Institut Puig Castellar

Projecte / Crèdit de síntesi

Document funcional

ALUMNE/GRUP: Yang yun Chen, Di Lu, Haoyang Xu

---

1. Introducció i context

El projecte Kontor Tek Inc. consisteix en el desenvolupament d'una **aplicació web** de subscripció que ofereix dos serveis principals als seus clients: un **programa de seguretat** per a la detecció i mitigació de vulnerabilitats, i un **servei de còpies de seguretat** al núvol.

- La necessitat que les empreses i usuaris amb serveis web disposin d'una solució integral i automatitzada per a la seguretat proactiva i la continuïtat del negoci.
- El client final són empreses o usuaris que requereixen protegir els seus serveis web i assegurar la disponibilitat de les seves dades mitjançant un model de subscripció mensual o anual.
- Es proposa una plataforma web dinàmica que centralitza la gestió de la seguretat i els backups. El propòsit és oferir una eina senzilla i potent que automatitzi tasques crítiques de TI.

2. Anàlisi de requisits

2.1. Requisits funcionals (RF)

Què ha de fer el sistema.
Enumera les funcions principals, numerades com RF1, RF2, etc.

Codi	Descripció del requisit funcional
RF1	El sistema permetrà la selecció i gestió de plans de subscripció (mensual/anual) i el processament de pagaments.
RF2	El sistema permetrà el bloqueig i desbloqueig d'adreces MAC per part de l'usuari subscrit.
RF3	El sistema implementarà un programa de seguretat capaç d'escanejar la xarxa per descobrir possibles vulnerabilitats.
RF4	El sistema generarà informes de seguretat detallats i accessibles des del panell de control.
RF5	El sistema permetrà la configuració de la freqüència i l'abast de les còpies de seguretat.
RF6	El sistema permetrà als usuaris accedir i gestionar les seves còpies de seguretat emmagatzemades.
RF7	El sistema implementarà un trigger que s'activi automàticament en detectar vulnerabilitats, bloquejant la MAC i posant-la en una llista negra.

2.2. Requisits no funcionals (RNF)

Codi	Descripció del requisit no funcional
RNF1	La interfície serà accessible des de dispositius mòbils.
RNF2	Les pàgines s'han de carregar en menys de tres segons.
RNF3	El sistema ha de ser compatible amb els navegadors web més utilitzats (Chrome, Firefox, Edge, Safari, Brave).
RNF4	El sistema ha d'utilitzar connexions segures (HTTPS) i aplicar mesures de protecció contra atacs comuns.

2.3. Restriccions

Condicions o limitacions del projecte.

- Llenguatges o tecnologies obligatòries:

El desenvolupament ha d'utilitzar Python, HTML/CSS, PHP, i la base de dades ha de ser MySQL. El servidor web serà Apache.

- Recursos disponibles (temps, equip, materials):

- Dependències o limitacions tècniques:

El servei de còpies de seguretat requereix un entorn web segur per a l'emmagatzematge i accés als arxius.

3. Anàlisi d'usuaris i rols

Objectiu: identificar qui farà servir el sistema i què podrà fer.

Descriu els diferents tipus d'usuari, les seves necessitats i els seus permisos.

Rol	Descripció	Permisos principals
Administrador	Personal intern responsable del manteniment i gestió de la plataforma.	Alta, baixa i modificació de dades. Gestió d'usuaris, gestió de subscripcions, monitorització de l'estat del servei i del sistema de seguretat.
Usuari	Client que ha contractat un pla i utilitza activament els serveis de seguretat i backup.	Accés al historial de seguretat, configuració frecuencia de backups, visualització d'informes, llistat de MACs bloquejades.
Visitant	Usuari que consulta la informació del servei i les opcions de subscripció.	Consulta de pàgines públiques, inici del procés de subscripció.

4. Casos d’ús / Escenaris d’ús

Codi	Nom del cas d’ús	Actor principal	Descripció	Resultat esperat
CU1	Registrar usuari	Visitant	L’usuari introdueix les seves dades i es crea un compte.	Usuari registrat correctament.
CU2	Subscriure's al servei	Visitant	El visitant selecciona un pla de subscripció (mensual/anual) i completa el procés de pagament.	Accés concedit al panell de control.
CU3	Veure Informe de Seguretat	Usuari	L'Usuari accedeix al panell de control i selecciona l'opció per revisar l'últim informe de vulnerabilitats.	Es mostra un informe detallat amb les vulnerabilitats detectades i les accions preses.
CU4	Bloquejar/Desbloquejar MAC	Usuari	L'Usuari gestiona manualment les adreces MAC a la llista negra de bloqueig.	L'adreça MAC és afegida o eliminada de la llista de bloqueig del programa de seguretat.
CU5	Gestió d'Usuaris	Administrador	L'Administrador accedeix al panell de gestió per donar d'alta, baixa o modificar les dades d'un usuari o la seva subscripció.	La informació de l'usuari o el seu estat de subscripció és actualitzada a la base de dades.

5. Model de dades o estructura de la informació

Objectiu: representar la informació que gestionarà el sistema.

Inclou les entitats principals (taules o objectes) i les relacions entre elles.

Entitats	
Usuari	id(PK), nom, email(Únic), data_registre, contrasenya, subscrit
Subscripció	id_subscripcio(PK), id_usuari(FK (Usuari)), tipus_pla, data inici, data fi, preu, estat_subscripcio
MACBloquejada	id_bloqueig(PK), data_bloqueig, id_usuari(FK (Usuari)), adreça_mac(Format: XX:XX:XX:XX:XX:XX)
Backup	id_backup(PK), id_usuari(FK (Usuari)), data, mida, ruta_emmagatzematge, freqüència
InformeSeguretat	id_informe(PK), id_usuari(FK (Usuari)), data_escaneig, resultat_general, num_vulnerabilitats, durada_escaneig
Vulnerabilitat	id_vulnerabilitat(PK), id_informe(FK (InformeSeguretat)), descripcio, nivell_risc, adreça_afectada, estat_mitigacio

Relacions principals:

•Un Usuari té una relació d'un a un amb Subscripció.

•Un Usuari pot tenir múltiples Backups.

•Un Usuari rep múltiples InformeSeguretats.

•Un InformeSeguretat conté múltiples Vulnerabilitats.

•Un Usuari pot tenir múltiples MACBloquejadas.

6. Disseny de la interfície

Pantalla	Funcionalitat	Casos d'us
Pàgina d'Inici	Presentació del servei, informació de preus i plans, i accés a registre/login.	CU1
Panell de Control	Dashboard principal amb resum de l'estat de seguretat i backups. Accés a totes les eines.	CU2, CU3, CU4
Configuració de Backups	Formulari per definir la freqüència, l'horari i els directoris per a les còpies de seguretat.	CU2
Visualització d'Informes	Interfície per navegar i veure els informes de seguretat històrics i el detall de les vulnerabilitats.	CU3
Gestió de MACs	Llistat d'adreces MAC bloquejades amb opcions per afegir o eliminar.	CU4
Panell d'Administració	Interfície per a la gestió d'usuaris, subscripcions i monitorització del sistema.	CU5

7. Planificació tècnica

Objectiu: planificar el desenvolupament del projecte.

Indica les tecnologies i eines que s'utilitzaran, i com s'organitzarà la feina.

- **Llenguatges i frameworks:**

PHP, Python, JavaScript, HTML, CSS, JSON

- **Base de dades:**

MySQL, per a l'emmagatzematge d'usuaris, subscripcions, configuracions de backup i informes de seguretat.

- **Eines de disseny o edició:** Apache, Visual Studio Code

- **Repartiment de tasques (si és en grup):**

Di Lu: encarregat del programa de detecció de malware.
Yang Yun: encarregat del servidor web, creació de la base de dades.
Haoyang: encarregat de donar suport en els altres treballs, redacció de documents, seguiment del projecte.

- **Cronograma:** (es pot incloure un diagrama de Gantt)

8. Anàlisi de riscos

8.1. Identificació de riscos

- Fallada de seguretat en el programa d'escaneig.
- Retard en el lliurament del projecte.
- Pèrdua de dades de còpies de seguretat.

8.2. Valoració i resposta

Classifica cada risc segons probabilitat i impacte, i indica com es mitigarà.

Risc	Probabilitat	Impacte	Pla de prevenció o contingència
Fallada de seguretat en el programa d'escaneig.	Mitjana	Alta	Realitzar proves de penetració exhaustives i utilitzar llibreries de seguretat actualitzades i ben documentades.
Retard en el lliurament del projecte.	Mitjana	Mitjana	Establir lliurables intermedis i realitzar seguiments setmanals per ajustar el cronograma.
Pèrdua de dades de còpies de seguretat.	Baixa	Crític	Implementar redundància en l'emmagatzematge i notificacions de fallada de backup.

9. Validació i criteris d’èxit

Objectiu: definir com sabrem que el projecte funciona correctament.

- Criteris d’acceptació.
    - El sistema compleix amb el 100% dels Requisits Funcionals (RF) definits.
    - El sistema compleix amb els Requisits No Funcionals (RNF) de rendiment i seguretat.
    - El programa de seguretat és capaç d'identificar almenys el 50% de les vulnerabilitats conegudes en un entorn de prova.
    - El sistema de còpies de seguretat realitza i restaura una còpia de prova amb èxit.

- Proves previstes (funcionals, d’usuari, de rendiment).
    - Proves funcionals: Verificació de cada RF (registre d'usuari, configuració de backup).
    - Proves de rendiment: Mesura del temps de càrrega de les pàgines.
    - Proves de seguretat: Verificació de la protecció contra injeccions i accessos no autoritzats.

- Indicadors de qualitat o resultats esperats.
    - El servidor web amb pàgines dinàmiques està operatiu.
    - El sistema de còpies de seguretat funciona correctament.
    - El programa de seguretat compleix amb l'objectiu mínim del 50% de funcions proposades.

10. Conclusió

L'anàlisi funcional del projecte Kontor Tek Inc. ha proporcionat una visió clara dels objectius, requisits i estructura del sistema amb funcions com la gestió de subscripcions, escaneig de vulnerabilitats, bloqueig de MACs, i servei de còpies de seguretat programades, fent servir tecnologies com PHP, Python, MySQL i Apache. Aportant automatització de la seguretat i la continuïtat del negoci per al client final mitjançant un model de servei de subscripció.

Els propers passos a seguir seran preparar les pàgines webs necessàries per aquest servei, la creació de la base de dades i la implementació del casos d'us. A partir d'aquí, comença la fase de desenvolupament.