FACULTAT D'INFORMÀTICA DE BARCELONA (FIB)

UNIVERSITAT POLITÈCNICA DE CATALUNYA (UPC)
- BARCELONATECH

GRAU EN ENGINYERIA INFORMÀTICA (GEI)

TECNOLOGIES DE LA INFORMACIÓ

Web Platform for Auditing as a Service

Memòria del projecte

Autor: Carles Llobet Pons

Data: 20/06/2017

supervisat per

DIRECTOR: ANTONIO RODRÍGUEZ GARCIA (INLABFIB - ESCERT)
PONENT: MANEL MEDINA LLINAS (AC)

Resum

El projecte Web Platform for Auditing as a Service (WPAaaS) de l'inLabFIB - esCERT s'encarrega de la instal · lació, configuració, i desenvolupament d'un servidor que serveixi una plataforma web a través de la qual usuaris externs puguin accedir a un conjunt d'eines d'auditoria pre-configurades (SQL Injections, Cross-Site Scripting (XSS), etc,...) de manera fàcil i còmode i sense coneixements específics d'aquestes, per auditar diferents serveis o sistemes sense haver d'instal · lar i configurar l'entorn i les eines adients, i amb l'avantatge de ser testejat des de fora de l'entorn de l'usuari.

A més, amb la garantia i seguretat que esCERT proporciona sobre les seves eines d'auditoría. Aquests usuaris externs, a través d'un contracte o una cessió, tindran accés a usuaris concrets per poder, en cas de mal ús de la plataforma, monitoritzar fàcilment qui, com, i què ha fet, així com restringir l'accés a l'eina.

Per això la seguretat ha d'estar present i té un paper essencial en tots els àmbits (xarxa, servei d'accès, desenvolupament de la plataforma, ...) d'aquesta nova eina que oferirà esCERT en forma d'aplicatiu web.

Resumen

El proyecto Web Platform for Auditing as a Service (WPAaaS) de l'inLabFIB - esCERT se encarga de la instalación, configuración, y desarrollo de un servidor que sirva una plataforma web a través de la cual usuarios externos puedan acceder a un conjunto de herramientas de auditoria pre-configuradas (SQL Injections, Cross-Site Scripting (XSS), etc,...) de manera fácil y cómoda y sin conocimientos específicos de éstas, para auditar diferentes servicios o sistemas sin tener que instalar y configurar el entorno y las herramientas adecuadas, y con la ventaja de ser testeado desde fuera del entorno del usuario.

Además, con la garantía y seguridad que esCERT proporciona sobre sus herramientas de auditoría. Estos usuarios externos, a través de un contrato o cesión, tendrán acceso a usuarios concretos para poder, en caso de un mal uso de la plataforma, monitorizar fácilmente quién, cómo, y qué han hecho, así como restringir el acceso a la herramienta.

Por eso la seguridad ha de estar presente y tiene un papel esencial en todos los ámbitos (red, servicio de acceso, desarrollo de la plataforma, ...) de esta nueva herramienta que ofrecerá esCERT en forma de aplicación web.

Abstract

The project Web Platform for Auditing as a Service (WPAaaS) of inLabFIB - esCERT is in charge of the installation, configuration, and development of a server that serves a web platform through which external users can access to an ensemble of pre-configured auditing tools (SQL Injections, Cross-Site Scripting (XSS), etc,...) in a easy and comfortable way, and without any required specific knowledge about them, to audit different services or systems without having to install and configure the environment of the appropriate tools, and with the advantage of being tested from outside of the user environment.

Furthermore, with the guarantee and security that esCERT provides to their auditing tools. This external users, through a contract or cession, will have access to specific users, to be able of monitoring bad usages of the platform, and know what have they done, as restricting access to the platform to them.

That is why security has to be present and has an essential role on all the fields (network, access service, platform development, ...) of this new tool that esCERT will offer as web application.

Agraïments

Aquest treball de fi de grau representa la feina realitzada durant tot l'últim any de carrera, i la guinda del pastís del Grau en Enginyeria Informàtica en que s'han centrat els últims quatre anys. Agraeixo profundament l'oportunitat que m'ha brindat inLab FIB d'enfocar la meva carrera professional cap al món de la seguretat informàtica, i la possibilitat de realitzar un projecte d'aquesta magnitud com a part de la recerca que es realitza al laboratori d'inLab FIB.

No puc deixar de mencionar la paciència i continuu suport que ha demostrat Antonio Rodríguez a l'hora de guiar i tutelar el projecte i totes les desviacions que han sorgit. Després d'un any d'esforç dedicat sota la seva supervisió i ajuda, no puc més que admirar la professionalitat i talent que demostra a l'hora de resoldre els problemes que sorgeixen tant en el camp de seguretat com de sistemes.

Agrair finalment el suport brindat per família i companys, que fan possible el fet de tirar endavant un projecte quan sorgeixen obstacles que semblen insuperables.

Índex

Índex de figures

Índex de taules

1 Introducció
1.1 Context . . . 6
1.2 Estat de l'art . . . 7
1.3 Formulació del problema . . . 9
1.4 Abast . . . 10
1.4.1 Descripció dels objectius del projecte . . . 11
1.4.2 Possibles riscs i desviacions . . . 11
1.5 Requeriments . . . 11
1.5.1 Requeriments funcionals . . . 12
1.5.2 Requeriments no funcionals . . . 12
1.5.3 Regulacions aplicables . . . 13
1.6 Metodologia i rigor . . . 14
1.6.1 Eines de desenvolupament . . . 14
1.6.2 Seguiment i validació del desenvolupament . . . 14
1.6.3 Alternatives . . . 15

2 Desenvolupament del projecte
2.1 Disseny . . . 16
2.1.1 Estructura de vistes . . . 16
2.1.2 Disseny de l'estructura . . . 17
2.1.3 Resultats finals . . . 18
2.2 Implementació . . . 23
2.2.1 Backend: Aplicació web . . . 23
2.2.2 Backend: Scripts i sistema de cues . . . 24
2.2.3 API . . . 26

3 Validació
3.1 Funcionament . . . 27
3.2 Seguretat . . . 28
3.3 Usabilitat . . . 29

4 Planificació del projecte
4.1 Planificació del projecte 30
4.1.1 Programa 30
4.1.2 Pla 30
4.1.3 Temps estimat dedicat 33
4.1.4 Pla d'acció 34
4.2 Pressupost 35
4.2.1 Recursos humans 37
4.2.2 Recursos Hardware 37
4.2.3 Recursos Software 38
4.2.4 Altres Recursos 38
4.2.5 Monitoratge dels Recursos 39
4.2.6 Cost total 39
4.3 Sostenibilitat 40
4.3.1 Econòmica 40
4.3.2 Social 40
4.3.3 Ambiental 41
4.3.4 Matriu de sostenibilitat 41

5 Obstacles trobats

6 Futures millores

7 Conclusions

Bibliografia

Índex de figures

1 *Estructura d'OpenVAS 7* 8

2 *Estructura de la plataforma* 17
3 *Les meves tasques* 18
4 *Tasca SQLmap amb resultats* 18
5 *Nova tasca d'SQLmap* 19
6 *Nova tasca d'OpenVAS* 19
7 *Nova tasca d'w3af* 20
8 *Eines online* 20
9 *Futures eines* 21
10 *Tutorial de la plataforma* 21
11 *Tutorial de l'eina SQLmap* 22
12 *Tutorial de l'eina OpenVAS* 22
13 *Tutorial de l'eina w3af* 23

14 *Diagrama de Gantt* 35

Índex de taules

1 *Escàners de vulnerabilitats més coneguts per a tipus d'auditoria* 9

2 *Relacions de temps estimat per fases* 33
3 *Codificació de les tasques* 36
4 *Pressupost de recursos humans* 37
5 *Pressupost de recursos Hardware* 37
6 *Pressupost de recursos Software* 38
7 *Pressupost d'altres recursos* 38
8 *Pressupost total* 39
9 *Matriu de sostenibilitat* 41

Introducció

Aquest projecte és un Treball de Fi de Grau realitzat per a la FIB - UPC, dirigit per Antonio Rodriguez, i supervisat per Manel Medina. S'ha desenvolupat a inLabFIB - esCERT, com a part del desenvolupament d'aplicacions per a la UPC.

L'objectiu inicial del treball és la realització d'una plataforma web que permeti autogestionar la seguretat interna dels diferents departaments de la UPC. Amb ella, els propis departaments podràn realitzar auditories bàsiques sobre els seus sistemes i serveis, per garantir seguretat constant entre auditories externes.

1.1 Context

Al títol del projecte ens trobem amb dos conceptes clau per definir aquest projecte: **Web Platform** i **Auditing As a Service**. Així que, què signifiquen?

Per a poder entendre el concepte **Auditing As a Service** primer hem d'entendre la definició de **Auditing**, de l'anglès *auditar*. Segons la RAE [4]:

> 1. f. Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse.

Així doncs, tota auditoria implica la revisió de certs estàndards i criteris, que en el cas d'aquest projecte, aquests es basen en la seguretat dels diferents sistemes i serveis que ofereixen els departaments de la UPC.
Amb la segona part del terme, **As a Service** (de l'anglès *com a servei*), es dona a entendre que aquest projecte oferirà un servei d'auditories de seguretat.
Finalment, **Web Platform** (de l'anglès *plataforma web*) ens indica que aquest servei s'oferirà a través d'una plataforma web que facilitarà la sol · licitació dels diferents tipus de servei d'auditoria.

Els diferents tipus d'auditoria que ofereix aquesta plataforma es veuen definits a través de les eines que implementa. Aquesta plataforma web inclou l'automatització d'eines d'auditoria de sistemes i xarxes (OpenVAS [1]), auditoria de bases de dades (SQLmap [2]), i auditoria d'aplicacions web (W3AF [3]).
Totes elles s'han automatitzat i es gestionen a través d'un sistema de cues intern a la plataforma, per tal que el flux de peticions dels diferents departaments estigui controlat.

Aquest projecte s'ha realitzat a inLabFIB - esCERT sota el nom de CoSA (Conjunto de Servicios de Auditoria).

El departament d'AC ha col · laborat amb inLabFIB proporcionant *feedback* i provant l'aplicació web i les seves diferents eines a durant totes les fases de desenvolupament.

El director d'aquest TFG és l'Antonio Rodríguez, responsable de l'àrea de ciberseguretat d'inLabFIB - esCERT. El ponent és en Manel Medina Llinas, director de l'esCERT i professor de la Facultat d'Informàtica de Catalunya. Antònia Gómez, responsable de tota l'àrea de Sistemes, Aules y Comunicacions (ASAC) d'inLabFIB, també ha seguit properament tot el projecte, proporcionant *feedback* i definint les diferents funcionalitats requerides per part de l'empresa.

Aquest projecte es desenvolupa per a la UPC (Universitat Politècnica de Catalunya), i l'utilitzaran els diferents administradors de sistemes de cada departament d'aquesta. Se'n beneficiaran a l'hora tant els propis departaments per una gestió automatitzada de la seva seguretat, com la UPC que podrà garantir uns mínims de seguretat a tots els seus departaments, com esCERT, que podrà auditar més a fons cadascun dels departaments que audita gràcies a la tranquil · litat que proporcionarà aquesta eina.

1.2 Estat de l'art

La seguretat informàtica o ciberseguretat és un punt cada cop més present entre nosaltres. Cada cop es troben majors quantitats de vulnerabilitats i diferents víes per a donar un mal us als recursos informàtics, cada cop més freqüents en tots els sectors.
Per aquest motiu, la necessitat d'auditories de seguretat i un bon control de les noves amenaces que a diari apareixen, aclapara cada cop més als administradors de sistemes i als auditors de seguretat, fent cada cop més necessàries eines de comprovació automàtica de vulnerabilitats i alertes de seguretat.

En l'àmbit de l'automatització d'auditories de seguretat, el precursor més gran és clarament **OpenVAS (Open Vulnerability Assessment System)**. Aquest framework de diferents eines i serveis ofereix un escàner de vulnerabilitats a través de la seva potent base de NVT (Network Vulnerability Tests), que és actualitzada a diari per incloure les proves que permeten identificar las noves vulnerabilitats emergents.

Un cop trobades aquestes vulnerabilitats, es relacionen a través del seu OID (Identificador únic de la vulnerabilitat) o CVE (Common Vulnerabilities and Exposures) amb la seva definició, solució, i altres informacions que puguin ser útils o rellevants per a l'auditor o administrador dels sistemes encarregat de llegir l'informe resultant de l'escaneig.

OpenVAS es compon modularment per un nucli format per l'escàner i el controlador (manager), i es gestiona a través de consola (OpenVAS CLI) o a través d'una aplicació web (Greenbone Security Assistant).

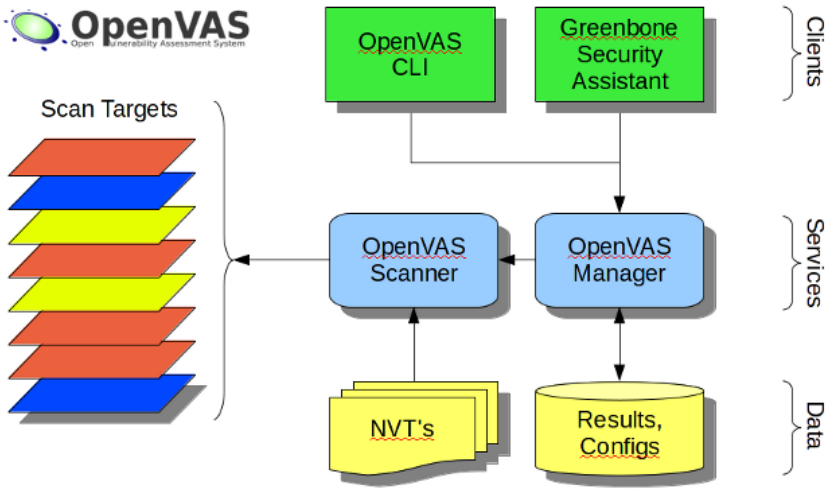

Figura 1: Estructura d'OpenVAS 7

Aquesta eina i similars, faciliten molt als auditors de seguretat les seves tasques rutinàries de comprovació, e inclús permeten en alguns casos (com OpenVAS) programar escanejos periòdics de les vulnerabilitats més generals i conegudes, permetent a aquests centrar-se en auditories manuals específiques, o donar prioritat a certes auditories on s'han detectat vulnerabilitat greus que hauríen de ser remeiades urgentment.

Aquest projecte aprofitarà vàries d'aquestes eines englobant-les en paquets modulars, i les gestionarà a través d'un sistema de cues i una interfície web per tal de proporcionar una eina unificada, potent i escalable que puguin utilitzar tots els administradors de sistemes de cadascun dels departaments de la UPC.

1.3 Formulació del problema

Tot i l'existència de totes aquestes eines d'auditoria per als diferents tipus de serveis a auditar, no hi ha una gran varietat d'eines per a cada tipus de servei, pel que han de ser eines molt completes, fet que implica cert grau de dificultat i coneixement de l'eina per a utilitzar-les correctament.

A continuació podem observar una taula de les diferents eines que hi ha per a certs tipus de serveis a auditar, que ens mostra la gran quantitat d'eines útils a l'hora d'auditar cadascun d'aquests serveis, extrets de la OWASP (Open Web Application Security Project) [7]:

Servei	**Eines**
Bases de dades	SQLmap SQLninja SQLsus ..
Infraestructura	OpenVAS Nessus Acunetix ..
Aplicacions Web	w3af Burp ..

Taula 1: Escàners de vulnerabilitats més coneguts per a tipus d'auditoria

Es per això, que auditar la seguretat d'una infraestructura o varis d'aquests serveis que pot oferir o requerir una empresa, requereixi una formació prèvia i hores de pràctica per a dominar cadascuna d'aquestes eines.
El poc coneixement i la necessitat de gent experta en l'àmbit de la seguretat fa que els auditors de seguretat siguin personal indispensable en qualsevol àmbit que ofereixi qualsevol tipus de solucions informàtiques.

La UPC consta de diversos departaments per facultat, en concret la Facultat d'Informàtica de Barcelona en té 8 [5], tots els quals s'han d'auditar contínuament ja que tots ells utilitzen diversos servidors des d'on ofereixen portals web, on emmagatzemen informació sensible, o inclús realitzen estudis i executen programes d'alta importància, i no poden estar exposats a vulnerabilitats que podrien implicar pèrdues d'informació, DOS (de l'anglès *Denial Of Service*, que significa denegacions de servei) o inclús pèrdues de control sobre els seus servidors.

Tot i així, la UPC no consta de prou personal expert en ciberseguretat per poder auditar a diari o setmanalment cada departament. Les auditories a 18 d'aquests departaments s'han dut a terme per inLabFIB - esCERT durant els darrers anys, i s'auditaven els departaments un rere l'altre en cicles. Aquests cicles implicaven que cada departament s'auditava aproximadament un cop cada dos anys, pel que durant gairebé dos any estaven exposats a possibles noves amenaces a la seguretat dels seus serveis.
A més, un departament podia obrir un nou servei, que podia estar gairebé un any sense ser auditat ni comprovada la seva seguretat.

Per tots aquests fets, era clara la necessitat d'una eina o plataforma que unifiqués els serveis més comuns i fes possible als administradors de sistemes de cada departament verificar uns mínims de seguretat de forma molt més freqüent, i que donés la possibilitat de verificar també nous serveis abans de posar-los en marxa, sense haver d'esperar a que es pogués auditar de manera completa el departament o servei un altre cop.

Aquesta eina, a més, havia de ser prou simple per tal que els administradors de sistemes la poguessin usar sense necessitat de coneixements previs en les diferents eines d'auditoria, però prou potent com per garantir per darrere un bon nivell de seguretat i cert grau de confiança en els resultats.

1.4 Abast

L'abast d'aquest TFG és el desenvolupament d'una plataforma que unifiqui diverses eines de seguretat i les automatitzi per a l´ús exclusiu dels departaments de la UPC en col · laboració amb inLabFIB. A través d'aquest portal, els administradors dels sistemes d'aquests departaments han de ser capaços de comprovar la seguretat de tots els tipus de serveis que ofereixen sense necessitat de conèixer completament el funcionament de cadascuna de les eines, i permetent deixar-les guardades i en execució periòdica automàticament.

D'aquesta manera, només s'hauran d'encarregar de llegir l'informe quan rebin el correu amb els resultats cada cop que executin un escaneig o s'executi perquè l'han programat prèviament per a executar-se amb certa periodicitat, i corregir els forats de seguretat trobats.

1.4.1 Descripció dels objectius del projecte

Desenvolupament d'una plataforma web que unifiqui i automatitzi l'ús de diverses eines de seguretat.

Els diversos administradors de sistemes de cada departament de la UPC han de ser capaços a través d'aquesta plataforma d'autoabastir la gestió d'uns mínims de seguretat continua o periòdicament. Ha de ser per conseqüent una eina enfocada a l'ús per persones sense suficients coneixements de les eines que s'utilitzen per darrere, facilitant la detecció d'errors o vulnerabilitats a l'administrador a través d'alguns paràmetres senzills i forçant l'ús d'altres paràmetres des del nostre punt de vista molt més expert en el camp de treball.

Ús i gestió de l'eina per als administradors de sistemes.

La plataforma web ha d'utilitzar el mateix format de gestió de tasques per a cada eina, independentment del tipus de servei al que està enfocada, per tal de garantir usabilitat i comprensibilitat a l'usuari.
A més, ha d'estar preparada per gestionar un gran volum de tasques de diferents departaments independents, sense afectar a la velocitat de l'eina, i a de permetre als usuaris despreocupar-se el més possible de la gestió de tasques, avisant per altres canals (com correu electrònic) en cas d'incidencia o finalització d'escaneig, adjuntant els resultats en un format comprensible per al administrador de sistemes.

1.4.2 Possibles riscs i desviacions

Aquesta plataforma web dependrà de la gestió de cada eina que es vulgui afegir a la plataforma, pel que depenent del tipus d'eina i les facilitats que doni a l'hora d'integrar-se o no a altres plataformes, pot modificar l'estructura de funcionament de la plataforma o inclús impossibilitar l'adició d'aquesta eina a la plataforma.
Depenent de les condicions que ens ofereixi el servidor on s'executarà l'eina, podria causar problemes a l'hora de gestionar les cues de tasques i inclús denegacions de servei.

1.5 Requeriments

En aquesta secció especificarem els requeriments funcionals i no funcionals definits durant el plantejament i planificament del projecte. Cal recordar que aquest requeriments han sigut definits conjuntament entre el Project Manager (Antonio Rodriguez) i l'alumne (Carles Llobet), i s'han proposat i validat per Antonia Gómez, cap del departament ASAC de inLabFIB.

1.5.1 Requeriments funcionals

- Els usuaris han de poder iniciar i tancar sessió
- Els usuaris han de poder navegar per la interfície web
- Els usuaris han de poder configurar i guardar tasques de les eines implementades
- Les tasques han de poder ser programables per a execucions periòdiques
- Els usuaris han de poder veure l'historial de tasques que s'han executat i tornar-les a executar
- Les tasques s'han de poder cancel · lar durant l'execució mentre no estiguin finalitzades
- Els resultats de les tasques s'han de poder exportar en el format adient depenent de l'eina utilitzada

1.5.2 Requeriments no funcionals

- Els usuaris no han de poder veure les tasques ni informació d'altres usuaris
- Les tasques només poden ser executades contra servidors o sistemes de la UPC
- Ha d'existir la figura d'administrador que pugui veure totes les tasques i usuaris existents, i gestionar-los
- Cada eina ha d'incorporar un sistema de cues per a les tasques, i executar paral · lelament un nombre predefinit de tasques concurrents
- Les tasques s'han d'executar per ordre cronològic de petició
- La plataforma ha d'incorporar les mesures de seguretat adients per controlar els possibles usos fraudulents
- La plataforma ha de ser compatible amb els navegadors més comuns (Google Chrome, Mozilla Firefox i Internet Explorer)
- La plataforma ha de ser modular per permetre l'extensibilitat futura a incorporacions de noves eines
- La plataforma ha de ser robusta i mantenir la seva integritat, assegurant que no es subjecte de possibles errors interns.

1.5.3 Regulacions aplicables

No es guarden dades de caràcter personal dels usuaris pel que no és necessària la realització de cap acció que requereixi el compliment legal del tractament de les dades. Els usuaris, per això, es fan responsables de la seguretat dels seus propis servidors i de la presa d'accions necessàries per a solucionar les vulnerabilitats que pugui trobar la plataforma als seus sistemes.

Tanmateix, si que s'utilitzen llibreries amb diferents llicències. Aquestes estan sota llicències de caràcter obert com *MIT* o *Apache 2.0*. La llicència *MIT* permet l'ús, còpia, modificació, distribució i/o venda de còpies del software sempre que es mantingui la capçalera original als arxius de codi. En canvi, la llicència *Apache 2.0* també dóna plena llibertat d'ús però requereix un arxiu LICENSE amb la còpia de la llicència i un arxiu NOTICE on s'indica si hi ha avisos obligatoris del software present, al directori principal del projecte. S'han respectat ambdues condicions, tant les de les llicències *MIT* com la d'*Apache 2.0*.

1.6 Metodologia i rigor

1.6.1 Eines de desenvolupament

Aquesta nova plataforma es formarà sobre dos servidors:

- Un d'ells s'encarregara de servir la plataforma web i d'executar les eines que pertoquin.
- L'altre l'utilitzarem per a la base de dades que emmagatzemara els usuaris, cues de tasques, etc.

La plataforma es desenvolupara amb el framework de python Django a través de la IDE PyCharm com a backend, que serà l'encarregat d'interactuar entre el frontend (pel qual s'utilitzara la plantilla SBAdmin2 de Bootstrap i codi en HTML natiu) i les bases de dades i scripts que controlaran i gestionaran els usuaris, les cues, permisos, i eines.

Per a la base de dades, utilitzarem el SGBD (Sistema de gestió de bases de dades) MySQL.

1.6.2 Seguiment i validació del desenvolupament

Seguiment S'utilitzarà la metodologia àgil Scrum [8] per al seguiment de tot el desenvolupament del projecte. Utilitzarem el sistema de kanban Trello per al seguiment de les tasques a desenvolupar, i tota la documentació del procediment seguit es farà a través del Redmine [6] privat de l'inLabFIB.
Finalment per al seguiment temporal de les tasques s'utilitzarà Toggl per a comptabilitzar les hores dedicades per tasca i poder comprovant si es segueixen els temps establerts aproximats al diagrama de Gantt.

Validació El director del TFG dura a terme un seguiment constant del progrès de desenvolupament per a enfocar correctament.
Es faran reunions de seguiment setmanals amb la cap del departament per valorar el progrès i proposar solucions i millores en els punts ja desenvolupats. Finalment hi haurà una reunió final amb el Responsable de Seguretat TIC i LOPD de la UPC, Víctor Huertas, per a una validació final del producte resultant.

Per al testeig i proves de la plataforma l'equip intern d'inLab anirà provant les diferents funcionalitats implementades setmanalment, i un cop la plataforma arribi a un punt de certa utilitat (una eina completa implementada i funcional) el departament d'AC s'encarregarà de fer les proves pilot al seu departament i donar el feedback corresponent.

1.6.3 Alternatives

Es important remarcar que l'abast d'aquest projecte es defineix en el marc de l'automatització de les auditories de seguretat, i es desenvoluparà a inLabFIB - esCERT. Com s'han utilitzat metodologies àgils, que impliquen la subdivisió d'aquestes tasques mencionades en tasques encara més petites i fàcils de controlar, han sorgit petites desviacions donada la constant revisió del procès.

Un dels possibles problemes que s'ha patit, ha estat la impossibilitat de donar el mateix patró de funcionament a una de les eines que es volia incorporar a la plataforma. En aquest cas, s'ha valorat la possibilitat de dissenyar un patró exclusiu de funcionament per a aquesta, i s'ha implementat. Aquesta solució ha afegit aproximadament 40 hores de treball, però no ha afectat pas als recursos.

Desenvolupament del projecte

2.1 Disseny

2.1.1 Estructura de vistes

Podem dividir la plataforma web en 3 tipologies de vistes clarament diferenciades, segons la seva relació amb les eines que formen aquesta plataforma:

1. **Comunes** Les vistes comunes són aquelles que comparteixen totes les eines. Aquí podem trobar des de la vista inicial on veiem totes les tasques en general sense dependre de l'eina, fins al menú superior desplegable del progrés de les tasques, o de notificacions de les tasques finalitzades.

2. **Específiques** Les vistes específiques són aquelles que només s'utilitzen per a una eina en concret, i que s'hauran d'incloure en el modul que les implementi. Aquestes són des de les vistes de totes les tasques d'una eina en concret (on es mostrara molta més informació que a la general) o la vista d'una tasca concreta d'aquella eina amb els seus resultats, fins al formulari d'inserció d'una nova tasca per a aquella eina o el tutorial de com funciona aquesta eina i els seus paràmetres.

3. **Independents** Finalment les vistes independents són aquelles que no depenen de cap eina ni tenen relació amb elles, sinó que són merament informatives o de gestió de la pròpia plataforma. Podem encabir en aquesta secció des de vistes com el tutorial de com funciona la plataforma en general, la d'altres eines online que podem trobar útils, o la vista amb les futures eines a implementar dins la plataforma, fins al panell d'administrador per als gestors o la pròpia vista d'inici de sessió.

2.1.2 Disseny de l'estructura

Degut a la claredat dels requeriments, sobretot aquell que implica la modularitat de la plataforma a dissenyar, el disseny de l'estructura va ser ràpidament resolt.

Com podem veure a la següent figura, l'usuari es comunica a través del navegador amb l'aplicació web, i interactua amb ella. El servidor de Django és l'encarregat de servir-li les vistes adients i de comunicar-se amb el Servidor de la Base de Dades a través de la API de Django per a consultar dades o inserir noves tasques, les quals aniran al sistema de cues de l'eina que pertoqui.
Finalment el servidor de Django tindrà també els scripts en el seu cron que seran els encarregats d'anar executant les tasques del sistema de cues, comunicant-se amb la BD a través de l'API. Un cop executades, enviarà els resultats a través de la API al servidor de la Base de Dades, i aquest les enviarà al Servidor de Django quan aquest les sol · liciti per poder-les mostrar a l'usuari a través de l'aplicació web.

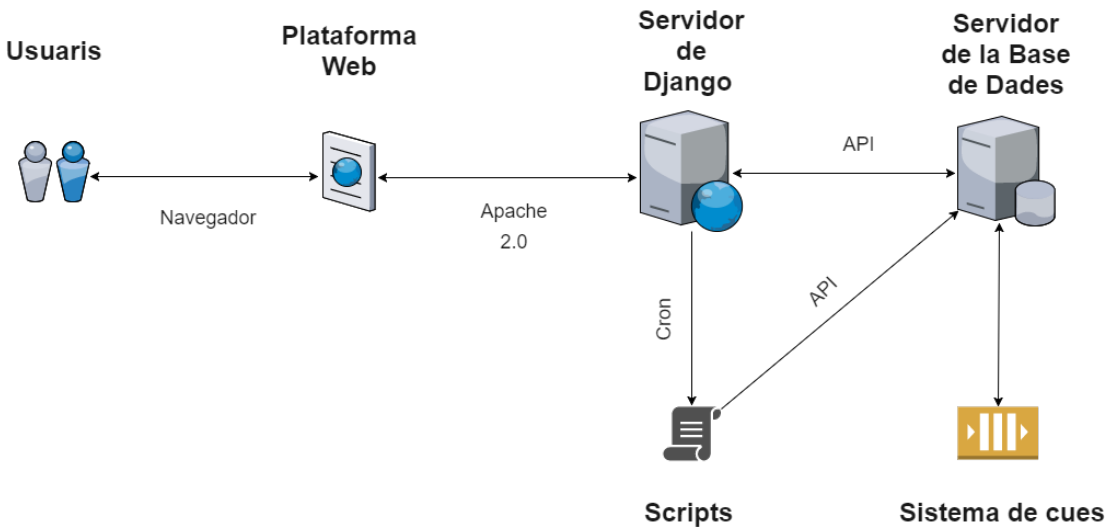

Figura 2: Estructura de la plataforma

2.1.3 Resultats finals

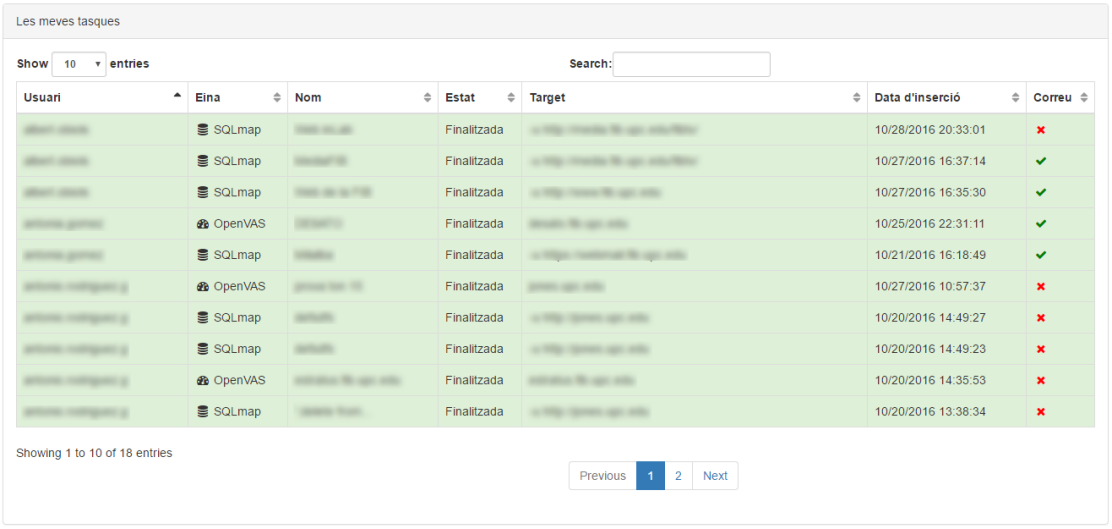

Figura 3: Les meves tasques

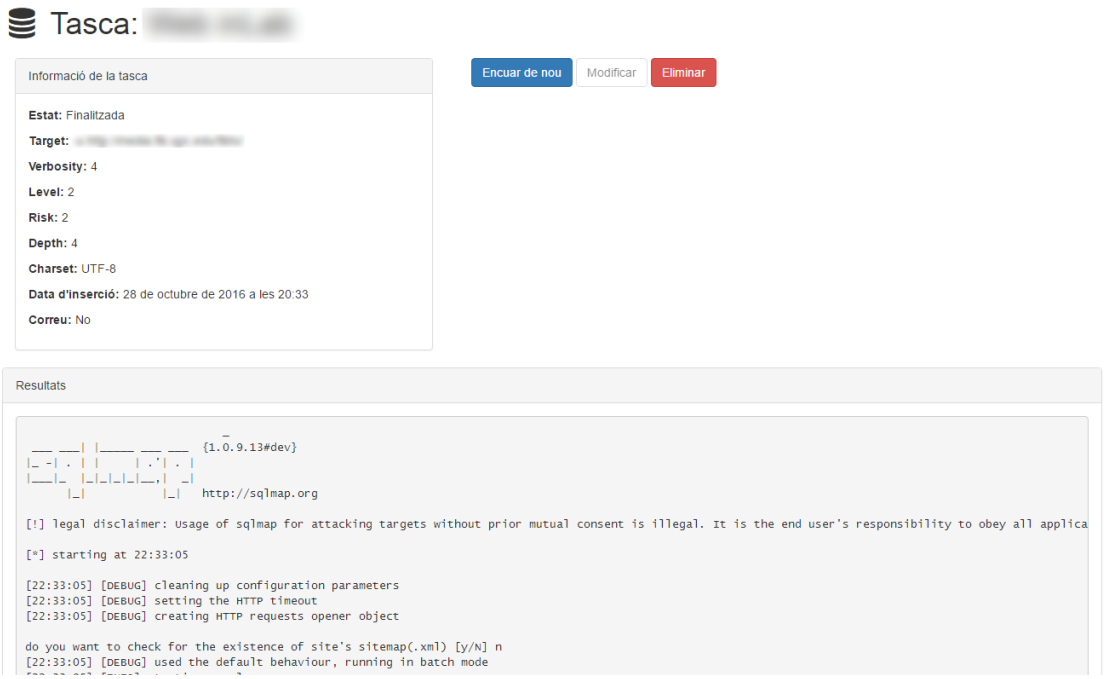

Figura 4: Tasca SQLmap amb resultats

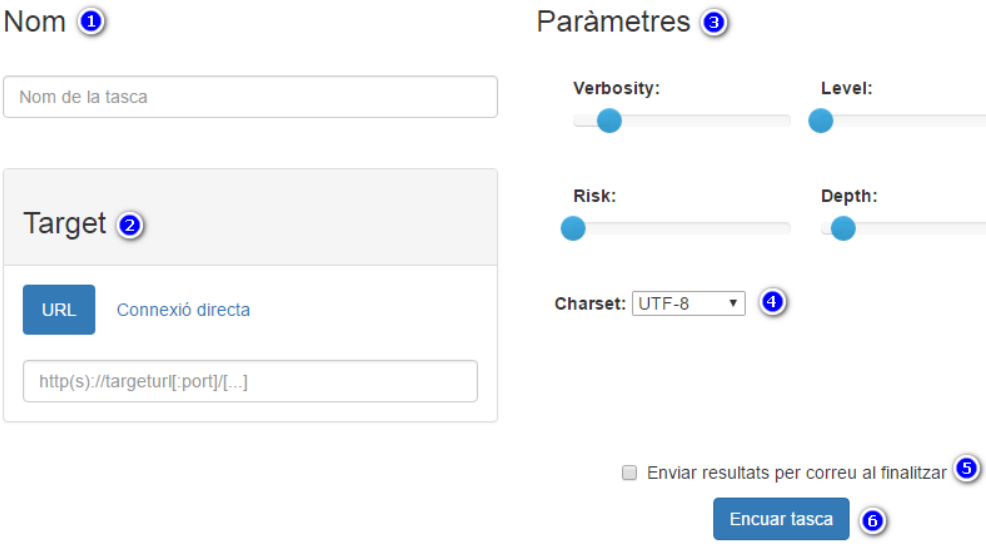

Figura 5: Nova tasca d'SQLmap

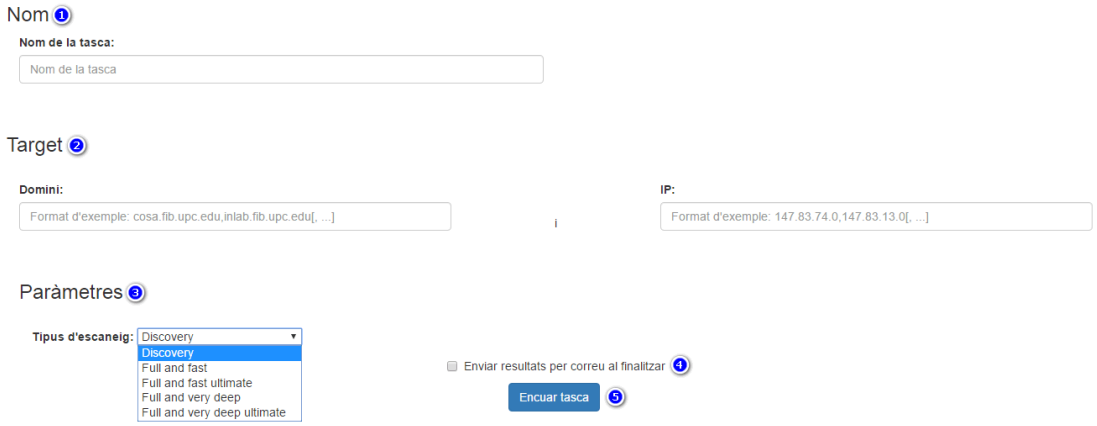

Figura 6: Nova tasca d'OpenVAS

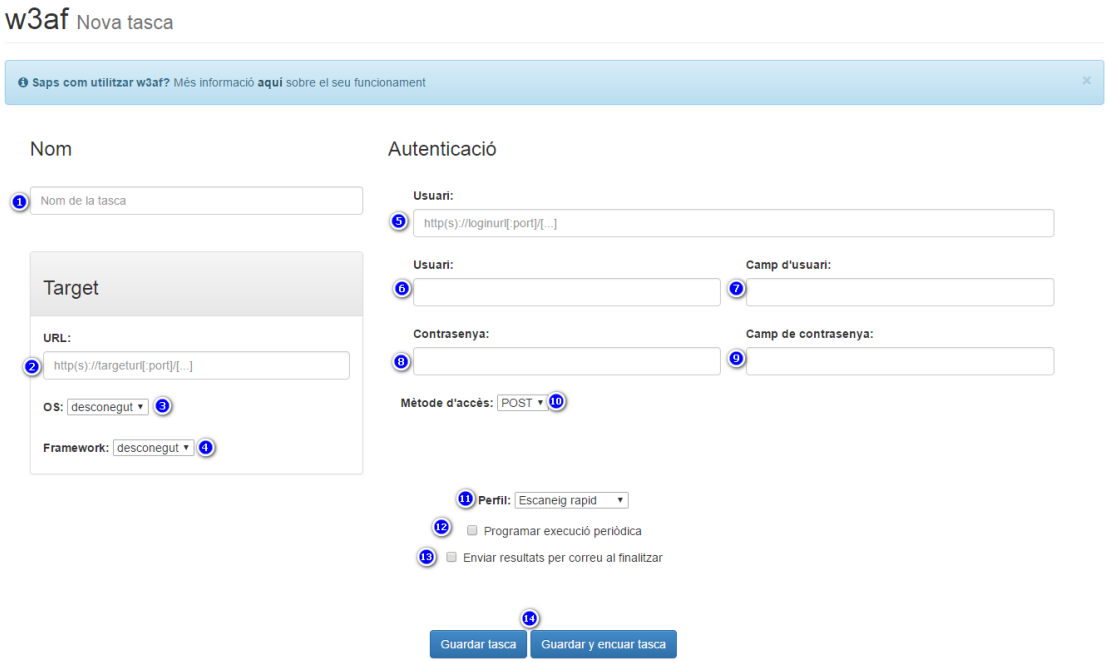

Figura 7: Nova tasca d'w3af

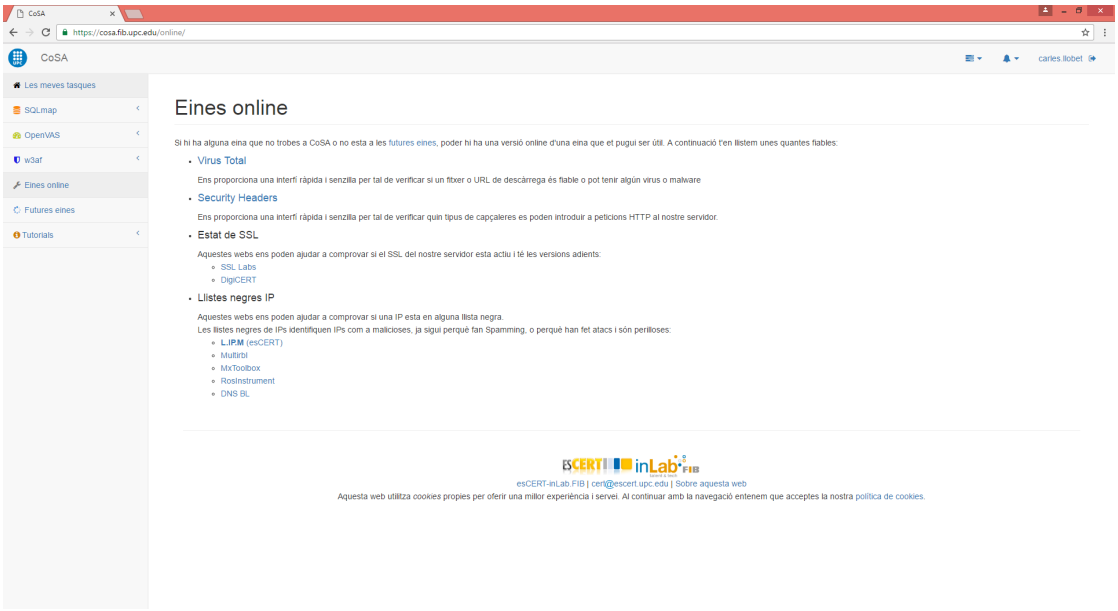

Figura 8: Eines online

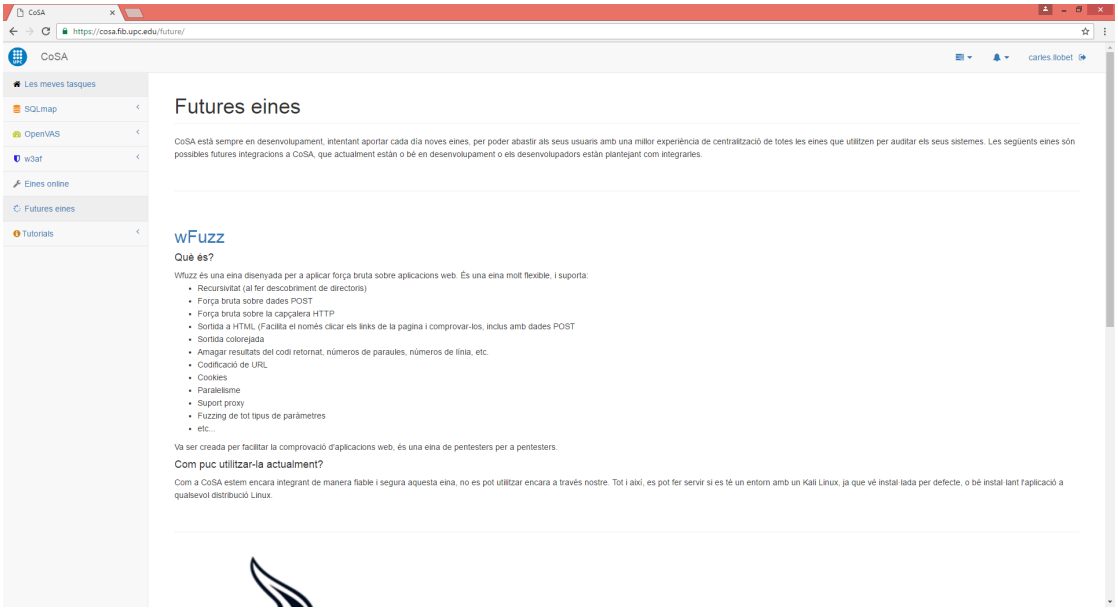

Figura 9: Futures eines

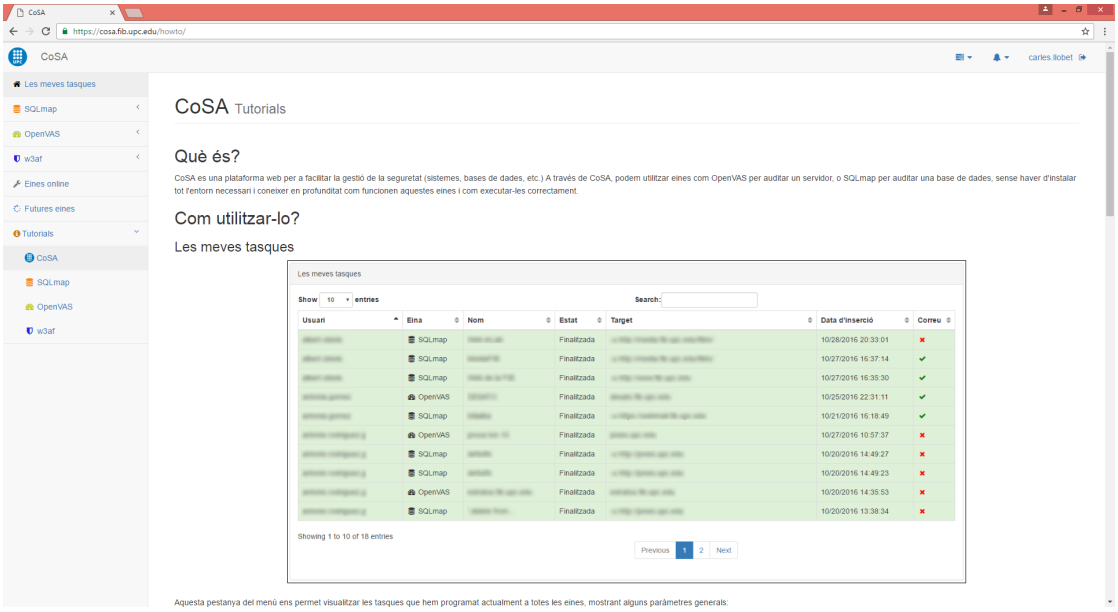

Figura 10: Tutorial de la plataforma

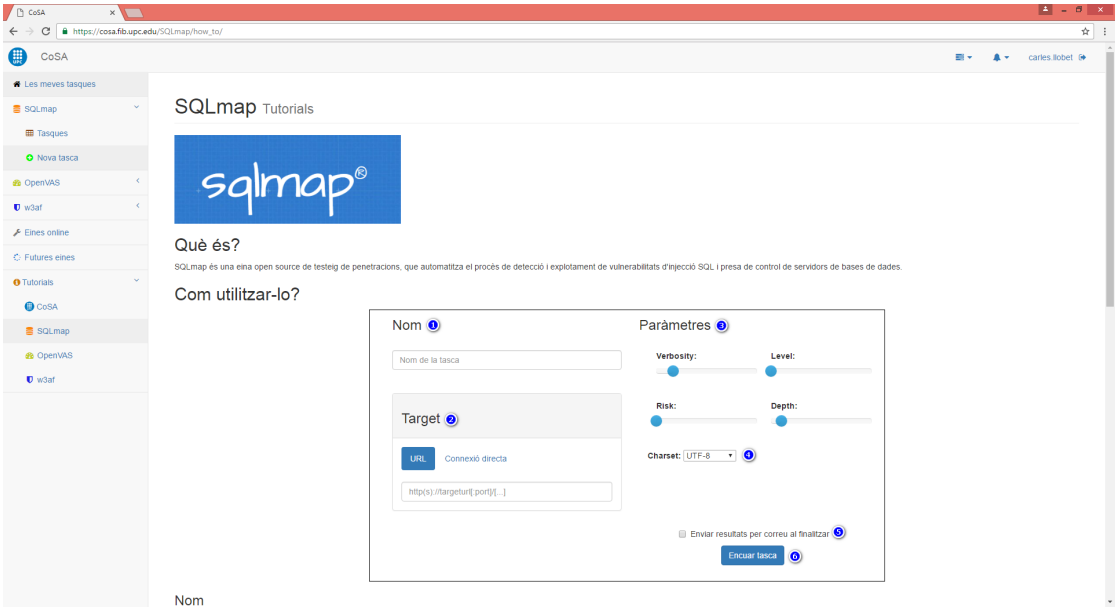

Figura 11: Tutorial de l'eina SQLmap

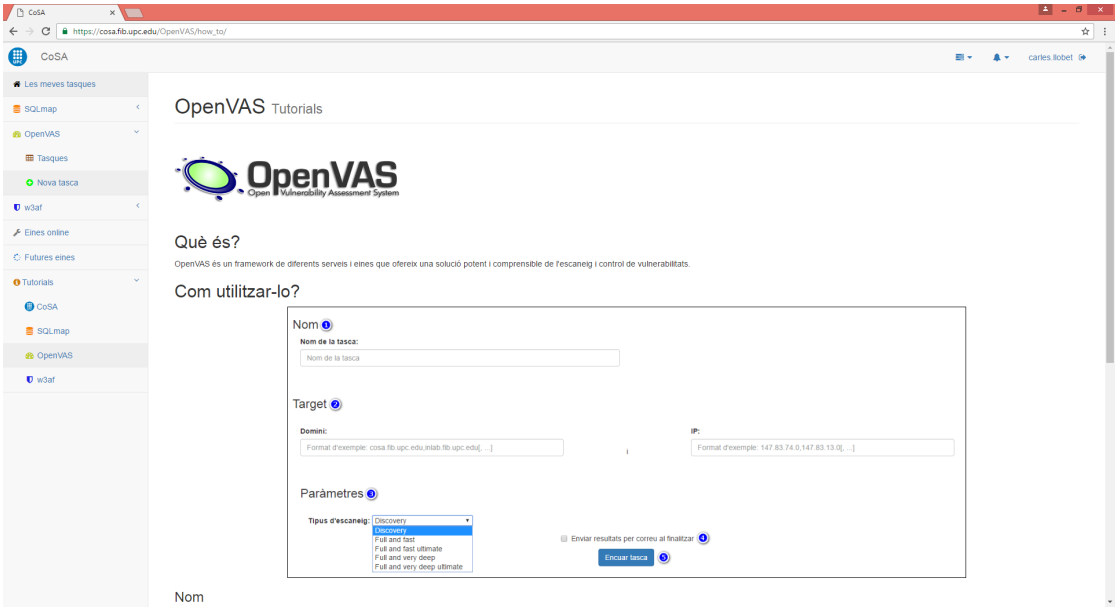

Figura 12: Tutorial de l'eina OpenVAS

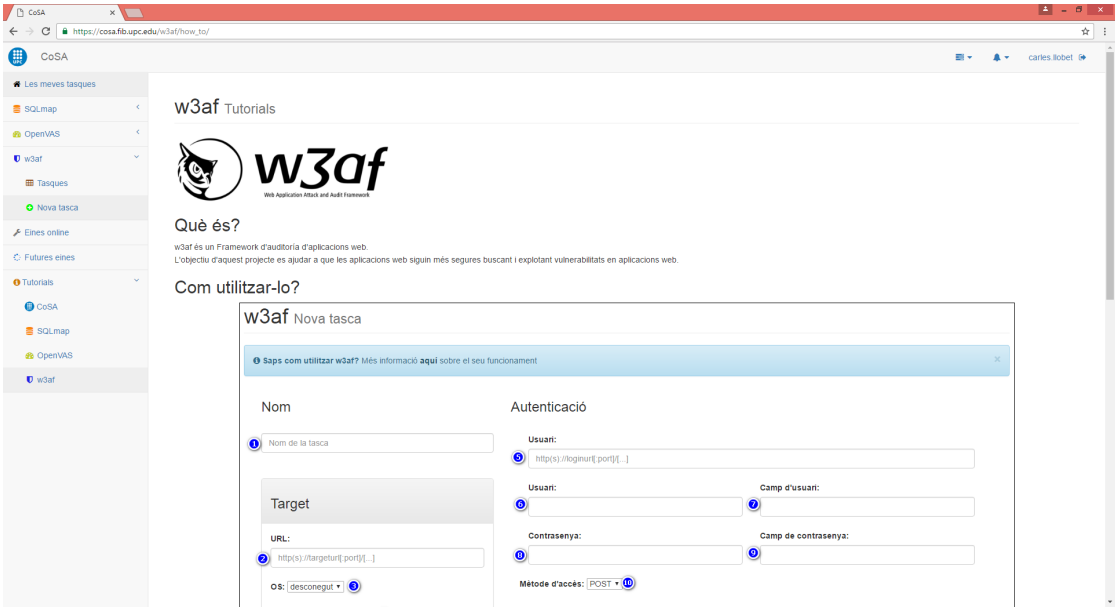

Figura 13: Tutorial de l'eina w3af

2.2 Implementació

En aquesta secció es detallarà la implementació de la plataforma en la mesura del possible donades les restriccions de l'empresa on s'ha realitzat. El codi i certes parts de l'estructura es mantindran ofuscades per mantenir la privacitat de inLabFIB-esCERT.

2.2.1 Backend: Aplicació web

L'aplicació web ha estat programada en Django, un framework de Python que s'encarrega de la gestió de les peticions als diferents enllaços i les vistes que els corresponen.
A més, s'encarrega també de la creació i gestió de la Base de Dades per tal d'afegir seguretat entre els formularis de generació de tasques i la inserció de les dades. Django afegeix diversos validadors propis dels tipus de dades a inserir, proporcionant seguretat a la plataforma amb aquests validadors i altres elements com tokens per a l'evasió d'atacs CSRF (Cross Site Request Forgery).

A l'aplicació podem trobar dos moduls principals (anomenats aplicacions a Django).
Un d'ells s'anomena igual que el projecte a l'empresa, ÇoSA", encarregat de les configuracions de la plataforma i la gestió de directoris com el de arxius estàtics (javascripts i css), o el de media (imatges i pujades d'arxius); i les configuracions pròpies de la base de dades i altres moduls a importar (com el CAS de la FIB per gestionar l'inici de sessió i l'autenticació).

El segon, anomenat Índex", s'encarrega de la resolució de totes les parts comunes de l'aplicació, tal com la pantalla inicial de vista de totes les tasques de l'usuari en general. Aquest mateix modul crea el context d'usuari que anomenem internament Çontext base", que servirà a tota la plataforma per a mantenir control de les dades generals com les de l'usuari o la informació bàsica de totes les tasques que conté.
Finalment aquest s'encarregarà també de servir les vistes comunes com les futures eines o les eines disponibles online.

A part d'aquests dos mòduls generals cada eina estarà composta per les seves vistes i enllaços a aquestes, que contenen la vista de la llista de tasques de la pròpia eina amb tota la informació d'aquesta, i el formulari de generació d'una tasca nova.

2.2.2 Backend: Scripts i sistema de cues

A dins del backend podem trobar també tota la gestió interna del servidor.
Aquesta part de la plataforma és molt més pròpia i independent de cada eina, depenent de la seva metodologia de funcionament, però podem trobar certs punts en comú. Exposarem aquells en comú de cada eina implementada, i a continuació els trets característics de cada eina. **Trets comuns**

Cada eina tindrà un script lligat a un cron al servidor que l'executarà cada minut. Aquest s'encarregarà de demanar a través de la API (2.2.3) de la plataforma si hi ha una tasca nova a executar. En cas d'existir una tasca d'aquella eina per executar, la API retornarà la tasca més antiga en ordre d'inserció, i els paràmetres necessaris per a executar aquella eina.
Un cop l'script ja té totes les dades, executarà la eina de manera específica a l'eina (podrem trobar les maneres d'execució pròpies de cada eina al següent apartat), i recollirà els resultats els quals enviarà de nou a través de la API a la plataforma, que els emmagatzemarà a la base de dades, ja sigui la referència a un fitxer de resultats o el propi resultat en el format que escaigui.
Cada eina tindrà un paràmetre a dalt de tot que permetrà modificar el nombre de tasques paral · leles o simultànies que es podran executar al servidor per cada eina, depenent de les característiques del servidor on es desplega la plataforma.

Trets específics Cada eina té les seves pròpies característiques sobretot a l'hora d'executar la tasca sol · licitada. A continuació s'exposen els trets característics propis de cada eina:

- **OpenVAS**
  OpenVAS es tracta d'una eina amb un sistema de cues propi, asíncrona, pel que el sistema de cues propi de la plataforma serà un segon nivell de cues per sobre del seu. Primer de tot es comprova si hi ha cap tasca en execució, i en aquest cas es comprova el seu estat. Si esta executant-se, es demana a través d'omp el progrés de la tasca, s'actualitza a través de la api, i finalment es comprova si l'usuari ha demanat aturar la tasca per tal de bloquejar-la i eliminar-la. Si pel contrari està finalitzada, es marca com a finalitzada a través de la API (fixar-se que els resultats no s'envien enlloc i es guarden a OpenVAS, i després al sol · licitar l'usuari els resultats es demanen al moment a OpenVAS, a diferència de les altres dues). Un cop es comprova que el servidor no està executant més tasques d'OpenVAS de les permeses, demana a la API la següent (si existeix), i prepara la tasca a executar. A OpenVAS les tasques a executar es preparen a través de la interfície d'OMP a través de certs passos:

  1. Es crea el target demanat si no existia encara
  2. Es selecciona la configuració d'escaneig escollida
  3. Es crea la tasca en si enllaçant-la al target i a la configuració
  4. S'executa la tasca

  Finalment té un script de neteja que s'executa també a través del cron que va netejant les tasques que els usuaris han demanat de cancel · lar de OpenVAS, i els targets antics.

- **SQLmap**
  SQLmap és una eina síncrona, pel que les execucions d'aquest script duren tant com l'escaneig SQLmap. Aquest fet s'ha de tenir en compte a l'hora de programar el màxim de tasques paral · leles a permetre.

  L'script comprova inicialment que no hi hagi més tasques de les permeses executant, i crida a l'api en busca dels paràmetres de la nova tasca a executar.
  Es crea un fitxer temporal amb la informació de la tasca a executar per a després poder saber quines s'estan executant, i es crida a SQLmap amb els paràmetres adient en background, quedant-nos amb el PID. L'script es queda esperant a que el procès de acabi, i de mentres va consultant la API per si el usuari vol cancel · lar la tasca, cas en que mataria el procès i esborraria els resultats.

  Un cop la tasca ha finalitzat, es passen els resultats en text per un parser i s'extreuen els resultats en html. Finalment ambdós s'envien a la API per emmagatzemar a la Base de Dades.

- **w3af**
  w3af, de la mateixa manera que SQLmap, és una eina síncrona. Per tant, de la mateixa manera que SQLmap, l'eina mira les tasques que hi ha en execució, demana una nova si escau, i executa l'w3af, esperant-se a que l'usuari cancel · li la tasca o aquesta finalitzi, per tal d'enviar els resultats en html a través de la API a la Base de Dades, amb la petita diferència que no necessita un parser específic ja que l'eina té l'opció de retornar els resultats en HTML directament.

  La diferència principal radica en la manera de cridar a l'eina.
  w3af és una eina interactiva, pel que tota la configuració es fa navegant per consola a través d'un menú, i posteriorment s'engega la tasca. Donada aquesta característica, des de l'script s'escriu un fitxer (que a la vegada ens serveix per a la identificació de les dades de la tasca en execució) amb les ordres necessàries per a la configuració de l'eina en base als paràmetres, i posteriorment s'executa l'eina amb aquest fitxer.

2.2.3 API

Com s'ha vist a l'anterior secció la API és l'encarregada de gestionar la comunicació entre totes les eines i la base de dades, per tal de servir totes les tasques encuades a aquestes, i guardar-ne els resultats. Cada eina te funcions per:

- Demanar la pròxima tasca
- Enviar el resultat en els formats pertinents
- Modificar i consultar l'estat de la tasca en execució
- Marcar la tasca com a cancel · lada per a la seva aturada i eliminació

I en concret OpenVAS té una funció que li permet modificar el percentatge de progrés en el que es troba, el qual s'actualitza cada minut quan l'script l'actualitza.

Validació

3.1 Funcionament

Amb l'objectiu de validar el bon funcionament de la plataforma, s'han dut a terme les diferents proves en diferents navegadors per tal de comprovar els següents criteris:

- **Fiabilitat**
  El funcionament correcte en un període de temps arbitrari.
- **Repetibilitat**
  Que la repetició de les mateixes proves sempre donen els mateixos resultats.
- **Reproductibilitat**
  Les mateixes proves en diferents condicions (navegador, sistema operatiu, programari, etc.) donen els mateixos resultats.

Les proves inclouran l'execució d'un seguit de tasques de les 3 eines implementades, comprovant que actuïn com toquen tant si la cua es troba plena o encara té espai per a més tasques, com si altres tasques d'altres usuaris s'estan corrent a la vegada per comprovar el funcionament de les cues amb diversos usuaris simultanis.

A més s'ha fet una prova de càrrega al sistema executant el màxim possible de tasques de cada eina per comprovar la seva fiabilitat en el màxim estrès possible.

3.2 Seguretat

Les proves mencionades a l'apartat anterior assumeixen un ús correcte i no fraudulent de l'aplicació web. Tot i així, la seguretat és un factor important a tenir en compte, pel que s'han tingut en compte els tipus d'atac informàtics més comuns a aplicacions web, i s'exposen a continuació:

- **Injeccions SQL**
  Les injeccions SQL són un atac en el qual s'insereixen sentències SQL malicioses als formularis o buscadors per tal que el servidor les executi i retorni o modifiqui la informació de la base de dades al gust de l'atacant. Com Django gestiona tota la base de dades utilitzada i els formularis corresponents, la plataforma no és vulnerable a aquest tipus d'atacs.

- **XSS**
  XSS o Cross-Site Scripting és una de les vulnerabilitats més comunes a les aplicacions web que utilitzen Javascript. Consisteix en inserir codi Javascript maliciós a formularis o buscadors per tal d'executar codi al servidor remot, o fer *defacing* de la plataforma. Com Django gestiona tots els formularis amb els seus pròpis validadors a més dels afegits per nosaltres, la plataforma no és vulnerable a aquest tipus d'atacs.

- **CSRF**
  CSRF o Cross-Site Request Forgery és un tipus d'exploit maliciós en el qual un atacant realitza accions amb un usuari que no li pertany, e inclús pot aconseguir realitzar accions a les que no estava autoritzat si l'usuari que aconsegueix té permisos de gestió o administració. Per a evitar atacs d'aquest tipus Django proporciona un *token* anomenat çsrf_token"que és necessari per realitzar peticions al servidor i només es pot aconseguir un cop es validen les credencials d'usuari. Com aquest *token* s'ha utilitzat, la plataforma tampoc és vulnerable a aquest tipus d'atacs.

3.3 Usabilitat

Donat que no ha estat possible l'estudi d'usabilitat amb els diferents usuaris implicats que requeriria, el desenvolupament s'ha desenvolupat sota una sèrie de criteris per garantir la bona usabilitat i experiència de l'usuari. A més, sempre s'han seguit les recomanacions i *feedback* proporcionat pel departament d'AC. Els criteris escollits s'exposen a continuació:

- Disseny responsiu per a tabletes o dispositius mòbils
- Disseny estètic o minimalista
- Mides de botons i texts adequat
- Colors diferents en funció del significat, i intuïtius
- Estructura intuïtiva de les diferents seccions
- Proporcionar a l'usuari les dades que més poden interessar-li en primer pla
- Assolir un temps de càrrega de la plataforma web prou ràpid
- Comprovació d'errors i de les dades introduïdes per l'usuari
- Avisos i explicacions de tots els possibles mals usos donats
- Evitar l'ús de banners dinàmics
- Evitar la sobrecàrrega visual de les diferents seccions

Planificació del projecte

4.1 Planificació del projecte

Aquesta és la planificació final del projecte, que s'ha dut a terme durant el projecte, just abans de GEP[1]. Gràcies a la metodologia àgil, només han sorgit desviacions **justificades** des del plantejament inicial.

4.1.1 Programa

La duració del projecte ha sigut d'un any aproximadament, des de Maig de 2016 on es comença a planificar, fins juny de 2017 on s'ha acabat de documentar. Les festivitats locals i nadal han estat contemplats. Utilitzant les metodologies àgils ha sigut possible el compliment del plaç inicial d'un any.

4.1.2 Pla

Les següents tasques han sigut realitzades per considerar el projecte com a finalitzat. Totes les tasques segueixen una dependència linear, així que han sigut completades en el mateix ordre. Podem dividir-les en 3 grans fases ben diferenciades, que plantegem a continuació.

[1] "Gestió de Projectes" assignatura de documentació per al Treball de Fi de Grau.

1. Planificació temporal inicial del projecte

Aquesta fase inclou el desenvolupament de tots els requisits de l'assignatura de GEP, requisits comuns per a la bona iniciació de qualsevol projecte, incloent les següents tasques:

- **Abast i context del projecte**:
  Descripció: L'objectiu es el plantejament i redacció de la contextualització del coneixement de l'àrea de treball a la que pertany el projecte. Per començar, s'ha de cercar tota la informació possible del camp, que a l'hora serà un bon filtre inicial per a trobar bones fonts d'informació. En segon lloc, un cop compresa tota la informació cercada, s'ha de descriure l'estat de l'art i el context del camp de treball. Finalment, s'han d'aclarir l'abast del projecte, objectius, i metodologies utilitzades per al desenvolupament.

  Recursos: Ordinador, accés a internet i a articles acadèmics, TeXstudio i LaTeX.

  Duració: 60 hores.

- **Planificació temporal**.
  Descripció: L'objectiu d'aquesta tasca es definir les tasques a realitzar per aconseguir l'objectiu del projecte, i la duració estimada d'aquestes. També defineix els recursos, la viabilitat, i alternatives.

  Recursos: Ordinador, Trello, TeXstudio i LaTeX.

  Duració: 80 hores.

- **Pressupost i recursos**.
  Descripció: Per a poder estimar el cost dels recursos utilitzats, aquest document ha de reflectir quins recursos humans i econòmics s'hauran d'utilitzar. La sostenibilitat del projecte serà avaluada juntament amb la viabilitat econòmica.

  Recursos: Ordinador, TeXstudio i LaTeX.

  Duració: 16 hores.

2. Desenvolupament del projecte

En aquesta fase, ja s'han definit la planificació i el pla d'acció, i la viabilitat del projecte en termes econòmics i temporals ha estat comprovada. El dividim en les següents tasques:

- **Preparació de l'entorn**.
  Descripció: Per a desenvolupar la plataforma web correctament, necessitarem instal · lar i configurar software i frameworks diversos.

  Duració: 40 hores.

- **Adquirir coneixement de Django**.
  Descripció: Tot el backend del portal web i la API que cridaran els diversos scripts del servidor estara desenvolupat en Django, un framework de Python molt potent. En aquesta tasca s'haura d'assolir un bon nivell sobre aquest llenguatge.

  Duració: 32 hores.

- **Plataforma web**.
  Descripció: Frontend i Backend del portal web. Consta de les vistes que els usuaris finals veuran es dissenyaran i implementaran, i de la programació de tot el comportament intern de la plataforma web, el *core* o nucli de la plataforma.

  Duració: 320 hores.

- **Backend: Scripts i Servidor**.
  Descripció: Cada eina requerira d'un o més scripts en constant execució per al control de la cua de tasques de cada eina, i l'execució de l'eina amb els paràmetres seleccionats. Els resultats s'han d'enviar per API al nucli de la plataforma per a la visualització.

  Duració: 100 hores.

- **Revisions i proves**.
  Descripció: Un cop funcional, s'ha de testejar tota la plataforma i comprovar tots els casos d'ús en busca de falles o manques de funcionalitat, a més de valorar si el resultat és el desitjat i possibles millores.

  Duració: 40 hores.

- **Desplegament al servidor definitiu**.
  Descripció: Un cop validada i donada per bona, s'ha de desplegar l'eina al servidor de producció i donar accés ja al public final.

  Duració: 20 hores.

Recursos generals: 1 ordinador, Django, 1 servidor de desplegament, 1 repositori de codi intern, 1 base de dades per als usuaris i peticions, i connexió a internet per a consultes.

3. Documentació del projecte

Un cop la plataforma hagi estat desenvolupada, s'ha de generar tota la documentació, i generar la presentació que s'utilitzarà per a la defensa del TFG davant del tribunal d'avaluació. Ho podem dividir en dues fases:

- **Documentació de desplegament**.
  Descripció: S'ha de deixar preparada la documentació de desplegament de l'eina, amb tot el procès de preparació d'un servidor recent instal · lat fins a un servidor que serveixi la plataforma.

  Recursos: Ordinador i Servidor intern amb Redmine.

  Duració: 80 hores.

- **Memòria i presentació del projecte**.
  Descripció: Finalment s'ha de documentar el projecte sencer, des d'aquesta pròpia memòria fins a la presentació que s'utilitzara per a defensar el TFG davant del tribunal d'avaluació.

  Recursos: Ordinador, TeXstudio i LaTeX.

  Duració: 160 hores.

4.1.3 Temps estimat dedicat

Fase	**Hores**
Planificació del projecte	156
Desenvolupament del projecte	552
Documentació del projecte	240
Total	**948**

Taula 2: Relacions de temps estimat per fases

4.1.4 Pla d'acció

Un cop obtinguda la planificació de les tasques com a guia a seguir, hi han activitats que s'han estès més del planificat, i altres menys. Aquest fet s'ha anat corregint a les reunions setmanals de seguiment.

La carrega de treball setmanal d'aquest TFG ha implicat aproximadament 20 hores setmanals.

Recursos

Com s'ha mencionat a la secció anterior, s'han utilitzat els següents recursos durant el projecte:

- 1 ordinador amb sistema operatiu Windows
- 1 Redmine intern per a la documentació de desplegament
- 1 Repositori de codi intern GitLab
- 1 servidor Linux per a la execució de la plataforma en producció
- 1 base de dades per als usuaris i les cues de peticions
- Software divers: Django, Python, TexStudio, etc.

Viabilitat

Com es pot veure en aquest document, aquest TFG ha sigut assequible en el temps proposat al programa.

Distribució temporal

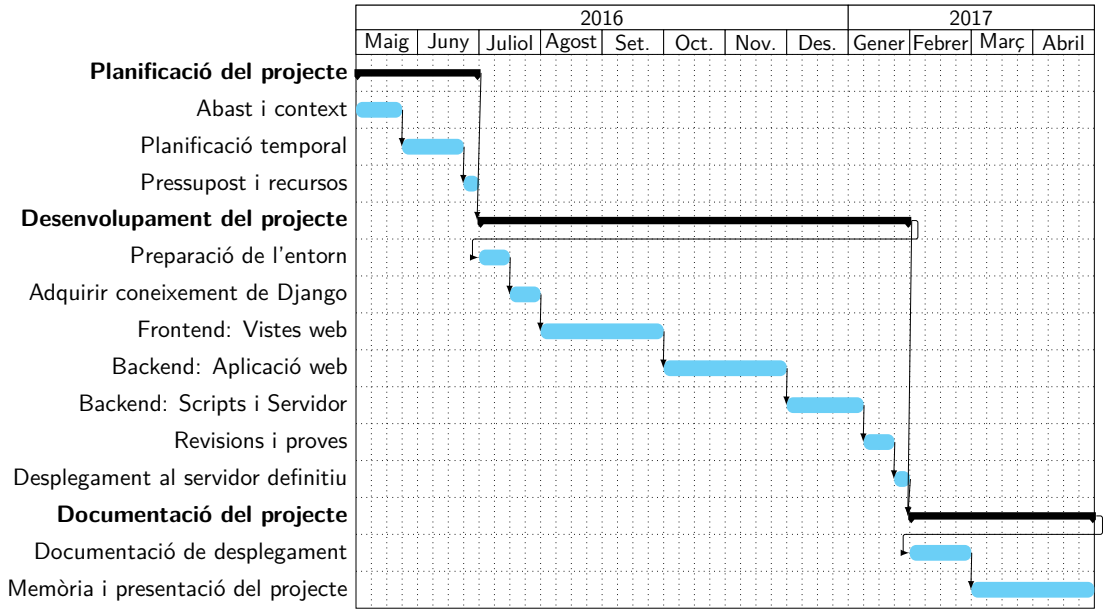

Figura 14: Diagrama de Gantt

4.2 Pressupost

Com s'ha vist a les seccions prèvies, per poder assolir l'objectiu d'aquest projecte són necessaris una sèrie de recursos. Aquests poden ser dividits en 4 grans grups: Recursos humans, recursos hardware, recursos software, i altres recursos.

Per a enllaçar correctament els recursos i les tasques definides prèviament, els hi assignarem els següents codis:

Tasca	Codi
Planificació temporal del projecte	**P**
Abast i context del projecte	P1
Planificació temporal	P2
Pressupost i recursos	P3
Desenvolupament del projecte	**D**
Preparació de l'entorn	D1
Adquirir coneixement de Django	D2
Plataforma web	D3
Backend: Scripts i Servidor	D4
Revisions i proves	D5
Desplegament al servidor definitiu	D6
Documentació del projecte	**F**
Documentació de desplegament	F1
Memòria i presentació del projecte	F2

Taula 3: Codificació de les tasques

4.2.1 Recursos humans

Com aquest projecte es desenvolupara únicament per un equip format per l'estudiant i el director del projecte dins l'empresa, aquests tindran els rols de Software Developer (Desenvolupador del codi) i de Project Manager (Cap de projecte) respectivament.

Conceptee	**Tasca**	**Hores**	**Preu/Hora**	**Total**
Project Manager	P	55 h	51 €/h	2.805,00 €
Software Developer	D,F	665 h	7.5 €/h	4.987,50 €
Total				7.792,50 €

Taula 4: Pressupost de recursos humans

4.2.2 Recursos Hardware

Durant el desenvolupament del TFG s'utilitzara hardware. A la Taula 5 trobem una llista de quin hardware serà necessari, amb la seva amortització tenint en compte el seu Temps de vida útil i l'ús que li donarem durant el desenvolupament (12 mesos).

Concepte	**Tasca**	**Preu**	**Temps de vida útil**	**Total**
Ordinador sobretaula	P,D,F	830,00 €	4 years	207,50 €
Servidor amb AMD Quad Core Opteron	D	2.700,00 €	4 years	675,00 €
Portàtil MSI CX62 6QD	P,F,D	749,00 €	4 years	187,25 €
Total				1.069,75 €

Taula 5: Pressupost de recursos Hardware

4.2.3 Recursos Software

Molts dels productes software que s'utilitzaran per al desenvolupament d'aquest projecte son *open-source* (software lliure), tot i que alguns implicaran costos de llicencia. A la Taula 6 en podem veure els costs.

Concepte	**Tasca**	**Preu**	**Temps de vida útil**	**Total**
Django 1.10	D2,D3	N/A	N/A	0,00 €
Python 2.7.13	D1,D2,D3,D4	N/A	N/A	0,00 €
PyCharm Pro	D2,D3,D4	N/A	N/A	0,00 € (UPC)
MiKTeX 2.9	P,F2	N/A	N/A	0,00 €
TeXstudio 2.12	P,F2	N/A	N/A	0,00 €
Redmine	F1	N/A	N/A	0,00 €
GitLab	D2,D3,D4,D6	N/A	N/A	0,00 €
Sublime Text 3	D4	N/A	N/A	0,00 €
OpenSUSE 12.2	D6	N/A	N/A	0,00 €
Windows 10 Professional	P,D,F	279,00 €	Vitalici	279,00 €
Total				279,00 €

Taula 6: Pressupost de recursos Software

4.2.4 Altres Recursos

S'hauran de comprar altres llicències i recursos per al desenvolupament d'aquest projecte. A part, també s'han d'assumir alguns costs indirectes al projecte. Tots aquests els podem veure detallats a la Taula 7.

Concepte	**Tasca**	**Preu**	**Temps de vida útil**	**Total**
Energia	P,D,F	300,00 €/any	N/A	300,00 €
Total				300,00 €

Taula 7: Pressupost d'altres recursos

4.2.5 Monitoratge dels Recursos

Com el projecte utilitzarà metodologies àgils per al desenvolupament, les possibles desviacions que poden sorgir es detectaran i corregiran més ràpidament A cada reunió de progrès del projecte s'actualitzaran, i s'avaluaran els possibles obstacles que poden aparèixer

Així que com a bon monitor de recursos humans, el desenvolupament del TFG ha de seguir el diagrama de Gantt prèviament definit. Això pot ajudar a detectar desviacions a les tasques dels recursos humans.

4.2.6 Cost total

Per poder estimar el cost total del projecte, s'han de sumar tots els pressuposts anteriors, com podem veure a la Taula 6.

Concepte	**Cost**
Recursos humans	7.792,50 €
Recursos Hardware	1.069,75 €
Recursos Software	279,00 €
Altres recursos	300,00 €
Possibles Desviacions (30h)	1.530,00 €
Total	10.971,25 €

Taula 8: Pressupost total

4.3 Sostenibilitat

4.3.1 Econòmica

Tenint en compte la secció anterior, tots els recursos humans i materials han estat estimats. Es important remarcar l'ús de una gran majoria de software lliure (open-source). A més, la UPC té llicències d'ús de moltes de les eines necessàries que necessitarem, pel que es viable i competitiu en termes econòmics.

La duració de cada tasca ha sigut estimada i ajustada en relació a la seva importància. Com s'ha manifestat al context del projecte, no hi ha cap solució funcional similar, pel que no es pot reutilitzar cap tecnologia ja existent que unifiqui eines de seguretat informàtica per a millorar-la. Com aquest TFG es un projecte desenvolupat per a inLabFIB - esCERT, la data límit serà estimada per ells.

A més, auqest TFG pot tenir un impacte a l'economia dels departaments de la UPC: Poden estalviar costs en auditories de seguretat fent un bon ús d'aquesta eina.

Finalment, hi ha una desviació de un 36% d'hores més dedicades al desenvolupament del projecte. També es tradueix a un increment del cost final. Aquesta desviació ha sigut causada per la incorporació d'una nova eina (w3af) que no es contemplava inicialment, però que ha acabat de fer la plataforma una eina completa per a l'auditoria automatitzada de qualsevol de les possibles necessitats d'un departament de la UPC.

4.3.2 Social

Aquest projecte ha estat desenvolupat com a part del sector de Enginyeria informàtica i Ciberseguretat de Catalunya, enfocada a un abast d'ús empresarial. Serà una eina per a l'auditoria de sistemes i solucions informàtiques de enginyers de tecnologies de la informació, que els permetrà mantenir un nivell de seguretat molt més acurat a tots els seus sistemes i serveis.

Com hem vist a la secció **Formulació del problema** hi ha una clara necessitat no només a nivell departamental dins la UPC sinó globalment d'una eina que permeti una gestió mínima automatitzada de la seguretat dels sistemes i serveis tecnològics que es poden oferir a una empresa a causa de la manca i cost de les auditories de seguretat de tots els tipus de servei. Al oferir aquesta automatització, la carrega de treball dels auditors de seguretat pot centrar-se molt més en punts específics i complexos de seguretat informàtica, i els sistemes i serveis que s'ofereixen poden garantir un mínim de seguretat periòdic amb molta més freqüència.

L'impacte directe d'aquest TFG serà delimitat per l'ús que li doni inLabFIB. Inicialment està enfocat únicament pels departaments de la UPC que auditaven fins al 2017 inLabFIB -

esCERT, però s'espera que a llarg plaç l'eina tingui un impacte molt major, distribuint-se a tots els demes departaments de la UPC, i inclús fins a entorns empresarials externs i aliens a la UPC. A més d'això, el desenvolupament d'aquest projecte no perjudicarà directa ni indirectament a cap col · lectiu

4.3.3 Ambiental

Considerant que a un projecte d'Informàtica hi haurà emissions de CO2 segures, el nostre principal objectiu serà reduir-les al mínim. Així doncs, assumirem que un ordinador de sobretaula consumeix uns 250 watts, i un portàtil personal uns 140 watts. El ordinador de sobretaula s'utilitzara un 80% del temps, i el portàtil el 20% restant. Tenint en compte aquests valors, l'energia consumida duran el temps estimat a la secció anterior, l'energia total consumida serà d'uns 123KW, així que l'impacte ecològic serà de 47.355 kg of CO2. Tota la informació i documentació necessària seran llegides digitalment, i no impreses.

El software desenvolupat en aquest TFG tindrà propietat intel · lectual de la UPC pel que no es podrà comercialitzar, però serà d'ús lliure per a la comunitat.

4.3.4 Matriu de sostenibilitat

La següent taula avalua la sostenibilitat de les tres àrees avaluades.

	Econòmic	**Social**	**Ambiental**	Total
Planificació	Viabilitat econòmica	Millora de la qualitat de vida	Anàlisi de recursos	27
Avaluació	10 (0:10)	10 (0:10)	7 (0:10)	(0:30)
Resultats	Cost final vs. Previsió	Impacte social	Consum de recursos	14
Avaluació	4 (-10:10)	7(-10:10)	3 (-10:10)	(-30:30)
Riscs	Adaptació a canvi d'escenaris	Social harm	Impacte mediambiental	-10
Avaluació	0 (-20:0)	0 (-20:0)	-10 (-20:0)	(-60:0)
Total	14 (-30:20)	17 (-30:20)	0 (-30:20)	**31** (-90:60)

Taula 9: Matriu de sostenibilitat

Obstacles trobats

Durant la realització del projecte han anat apareixent diversos obstacles i desviacions que han afectat en major o menor mesura alguns dels aspectes del planificació del projecte (capítol 4.1).
A continuació destacarem aquells més importants i que han tingut major impacte a la planificació inicial:

- **Canvi de servidor de l'inicial a UPCnet a un servidor propi de l'inLab**
  Per motius interns entre inLab i UPCnet, un cop es va fer la primera entrega del projecte per a rebre feedback i poder fer correccions, el projecte va haver de migrar-se des del servidor on estava a un servidor intern d'inLab. Aquesta migració va ser un gran obstacle degut a que OpenVAS 8 encara no està ben suportat a totes les distribucions de Linux, i es va haver d'adaptar el projecte per passar d'OpenSUSE a Ubuntu 14.
  Tot i això, es va poder aprofitar l'obstacle i millorar la plataforma, ja que es va passar de OpenVAS 7 al 8, una gran actualització que comporta millores com un nou paràmetre (QoD, *Quality of Detection*) que dóna informació sobre la fiabilitat de detecció de cadascuna de les vulnerabilitats trobades.

- **Adició d'una nova eina no prevista**
  El projecte es va planificar per treballar inicialment dues eines, SQLmap i OpenVAS. Un cop aquestes estaven funcionals, i s'estava treballant amb els aspectes de disseny i visuals, vam descobrir que w3af comptava amb una api per a treballar des de consola, i no només des d'interfície gràfica. Arrel d'això es va decidir en una de les contínues reunions de seguiment la implementació d'aquesta per incloure-la al projecte. Es va poder incloure segons els temps previstos gràcies a les metodologies àgils emprades. Tot i així, aquesta nova incorporació va implicar un petit canvi de l'estructura interna del sistema de cues per poder treballar amb ella, que no estava planificat, millorant la modularitat i escalabilitat del sistema en conjunt.

- **Autenticació bàsica a w3af**
  Un cop entregada l'eina a inLab i en la fase de documentació de la plataforma, sorgeix la necessitat d'implementar la gestió d'autenticació HTTP bàsica amb w3af, pel que es reobre el projecte a *pre* i es torna a fer tot el desplegament al servidor de *pro*.

Futures millores

Donada l'escalabilitat i modularitat del projecte, durant tot el desenvolupament i la documentació, han aparegut constantment idees de possibles millores de la plataforma.
A continuació s'exposen aquelles més viables i que es preveuen poder desenvolupar durant el pròxim any:

- **Millora del seguiment del progrés de les tasques**
  A la plataforma es permet veure el progrés d'una tasca, però així com d'OpenVAS es pot demanar a través de consultes a la seva API interna i actualitzar cada minut de manera còmoda, a SQLmap i w3af de moment només es veu l'estat de la tasca. Una futura millora podria incloure la interpretació del punt on es troba l'eina escanejant per poder brindar més informació sobre l'estat de la tasca a l'usuari.

- **Parser SQLmap funcional**
  Durant el projecte es va implementar un *parser* de la sortida de l'eina SQLmap per a mostrarla en un HTML més llegible i fàcil de veure per a l'usuari, similar a la sortida de w3af que ja implementa la possibilitat de veure la sortida en HTML.
  No s'ha utilitzat finalment donat que s'havia de millorar el filtre de etiquetes que agafava només la informació que ens convenia, però en un futur es podria decidir que es vol filtrar i utilitzar-lo.

- **Ampliació del ventall d'eines**
  Hi ha diverses eines que s'han trobat candidates vàlides per a suportar-se dins de la plataforma, tenint en compte el servei que proporciona cadascuna d'elles i si compleix els requeriments necessaris per a incloure's al sistema, com tenir interfície a través de consola per poder automatitzar el procès i incloure-la als scripts del sistema de cues.
  Les podem trobar detallades a la secció de *Futures eines* dins de la pròpia plataforma, i són les següents: wFuzz, BeEF, i FOCA.

Conclusions

Els objectius principals d'aquest projecte eren el desenvolupament i desplegament d'una nova plataforma que millorés el sistema d'auditories que s'utilitzava als departaments de la UPC anteriorment, per tal de garantir seguretat i integritat constant dels sistemes d'aquests entre auditories, i ambdós s'han pogut realitzar.

Durant el desenvolupament d'aquest projecte, les metodologies àgils utilitzades han sigut de gran ajuda a l'hora de mantenir els objectius clars quan sorgien desviacions, facilitant la seva resolució. Aquestes desviacions (detallades al capítol 5), han fet que el projecte es veies afectat sobretot en el planeig temporal (detallat a la secció 4.1). Aquestes afectacions, però, s'han vist compensades amb la bona gestió d'altres parts del projecte que s'han vist completades en menys temps del planejat. Això és conseqüència directa de la bona gestió setmanal i reunions constants per decidir instantàniament com gestionar les desviacions que apareixien, per tal de minimitzar el temps afectat. Per tant, la metodologia que s'ha seguit ha estat la correcta.

Per concloure, com explicat al capítol 6 (Futures millores), aquesta eina té un potencial molt gran degut a la seva gran escalabilitat, donada per la seva estructura modular. Els resultats d'aquesta primera versió de la plataforma són els esperats, però un cop arribats a aquest punt, es pot observar tot un nou camí de possibilitats cap a la plataforma, que poden incrementar la seva potència i autonomia.

Bibliografia

[1] Openvas. URL http://openvas.org/software.html.

[2] Sqlmap. URL http://sqlmap.org/.

[3] w3af. URL http://w3af.org/.

[4] R. A. Española. Diccionario de la lengua española, 2014. URL http://dle.rae.es/?id=4NVvRTc.

[5] FIB. Departaments fib. URL www.fib.upc.edu/fib/centre/departaments.html.

[6] J.-P. Lang. Redmine oficial website. URL https://www.redmine.org.

[7] OWASP. Eines d'escaneig de vulnerabilitats. URL https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools.

[8] Wikipedia. Scrum. URL https://ca.wikipedia.org/wiki/Scrum.