Tale BAC Pro CIEL	ABETECH Les secrets d'un site web	Année 2026/2027

Nom		
Prénom		
Date		
<u>Matériel</u> <u>Outillage</u>	⇨ PC ⇨ Site Web ABETech (Docker)	<u>Durée</u> : 3H
<u>Travaux à réaliser</u>	⇨ Reconnaissance du site ⇨ Découverte d'info confidentielle ⇨ Vérification protection espace privé ⇨ Analyse des autorisations ⇨ Rédaction du rapport d'audit de sécurité	

<u>Pôle d'activité :</u> Valorisation de la donnée et cybersécurité

<u>Activités :</u>

⇨ **D3** : Gestion d'incidents

<u>Tâches :</u>

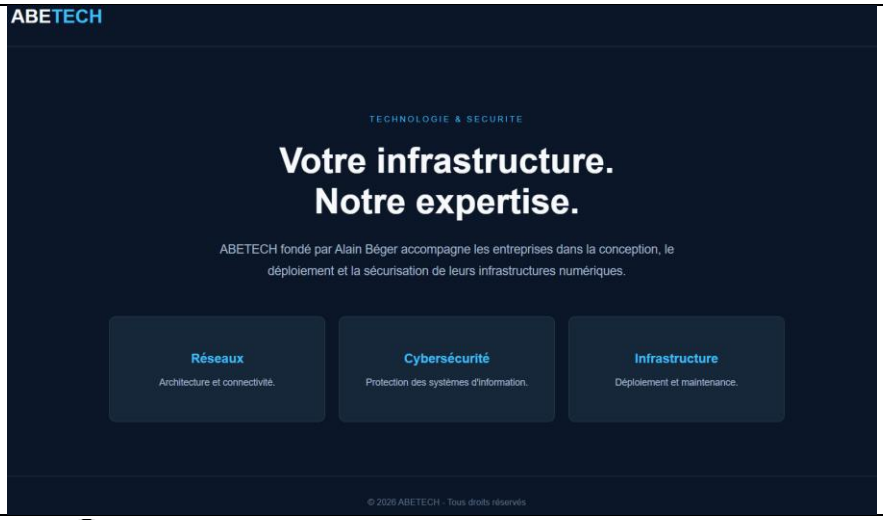
⇨ **T2** : Traiter les tickets

⇨ **T4** : Elaborer les rapports d'incidents

<u>Compétences :</u>

⇨ **C04** : Analyser une structure matérielle et logicielle

⇨ **C06** : Valider la conformité d'une installation



Lorsque le logo apparaît, il est indispensable d'appeler l'enseignant pour vérification.

A. Compétences

C01	**COMMUNIQUER EN SITUATION PROFESSIONNELLE (ANGLAIS/FRANÇAIS)**	
	La présentation (typographie, orthographe, illustration, lisibilité) est soignée et soutient le discours avec des enchaînements cohérents	
	La présentation orale (support et expression) est de qualité et claire	
	L'argumentation développée lors de la présentation et de l'échange est de qualité	
	L'argumentation tient compte des éventuelles situations de handicap des personnes avec lesquelles il interagit	
C03	**PARTICIPER A UN PROJET**	
	Les rôles et tâches de chacun sont identifiés ; le cas échéant, les besoins spécifiques des personnes en situation de handicap sont pris en compte	
	Le planning prévisionnel est compris	
	Le suivi du projet est respecté	
	L'espace collaboratif est correctement utilisé	
C04	**ANALYSER UNE STRUCTURE MATÉRIELLE ET LOGICIELLE**	
	Le besoin est identifié ainsi que les ressources matérielles, logicielles et humaines	
	Les logiciels d'analyse et de tests sont utilisés selon les procédures de traitement d'incidents	X
	Les informations nécessaires sont extraites des documents réglementaires et/ou constructeurs	
	Les indicateurs de fonctionnement sont interprétés	X
	Les fiches de test ou d'intervention sont renseignées	X
C06	**VALIDER LA CONFORMITÉ D'UNE INSTALLATION**	
	Les exigences du cahier des charges sont respectées	
	Les tests sont effectués	X
	Les résultats attendus sont vérifiés	X
	La procédure de test est respectée	X
C07	**RÉALISER DES MAQUETTES ET PROTOTYPES**	
	Le placement et routage sont conformes au cahier des charges	
	La génération des fichiers de fabrication du PCB est conforme aux attentes	
	Le PCB est réalisé, contrôlé et conforme aux IPC (tolérances mécaniques, finition de surface, propreté, ESD etc.)	
	Les composants sont conformes à la nomenclature (marquage, étiquetage)	
	La nomenclature des composants est respectée	
	Le brasage de la carte est conforme à la nomenclature et aux IPC	
	Les contraintes liées aux impacts environnementaux sont intégrées	
	Le contrôle visuel de la carte assemblée est conforme au dossier de fabrication	
	Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C08	**CODER**	
	Les environnements de développement et de test sont mis en oeuvre en tenant compte des contraintes de fonctionnalités et de sécurité	
	Le module logiciel est débogué et syntaxiquement correct	
	Les composants logiciels individuels sont développés et testés conformément aux spécifications du cahier des charges et des bonnes pratiques	
	La solution (logicielle et matérielle) est intégrée et testée conformément aux spécifications du cahier des charges et des bonnes pratiques	
	Le code est commenté et le logiciel est documenté	
C09	**INSTALLER LES ÉLÉMENTS D'UN SYSTÈME ÉLECTRONIQUE OU INFORMATIQUE**	
	L'ensemble des éléments pour l'installation du système est complet et vérifié par rapport au cahier des charges	
	Les éléments du système sont installés et raccordés selon une procédure	
	La configuration est réalisée	
	La mise en service est réalisée	
	L'état de l'installation est renseigné de manière écrite ou orale	
	Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C10	**EXPLOITER UN RÉSEAU INFORMATIQUE**	
	Les alertes et problèmes rencontrés sont renseignés	
	Les différents éléments d'un réseau ou d'un système à partir d'un schéma fourni sont identifiés	
	La mise à jour des équipements (iOS, OS, logiciel, firmware) est effectuée	
	Les optimisations nécessaires sont effectuées	
C11	**MAINTENIR UN SYSTÈME ÉLECTRONIQUE OU RÉSEAU INFORMATIQUE**	
	L'intervention est préparée	
	Le dysfonctionnement est constaté	
	La maintenance ou la réparation est réalisée	
	La fiche d'intervention est correctement renseignée	
	Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	

Nature de complexité de l'activité

Découverte	
Intermédiaire	X
Bac Pro	

B. Mise en contexte

L'entreprise ABETECH est spécialisée dans l'installation, l'administration et la sécurisation des infrastructures informatiques de ses clients.

Elle vient de déployer son nouveau site Internet, qui comporte une page d'accueil destinée au public ainsi qu'un espace réservé à ses collaborateurs. Ce dernier permet notamment de consulter des documents techniques confidentiels et de suivre les interventions réalisées chez les clients.

L'administrateur du site affirme que les informations sensibles sont correctement protégées. En effet, aucun lien présent sur la page d'accueil ne permet d'accéder aux ressources internes, et un système d'authentification a été mis en place.

Toutefois, à la suite d'un signalement concernant une possible fuite d'informations, la direction d'ABETECH souhaite faire vérifier la sécurité de son site.

Vous intervenez en qualité d'auditeur en cybersécurité. Votre mission consiste à examiner le site, identifier les éventuelles vulnérabilités et proposer des mesures correctives afin de protéger les informations de l'entreprise et de ses clients.

C. Problématique

L'absence de liens visibles et la présence d'une page d'authentification suffisent-elles à protéger les ressources sensibles d'un site web ?



D. Environnement de travail

Vous disposez d'un poste informatique disposant d'un navigateur web et d'un accès au serveur ABETECH.

L'adresse du site est communiquée par l'enseignant.

L'audit est exclusivement autorisé sur le serveur pédagogique ABETECH. Les informations recueillies sont fictives et ne doivent pas être diffusées en dehors de l'activité.

E. Reconnaissance du site (30 min)

Accéder à la page d'accueil de l'entreprise ABETECH.

Consulter la page d'accueil et **identifier** les possibilités de navigation (lien).

`Un site web peut contenir de nombreuses ressources qui ne sont pas directement visibles depuis sa page d'accueil.`

1) Découverte du fichier robots.txt

Lorsqu'un moteur de recherche, comme Google ou Bing, explore un site web, il utilise des programmes automatisés appelés robots d'indexation.

Les administrateurs peuvent placer à la racine de leur site un fichier nommé `robots.txt`, qui contient des consignes destinées à ces robots.

Ce fichier peut notamment :

- ⇨ Indiquer les parties du site que les robots ne doivent pas explorer
- ⇨ Autoriser ou limiter l'exploration de certaines ressources
- ⇨ Fournir l'adresse d'un fichier contenant la liste des ressources du site

Le fichier `robots.txt` est généralement accessible depuis l'adresse suivante :

`http://adresse-du-site/robots.txt`

Accéder au fichier robots.txt du site ABETECH.

Observer son contenu et identifier l'adresse d'un autre fichier mentionné.

Relever le nom de ce fichier : _____



2) Découverte du fichier sitemap.xml

Un sitemap (plan du site) est un fichier, généralement au format XML, permettant de communiquer aux moteurs de recherche les adresses des ressources présentes sur un site web.

Il peut notamment référencer des pages HTML, des documents PDF ou d'autres contenus.

Sur les sites comportant de nombreuses ressources, un sitemap principal peut également référencer plusieurs sitemaps secondaires.

Contrairement à un menu de navigation, ces fichiers ne sont pas nécessairement visibles depuis la page d'accueil.

Accéder au fichier identifié précédemment.

Examiner sa structure et **relever** les adresses des éventuels sitemaps secondaires :

_____

_____

Consulter ces différents fichiers afin de découvrir les ressources référencées

Dresser l'inventaire des ressources identifiées dans le tableau suivant.

Adresse de la ressource	Type de ressource	Fonction supposée

3) Analyse des découvertes

Le site ABETECH **possède**-t-il uniquement une page d'accueil ? **Justifier.**

Certaines ressources découvertes **semblent**-elles destinées à un usage interne ?

Pourquoi un administrateur doit-il être vigilant lorsqu'il référence des ressources dans un sitemap ?

Attention : les fichiers robots.txt et sitemap.xml sont normalement publics. Ils ne constituent pas des mécanismes de sécurité et ne permettent pas, à eux seuls, de protéger les ressources d'un site web.

F. Découverte des informations confidentielles (25 min)

L'administrateur d'ABETECH affirme que les documents internes de l'entreprise ne sont pas accessibles aux visiteurs du site web. Selon lui, l'absence de liens vers ces documents depuis la page d'accueil garantit leur confidentialité.

Lors de votre précédente investigation, vous avez pourtant découvert plusieurs ressources grâce aux fichiers de référencement du site.

Votre mission consiste désormais à vérifier si certaines informations internes peuvent être consultées par un visiteur non authentifié.

1) Analyse des documents accessibles

À partir des adresses découvertes dans le sitemap des documents :

- ⇨ **Accéder** aux différents documents PDF référencés
- ⇨ **Identifier** leur nature et **déterminer** s'ils semblent destinés au public ou réservés à un usage interne
- ⇨ **Relever** les informations qui permettent de distinguer un document public d'un document confidentiel

Compléter le tableau suivant :

Document	Public/Confidentiel	Justification



2) Identification des informations sensibles

Un document interne peut contenir des informations qui, sans constituer directement une faille informatique, facilitent la préparation d'une attaque.

Il peut notamment révéler l'organisation du réseau informatique d'une entreprise, les caractéristiques de ses équipements ou l'existence de services internes.

Identifier les informations techniques sensibles présentes dans le document confidentiel.

Relever les adresses IP, les noms des équipements ou les indications concernant l'infrastructure informatique.

Adresse IP	Nom équipement	Système	Fonction

Expliquer comment ces informations pourraient être utilisées par une personne malveillante pour préparer une attaque contre l'entreprise

3) Analyse de vulnérabilité

Vous avez réussi à consulter un document présenté comme confidentiel sans fournir d'identifiant ni de mot de passe.

Le fait de ne pas afficher de lien vers un document sur la page d'accueil **suffit**-il à empêcher sa consultation ? **Justifier**.

Pourquoi la présence d'un document confidentiel dans un sitemap présente-t-elle un risque ?

Si l'administrateur supprime simplement ce document du sitemap, **sera**-t-il définitivement inaccessible aux visiteurs ? **Justifier**.

Quelle mesure de sécurité faudrait-il mettre en œuvre pour garantir que seules les personnes autorisées puissent consulter ce document ?

G. Vérification de la protection de l'espace privé (30 min)

L'entreprise ABETECH dispose d'un espace interne réservé à ses collaborateurs. Cet espace permet notamment de consulter des informations techniques relatives à son infrastructure informatique.

Pour protéger ces informations, l'administrateur a mis en place une page d'authentification nécessitant la saisie d'un identifiant et d'un mot de passe.

Cependant, à la suite de la découverte de documents confidentiels accessibles publiquement, la direction souhaite vérifier que les autres ressources internes bénéficient d'une protection efficace.

1) Authentification et contrôle d'accès

La sécurité d'un site web repose notamment sur deux mécanismes complémentaires :

- ⇨ **L'authentification** consiste à vérifier l'identité d'un utilisateur, généralement à l'aide d'un identifiant et d'un mot de passe
- ⇨ Le **contrôle d'accès c**onsiste à vérifier qu'un utilisateur possède les autorisations nécessaires pour consulter une ressource ou effectuer une action

Ainsi, un utilisateur peut être correctement authentifié sans pour autant être autorisé à accéder à toutes les ressources d'un site web.

Un site correctement sécurisé doit donc vérifier les autorisations d'accès à chaque ressource sensible, et pas uniquement lors de l'accès à la page d'accueil d'un espace privé.

2) Vérification du mécanisme d'authentification

Lors de la première mission, vous avez découvert plusieurs pages web référencées dans le sitemap d'ABETECH.

Retrouver l'adresse de la page d'authentification du site : _____

Accéder à cette page et **observer** les informations demandées.

Sans saisir d'identifiant ni de mot de passe, **tenter** d'accéder directement à la page d'accueil de l'espace privé.

Observer et **décrire** le comportement du site

3) Recherche d'un défaut de contrôle d'accès

Un navigateur permet d'accéder directement à une ressource web en saisissant son adresse URL, sans nécessairement passer par les pages précédentes du site.

L'administrateur doit donc s'assurer que les contrôles d'accès sont appliqués à chaque ressource confidentielle.

Examiner les autres adresses de pages web découvertes dans le sitemap.

Identifier une ressource semblant appartenir à l'espace privé.

Tenter de consulter directement cette ressource, sans être authentifié

Comparer le comportement observé avec celui de la page d'accueil de l'espace privé.

Compléter le tableau suivant :

Ressource testée	Authentification demandée ?	Accès au contenu possible ?
Page d'accueil de l'espace privé		
Ressource interne identifiée		

4) Analyse de la vulnérabilité

Pourquoi certaines ressources de l'espace privé sont-elles accessibles alors que d'autres nécessitent une authentification ?

Quelle différence existe-t-il entre masquer l'accès à une page et protéger réellement son contenu ?

Quels risques cette vulnérabilité présente-t-elle pour l'entreprise ABETECH ?

Quelle mesure corrective proposeriez-vous pour empêcher un utilisateur non authentifié d'accéder directement aux informations confidentielles ?

H. Analyse des autorisations (35 min)

L'entreprise ABETECH dispose d'une application interne permettant à ses techniciens de consulter les fiches des interventions réalisées auprès de ses clients.

Chaque technicien possède un compte personnel et ne doit pouvoir consulter que les interventions pour lesquelles il dispose d'une autorisation.

Dans le cadre de votre audit de cybersécurité, l'administrateur d'ABETECH vous fournit les identifiants d'un compte de technicien disposant d'un accès limité à l'intervention n°101.

Votre mission consiste à vérifier si l'application respecte effectivement les autorisations attribuées aux utilisateurs.

1) Découverte de l'application de suivi des interventions

Pour réaliser cette investigation, utilisez les identifiants suivants :

Identifiant : **`technicien`**

Mot de passe : **`BacProCiel2026!`**

Accéder à la page d'authentification d'ABETECH et **s'authentifier** avec les identifiants fournis.

Consulter l'espace interne et **identifier** le lien permettant d'accéder au suivi des interventions.

Ouvrir la fiche d'intervention n°101 et **relever** les principales informations qu'elle contient.

Examiner attentivement l'adresse URL affichée dans le navigateur.

Identifier le paramètre présent dans l'URL permettant au serveur de déterminer quelle fiche d'intervention doit être affichée.

2) Vérification des autorisations

L'identifiant numérique présent dans l'adresse URL permet à l'application de sélectionner une fiche d'intervention.

Cependant, la possibilité de demander une ressource ne signifie pas nécessairement que l'utilisateur dispose de l'autorisation de la consulter.

Modifier la valeur de l'identifiant numérique présent dans l'URL afin de demander une autre intervention.

Observer le comportement de l'application

Renouveler l'opération avec un autre identifiant numérique.

Déterminer si les fiches d'intervention d'autres clients sont accessibles malgré les restrictions du compte utilisé.

Compléter le tableau suivant :

N° d'intervention	Client concerné	Consultation possible ?	Accès autorisé ?
101			
102			
103			



Le serveur **vérifie**-t-il correctement que le technicien possède les droits nécessaires pour consulter chaque intervention ? **Justifier**.

3) Identification de la vulnérabilité IDOR

La vulnérabilité **IDOR** (Insecure Direct Object Reference), ou référence directe non sécurisée à un objet, apparaît lorsqu'une application permet d'accéder à une ressource en modifiant son identifiant, sans vérifier correctement les autorisations de l'utilisateur.

Cette vulnérabilité peut concerner des documents, des comptes utilisateurs, des commandes ou encore des informations personnelles.

Expliquer pourquoi le défaut identifié dans l'application ABETECH correspond à une vulnérabilité IDOR

Préciser pourquoi la présence d'un système d'authentification ne suffit pas à empêcher cette exploitation.

Identifier les risques pour les clients de l'entreprise si cette vulnérabilité était exploitée par un utilisateur malveillant.

Proposer une mesure corrective permettant d'empêcher un technicien d'accéder aux interventions pour lesquelles il ne dispose d'aucune autorisation.

I. Rédaction du rapport d'audit de sécurité (40 min)

Votre investigation du site web ABETECH est désormais terminée.

Au cours de votre intervention, vous avez identifié plusieurs vulnérabilités susceptibles de compromettre la confidentialité des informations de l'entreprise et de ses clients.

La direction d'ABETECH vous demande de rédiger un rapport d'audit présentant les failles découvertes, les risques associés et les mesures correctives à mettre en œuvre.

1) Synthèse des vulnérabilités

À partir des résultats de vos précédentes investigations, **compléter** le tableau suivant :

Ressource concernée	Vulnérabilité identifiée	Risque associée	Correction proposée
Documents pdf			
Espace privé			
Suivi des intervention			

2) Evaluation de la gravité des vulnérabilités

Toutes les vulnérabilités informatiques ne présentent pas le même niveau de risque. Leur gravité dépend notamment de la facilité avec laquelle elles peuvent être exploitées et des conséquences potentielles pour l'entreprise.

Pour chacune des trois vulnérabilités identifiées, **estimer** son niveau de gravité (faible, modéré, élevé ou critique) et **justifier** brièvement le niveau retenu en tenant compte de la facilité d'exploitation et des informations exposées.

Vulnérabilité	Niveau de gravité	Justification
Accès aux documents confidentiels		
Accès direct à une page privée		
Consultation des interventions d'autre clients		

3) Conclusion de l'audit

Rédiger une conclusion professionnelle de 5 à 10 lignes, destinée à la direction d'ABETECH.

Cette conclusion devra préciser l'état général de sécurité du site, les principaux risques encourus par l'entreprise, les mesures prioritaires à mettre en œuvre et votre avis sur la possibilité d'utiliser ce site pour héberger des informations confidentielles.

J. Livrable

Renommer ce fichier « NOM-SecretWebSite.pdf » avec votre « NOM » nom de famille.

Téléverser le fichier.