



Demo Corporation

Auditoria de seguretat externa

Informe demostratiu

Versió del document: v1

Autor: Ferran Verdés

Data: Gener 12, 2021

Índex de Contingut

1	<i>Introducció.....</i>	<i>4</i>
1.1	Conceptes preliminars.....	4
1.2	Fonaments i aspectes a considerar	4
1.3	Objectius establerts	5
1.4	Marc i limitacions.....	5
1.5	Procediments dels serveis de seguretat	5
1.5.1	Recopilació d'informació.....	6
1.5.2	Identificació de vulnerabilitats.....	6
1.5.3	Explotació i comprovació de les vulnerabilitats.....	7
1.5.4	Establiment d'accés permanent.....	7
1.5.5	Anàlisi de les dades obtingudes i redacció de l'informe	8
1.6	Criteri de classificació de vulnerabilitats	8
2	<i>Resum dels riscos detectats</i>	<i>10</i>
2.1	Actius analitzats.....	10
2.2	Conclusions i recomanacions	10
3	<i>Informació i desenvolupament de les debilitats identificades</i>	<i>13</i>
3.1	Resum de les incidències	13
3.2	Incidències de risc crític.....	15
3.2.1	Detecció de sistema operatiu UNIX no suportat	15
3.2.2	Detecció de versió de PHP no suportada.....	15
3.3	Incidències de risc alt	17
3.3.1	Detecció del protocol SSL en les versions 2.0 i/o 3.0.....	17
3.4	Incidències de risc mitjà	19
3.4.1	Detecció del protocol TLS en la versió 1.0	19
3.4.2	No és possible confiar amb el certificat SSL.....	19
3.4.3	Xifratges SSL dèbils suportats	20
3.4.4	Algoritmes de xifratge dèbils suportats pel protocol SSH	21
3.5	Incidències de risc baix.....	23
3.5.1	Inici de sessió sense xifratge permès a POP3	23
3.5.2	Inici de sessió sense xifratge permès a SMTP	23
3.6	Informació addicional	25
3.6.1	Fitxer robots.txt detectat al servidor web	25
4	<i>Anàlisi i investigació tècnica</i>	<i>27</i>
4.1	Accés des de xarxes d'anonimat	27
4.2	Indexació detectada al buscador Shodan	28

4.3	Reputació IP	29
4.4	Localització de metadades	30
4.5	Descobrimet de subdominis	32
4.6	Transferència de zona DNS.....	33
4.7	Recerca de correus.....	34
4.8	Configuració dèbil del servei SMTP	35
4.9	Auditoria web bàsica.....	36
4.9.1	Anàlisi del certificat SSL.....	36
4.9.2	Aplicació de força bruta	37
4.9.3	Injeccions SQL.....	40
4.9.4	Stored Cross-Site Scripting (XSS)	44

1 Introducció

Aquest document conté informació relativa a possibles vulnerabilitats i mètodes que un atacant podria emprar amb l'objectiu d'explotar en benefici propi els diferents actius analitzats durant el procés d'auditoria. Per aquest motiu, *Vulnerable* recomana amb insistència la presa de les precaucions necessàries per tal de garantir la confidencialitat sobre el contingut que aquest presenta.

1.1 Conceptes preliminars

El primer punt a tractar té relació amb la definició de dos termes que s'utilitzen amb freqüència dins del context de la seguretat de la informació. En primer lloc, cal fer referència al concepte de vulnerabilitat, el qual representa una debilitat o mancança en un sistema digital que posa en risc el mateix permetent que un atacant pugui comprometre'n la seva integritat, disponibilitat o confidencialitat. Les vulnerabilitats poden tenir diferents orígens, encara que els més habituals són els errors de disseny o de configuració i la falta de procediments estandarditzats.

Per altra banda, el segon terme és el que és coneix com a amenaça, el qual representa tota acció que aprofita una vulnerabilitat per atemptar contra la seguretat d'un sistema i generar un efecte negatiu. Les amenaces poden procedir d'atacs, ja sigui a través de *malware* o robatoris d'informació sensible, o inclús de la negligència i decisions corporatives, per exemple, degut a un mal maneig de contrasenyes o a la mala pràctica de no aplicar cap tipus de xifratge als protocols de comunicació o a les dades emmagatzemades. A més, des del punt de vista d'una organització, les amenaces poden ser tant internes, ja siguin treballadors propis de l'empresa, com externes, fent referència a internautes amb intencions malicioses.

1.2 Fonaments i aspectes a considerar

Les proves d'intrusió que realitza un analista de seguretat, també anomenades proves de *pentesting* o *hacking ètic*, són un procés incert basat en les experiències del passat, en les amenaces conegudes de l'actualitat i en els potencials atacs que poden esdevenir-se en un futur no molt llunyà. S'ha d'entendre que tots els sistemes de la informació, per la seva naturalesa, són dependents d'éssers humans, un que fet comporta a què sempre són vulnerables en cert grau i, per tant, encara que un consultor de seguretat pugui identificar la majoria de les vulnerabilitats dels sistemes que analitza, mai es garanteix que qualsevol exercici d'aquesta matèria sigui suficient per mitigar els riscos presents, així com els que seran descoberts i publicats durant els propers dies o setmanes.

D'aquesta manera, l'objectiu final que persegueix aquest document és proporcionar, de la forma més detallada possible, el conjunt de vulnerabilitats que s'han pogut identificar en el precís moment en que s'ha portat a terme l'auditoria. Tanmateix, atès que les tecnologies i els riscos canvien amb el temps, les vulnerabilitats associades amb el funcionament dels actius que es descriuen en l'informe així com les accions necessàries per reduir l'exposició a aquestes debilitats també poden canviar, la qual cosa significa que una prolongació de la seva

correcció pot esdevenir un factor clau, derivant a l'existència de la possibilitat d'obtenir efectes agreujants.

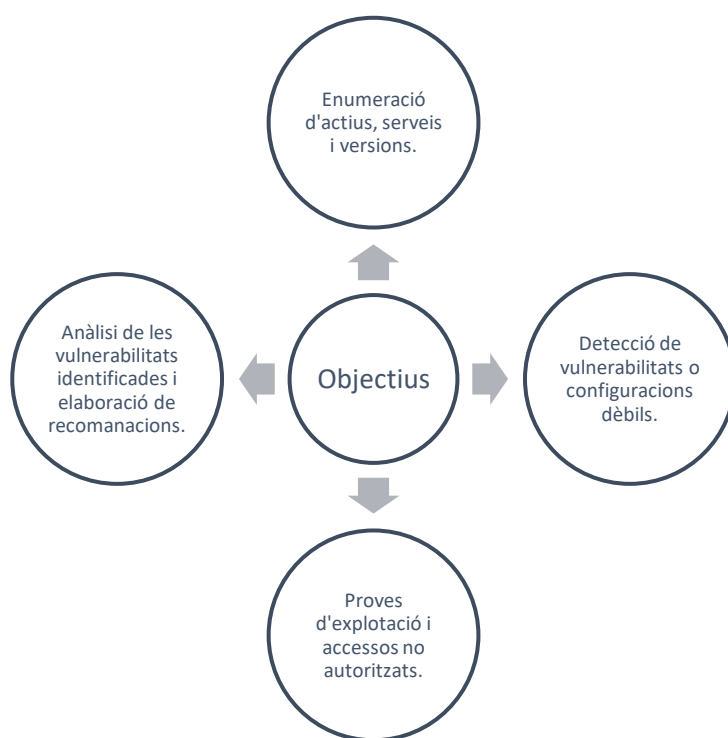
1.3 Objectius establerts

Vulnerable ha portat a terme l'exercici d'un dels serveis disponibles del centre d'operacions de seguretat del qual disposa amb la finalitat d'analitzar i obtenir informació relacionada amb la seguretat digital dels sistemes d'informació que es prenen com a actius en el present document.

L'objectiu d'aquest servei és poder facilitar a l'equip en capacitat de gestió administrativa dels sistemes mencionats l'estat de seguretat dels mateixos, tot determinant i donant a conèixer els riscos als quals poder estar exposats i també algunes de les recomanacions que poder ser d'utilitat per tal de mitigar o reduir aquestes contingències.

1.4 Marc i limitacions

D'acord amb la finalitat esmentada, s'adjunta un esquema organitzatiu encarregat de constituir els diferents enfoc de treball que són considerats en el procés d'auditoria:



Il·lustració 1 Representació gràfica dels objectius principals d'una auditoria de seguretat.

D'aquesta manera, el conjunt d'interaccions que s'ha portat a terme contra els sistemes considerats en el present exercici ha perseguit les diferents finalitats mostrades, tenint en compte tota aquella informació que s'hagi pogut donar per avançat en referència a la topologia d'auditoria portada a terme, ja sigui *Black*, *Gray* o *White Box*.

1.5 Procediments dels serveis de seguretat

Posant els objectius recentment esmentats en el punt de mira, per tal de posar en pràctica qualsevol anàlisi de seguretat dels sistemes de la informació, es consideren un total de cinc

fases, les quals han estat consensuades globalment pels professionals de l'àmbit de la seguretat informàtica:

Fases d'una auditoria de seguretat

FS1	Recopilació d'informació
FS2	Identificació de vulnerabilitats
FS3	Explotació i comprovació de les vulnerabilitats
FS4	Establiment d'accés permanent
FS5	Anàlisi de les dades obtingudes i redacció de l'informe

Taula 1 Fases d'un auditoria de seguretat.

Cada una d'aquestes fases es troba detallada en els següents subapartats.

1.5.1 Recopilació d'informació

La recopilació d'informació representa l'etapa inicial de qualsevol prova d'intrusió o *pentesting*. Es tracta de la recerca sobre la màxima quantitat de dades rellevants que els consultors de seguretat intenten recopilar sobre els diferents actius amb la finalitat d'incrementar la probabilitat d'obtenir resultats significatius i exitosos en fases posteriors. Es considera una de fases les més llargues i laborioses del cicle d'auditoria i sovint és un determinant important de l'èxit o el fracàs de la mateixa.

1.5.2 Identificació de vulnerabilitats

Seguidament, la següent etapa correspon a l'escaneig dels sistemes per tal de descobrir els diferents serveis i aplicacions en execució així com la seva versió, a la vegada que s'identifiquen configuracions febles i possibles vulnerabilitats. Cal destacar que no només es consideren els ports més freqüents, sinó que es tenen en compte els 65535 ports disponibles, tant de TCP com d'UDP.

En general, la identificació de les vulnerabilitats pot categoritzar-se en funció de la seva naturalesa i dels processos que es porten a terme per a la seva detecció. En altres paraules, existeix una diferència clara entre les debilitats relacionades amb, per exemple, la versió dels sistemes operatius o de programari respecte les aplicacions *web* o les aplicacions per dispositius mòbils. Cada un dels àmbits s'arrela als seus propis fonaments i, en conseqüència, el descobriment de les diferents vulnerabilitats associades també es porta a terme mitjançant l'ús de metodologies i eines específiques. En aquest sentit, el llistat que s'adjunta a continuació pot ser d'utilitat per tal de donar èmfasis als diferents aspectes que habitualment són considerats en una auditoria externa.

Test d'intrusió extern (simulant un potencial atacant fora de l'àmbit corporatiu)

- Descobrimet de dispositius, xarxes, serveis i protocols per a la seva posterior avaluació i investigació d'*exploits* disponibles que permetin comprometre i posar en risc la seguretat dels sistemes.

- *Search Engine Hacking* per a la identificació de dades sensibles, tals com contrasenyes, *emails (email harvesting)* o fugues d'informació, ja siguin relacionades amb dades privades i personals o bé corporatives.
- Anàlisi de la indexació dels servidors i serveis públics mitjançant cercadors específics com *Shodan*.
- Test de reputació IP dels diferents servidors.
- Recerca de metadada sobre fitxers publicats a *Internet*.
- Proves d'accés mitjançant xarxes d'anonimat com TOR o I2P.
- Anàlisis de servidors DNS aplicant tècniques de *Wildcarding DNS* i *Zones Transfer Test*.
- Detecció i test de *bypass* de la seguretat perimetral (*Firewalls/IDS/IPS*).
- Descobriment i proves de funcionament sobre els servidors SMTP.
- Test de força bruta sobre els diferents serveis publicats.
- Comprovació de les suites de xifratge disponibles pels certificats SSL/TLS.
- Addicionalment, proves d'enginyeria social a través de correu electrònic i altres medis (campanya de *phishing*).

Una vegada llistat un resum dels diferents punts, un segon aspecte rellevant a tenir en compte pel que fa a la identificació de vulnerabilitats té relació amb el conjunt de processos que un consultor de seguretat porta a terme per aconseguir-ho. Concretament, existeixen eines al mercat que implementen processos d'escaneig automatitzat i que són útils per obtenir una aproximació de l'estat actual de seguretat digital en el qual es troben els diferents actius. Aquests porten a terme un conjunt de proves per tal de contrastar els resultats obtinguts contra una base de dades que conté les vulnerabilitats publicades i reconegudes i extreure'n resultats significatius.

Per una altra part, existeix el factor humà, és a dir, l'experiència i el coneixement personal de l'analista de seguretat, el qual atorga la possibilitat d'analitzar diferents aspectes que les eines automatitzades no en tenen capacitat, com per exemple, les parts relacionades amb la lògica d'una aplicació o l'aportació de la pròpia intuïció humana per a la recerca de debilitats, en ocasions, determinant en els processos d'auditoria.

1.5.3 Explotació i comprovació de les vulnerabilitats

Un vegada la detecció de les vulnerabilitats s'ha fet efectiva, per tal de comprovar la seva existència i garantir que no es tracta d'un conjunt de falsos positius, en el cas que els termes d'auditoria ho permetin, es procedeix amb les proves d'explotació corresponents d'aquelles més crítiques. D'aquesta manera, s'exemplifica d'una forma precisa i concreta com un atacant podria fer-ne ús per a un benefici propi a la vegada que es recopila informació rellevant de cara a l'elaboració de l'informe d'auditoria, especialment útil des del punt de vista de l'administració tècnica dels sistemes afectats.

1.5.4 Establiment d'accés permanent

En algunes ocasions, concretament quan el procés d'auditoria té per objectiu simular un ciberatac real, si l'explotació d'alguna de les vulnerabilitats prèviament identificada ha tingut



èxit, seguidament s'apliquen tècniques que permeten mantenir l'accés a el recurs compromès per tal de procedir amb altres vectors d'atac sobre l'organització, un concepte conegut com a *pivoting*. En altres paraules, es tracta d'un mètode que utilitza el sistema compromès per atacar altres dispositius de la mateixa xarxa evitant restriccions com, per exemple, aquelles aplicades pels elements de seguretat perimetral, les quals poden prohibir l'accés directe a altres màquines. L'execució d'aquest mecanisme pot derivar, sens dubte, al descobriment de més punts febles corporatius.

1.5.5 Anàlisi de les dades obtingudes i redacció de l'informe




Finalment, una vegada executades totes les fases tècniques anteriors, ha arribat el moment d'organitzar la informació recopilada. En aquesta última etapa, els auditors procedeixen a redactar un document final, el qual inclou les conclusions referents a l'anàlisi de les diferents vulnerabilitats detectades, útil per tal de donar a conèixer l'estat actual dels actius analitzats a la vegada que es proporcionen alguns dels aspectes tècnics per a que un administrador de sistemes pugui solucionar les inconveniències trobades.

1.6 Criteri de classificació de vulnerabilitats

Per tal de facilitar la comprensió de la informació sobre vulnerabilitats que s'exposa en el present informe, *Vulnerable* ha adoptat l'ús de *Common Vulnerability Scoring System v3.0* (CVSSv3)¹, un sistema de puntuació dissenyat per a proporcionar un mètode obert i estandarditzat que permet estimar l'impacte derivat de vulnerabilitats identificades en els sistemes de la informació i que contribueix a quantificar la severitat que poden representar aquestes debilitats i el seu risc associat. D'aquesta manera, CVSS s'utilitza com una de mesura per a les organitzacions i entitats que necessiten puntuar l'impacte de vulnerabilitats de forma precisa i consistent. A continuació, s'adjunta un extracte que permet resumir la qualificació que s'empra en el sistema mencionat:

CVSS	Risc associat	Descripció	Urgència de resolució
9.0 – 10.0	Crític	Una vulnerabilitat de risc crític pot tenir un impacte nefast, ja que existeixen facilitats per explotar-la tot obtenint una execució exitosa. Aquest tipus d'incidències s'han de resoldre de forma immediata.	
7.0 – 8.9	Alt	Una vulnerabilitat de risc greu, encara que amb més dificultat que en el cas anterior, pot tenir un impacte nefast, ja que també continua oferint una probabilitat molt alta d'explotació i execució exitosa. Es recomana que aquest tipus d'incidències també siguin resoltes de forma immediata.	

¹ <https://www.first.org/cvss/v3.0/specification-document>

4.0 – 6.9	Mitjà	Una vulnerabilitat de risc mitjà pot potencialment tenir un alt impacte, encara que té una probabilitat baixa de ser explotada i executada satisfactòriament. Aquestes incidències s'han de resoldre ràpidament per minimitzar l'exposició.	
0.1 – 3.9	Baix	Una vulnerabilitat de risc baix té una probabilitat baixa d'explotació i en el cas que sigui explotada ocasiona un baix impacte. No obstant, aquestes incidències han de ser resoltes, en la mesura que sigui possible, per tal de reduir al mínim una exposició addicional i adherir-se a unes millors pràctiques.	
0.0	Info	Les incidències categoritzades com a informació no constitueixen una vulnerabilitat pròpiament, sinó que es tracta de la mostra de dades d'interès o bé de recomanacions i bones pràctiques que tenen per objectiu implementar les millors polítiques de seguretat existents.	

Taula 2 Extracte de la qualificació de vulnerabilitats que s'empra en el sistema CVSS.

Com a resolució, l'impacte de negoci resultant de la classificació obtinguda per a les diferents vulnerabilitats que s'exposen en el document present s'atorga al propi personal al que va dirigit, atenent al seu pla de riscos particular i d'acord a les polítiques internes i el model de negoci establert.

2 Resum dels riscos detectats

A continuació, es troben escrites les conclusions referents a l'anàlisi efectuat sobre els diferents actius inspeccionats. Es tracta d'una síntesi que no entra en qüestions tècniques ni especificacions concretes, sinó que proporciona una visió global de l'estat de risc obtingut en la present auditoria i que sovint es denomina informe executiu.

2.1 Actius analitzats

Abans però, cal fer menció sobre l'abast d'aquest document, el qual contempla la següent llista de direccions IP (fictícies):

- 8.8.8.1
- 8.8.8.2
- 8.8.8.5
- 8.8.8.6
- 8.8.8.9
- 8.8.8.10
- 8.8.8.11

2.2 Conclusions i recomanacions

El primer punt a mencionar referent a l'anàlisi de ports, serveis i sistemes operatius efectuat sobre les màquines que es troben exposades públicament és que l'estat en termes de seguretat digital és acceptable, però millorable. En altres paraules, la identificació de dues vulnerabilitats de caràcter crític indica que cap d'aquestes es troba relacionada amb una explotació directa i imminent. No obstant, sí que és possible observar amb claredat, entre altres aspectes, una mancança pel que fa a l'actualització i manteniment de programari emprat.

Un exemple clar és el fet que existeix una màquina que utilitza una versió obsoleta del sistema operatiu Linux, concretament Debian 7.0, una qüestió que deriva directament a l'existència d'incidències crítiques pel fet que aquest dispositiu no rep actualitzacions de seguretat dels propis desenvolupadors, la qual cosa pot permetre a un adversari, en el pitjor dels casos, obtenir el control total del sistema si determinades vulnerabilitats existents són correctament aprofitades. És per aquest motiu que es prega la intervenció apropiada donada la importància que aquest risc suposa, en aquest cas, efectuant l'actualització a l'última versió estable disponible o bé a aquella establerta per a les polítiques d'actualització corporatives.

El mateix succeeix amb l'ús de versions obsoletes de PHP, un fet que probablement és degut a la falta de manteniment del sistema i una correcta aplicació d'actualitzacions dins l'àmbit web. S'ha de tenir en compte que les versions antigues de PHP són susceptibles a diferents debilitats que poden permetre l'execució de codi al servidor, un aspecte que podria significar un punt de partida per un adversari.

Seguidament, cal fer referència a la configuració establerta en diferents serveis web, la qual permet l'ús de conjunts de xifratge obsolets i insegurs, com són a dia d'avui totes les versions derivades de SSL i, inclús, les versions de TLS 1.0 i 1.1. Cal tenir en compte que les connexions xifrades que fan ús d'aquests protocols es troben afectades per varis defectes criptogràfics i podrien arribar a ser compromeses. D'aquesta manera, es recomana la configuració pertinent als serveis afectats per tal de mitigar aquesta possibilitat.

Per altra banda, també s'ha pogut identificar un conjunt de males pràctiques com és l'ús de certificats autosignats. És important destacar que qualsevol interrupció en la cadena de certificats d'aquest tipus fa que sigui més difícil pels usuaris verificar l'autenticitat i identitat del servidor web i, per tant, s'incrementen de forma extraordinària les possibilitats que els mateixos usuaris siguin víctimes d'atacs d'enginyeria social i tècniques com el phishing.

Una altra característica a comentar és la navegació a través de xarxes anònimes com és TOR, la qual està permesa. Aquest fet suposa l'exposició a múltiples vectors d'atac per part de pirates informàtics degut a la impossibilitat de rastreig i la privacitat que els hi atorguen aquestes xarxes.

També és possible la suplantació d'identitat en l'enviament de correu mitjançant el servei SMTP. Resulta interessant millorar la configuració d'aquest servei, per exemple, comprovant si la IP que ha obert la sessió SMTP té permís per enviar correu en nom de la bústia emissor que s'indica. Existeixen protocols, com ara SPF, que realitzen una protecció contra la falsificació d'adreces en l'enviament de correu electrònic.

No es pot passar per alt la possibilitat d'aplicar mètodes de força bruta a diferents serveis actius en el servidor. S'ha de tenir present que els vectors de força bruta són extremadament fàcils de portar a terme i tenen una probabilitat de donar positiu suficientment perillosa quan no es restringeixen els múltiples intents d'accés, com és el cas. De fet, tant és així que ha estat possible obtenir les credencials de varis usuaris legítims de la plataforma mitjançant l'execució d'aquesta tècnica, les quals en una ocasió han atorgat accés al panell administratiu en rol d'administrador.

Aquest succés també implica una altra característica a remarcar, com és la definició d'una política de contrasenyes adequada, la qual es tracta d'un aspecte fonamental a considerar. Únicament si aquestes presenten una complexitat adient dificulten qualsevol procés que un intrús podria aplicar per a l'obtenció de les mateixes, en cas contrari, el risc de revelació és elevat.

Seguidament, també existeix la possibilitat d'obtenir informació emmagatzemada a la base de dades sobre la qual s'ostenta l'aplicació web a partir d'una tècnica coneguda com a SQL Injection. En aquest cas, es tracta d'un error greu de seguretat pel fet que qualsevol usuari malintencionat i extern a l'entitat corporativa pot tenir-hi accés i, per tant, entre altres aspectes, existeix una violació clara del compromís de confidencialitat de la informació, incloent la revelació explícita de credencials administratives.

Finalment, el darrer aspecte rellevant a tenir en compte fa referència a l'existència d'una mancança que permet l'aplicació del que s'anomena Cross-site Scripting (XSS), més concretament, Stored Cross-site Scripting (Stored XSS). Quan una aplicació web recopila informació proporcionada per un usuari i l'emmagatzema pel seu posterior ús sense tenir en compte els controls necessaris en el filtratge de les dades d'entrada, és aleshores quan existeix la possibilitat de que aquesta informació aparegui com a contingut del portal web i sigui interpretada en el navegador dels mateixos usuaris. D'aquesta manera, si el contingut introduït és maliciós, es podria aconseguir el segrest de la sessió dels usuaris administradors, la captura d'informació sensible, el canvi de l'aparença visual del portal web o l'execució d'exploits destinats al navegador, per citar alguns exemples.

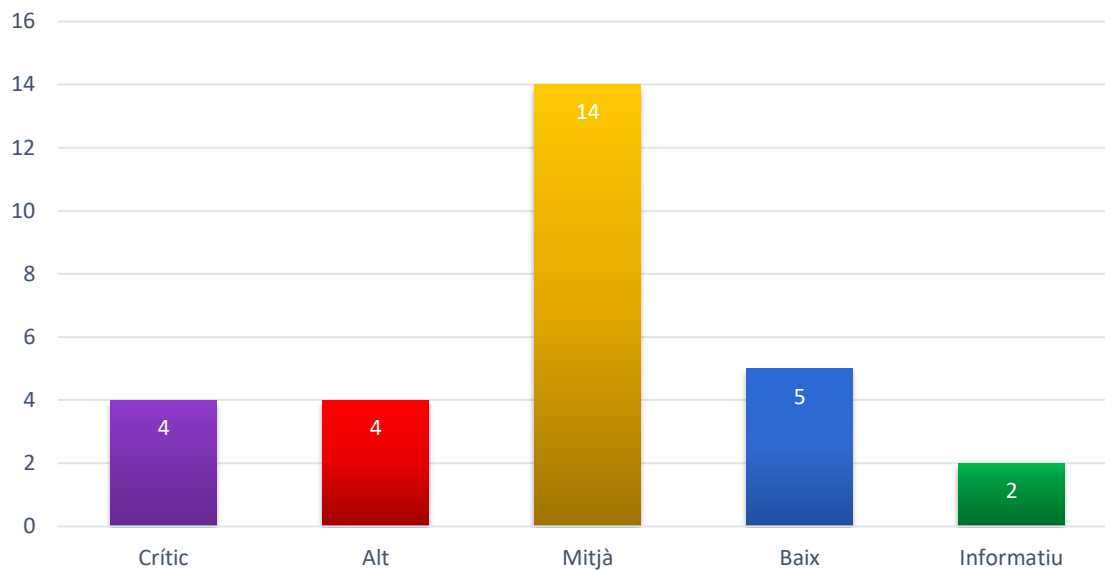
3 Informació i desenvolupament de les debilitats identificades

Seguidament, s'adjunta tota la informació relativa a les vulnerabilitats detectades en els diferents sistemes analitzats, en la qual queden descrits els aspectes tècnics necessaris, incloent recomanacions i referències externes, per tal de donar solvència a les mateixes.

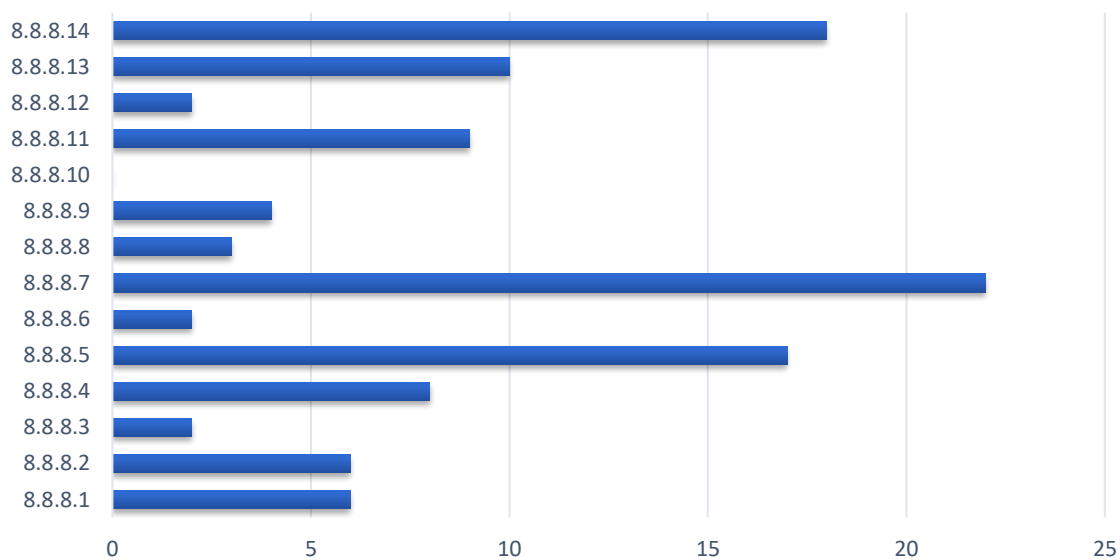
3.1 Resum de les incidències

Nom de la vulnerabilitat	Risc	Dispositius afectats
Detecció de sistema operatiu UNIX no suportat	Crític	8.8.8.5 8.8.8.8
Detecció de versió de PHP no suportada	Crític	8.8.8.8
Detecció del protocol SSL en les versions 2.0 i/o 3.0	Alt	8.8.8.6 8.8.8.8
Detecció del protocol TLS en la versió 1.0	Mitjà	8.8.8.8 8.8.8.10 8.8.8.11
No és possible confiar amb el certificat SSL	Mitjà	8.8.8.8
Xifratges SSL dèbils suportats	Mitjà	8.8.8.8
Algoritmes de xifratge dèbils suportats pel protocol SSH	Mitjà	8.8.8.1 8.8.8.1 8.8.8.8
Inici de sessió sense xifratge permès a POP3	Baix	8.8.8.8
Inici de sessió sense xifratge permès a SMTP	Baix	8.8.8.8
Fitxer robots.txt detectat al servidor web	Info	8.8.8.8

Número de vulnerabilitats per classificació de risc



Número de vulnerabilitats per direcció IP



3.2 Incidències de risc crític

3.2.1 Detecció de sistema operatiu UNIX no suportat

CVE: n/a

CVSSv3: 10.0

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	n/a

Descripció de la vulnerabilitat:

Segons la identificació efectuada en el dispositiu remot, aquest es troba executant una versió de sistema operatiu UNIX que actualment ja no es troba suportada, la qual cosa significa que no es proporcionen correccions de seguretat per a les noves vulnerabilitats que afecten al sistema.

Evidències:

8.8.8.8 en el port n/a:

Debian 7.0 support ended on 2016-04-26 end of regular support / 2018-05-01 (end of long-term support for Wheezy-LTS).
Upgrade to Debian Linux 9.x ("Stretch").
For more information, see : "<http://www.debian.org/releases/>":<http://www.debian.org/releases/>

Recomanacions:

Actualitzar la versió del sistema operatiu UNIX a una versió compatible i suportada.

Referències:

n/a

3.2.2 Detecció de versió de PHP no suportada

CVE: n/a

CVSSv3: 10.0

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/443

Descripció de la vulnerabilitat:

Segons la identificació efectuada en el dispositiu remot, aquest es troba executant una versió de PHP que actualment ja no es troba suportada, la qual cosa significa que no es proporcionen correccions de seguretat per a les noves vulnerabilitats que afecten al programari.

Evidències:

8.8.8.8 en el port tcp/443:

```
Source      : X-Powered-By: PHP/5.4.4-14+deb7u12
Installed version : 5.4.4-14+deb7u12
End of support date : 2015/09/03
Announcement   : "http://php.net/supported-versions.php":http://php.net/supported-versions.php
Supported versions : 7.1.x / 7.2.x / 7.3.x
```

Recomanacions:

Actualitzar la versió de PHP a una versió compatible i suportada.

Referències:

<http://php.net/eol.php>

<https://wiki.php.net/rfc/releaseprocess>

3.3 Incidències de risc alt

3.3.1 Detecció del protocol SSL en les versions 2.0 i/o 3.0

CVE: n/a

CVSSv3: 7.5

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/443

Descripció de la vulnerabilitat:

El dispositiu remot accepta connexions xifrades mitjançant les versions 2.0 i/o 3.0 de SSL, les quals es troben afectades per varis defectes criptogràfics. Tant és així que l'Institut Nacional d'Estàndards i Tecnologia (NIST) ha determinat que aquestes versions no són acceptables per a l'establiment de comunicacions segures.

Un atacant pot explotar aquestes debilitats per tal de realitzar atacs Man in The Middle (MiTM) o per a desxifrar les comunicacions entre els serveis i els seus clients.

Evidències:

8.8.8.8 en el port tcp/443:

- SSLv3 is enabled and the server supports at least one cipher.

Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
EDH-RSA-DES-CBC3-SHA			DH	RSA 3DES-CBC(168)	SHA1
ECDHE-RSA-DES-CBC3-SHA			ECDH	RSA 3DES-CBC(168)	SHA1
DES-CBC3-SHA		RSA	RSA	3DES-CBC(168)	SHA1

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
DHE-RSA-AES128-SHA			DH	RSA AES-CBC(128)	SHA1
DHE-RSA-AES256-SHA			DH	RSA AES-CBC(256)	SHA1
DHE-RSA-CAMELLIA128-SHA			DH	RSA Camellia-CBC(128)	SHA1
DHE-RSA-CAMELLIA256-SHA			DH	RSA Camellia-CBC(256)	SHA1
DHE-RSA-SEED-SHA			DH	RSA SEED-CBC(128)	SHA1
ECDHE-RSA-AES128-SHA			ECDH	RSA AES-CBC(128)	SHA1
ECDHE-RSA-AES256-SHA			ECDH	RSA AES-CBC(256)	SHA1
ECDHE-RSA-RC4-SHA			ECDH	RSA RC4(128)	SHA1
AES128-SHA		RSA	RSA	AES-CBC(128)	SHA1
AES256-SHA		RSA	RSA	AES-CBC(256)	SHA1

CAMELLIA128-SHA	RSA	RSA	Camellia-CBC(128)	SHA1
CAMELLIA256-SHA	RSA	RSA	Camellia-CBC(256)	SHA1
RC4-SHA	RSA	RSA	RC4(128)	SHA1
SEED-SHA	RSA	RSA	SEED-CBC(128)	SHA1
DHE-RSA-AES128-SHA256		DH	RSA AES-CBC(128)	SHA256
DHE-RSA-AES256-SHA256		DH	RSA AES-CBC(256)	SHA256
ECDHE-RSA-AES128-SHA256		ECDH	RSA AES-CBC(128)	SHA256
ECDHE-RSA-AES256-SHA384		ECDH	RSA AES-CBC(256)	SHA384
RSA-AES128-SHA256	RSA	RSA	AES-CBC(128)	SHA256
RSA-AES256-SHA256	RSA	RSA	AES-CBC(256)	SHA256

Recomanacions:

Consultar la documentació oficial del programari emprat per tal de desactivar l'ús de SSL 2.0 i 3.0, permetent únicament les versions de TLS que contenen conjunts de xifratge segurs.

Referències:

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<https://support.microsoft.com/en-us/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat>

<https://web.archive.org/web/20140909130341/http://www.linux4beginners.info/node/disable-sslv2>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

https://www.pcisecuritystandards.org/pdfs/15_02_12_PCI_SSC_Bulletin_on_DSS_revisions_SSL_update.pdf

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

3.4 Incidències de risc mitjà

3.4.1 Detecció del protocol TLS en la versió 1.0

CVE: n/a

CVSSv3: 6.5

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/443

Descripció de la vulnerabilitat:

El dispositiu remot accepta l'establiment de connexions xifrades emprant la versió 1.0 de TLS, la qual es troba afectada per varis defectes criptogràfics. Les versions més recents del protocol estan dissenyades en contra d'aquest problemes i, per tant, han d'utilitzar-se al seu lloc sempre que sigui possible.

Recomanacions:

Activar el suport per a TLS 1.2 i 1.3 i desactivar la versió 1.0.

Referències:

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

3.4.2 No és possible confiar amb el certificat SSL

CVE: n/a

CVSSv3: 6.5

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/25

Descripció de la vulnerabilitat:

No és possible confiar amb el certificat X.509 que ofereix el servidor, un fet que pot produir-se per diferents motius, tal i com s'indica a continuació:

- La part superior de la cadena de certificats enviada pel servidor pot no derivar d'una autoritat de certificació pública coneguda. Aquesta situació pot tenir lloc quan la part superior de la cadena es un certificat autosignat no reconegut o bé quan existeix una mancança de certificats intermedis que connecten la part superior de la cadena de certificats a una autoritat de certificació pública coneguda.

- La cadena de certificats inclou un certificat que no es vàlid pel que fa a les dates establertes de les propietats “notBefore” i/o “notAfter”.
- La cadena de certificats inclou una signatura que no coincideix amb la informació del certificat o bé que no s’ha pogut verificar. Les signatures errònies es poden corregir simplement fent que l’emissor signi de nou el certificat.

És important destacar que quan el dispositiu remot es tracta d'un sistema en producció, qualsevol interrupció en la cadena de certificats fa que sigui més difícil pels usuaris verificar l'autenticitat i identitat del servidor web. Aquest fet, encara que a simple vista sembla irrellevant, podria facilitar l'aplicació de diferents vectors d'atac, entre ells el clàssic Man in The Middle (MiTM), que un atacant podria efectuar contra el servidor remot.

Evidències:

8.8.8.8 en el port tcp/25:

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

| -Subject : OU=Domain Control Validated/CN=*.demo.com
| -Issuer : C=ES/ST=Illes Balears/L=Manacor/O=Soluciones Corporativas IP, SL/CN=Don Dominio / MrDomain
RSA DV CA

Recomanacions:

Generar o comprar un certificat SSL adequat pel servei.

Referències:

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

3.4.3 Xifratges SSL dèbils suportats

CVE: n/a

CVSSv3: 5.3

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/7002

Descripció de la vulnerabilitat:

El dispositiu remot permet l'ús xifratges SSL dèbils, els quals poder ser fàcilment violats si l'atacant es troba en la mateixa xarxa física.

Evidències:

8.8.8.8 en el port tcp/7002:

Here is the list of weak SSL ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC
EDH-RSA-DES-CBC-SHA		0x00, 0x15	DH	RSA	DES-CBC(56)SHA1
DES-CBC-SHA		0x00, 0x09	RSA	RSA	DES-CBC(56)SHA1

The fields above are :

{Tenable ciphername}

{Cipher ID code}

Kex={key exchange}

Auth={authentication}

Encrypt={symmetric encryption method}

MAC={message authentication code}

{export flag}

Recomanacions:

Configurar l'aplicació afectada per tal d'evitar l'ús de xifratges dèbils.

Referències:

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

3.4.4 Algoritmes de xifratge dèbils suportats pel protocol SSH

CVE: n/a

CVSSv3: 4.7

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/22

Descripció de la vulnerabilitat:

S'ha detectat que el servidor SSH del dispositiu remot es troba configurat per acceptar el xifratge de flux Arcfour o bé, inclús, cap xifratge. Segons l'especificació RFC 4253 es recomana desactivar Arcfour a causa d'un problema relacionat amb l'ús de claus febles.

Evidències:

8.8.8.8 en el port tcp/22:

The following weak server-to-client encryption algorithms are supported :

```
arcfour  
arcfour128  
arcfour256
```

The following weak client-to-server encryption algorithms are supported :

```
arcfour  
arcfour128  
arcfour256
```

Recomanacions:

Consultar la documentació oficial del programari per tal d'eliminar les xifres dèbils.

Referències:

<https://tools.ietf.org/html/rfc4253#section-6.3>

3.5 Incidències de risc baix

3.5.1 Inici de sessió sense xifratge permès a POP3

CVE: n/a

CVSSv3: 3.4

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/110

Descripció de la vulnerabilitat:

El dispositiu remot es troba executant un servei POP3 que permet iniciar sessió a través de connexions no xifrades. Un atacant podria arribar a capturar les credencials emprades pels usuaris si aconsegueix interceptar el tràfic destinat al servei POP3 quan aquests utilitzen un mecanisme d'autenticació de baixa seguretat com ara USER command, AUTH PLAIN o AUTH LOGIN.

Evidències:

8.8.8.8 en el port tcp/110:

The following cleartext methods are supported :
USER

Recomanacions:

Configurar el servei POP3 per a permetre únicament inicis de sessió a través de túnels SSL/TLS.

Referències:

<https://tools.ietf.org/html/rfc2222>

<https://tools.ietf.org/html/rfc2595>

3.5.2 Inici de sessió sense xifratge permès a SMTP

CVE: n/a

CVSSv3: 3.4

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/587

Descripció de la vulnerabilitat:

El dispositiu remot es troba executant un servei SMTP que permet iniciar sessió a través de connexions no xifrades. Un atacant podria arribar a capturar les credencials emprades pels usuaris si aconsegueix interceptar el tràfic destinat al servei SMTP quan aquests utilitzen un mecanisme d'autenticació de baixa seguretat com ara LOGIN o PLAIN.

Evidències:

8.8.8.8 en el port tcp/587:

The SMTP server advertises the following SASL methods over an unencrypted channel :

All supported methods : CRAM-MD5, LOGIN, PLAIN

Cleartext methods : LOGIN, PLAIN

Recomanacions:

Configurar el servei SMTP per a permetre únicament els inicis de sessió que utilitzen mecanismes d'autenticació de baixa seguretat a través de túnels SSL/TLS.

Referències:

<https://tools.ietf.org/html/rfc4422>

<https://tools.ietf.org/html/rfc4954>

3.6 Informació addicional

3.6.1 Fitxer robots.txt detectat al servidor web

CVE: n/a

CVSSv3: 0.0

Hosts afectats:

La següent taula mostra el llistat dels diferents dispositius afectats:

Host	Port
8.8.8.8	tcp/443

Descripció de la vulnerabilitat:

El servidor web remot conté un fitxer anomenat “robots.txt” que pretén evitar que els *crawlers* pertanyents als motors de cerca visitin certs directoris o arxius del portal web per a finalitats de manteniment o indexació. No obstant, un usuari malintencionat pot utilitzar el contingut d’aquest fitxer per tal de conèixer documents o directoris confidencials i accedir-hi directament o procedir amb l’aplicació d’altres vectors d’atac més específics.

Evidències:

8.8.8.8 en el port tcp/443:

Contents of robots.txt :

```
User-agent: *
Disallow: /.XHTML/
Disallow: /All/
Disallow: /apple-touch-icon.png
Disallow: /BES/
Disallow: /Branding/
Disallow: /ckeditor/
Disallow: /ComAgentInstall.exe
Disallow: /Debug/
Disallow: /favicon.ico
Disallow: /font-awesome/
Disallow: /Help/
Disallow: /Lite/
Disallow: /LookOut/
Disallow: /MDAirSync.dll
Disallow: /MDAutoDiscover.dll
Disallow: /MDBis.dll
Disallow: /MDSyncML.dll
Disallow: /Mobile/
Disallow: /PDFJS/
Disallow: /sapi/
Disallow: /WorldClient/
```

Recomanacions:

Revisar el contingut del fitxer robots.txt del portal web i, opcionalment, utilitzar les etiquetes HTML META per substituir les entrades del fitxer. En cas contrari, ajustar els controls d'accés al servidor web per tal de limitar i protegir accessos no desitjats a material confidencial.

Referències:

<http://www.robotstxt.org/orig.html>

4 Anàlisi i investigació tècnica

El darrer apartat d'aquest document correspon a l'estudi portat a terme en relació a diferents vessants tècniques que han estat considerades en funció de la topologia dels sistemes presents i les seves característiques.

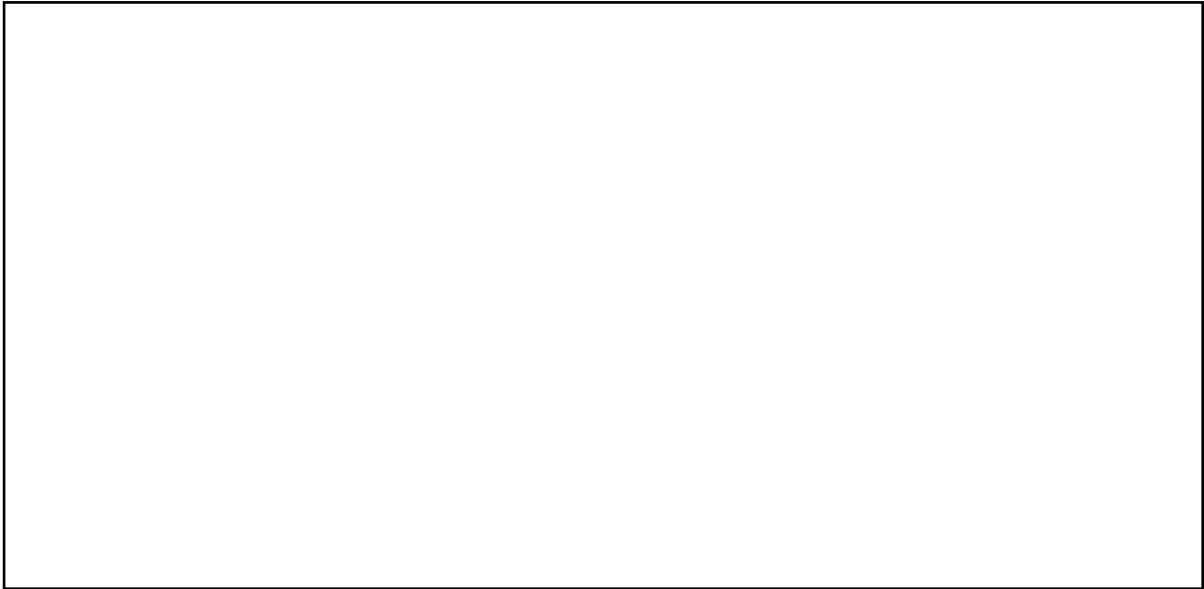
4.1 Accés des de xarxes d'anonimat

En primer lloc, cal fer esment que actualment resulta possible accedir a tota la infraestructura corporativa a través de xarxes d'anonimat com, per exemple, la xarxa TOR, el que significa un risc addicional davant d'atacs malintencionats, ja que és impossible el rastrejament d'un potencial intrús degut a la privacitat que atorguen aquest tipus de xarxes.

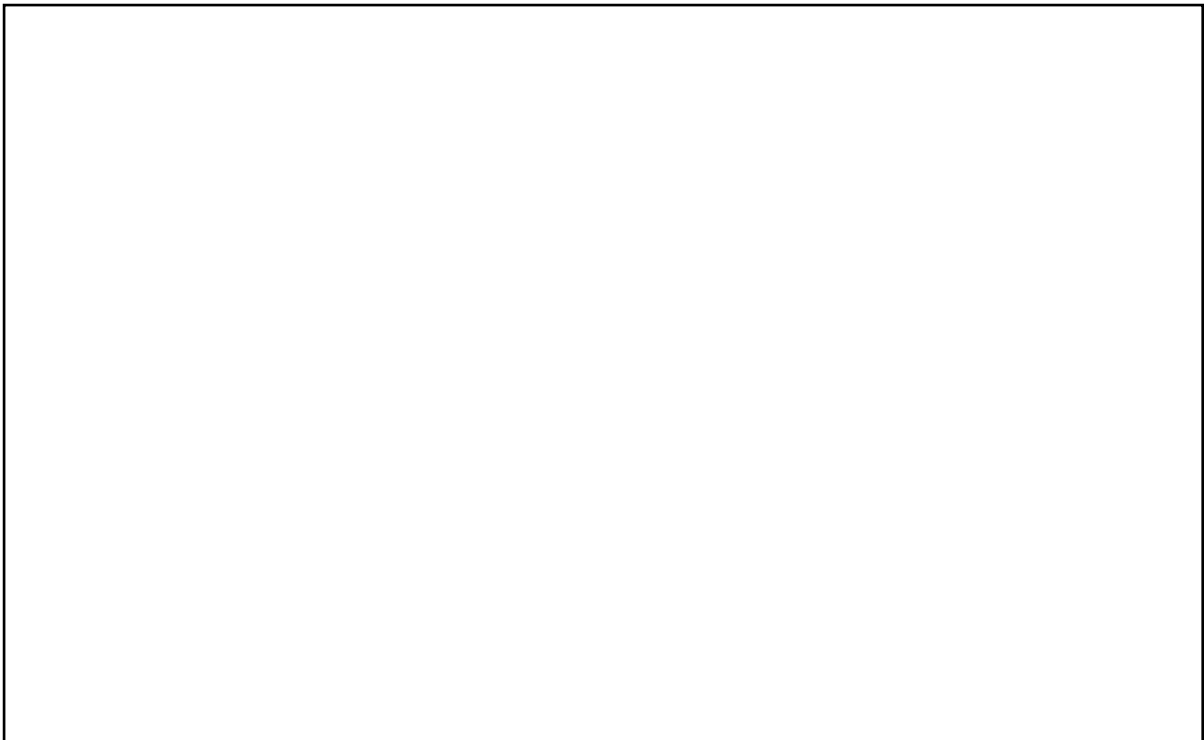


Il·lustració 2 Accés a la pàgina principal.

(espai en blanc intencionat)



Il·lustració 3 Accés a l'aplicació onwcloud.



Il·lustració 4 Accés al portal d'extranet.

Donada la casuística, es recomana bloquejar els accessos anònims, de la forma més convenient, a les diferents aplicacions web i serveis actius.

4.2 Indexació detectada al buscador Shodan

Mitjançant tècniques de recopilació d'informació a través de motors de cerca, en aquest cas Shodan, és possible obtenir, de forma totalment passiva, informació referent als equips corporatius que es troben exposats públicament, la qual cosa suposa un factor que un adversari podria utilitzar com a punt de partida per tal d'ostentar la base d'un atac dirigit o qualsevol altre tipus d'acció maliciosa.

Es important destacar que si un potencial intrús disposa d'aquest tipus d'informació, és a dir, que és capaç de recopilar dades sensibles sense necessitat d'executar cap aplicació, pot evitar la interacció directa amb les màquines corporatives durant la recerca de ports i serveis, així com les seves corresponents vulnerabilitats. D'aquesta manera, passa a ser indetectable en una de les fases més identificables d'un atac, com és la fase de recopilació d'informació.

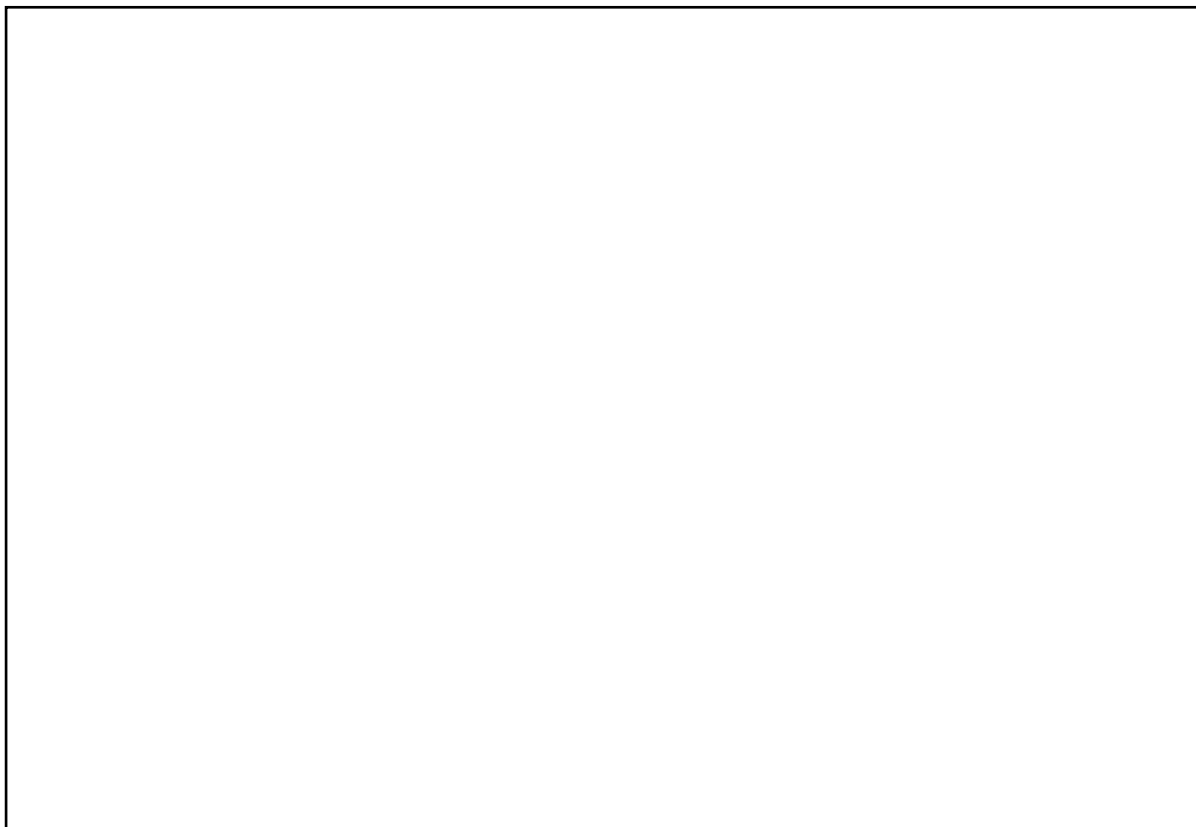


Il·lustració 5 Informació sensible proporcionada per Shodan.

Es recomana prevenir que els bots d'aquest tipus puguin incloure i indexar en les seves bases de dades la informació sensible que són capaços d'identificar dels dispositius que no tenen cap necessitat de ser rastrejats. En altres paraules, si es disposa d'accés als serveis de seguretat perimetral, com ara tallafocs, pot resultar d'utilitat emprar una llista negra d'adreces IP (en anglès, blacklist) per tal de denegar les consultes originades per aquestes màquines i ocultar així informació sensible que podria resultar d'utilitat en determinats vectors d'atac.

4.3 Reputació IP

La reputació IP analitza si alguna de les IPs facilitades està marcada en una llista negra. Aquesta circumstància té lloc quan un servidor, un servei web, un servei de correu o qualsevol altre tipus de servei porta a terme accions il·legítimes, tals com l'enviament de spam o de malware, per citar alguns exemples.



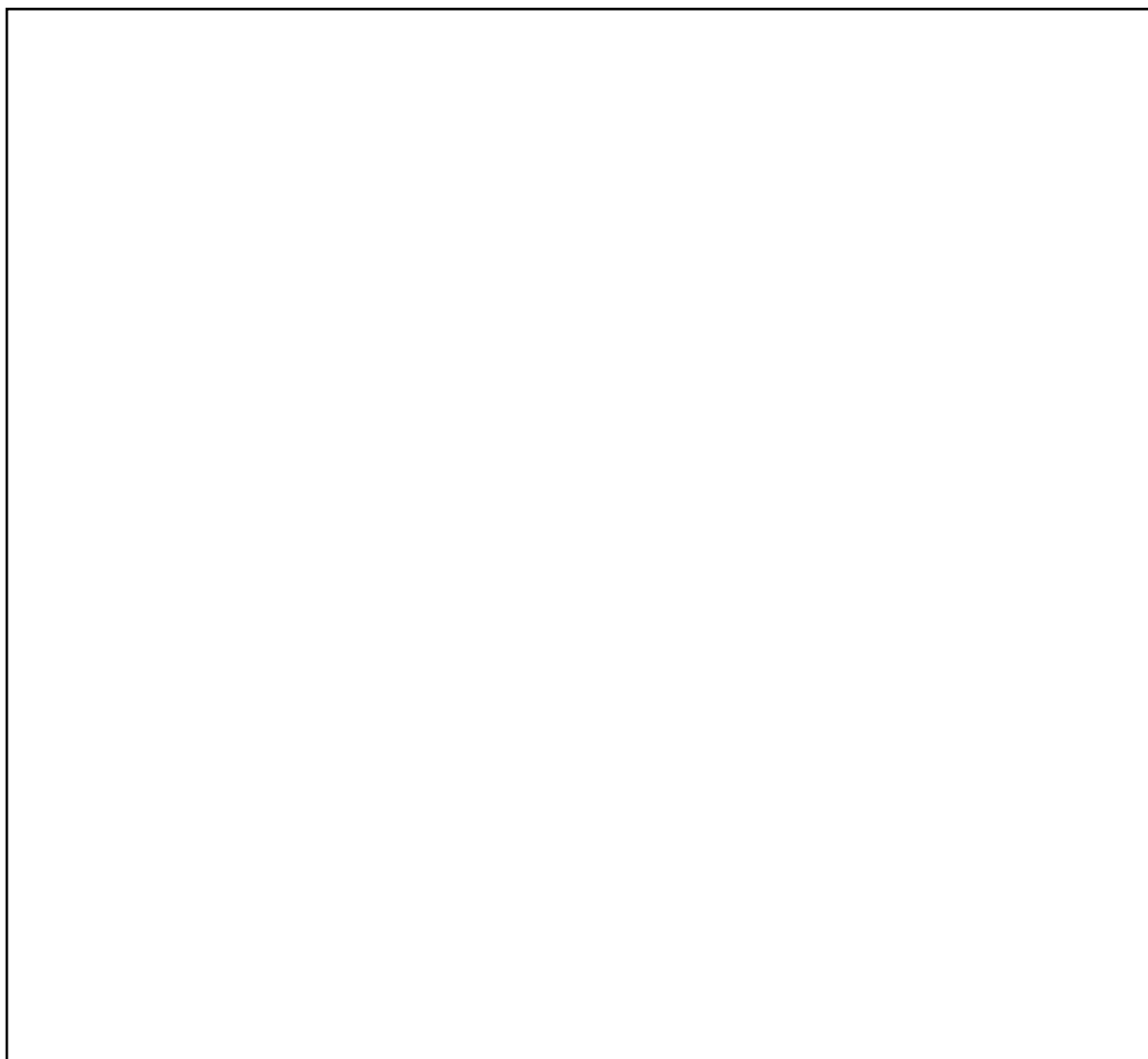
Il·lustració 6 Anàlisi de la reputació IP per a les diferents IPs públiques proporcionades.

Si una IP apareix en una llista es convenient analitzar el motiu i posteriorment sol·licitar al servei corresponent l'eliminació d'aquest registre. No obstant, en l'anàlisi realitzat per la present auditoria no s'ha detectat cap direcció IP en una llista negra tal i com es demostra en la imatge anterior.

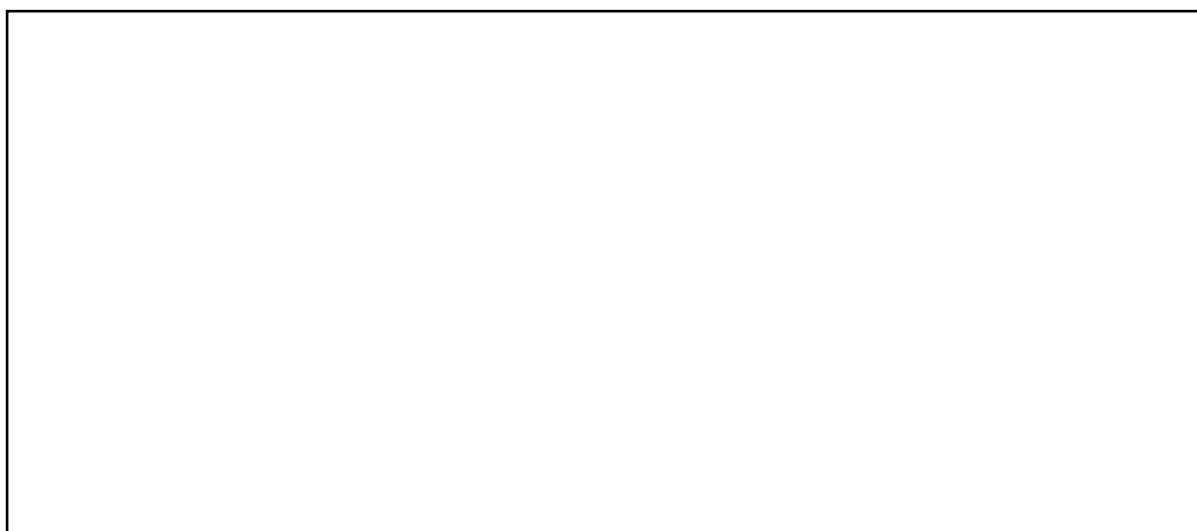
4.4 Localització de metadades

Ha estat possible identificar diferents documents indexats als cercadors, com ara Bing o Google, que són referents al domini *demo.com*. Aquests fitxers contenen informació addicional, anomenada en el seu conjunt metadades, que no ha estat eliminada prèviament a la pujada al servidor per a que qualsevol internauta pugui descarregar-los.

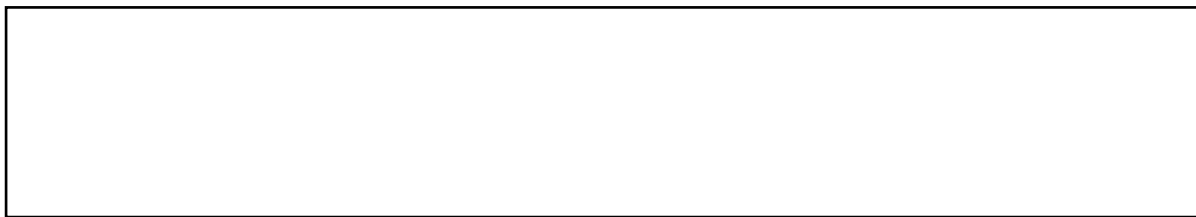
A continuació, s'adjunten les captures de pantalla de l'anàlisi realitzat sobre aquestes metadades, en el qual és possible observar, entre altres coses, el llistat de documents, el software emprat per la seva elaboració, les dates de creació i modificació i també l'autor o propietari per a cada un dels documents localitzats:



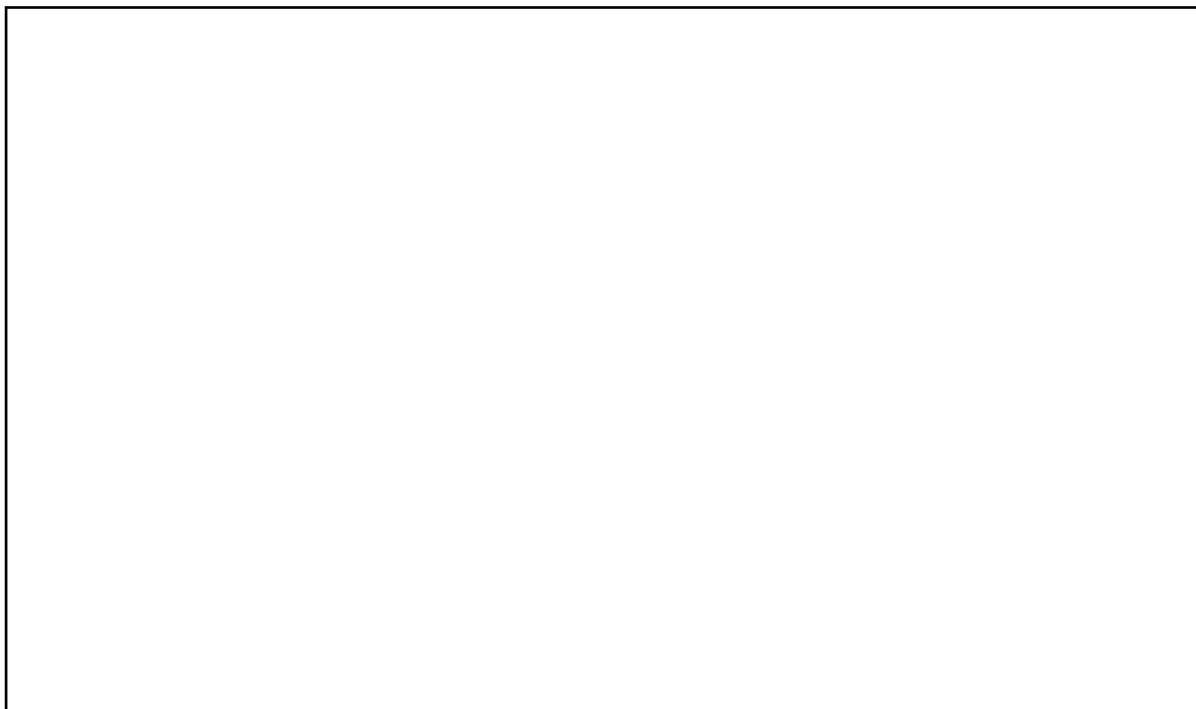
Il·lustració 7 Llistat de fitxers localitzats.



Il·lustració 8 Software emprat per a la creació dels documents.



Il·lustració 9 Autors i propietaris dels fitxers.

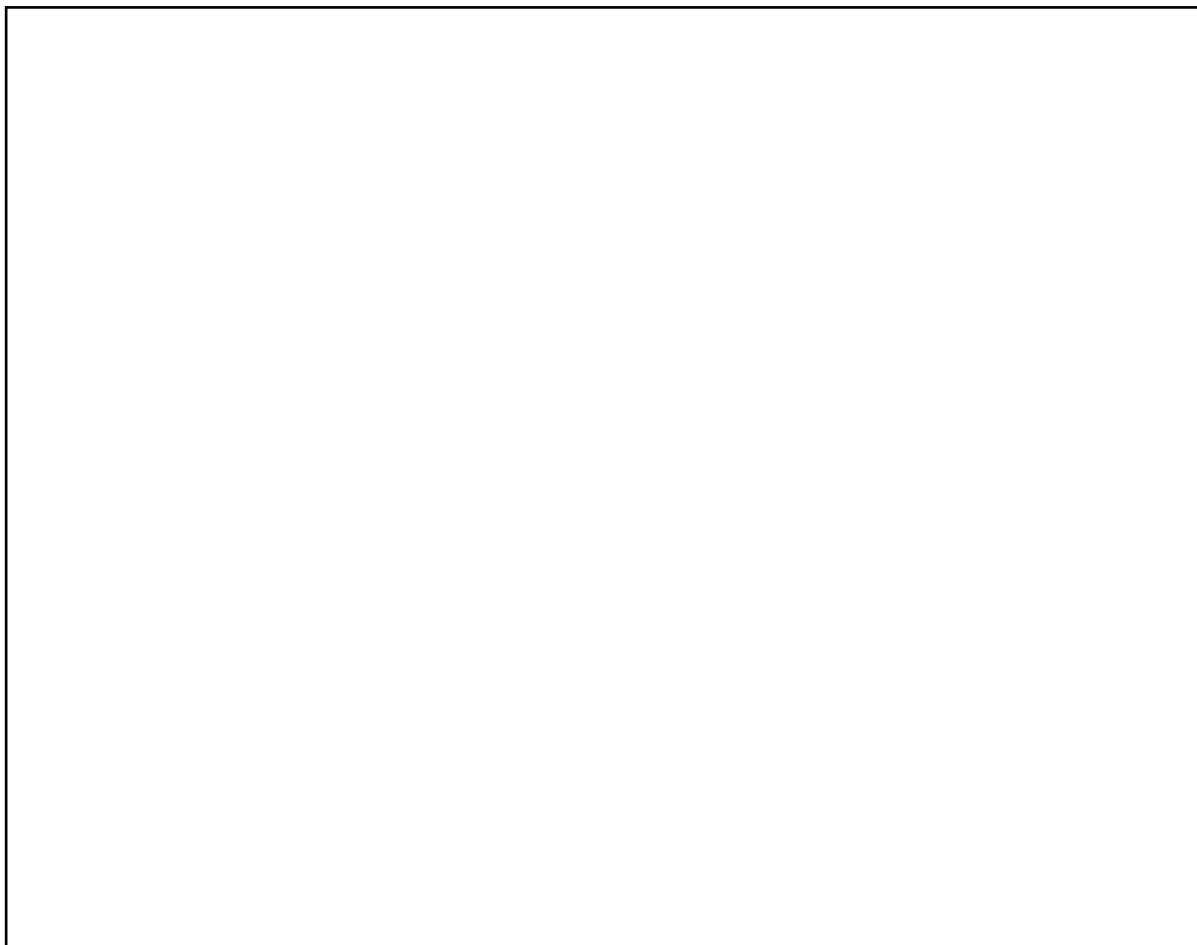


Il·lustració 10 Llistat de telèfons i persones relacionades amb els documents.

Com a mesura de seguretat, es recomana eliminar les metadades dels fitxers que es publiquen a Internet i, en aquest sentit, existeixen diferents maneres de portar-ho terme sempre depenent del software que s'està emprant. Per exemple, en alguns casos, es poden esborrar simplement editant les propietats del document a la pestanya "Detalls" si s'utilitza el sistema operatiu Windows. També poden ser eliminades configurant el propi processador de text, el qual, en funció del fabricant i la seva versió, pot ser configurat per aquesta tasca. Finalment, pel que fa als documents PDF, existeixen manuals del propi creador *Adobe* que també permeten l'eliminació de les metadades incrustades i l'aplicació d'aquesta bona pràctica.

4.5 Descobriment de subdominis

S'ha portat a terme una recerca de subdominis a partir del domini principal per tal d'esbrinar la presència d'algun tipus de servei actiu en un subdomini que podria arribar a ser explotable. Tal i com es pot observar en la següent imatge, no s'ha trobat informació rellevant al respecte:

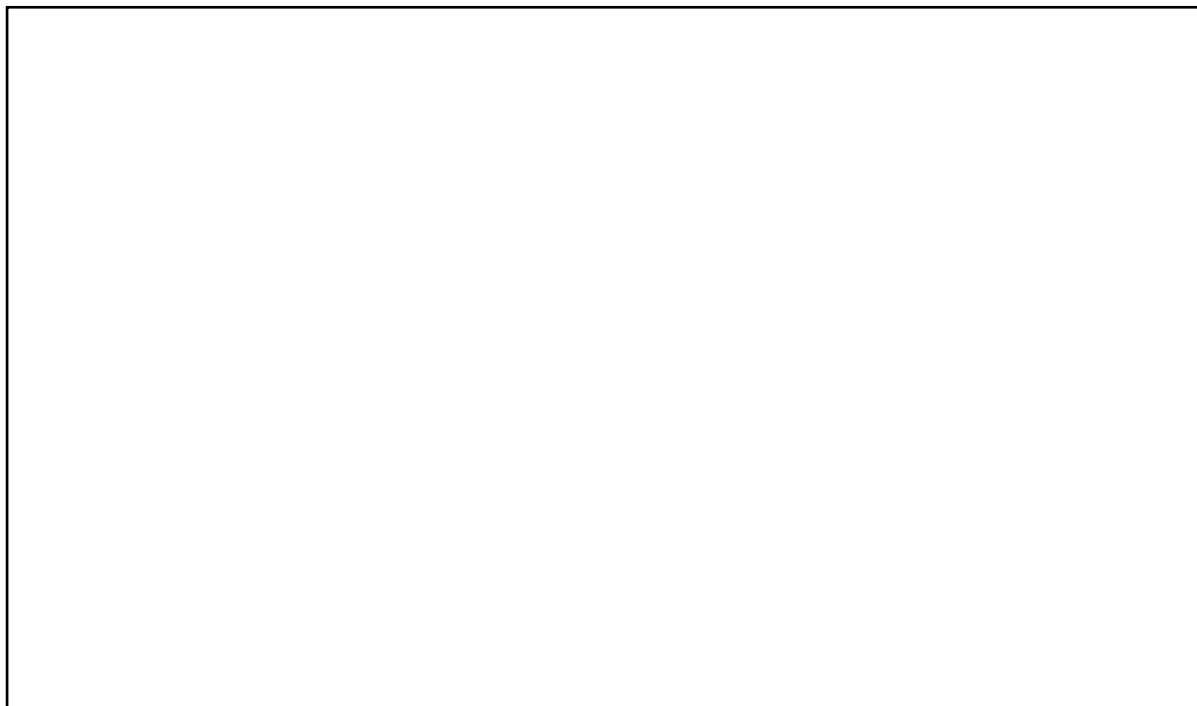


Il·lustració 11 Descobriments de subdominis a partir del domini principal.

Aquesta tècnica no representa cap tipus d'incidència o debilitat, sinó simplement una mostra de com és possible obtenir informació per tal d'identificar subdominis que contenen més portals web o altres serveis, els quals també requereixen, naturalment, d'una fortificació adequada.

4.6 Transferència de zona DNS

S'ha intentat extraure informació mitjançant el procés conegut com a transferència de zona obtenint un resultat positiu, és a dir, derivant a una denegació del procediment. Per tant, existeix una configuració apropiada en els servidors DNS que són autoritaris del domini *demo.com*.



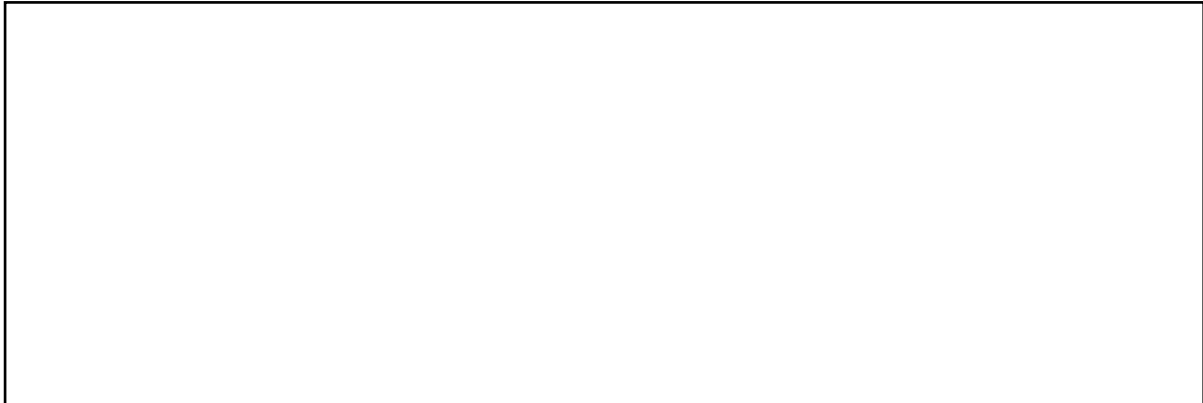
Il·lustració 12 Intent d'execució del procés de transferència de zona.



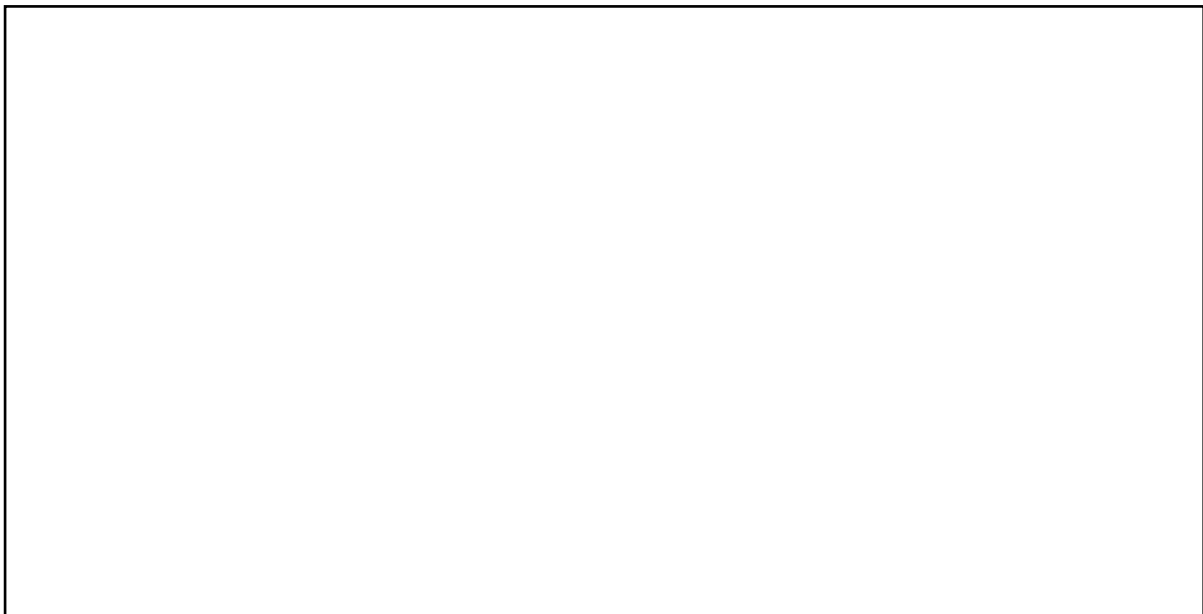
Il·lustració 13 Segon intent d'execució del procés de transferència de zona.

4.7 Recerca de correus

A través d'eines automatitzades s'ha aconseguit un llistat de correus electrònics pertanyents al domini *demo.com*. Un atacant podria recopilar aquesta informació per tal d'intentar, per exemple, un atac de phishing amb la finalitat d'obtenir les credencials d'accés d'algun d'aquest comptes de correu o servei vinculat. Els comptes identificats són els següents:



Il·lustració 14 Direccions de correu identificats a Bing referents al domini demo.com.



Il·lustració 15 Direccions de correu identificats a Google referents al domini demo.com.

Es recomana evitar publicar les direccions de correu electrònic en el portal web que no són destinades al públic. En altres paraules, s'aconsella analitzar quines direccions són aptes per a ser públiques i quines no, ja que si s'afegeixen direccions que no han de ser mostrades per privacitat, aquestes podrien ser recol·lectades mitjançant les tècniques que s'han mostrat en les captures de pantalla i posteriorment ser emprades en determinats vectors d'atac dirigits. La reducció de la superfície d'exposició és sempre una bona pràctica a seguir.

4.8 Configuració dèbil del servei SMTP

S'ha detectat una configuració dèbil al servei SMTP del servidor *smtp.demo.com*. En la següent il·lustració es pot comprovar com és possible l'enviament de correu falsejant el seu remitent real:



Il·lustració 16 Enviament de correu il·legítim mitjançant el servidor smtp.demo.com.

La imatge mostra una connexió Telnet al servei SMTP en la qual s'envia un correu del remitent nom.cognom@demo.com a la bústia comptabilitat@demo.com indicant, tant a l'assumpte com al cos, que es tracta d'un correu de prova. Com es pot veure, el servidor ha acceptat el correu a la cua per a la seva entrega.

Es recomana millorar la configuració del servei SMTP del servidor, per exemple, comprovant si la IP que ha obert la sessió té permisos per enviar correu en nom de la bústia que indica. Existeixen protocols, com ara SPF, que porten a terme una protecció contra la falsificació de direccions en l'enviament de correu electrònic.

4.9 Auditoria web bàsica

Seguidament es troben descrites diferents debilitats que han estat identificades en el portal web que respon al domini principal. Com es pot comprovar, les dues darreres incidències són caràcter crític i, per tant, es recomana que siguin resoltes en el mínim període de temps possible.

4.9.1 Anàlisi del certificat SSL

Els certificats SSL no només permeten xifrar les dades transmeses entre el navegador d'un visitant i el servidor, sinó que també s'encarreguen de proporcionar la identitat dels portals web i és per aquest motiu que en són una part fonamental, ja que, d'alguna manera, són un dels elements que generen confiança al usuari. Per tant, és important destacar que qualsevol problema relacionat amb l'autenticitat i identitat del servidor dificulta la identificació i detecció d'atacs que els usuaris que fan ús del mateix poder sofrir, com és la suplantació d'identitat.

És per aquest motiu que s'ha portat a terme un anàlisi de les característiques del certificat SSL que proporciona el servidor que allotja la web del domini principal. Com es podrà comprovar, en la següent il·lustració apareix un resum gràfic en el que s'indica una lletra com a resultat,

la qual té per objectiu determinar la qualificació del nivell de seguretat referent al protocol HTTPS. En el cas present, es possible visualitzar una qualificació B, que significa l'obtenció d'un resultat acceptable però amb oportunitats de millora:



Il·lustració 17 Qualificació obtinguda del servei HTTPS pel domini demo.com.

Una característica negativa és que el servei remot utilitza una cadena de certificats SSL que han estat signats mitjançant un algoritme de hash criptogràficament dèbil com ara MD2, MD4, MD5 o SHA1. S'ha demostrat que aquest tipus de hashes són vulnerables a atacs de col·lisió, el que significa que un adversari podria explotar aquesta feblesa per tal de generar un altre certificat amb exactament la mateixa signatura digital i fer-se passar pel servei ofert suplantant la identitat del portal web.

4.9.2 Aplicació de força bruta

Es possible l'aplicació d'atacs de força a bruta a diferents serveis, ja que aquests admeten infinitat d'intents de connexió. Les tècniques de força bruta representen una metodologia que s'empra amb freqüència en atacs dirigits sobre infraestructures de petita i mitjana escala, ja que són extremadament fàcils de portar a terme i tenen una probabilitat de donar positiu suficientment perillosa quan no es restringeix els múltiples intents d'accés, com és el cas. Per tant, es necessari que els administradors de sistemes trobin com mitigar aquesta problemàtica.



Il·lustració 18 Exemple d'aplicació de força bruta al portal web.

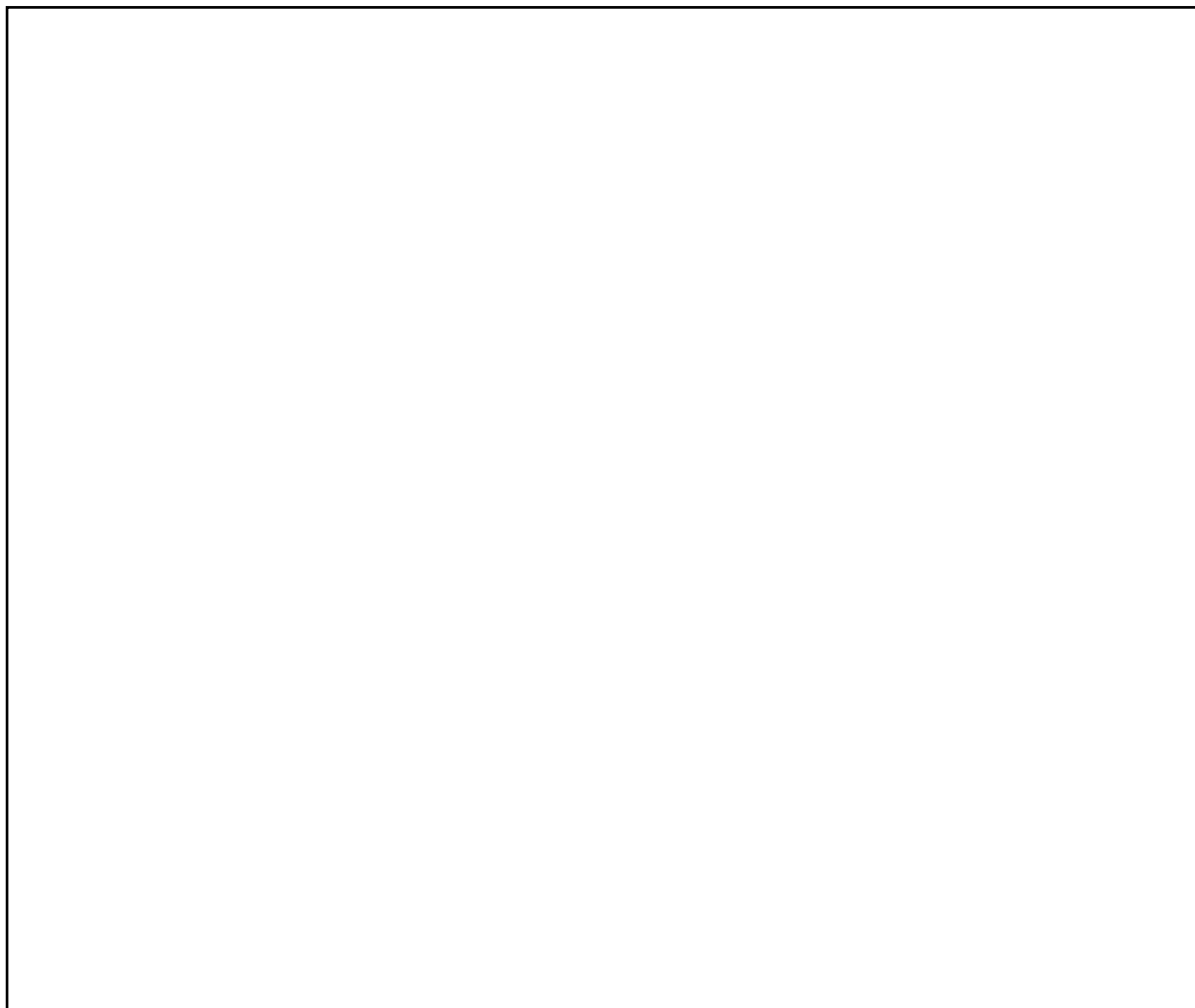
En la figura mostrada, es pot observar els intents que s'han provat, remarcats en vermell, amb una durada inferior a 20 segons de l'atac. La següent imatge és una demostració del conjunt de credencials legítimes obtingudes amb un temps d'execució relativament més llarg:



Il·lustració 19 Obtenció de 22 credencials vàlides a partir de l'atac de força bruta.

Tal com és possible observar, ha estat possible extreure un total de 22 credencials vàlides, les quals corresponen a usuaris registrats al portal web, un fet exemplificat per la imatge que procedeix a continuació:

(espai en blanc intencionat)



Il·lustració 20 Accés al portal corporatiu amb una de les credencials d'accés obtingudes.

Resulta convenient establir mesures preventives als serveis corresponents per tal d'eliminar aquest vector d'atac, ja sigui en el propi dispositiu que ofereix el servei o en els elements de xarxa intermedis com ara tallafocs, si aquests existeixen dins del àmbit corporatiu. Per exemple, a nivell de servei es poden aplicar manualment configuracions com les següents:

- Limitar els intents d'accés i vanejar temporalment les adreces IP que introdueixin credencials errònies.
- Forçar l'ús d'autenticació a través de certificats digitals.
- Denegar l'accés a usuaris per defecte, com poden ser root, admin, administrador, etc.

Una altra alternativa és la instal·lació d'aplicacions senzilles, com ara fail2ban, els quals faciliten la implementació d'aquest tipus de polítiques, com és la limitació del nombre d'intents fallits per accedir a un servei concret, per exemple, FTP o SSH.

Finalment, també caldria revisar el conjunt de serveis exposats i desactivar aquells que no són usats amb freqüència, amb l'objectiu de reduir l'exposició del conjunt de vies que un atacant pot recórrer per trobar un punt dèbil de seguretat o simplement aplicar tècniques com la recentment mostrada.

4.9.3 Injeccions SQL

Un atac d'injecció SQL consisteix en la inserció d'una consulta SQL, ja sigui parcial o completa, a través de l'entrada de dades o del navegador client que interactua amb l'aplicació web. Una tècnica d'aquestes característiques executada satisfactòriament pot permetre multitud d'accions, com ara la lectura de dades confidencials de la base de dades, la seva modificació (inserció, actualització o eliminació), l'execució d'operacions d'administració sobre el gestor de base de dades, l'obtenció del contingut d'arxius existents en el sistema DBMS o també l'escriptura d'arxius arbitraris en el sistema de fitxers i, fins i tot, l'execució de comandes al sistema operatiu.

Els atacs d'injecció SQL es porten a terme quan les pròpies comandes SQL poden ser injectades en el procés d'entrada de dades per tal d'afectar l'execució de les consultes SQL ja establertes. Aquest fet té origen en la forma en que les aplicacions web constitueixen les sentències SQL, les quals normalment parteixen de codi prèviament escrit pel programador conjuntament amb altres dades proporcionades per l'usuari, tal i com representa el següent exemple:

```
select title, text from news where id=$id
```

En la sentència anterior, la variable "\$id" conté l'identificador d'usuari que ha estat proporcionat com a paràmetre d'entrada, mentre que la resta de la consulta SQL constata la part estàtica que ha estat definida pel programador, aconseguint d'aquesta manera que la declaració SQL sigui dinàmica en funció de les dades proporcionades a l'aplicació web.

No obstant, degut a la forma en que s'ha construït, l'usuari podria enviar com a paràmetre d'entrada un valor especialment dissenyat per tal que la instrucció SQL original executi accions arbitràries a elecció d'aquest. Per exemple, podria ser possible proporcionar "10 or 1=1", canviant d'aquesta manera la lògica de la declaració SQL i modificant la clàusula WHERE, és a dir, afegint una condició sempre verídica com és "or 1=1":

```
select title, text from news where id=10 or 1=1
```

Els atacs d'injecció SQL es poden categoritzar en funció del medi pel qual un atacant obté els resultats desitjats:

- Inband: les dades s'extreuen emprant el mateix canal que s'utilitza per injectar el codi SQL. Es tracta del tipus d'atac més directe en que les dades recuperades són presentades directament a la pàgina web de l'aplicació.
- Out-of-band: les dades es recuperen a través d'un canal diferent. Per exemple, es genera un correu electrònic amb els resultats de la consulta i s'envia a una bústia externa.
- Blind: no existeix una transferència de dades real, però l'atacant pot reconstruir la informació enviant peticions particulars i observant el comportament resultant del servidor de base de dades.

En qualsevol cas, un atac d'injecció SQL satisfactori requereix que l'atacant elabori una consulta SQL sintèticament correcta i, quan l'aplicació retorna un missatge d'error generat per una consulta incorrecta, és aleshores quan és més fàcil reconstruir la lògica de la consulta original i, per tant, entendre com cal realitzar la inserció correctament. No obstant, si l'aplicació oculta els detalls d'un error, l'atacant està obligat a realitzar enginyeria inversa en la lògica de la consulta original per tal de generar una sentència vàlida.

Pel que fa a les tècniques que s'utilitzen per explotar les debilitats d'injeccions SQL, majoritàriament existeixen cinc tipus diferents, encara que aquestes poden utilitzar-se de forma combinada:

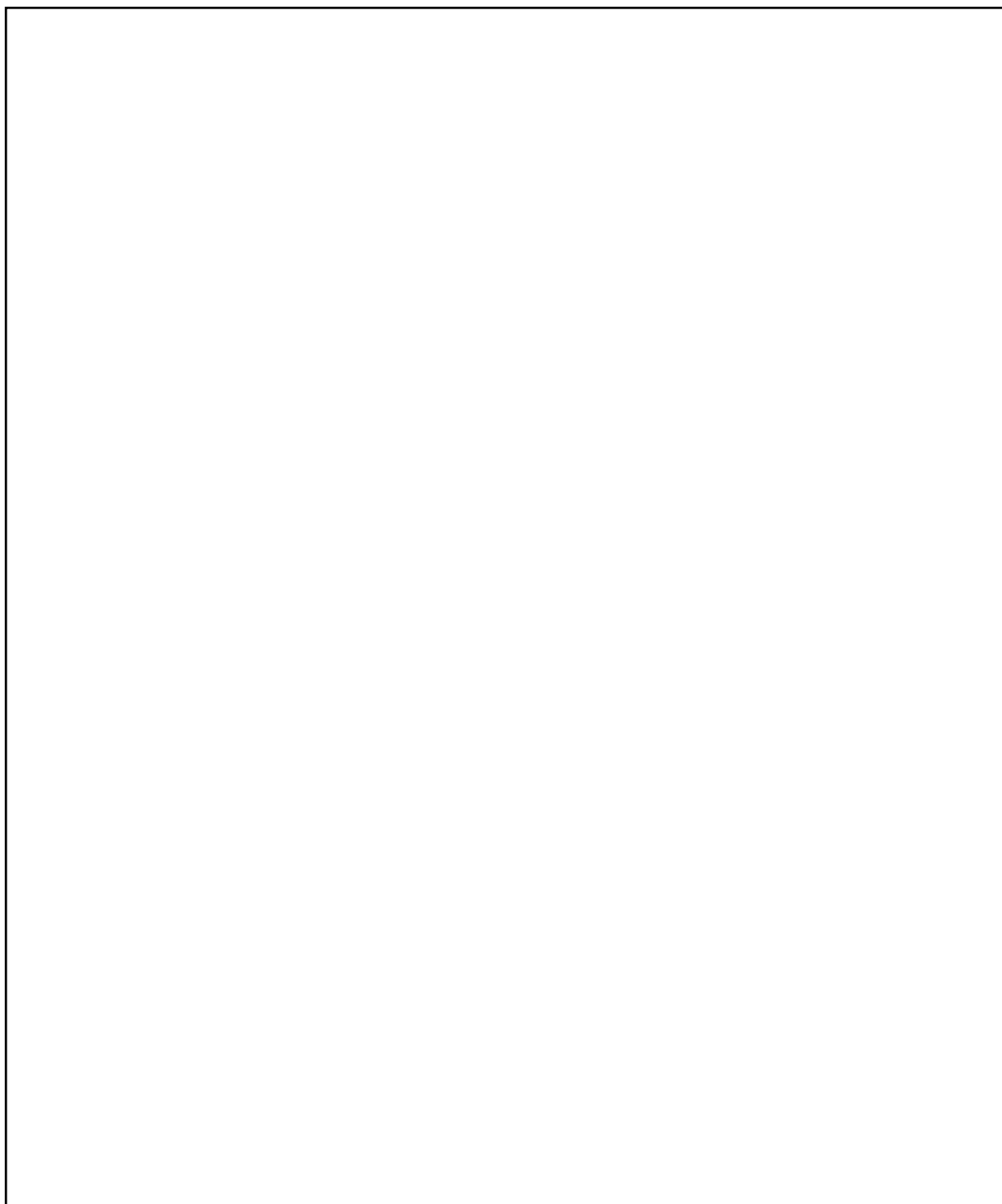
- Operador d'unió: l'ús de l'operador UNION és possible quan es tracta d'una consulta SELECT, la qual cosa permet combinar dos peticions en un únic resultat.
- Boolean: s'utilitza una condició booleana per tal de verificar si determinades condicions són certes o falses.
- Error-based: fa referència a les tècniques que obliguen a la base de dades a generar un error proporcionant informació a l'adversari per tal de millorar la injecció.
- Out-of-band: és la tècnica utilitzada per recuperar dades utilitzant un canal diferent, per exemple, creant una connexió HTTP per tal d'enviar els resultats a un servidor web.
- Time delay: s'utilitzen comandes de base de dades com "sleep" per retardar les respostes a consultes condicionals. És útil quan l'atacant no té cap tipus de resposta (resultat, sortida o error) de l'aplicació web.

D'aquesta manera, aplicant tècniques com les recentment mencionades, ha estat possible obtenir informació sensible com ara les bases de dades disponibles al sistema:

La revelació del nom d'usuari que gestiona el sistema de base dades:

(espai en blanc intencionat)

El conjunt de taules existents per a la base de dades “demo”:



(espai en blanc intencionat)

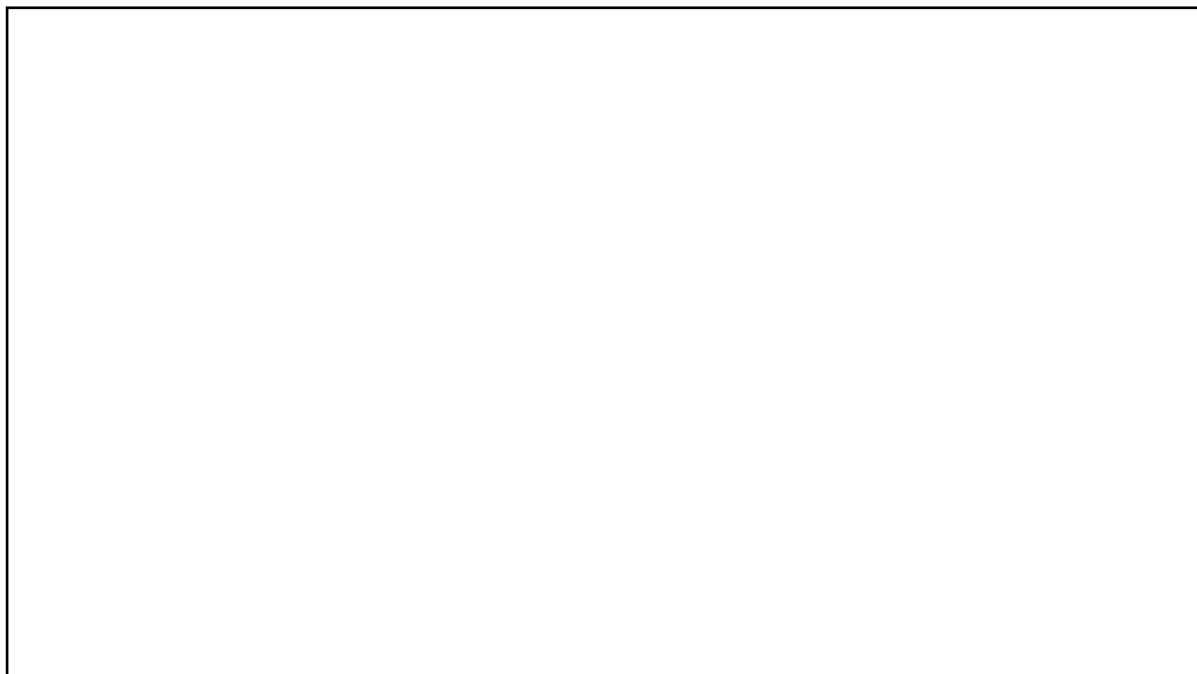
Enumeració de columnes per a la taula “usuaris” de la base de dades “demo”:



Extracció de l'usuari administrador del portal web:



Extracció dels registres de la taula “usuaris” pertanyents a la base de dades “demo”. Revelació de les contrasenyes emprades pels mateixos en clar. Ha estat possible obtenir un total de 383 usuaris:



El conjunt de les evidències mostrades és només un resum del total d'accions que es poden arribar a executar i, malauradament, no és possible proporcionar una solució genèrica que sigui aplicable a un cas d'injecció SQL específic. No obstant, existeix un gran volum d'informació al respecte que pot ajudar a prevenir la potencial execució d'aquests tipus de

tècniques, la qual generalment està relacionada amb l'ús de consultes parametritzades, la validació de les dades d'entrada, la limitació de privilegis, l'ús de procediments emmagatzemats (en anglès, Stored Procedures), l'ocultació dels missatges d'error, la segmentació i separació de les credencials d'usuari i el xifratge d'aquestes o la desactivació de l'accés a consola i altres funcionalitats que són rarament emprades.

4.9.4 Stored Cross-Site Scripting (XSS)

L'anomenada tècnica Stored Cross-Site Scripting (XSS) és la més perillosa d'aquest tipus de vulnerabilitat informàtica. Totes les aplicacions web que permeten als usuaris afegir dades es troben exposades a l'execució d'aquest mecanisme si no es tenen en compte els controls necessaris.

La presència de Stored XSS es dona quan una aplicació web recopila informació proporcionada per un usuari, la qual pot ser maliciosa, i l'emmagatzema pel seu posterior ús. Si l'entrada de les dades no és filtrada correctament és aleshores quan existeix la possibilitat de que la informació aparegui com a contingut del portal web i, per tant, s'executi en el navegador dels usuaris i internautes amb els permisos que han estat concedits a la pròpia aplicació.

Es tracta d'una debilitat que pot ser emprada per a portar a terme una sèrie d'atacs basats en el navegador, els quals inclouen:

- El segrest de la sessió de l'usuari.
- La captura d'informació sensible que és visible pels usuaris de l'aplicació.
- El canvi de l'aparença visual del portal web.
- L'execució d'exploits destinats al navegador.

Una de les diferències més important respecte els altres tipus de XSS és que, en aquest cas, no es necessita un enllaç maliciós sinó que per una explotació exitosa només cal que un usuari visiti la pàgina que conté el XSS emmagatzemat. Un exemple representatiu d'aquest procediment podria ser el següent:

- L'atacant explota una vulnerabilitat de XSS i aconsegueix emmagatzemar codi JavaScript maliciós en una de les pàgines del portal web.
- L'usuari s'autentica a l'aplicació.
- L'usuari posteriorment visita la pàgina infectada.
- El navegador de l'usuari executa el codi maliciós introduït per l'atacant prèviament.

Tal i com es pot pensar, la tipologia de Stored XSS és especialment perillosa en les àrees de l'aplicació on hi accedeixen els usuaris que disposen d'alts privilegis. Si un administrador visita una pàgina vulnerable i executa automàticament el codi arbitrari, es pot derivar a un problema de seguretat crític com podria ser l'exposició d'informació sensible o l'obtenció de la seva sessió d'usuari.



Il·lustració 21 Petició HTTP per a la creació d'un fitxer al servidor amb codi Javascript.



Il·lustració 22 Demostració de l'execució del fitxer amb el codi anteriorment mostrat.



Il·lustració 23 Vulnerabilitat posada en pràctica en situació real.



Il·lustració 24 Quantitat d'usuaris que han seguit l'enllaç publicat (durant 25 minuts) i han esdevingut víctimes.



Il·lustració 25 Obtenció de les cookies de sessió dels usuaris que han fet click amb possible robatori de sessió (hijacking).

La prevenció de les tècniques XSS és trivial en alguns casos però pot resultar ser especialment complicada en aplicacions on la forma en que es gestionen les dades controlades pels usuaris i el seu esquema de treball és complex.

En general, una prevenció efectiva de les vulnerabilitats XSS implica una combinació de les següents mesures:

- Filtratge de les dades d'entrada. Cal analitzar i verificar el contingut enviat per un usuari en la pujada d'informació permeten únicament el tipus de dada esperat.
- Utilitzar capçaleres de resposta adequades. En les respostes HTTP que no estan destinades a incloure HTML o JavaScript és possible utilitzar les capçaleres "Content-Type" i "X-Content-Type-Options" per assegurar-se de que els navegadors les interpreten de la forma desitjada.
- Codificació de dades a la sortida. Quan les dades controlades per un usuari s'inclouen en respostes HTTP pot resultar útil codificar-les per evitar que s'interpreti com a contingut actiu. Depenent del context de sortida, aquest aspecte pot requerir la codificació d'HTML, JavaScript, CSS i la pròpia URL.
- Content Security Policy (CSP). Com a última línia de defensa és possible emprar la capa de política de seguretat de contingut per tal de reduir la gravetat de les vulnerabilitats XSS que puguin aparèixer.