مجموعة واسعة من التهديدات الأمنية ، بما في ذلك ولكن لا تقتصر على هجمات القوة الغاشمة. على الرغم من أنه يوفر آلية دفاع قوية ، إلا أنه من الضروري الاعتراف بأن أي حل أمان لا يمكن أن يوفر حماية مطلقة ضد جميع أنواع الهجمات.

يمكن أن تكون هجمات القوة الغاشمة ، حيث يحاول المهاجم بشكل منهجي مختلف مزيجات من أسماء المستخدمين وكلمات المرور للحصول على وصول غير مصرح به ، صعبة التحكم بالكامل. فيما يلي بعض الاعتبارات:

**تعقيد الهجمات:** قد تنطوي هجمات القوة الغاشمة المتطورة على تكتيكات تحاكي سلوك المستخدم الشرعي ، مما يجعل من الصعب على أي أداة أمان ، بما في ذلك AWS WAF ، التمييز بين حركة المرور الخبيثة والشرعية.

**التهديدات الناشئة:** يقوم المهاجمون باستمرار بتطوير تقنياتهم ، ويمكن ظهور طرق جديدة لتجاوز تدابير الأمان. يتم تحديث AWS WAF بانتظام لمعالجة الثغرات المعروفة ، ولكن قد يكون هناك حالات يتم فيها عدم الاعتراف بمتجهات الهجوم الجديدة على الفور.

**استغلالات Zero-Day:** في الحالات التي يستغل فيها المهاجمون الثغرات الغير معروفة مسبقًا (استغلالات Zero-Day) ، قد يكون هناك نافذة من الضعف قبل تحديث حلول الأمان ، بما في ذلك AWS WAF ، بالحمايات اللازمة.

**التكوين والمراقبة:** تعتمد فعالية AWS WAF أيضًا على مدى تكوينها ومراقبتها بشكل جيد. إعادة مراجعة وتحديث مجموعات القواعد بانتظام ، ومراقبة السجلات ، وضبط سياسات الأمان بناءً على التهديدات المتطورة هي جوانب حاسمة للحفاظ على موقف أمان قوي.

رسم التشابهات بين اختبار Brute-Force Robot-Paid Attack الخاص بي والدروس المحتملة لاستراتيجية أماني:

يعتبر حادث Brute-Force Robot-Paid Attack في TaoBao في عام 2015 تذكيرًا صارخًا بالتهديدات المستمرة التي تواجهها المنصات عبر الإنترنت. في اختبار الأمان الأخير الخاص بي، استغل المهاجمون الثغرات لهجمات Brute-Force Robot-Paid Attack، تمامًا مثل حادثة TaoBao. الخيط المشترك هو نشر الروبوتات المؤتمتة التي تحاول الحصول على وصول غير مصرح به عن طريق اختبار مختلف مزيجات من بيانات الاعتماد بشكل منهجي.

التشابهات الرئيسية:

هجوم Brute-Force Robot-Paid Attack: مثل TaoBao، كشف اختبار الأمان الأخير الخاص بي عن ثغرات لهجمات Brute-Force Robot-Paid Attack. قد تختلف التفاصيل الخاصة، ولكن التحدي الأساسي يكمن في الدفاع عن المحاولات المؤتمتة للحصول على وصول غير مصرح به.

حسابات المستخدم المخترقة: تنطوي كلا الحادثتين على اختراق عدد كبير من حسابات المستخدمين. فهم الأثر المحتمل على بيانات المستخدم والخصوصية أمر حاسم للحد من مثل هذه المخاطر، خاصةً في سياق منصتي.

استغلال الحسابات للغش: استغل المهاجمون TaoBao الحسابات المخترقة لأنشطة احتيالية. يتوازى هذا مع التهديد المزدوج للوصول غير المصرح به وسوء استخدام الحسابات المخترقة لاحقًا، كما تم تحديده في اختبار الأمان الخاص بي.

اكتشفته السلطات: تم اكتشاف حادث TaoBao من قبل السلطات الصينية. وهذا يؤكد أهمية المراقبة الاستباقية واستجابة الحوادث. في استراتيجية الأمان الخاصة بي، من الضروري وجود آليات للكشف الفوري والاستجابة لانتهاكات الأمان المحتملة.

**References :**

**Task A 1.a**

[Why standards are so important to security professionals - City Security Magazine](https://citysecuritymagazine.com/risk-management/security-standards/#:~:text=Why%20should%20security%20professionals%20use%20standards%3F%20Partly%20because,standards%20are%20a%20considerable%20help%20with%20regulatory%20compliance.)

[The Importance of Cybersecurity Standards - CyberExperts.com](https://cyberexperts.com/the-importance-of-cybersecurity-standards/#:~:text=The%20adoption%20of%20standards%20can%20help%20create%20a,further%20develop%20an%20understanding%20of%20the%20business%E2%80%99s%20needs.)

[What is ISO 27001? A detailed and straightforward guide (advisera.com)](https://advisera.com/27001academy/what-is-iso-27001/)

[Quick Start Guide to Security Compliance | Cybersecurity | CompTIA](https://www.comptia.org/content/guides/quick-start-guide-to-security-compliance)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Task A 1.b**

[SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)](https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)

[NIST SP 800-53 Explained | Detailed Guide to Compliance - CYVATAR.AI](https://cyvatar.ai/nist-sp-800-53-explained/)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

[ISO 27001 scope statement | How to set the scope of your ISMS (advisera.com)](https://advisera.com/27001academy/knowledgebase/how-to-define-the-isms-scope/)

[12 Benefits of ISO 27001 Compliance and Certification - DataGuard](https://www.dataguard.co.uk/blog/benefits-of-iso-27001#two)

[What Are the 10 Clauses of ISO 27001? – ISO Templates and Documents Download (iso-docs.com)](https://iso-docs.com/blogs/iso-27001-faq/what-are-the-10-clauses-of-iso-27001#:~:text=The%2010%20clauses%20of%20ISO%2027001%20include%20context%2C,leadership%2C%20planning%2C%20support%2C%20operation%2C%20performance%2C%20evaluation%2C%20and%20improvement.)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Task A 1.c**

[Actifile Announces a Sizable Investment Round to Accelerate the Company Growth - Actifile](https://actifile.com/actifile-announces-a-sizable-investment-round-to-accelerate-the-company-growth/)

ملاحظه : بعض المعلومات التي استخدمت لاكمال هذه المهم تم اخذها من المراجع التي استخدمت ل حل المهمه 1.b و 1.a

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Task A.2**

[Cryptographic Hash Functions: Definition and Examples (investopedia.com)](https://www.investopedia.com/news/cryptographic-hash-functions/)

[Hashing in Cloud Computing: Unveiling the Key to Data Security | kili](https://kili.io/2023/11/17/hashing-in-cloud-computing-unveiling-the-key-to-data-security/)

(274-251) Krutz, R. L., & Vines, R. D. (2010). Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing. Inc. Indianapolis, Indiana

[What Are Digital Certificates? | Fortinet](https://www.fortinet.com/resources/cyberglossary/digital-certificates)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Task C.3  
[Massive Brute-Force Attack on Alibaba Affects Millions - Infosecurity Magazine (infosecurity-magazine.com)](https://www.infosecurity-magazine.com/news/massive-bruteforce-attack-on/)

[Brute-Force Attacks Affects Millions of Alibaba Accounts (lifars.com)](https://www.lifars.com/2016/02/brute-force-attacks-affects-millions-of-alibaba-accounts/)

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

**Student Declaration**

|  |
| --- |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.  Student signature: ahmad kallab Date: 24/Dec/2023 |