ANEXA 2 - METODOLOGII DE TESTARE

1. Testare securitate la nivel aplicatie informatica

In urma analizei arhitecturii si a documentelor de solutie au fost identificate urmatoarele teste ce trebuie efectuate pentru identificare vulenrabilitati la nivelul aplicatiei informatice.

Tabelul contine:

- Identificator test;
- Denumire test;
- Descriere Test;
- Conditie esec;
- Conditie succes ;

ID test	Denumire test	Descriere test	Conditie esec	Conditie succes
1	Test pentru aplicatii de amprenta digitala	Acest test este axat pe descoperirea si divulgarea numelor si versiunilor serverelor de aplicatii.	Serverele de aplicatii isi divulga numele si versiunile.	Serverele de aplicatii nu isi dezvaluie numele si versiunile.
2	Test pentru coduri si mesaje de eroare	Testul trebuie sa identifice dacă generarea codurilor de eroare de catre serverele de aplicatii sau web dezvăluie informații despre bazele de date, bug-uri, și alte componente tehnologice legate direct de aplicatii web sau nu.	Codurile de eroare generate de servere dezvăluie informații despre bazele de date, bug-uri, și alte componente tehnologice legate de aplicații web.	Codurile de eroare generate de servere nu dezvăluie informații despre bazele de date, bug-uri, și alte componente tehnologice legate de aplicații web.
3	Test pentru dezvaluirea datelor senzitive	Acest test se bazeaza pe verificarea protectiei datelor senzitive, testarea divulgarii sau dezvaluirii datelor care se intentioneaza sa nu fie disponibile pentru un anumit utilizator si/sau accesul la codul sursa.	Aplicatia dezvaluie date sensibile si/sau permite accesul la codul sursa.	Aplicatia nu permite dezvaluirea datelor sensibile si/sau accesul la codul sursa.

Digitally signed by Odobescu Viorica
Date: 2019.12.13 11:54:55 EET
Reason: MoldSign Signature
Location: Moldova

4	Test pentru SSL-TLS	Testul este realizat în scopul de a descoperi dacă există configurări greșite ale serverului, care ar putea fi folosite pentru a forța folosirea unui cod mai slab pentru a obține acces la un presupus canal de comunicație securizat.	Au fost gasite erori de configurare a serverului care ar putea duce la utilizarea unui cod mai slab.	Nu au fost gasite erori de configurare a serverului care ar putea duce la utilizarea unui cod mai slab.
5	Test pentru Managementul configurarii infrastructurii	Acest test se concentreaza asupra securitatii infrastructurii serverului web, care este extrem de importanta in scopul de a pastra securitatea intregii aplicatii.	Securitatea infrastructurii serverului de web nu este suficient de puternica.	Securitatea infrastructurii serverului de web este suficient de puternica.
6	Test pentru Managementul configurarii aplicatiei	Acest test verifica configurarea corecta a elementelor unice care alcatuiesc arhitectura aplicatiei, cum ar fi eliminarea exemplelor, documentatiei si a paginilor de test inainte de implementare.	Au fost identificate exemple, documentatii si pagini de test utilizate in timpul implementarii.	Nu au fost identificate exemple, documentatii si pagini de test utilizate in timpul implementarii.
7	Test pentru manipularea extensiilor de fisiere	Testul este efectuat pentru a identifica daca serverul de web dezvaluie informatii legate de tehnologiile, limbile, si plugin-urile folosite pentru a completa cererea web.	Serverele de web dezvaluie informatii cu privire la tehnologiile, limbile si plugin-urile folosite pentru a completa cererea web.	Serverele de web nu dezvaluie informatii cu privire la tehnologiile, limbile si plugin-urile folosite pentru a completa cererea web.
8	Test pentru fisierele vechi de backup si fara referinta	Acest test identifica prezenta fisierelor fara referinta si/sau uitate, versiunilor vechi redenumite ale fisierelor modificate, fisiere de incluziune care sunt incarcate in limbajul de alegere si pot fi descarcate ca sursa, sau backup-uri automate sau manuale.	Au fost gasite fisiere fara referinta si/sau uitate, versiuni vechi redenumite ale fisierelor modificate sau fisiere de incluziune	Nu au fost gasite fisiere fara referinta si/sau uitate, versiuni vechi redenumite ale fisierelor modificate sau fisiere de incluziune
9	Test pentru Admin Interfaces	Acest test este efectuat in scopul de a descoperi daca si cum un utilizator neautorizat sau standard poate accesa interfete administrative.	Utilizatorii neautorizati sau standard au acces la interfetele administrative.	Utilizatorii neautorizati sau standard nu au acces la interfetele administrative.

10	Test pentru metodele HTTP si XST	Testul verifica daca metodele HTTP care ar reprezenta un risc pentru aplicatie(PUT, GET, CONNECT, TRACE) sunt dezactivate. Mai mult decat atat, se va testa daca aplicatia este vulnerabila la Cross Site Tracing.	Metodele HTTP care ar putea reprezenta un risc pentru aplicația nu sunt dezactivate	Metodele HTTP care ar putea reprezenta un risc pentru aplicația sunt dezactivate
11	Test pentru acreditarile transportate pe un canal criptat	Scopul acestui test este de a verifica daca datele de autentificare ale utilizatorului sunt transferate prin intermediul unui canal criptat și dacă aplicația utilizează un protocol securizat, cum ar fi HTTPS.	Datele de autentificare ale utilizatorului nu sunt transferate printr-un canal criptat și aplicația nu utilizează un protocol securizat.	Datele de autentificare ale utilizatorului sunt transferate printr-un canal criptat și aplicația utilizează un protocol securizat.
12	Test pentru enumerarea utilizatorilor	Acest test este realizat în scopul de a verifica dacă un atacator poate colecta un set de nume de utilizatori valabile și daca aplicațiile web dezvăluie daca un nume de utilizator există in sistem.	Aplicatiile web arata cand un nume de utilizator exista in sistem si un posibil atacator poate colecta un set de nume de utilizatori valide.	Aplicatiile web nu arata cand un nume de utilizator exista in sistem si un posibil atacator nu poate colecta un set de nume de utilizatori valide.
13	Test pentru conturi de utilizatori impliciti sau usor de ghicit	Acest test verifica daca acreditarile implicite prevazute pentru autentificarea si configurarea initiala sunt actualizate si daca aplicatia impune sau nu politici puternice pentru parola.	Acreditările implicite prevăzute pentru autentificarea și configurarea inițială nu sunt actualizate, iar aplicatia nu impune politici puternice pentru parola.	Acreditările implicite prevăzute pentru autentificarea și configurarea inițială sunt actualizate, iar aplicatia impune politici puternice pentru parola.
14	Test pentru Brute Force	Scopul acestui test este de a verifica diferite tipuri de scheme de autentificare si eficienta diferitelor atacuri de tip brute-force care vizeaza aplicatiile web.	Aplicatia este vulnerabila la atacurile de tip brute-force.	Aplicatia nu este vulnerabila la atacurile de tip brute-force.
15	Test pentru Bypassing Authentication Schema	Acest test este efectuat pentru a determina daca schema de autentificare poate fi ocolita pur si simplu, trecand direct la o pagina interna sau alterand cererea pacalind	Schema de autentificare poate fi ocolita.	Schema de autentificare nu poate fi ocolita.

		astfel aplicatia, sa para ca deja s-a facut autentificarea.		
16	Test pentru vulnerabilitatea la memorarea parolei sau resetarea ei	Acest test este centrat pe verificarea functiei ce permite utilizatorilor sa isi reseteze parola este corect implementata si daca aplicatia permite utilizatorilor sa salveze parola in browser	Functia ce permite utilizatorilor sa isi reseteze parola NU este corect implementata si daca aplicatia NU permite utilizatorilor sa salveze parola in browser	Functia ce permite utilizatorilor sa isi reseteze parola este corect implementata si daca aplicatia permite utilizatorilor sa salveze parola in browser
17	Test pentru Logout si Browser Cache Management	Scopul acestui test este de a verifica faptul ca functia de logout este corect implementata, ca nu este posibil de a "reutiliza" sesiunea dupa logout, ca aplicatia automat face logout daca userul nu a avut activitate pentru o perioada de timp, si ca nu raman date senzitive salvate in cache-ul browserului.	Functia de logout NU este corect implementata.	Functia de logout este corect implementata.
18	Test pentru Captcha	Acest test este facut pentru a testa daca implementarile Captcha sunt vulnerabile la atacuri malicioase.	Implementarile Captcha sunt vulnerabile la atacuri malicioase.	Implementarile Captcha nu sunt vulnerabile la atacuri malicioase.
19	Testarea autentificarii prin factori multiplii	Scopul acestui test este sa evalueze puterea procesului de autentificare.	Cererea implementeaza un proces de autentificare puternic.	Cererea nu implementeaza un proces de autentificare puternic.
20	Test pentru Race Conditions	Acest test este efectuat în scopul de a descoperi dacă o problemă potențială a concurenței ar putea să apară și dacă aceasta produce un rezultat neașteptat.	Problema potentiala a concurentei apare.	Problema potentiala a concurentei nu apare.
21	Testare pentru criptarea parolelor	Domeniul de aplicare al acestui test este de a determina dacă parolele sunt criptate sau nu și dacă persoană care are acces la fișierele de configurare le poate citi.	Parolele nu sunt criptate si pot fi citite de persoana care are acces la fisierele de configurare.	Parolele sunt criptate si nu pot fi citite de persoana care are acces la fisierele de configurare.

22	Testarea schemei de management a sesiunii	Acest test verifica dacă cookie-uri și celelalte token-uri sesiune sunt create într-un mod sigur și imprevizibil și că un atacator nu este capabil de a deturna sesiunile utilizatorilor legitimi.	Cookie-urile si celelalte token-uri sesiune nu sunt create intr-un mediu sigur si un atacator este capabil sa deturneze sesiunile utilizatorilor legitimi.	Cookie-urile si celelalte token-uri sesiune sunt create intr-un mediu sigur si un atacator nu este capabil sa deturneze sesiunile utilizatorilor legitimi.
23	Test pentru atributele cookie-urilor	Scopul testului este sa verifice masurile intreprinse pentru a proteja cookie-urile.	Atributele cookie-urilor nu sunt protejate.	Atributele cookie-urilor sunt protejate.
24	Test pentru blocarea sesiunii	Testul verifica daca aplicatia reinnoieste cookie-ul sesiune, dupa o autentificare valida si daca exista posibilitatea sa se gaseasca vulnerabilitati la blocarea sesiunii si daca un utilizator poate fi fortat sa foloseasca un cookie cunoscut de catre atacator si, sa obtina astfel, deturnarea sesiunii valide.	Aplicatia nu reinnoieste cookie-urile sesiune dupa autentificarea cu succes a utilizatorului si un atacator este capabil sa deturneze o sesiune valida.	Aplicatia reinnoieste cookie-urile sesiune dupa autentificarea cu succes a utilizatorului si un atacator nu este capabil sa deturneze o sesiune valida.
25	Testarea variabilelor expuse ale sesiunii	Testul verifica daca tokenurile sesiune(Cookie, SessionID, Hidden Field) sunt expuse si daca acestea sunt protejate de la interceptare atunci cand sunt in tranzit intre browser-ul clientului si serverele de aplicatie.	Token-urile sesiune sunt expuse si nu sunt protejate de interceptare atunci cand sunt in tranzit.	Token-urile sesiune nu sunt expuse si sunt protejate de interceptare atunci cand sunt in tranzit.
26	Test pentru Cross Site Request Forgery	Testul se concentreaza pe urmatoarea verificare: daca un atacator poate insela utilizatorii aplicatiei prin incarcarea unei pagini care contine o cerere malicioasa, facand aplicatia vulnerabila la falsa Cross Site Request.	Aplicatia este vulnerabila la falsa Cross Site Request.	Aplicatia nu este vulnerabila la falsa Cross Site Request.
27	Test pentru Path Traversal	Testul verifica daca metodele de validare a intrarilor au fost bine proiectate sau implementate, si in cazul in care un agresor ar putea exploata sistemul pentru a citi/scrie fisiere care nu sunt destinate sa fie accesibile.	Metodele de validare a intrarilor nu sunt bine proiectate sau implementate si un agresor este capabil sa	Metodele de validare a intrarilor sunt bine proiectate sau implementate si un agresor nu este capabil sa exploateze sistemul.

			exploateze sistemul.	
28	Testarea schemei de ocolire a autorizarii	Domeniul de aplicare al acestui test este de a verifica modul in care a fost pusa in aplicare schema de autorizare pentru fiecare rol si/sau drept, in scopul de a accesa functii restranse si/sau resurse.	Schema de autorizare nu este bine implementata pentru fiecare rol si/sau privilegiu si poate fi ocolita.	Schema de autorizare este bine implementata pentru fiecare rol si/sau privilegiu si nu poate fi ocolita.
29	Test pentru escaladarea drepturilor	Acest test verifica daca este posibil ca un utilizator sa-si modifice drepturile si/sau rolurile in interiorul aplicatiei si, astfel sa permita atacuri de escaladare a drepturilor.	Un utilizator isi poate modifica drepturile si/sau rolurile in cadrul aplicatiei si aplicatia permite atacuri de escaladare a drepturilor.	Un utilizator nu isi poate modifica drepturile si/sau rolurile in cadrul aplicatiei si aplicatia nu permite atacuri de escaladare a drepturilor.
30	Testarea logicii afacerii	Acest test este efectuat pentru a determina daca logica operationala prezinta brese de securitate care sa permita utilizatorilor sa faca lucruri nepermise de afacere.	Logica operationala are brese de securitate care permit unui utilizator sa faca lucruri interzise.	Logica operationala nu are brese de securitate care nu permit unui utilizator sa faca lucruri interzise.
31	Test pentru Reflected Cross site scripting	Acest test descopera daca aplicatia permite intrari nevalidate trimise prin cereri ale clientilor, o vulnerabilitate exploatata de atacatori in scopul de a instala key loggers, de a fura cookie-uri victimei, de a fura memoria temporara si de a schimba continutul paginii.	Aplicatia permite intrari nevalidate trimise prin cererea clientului.	Aplicatia nu permite intrari nevalidate trimise prin cererea clientului.
32	Test pentru Stored Cross Site Scripting	Testul descopera daca aplicatia web descarca intrari malicioase de la utilizator si apoi inmagazineaza aceste intrari pentru o utilizare ulterioara, permitand astfel datelor malicioase sa apara ca fiind parte a site-ului web si sa ruleze in browser-ul utilizatorului conform drepturilor aplicatiei web.	Aplicatia web aduna intrari malicioase de la utilizator si le inmagazineaza pentru o utilizare ulterioara, permitand datelor sa apara	Aplicatia web nu descarca intrari malicioase de la utilizator.

			ca facand parte din site.	
33	Test pentru DOM based Cross Site Scripting	Scopul testului este de a descoperi bug-uri Cross Site Scripting(XSS), ceea ce duce la executarea de cod injectat.	S-au gasit bug-uri XSS.	Nu s-au gasit bug-uri XSS.
34	SQL Injection	Acest test este axat pe descoperirea cazului în care aplicatia este vulnerabilă la introducerea sau "injectarea" unei interogari SQL în aplicație prin intermediul datelor de intrare de la client.	Aplicația este vulnerabilă la introducerea sau "injectarea" unei interogari SQL.	Aplicația nu este vulnerabilă la introducerea sau "injectarea" unei interogari SQL.
35	LDAP Injection	Scopul acestui test este de a verifica dacă informațiile sensibile despre utilizatori și gazde(host-uri) reprezentate într-o structură LDAP pot fi divulgate, modificate sau introduse.	Informatiile sensibile despre utilizatori si host-uri reprezentate intr-o structura LDAP pot fi dezvaluite, modificate sau introduse.	Informatiile sensibile despre utilizatori si host-uri reprezentate intr-o structura LDAP nu pot fi dezvaluite, modificate sau introduse.
36	Test pentru ORM Injection	Acest test este efectuat pentru a descoperi daca aplicatia este vulnerabila la un atac de tipul injectie SQL intr-un obiect de date generat de nivelul ORM (Object Relational Mapping) al aplicatiei.	Aplicatia este vulnerabila la un atac de tipul injectie SQL intr-un obiect de date generat de nivelul ORM al aplicatiei.	Aplicatia nu este vulnerabila la un atac de tipul injectie SQL intr-un obiect de date generat de nivelul ORM al aplicatiei.
37	Test pentru XML Injection	Acest test incearca sa determine daca analizorul XML nu reușește să facă o validare de date corespunzătoare la incercarea de injectare a unui document XML în aplicație.	Analizorul XML nu reuseste sa execute o validare de date corespunzatoare la incercarea de injectare a unui document XML in aplicatie.	Analizorul XML reuseste sa execute o validare de date corespunzatoare la incercarea de injectare a unui document XML in aplicatie.
38	Test pentru SSI Injection	Scopul acestui test este de a verifica daca este posibil sa se injecteze in aplicatie date care vor fi interpretate prin mecanisme SSL, permitand astfel unui atacator sa injecteze cod in	Este posibila injectarea in datele aplicatiei care vor fi	Nu este posibila injectarea in datele aplicatiei care vor fi interpretate de mecanisme SSL.

		pagini HTML sau chiar sa execute cod de la distanta.	interpretate de mecanisme SSL.	
39	Test pentru XPath Injection	Testul acesta este bazat pe verificarea posibilitatii de a injecta date in aplicatii pentru a executa interogari Xpath controlate de utilizator, permitand astfel unui atacator sa ocoleasca mecanismele de autentificare sau informatiile de acces fara o autorizatie adecvata.	Este posibilă injectarea de date în aplicații pentru a executa interogări XPath controlate de utilizator.	Nu este posibilă injectarea de date în aplicații pentru a executa interogări XPath controlate de utilizator.
40	Test pentru IMAP/SMTP Injection	Acest test verifica capacitatea de a injecta arbitrar comenzi IMAP/SMTP in servere de mail, din cauza datelor de intrare care nu sunt curatate in mod corespunzator.	Datele de autentificare ale utilizatorului nu sunt transferate printr-un canal criptat și aplicația nu utilizează un protocol securizat.	Datele de intrare nu sunt curatate in mod corespunzator si pot fi injectate comenzi IMAP/SMTP arbitrar in serverele de e-mail.
41	Test pentru Code Injection	Acest test se face in scopul de a descoperi daca este posibil sa fie introdus cod ca intrare pe o pagina web si sa fie executat de serverul de web.	Se permite sa se introduca cod ca date de intrare pe pagina web si acesta este executat de catre serverul de web.	Nu se permite introducerea de cod ca date de intrare pe pagina web si acesta nu este executat de catre serverul de web.
42	Test pentru Command Injection	Acest test este efectuat în scopul de a descoperi dacă interfețe web nu sunt curățate în mod corespunzător, permițând astfel unui atacator de a încărca programe malware sau chiar sa obțina parole.	Interfețele web nu sunt curățate în mod corespunzător și un atacator poate încărca programe malware sau poate obține parole.	Interfețele web sunt curățate în mod corespunzător și un atacator nu poate încărca programe malware si nu poate obține parole.
43	Test pentru HTTP Splitting Smuggling	Scopul acestui test este să verifice dacă aplicația este vulnerabilă la atacurile care exploatează funcții specifice ale protocoalelor HTTP, fie punctele slabe ale aplicației web sau particularități în modul prin care	Aplicația este vulnerabilă la atacurile care exploatează funcții specifice ale	Aplicația nu este vulnerabilă la atacurile care exploatează funcții specifice ale protocoalelor HTTP.

		diferitii agenți interpretează mesajele HTTP.	protocoalelor HTTP.	
44	Test pentru SQL Wildcard Attacks	Acest test este efectuat pentru a determina dacă baza de date poate fi forțata să efectueze interogări CPU-intensive prin utilizarea mai multor metacaractere, care fac aplicatia vulnerabilă la atacurile DoS.	Baza de date poate fi forțata să efectueze interogări CPU-intensive prin utilizarea mai multor metacaractere.	Baza de date nu poate fi forțata să efectueze interogări CPU-intensive prin utilizarea metacaracterelor.
45	Test pentru DoS Locking Customer Accounts	Domeniul de aplicare ale acestui test este de a determina dacă un atacator poate bloca conturi de utilizator valide prin incercari repetate de a se conecta cu parolă greșită.	Un atacator poate bloca conturi de utilizator valide prin incercari repetate de a se conecta cu parolă greșită.	Un atacator nu poate bloca conturi de utilizator valide prin incercari repetate de a se conecta cu parolă greșită.
46	Test pentru DoS Buffer Overflows	Acest test este axat pe descoperirea dacă este posibil de a provoca o condiție de refuz al serviciului prin refuzul uneia sau mai multor structuri de date ale aplicației țintă.	Este posibil sa se provoace o condiție de refuz al serviciului prin refuzul uneia sau mai multor structuri de date ale aplicației țintă.	Nu este posibil sa se provoace o condiție de refuz al serviciului prin refuzul uneia sau mai multor structuri de date ale aplicației țintă.
47	Test pentru DoS User Specified Object Allocation	Scopul acestui test este de a descoperi dacă este posibil să se epuizeze resursele serverului făcându-l sa aloce un număr foarte mare de obiecte.	Este posibil să se epuizeze resursele serverului făcându-l sa aloce un număr foarte mare de obiecte.	Nu este posibil să se epuizeze resursele serverului făcându-l sa aloce un număr foarte mare de obiecte.
48	Test pentru User Input as a Loop Counter	Acest test se concentreaza asupra determinării dacă este posibil să se forțeze aplicația sa sara(sa faca o bucla) printrun segment de cod care are nevoie de resurse de calcul mari, cu scopul de a scădea performanța sa de ansamblu.	Este posibil să se forțeze aplicația sa sara(sa faca o bucla) printrun segment de cod care are nevoie de resurse de calcul mari.	Nu este posibil să se forțeze aplicația sa sara(sa faca o bucla) printrun segment de cod care are nevoie de resurse de calcul mari.

49	Test pentru Writing User Provided Data to Disk	Acest test este realizat pentru a stabili dacă este posibil sa se provoace o conditie de negare a serviciilor prin completarea discurilor țintă cu datele de log.	O conditie de Denial of Service poate fi provocata prin completarea discurilor tinta cu datele de log.	O conditie de Denial of Service nu poate fi provocata prin completarea discurilor tinta cu datele de log.
50	Test pentru DoS Failure to Release Resources	Scopul acestui test este sa determine daca aplicatia elibereaza in mod corespunzator resursele (fisiere si/sau memorie) dupa ce au fost folosite.	Resursele nu au fost golite corespunzator dupa ce au fost utilizate.	Resursele au fost golite corespunzator dupa ce au fost utilizate.
51	Test pentru Storing too Much Data in Session	Obiectivul testului este de a observa daca se aloca cantitati mari de date in sesiunea utilizatorului cu scopul de a determina serverul sa epuizeze resursele de memorie.	Cantitati mari de date pot fi alocate in sesiunea unui utilizator.	Cantitati mari de date nu pot fi alocate in sesiunea unui utilizator.
52	Test pentru politica de parole	Acest test verifica daca aplicatia impune o politica puternica de parole, in scopul de a preveni configurarea de parole slabe, usor de ghicit sau vulnerabile la atacuri de tip brute-force.	Aplicatia nu obliga la o politica puternica de parole.	Aplicatia forteaza la o politica puternica de parole.

Testare securitate la nivel infrastructura

Obiectivul testarii este sa gaseasca vulnerabilitatile solutiei, sa creasca gradul de incredere in solutie si sa reduca riscurile in cazul in care sistemul informatic este atacat.

Identificarea sistemelor de operare

Atunci cand se identifica componentele unei retele pentru un audit de securitate sau pentru inventariere sau administrare se doreste ca pe langa adresa IP a masini identificate sa se cunoasca si sistemul de operare ce ruleaza pe aceasta. Detectarea versiuni a sistemului de operare (de ex diferentierea intre Windows XP si Windows 7) este utila pentru a determina vulnerabilitati specifice pentru fiecare masina identificata.

Cod	TSS01
Nume test	Identificarea sistemelor de operare
Mod testare	Trimiterea de pachete speciale la nivel de retea catre masinile din retea, identificarea de servicii sau aplicatii specifice unui anumit sistem de operare.
Rezultate asteptate	Tip sistem de operare(Windows, Unix, Linux , OSX,Android,iOS), Versiune sistem de operare, Tip device(Server, statie de lucru, mobil, imprimanta, router/switch)

Identificarea patch-urilor de securitate lipsa pe un anumit sistem de operare

Lipsa patch-urilor de securitate poate provoca gauri de securitate ce pot compromite atat integritatea cat si confidentielitatea datelor ce se afla salvate pe o masina . In urma vulnerabilitatilor cunoscute, producatorii de sisteme de operare publica anumite patch-uri pentru a rezolva anumite problem de securitate. Aceast test verifica daca pe un anumit sistem de securitate aceste patch-uri acopera toate problemele de securitate.

Cod	TSS02
Nume test	Identificarea patch-urilor de securitate lipsa pe un anumit sistem de operare
Mod testare	Analizarea sistemului de operare si compararea patchu-urile instalate cu cele puse la dispozitie de catre producator.
Rezultate asteptate	Lista cu patchuri ne-aplicate pe un anumit sistem de operare.

Determinarea vulnerabilitatilor cunoscute la nivelul sistemelor de operare

Odata ce patchurile ce nu au fost instalate la nivel de sistem de operare au fost descoprite aceastea trebuie investigate pentru a determina daca prezinta o vulnerabilitate pentru sistemul de operare.

Cod	TSS03
Nume test	Determinarea vulnerabilitatilor cunoscute la nivelul sistemelor de operare
Mod testare	In urma identificarii unor patch-uri lipsa se va stabili daca exista probleme de securitate pe un anumit sistem de operare.
Rezultate asteptate	Lista cu vulnerabilitati per sistem de operare impreuna cu un scor de risc si criticalitate a fiecarei vulnerabilitati descoperite.

Identificarea porturilor deschise

In urma unei scanari se va identificara toate porturile deschise pe TCP si UDP si ce servicii ruleaza impreuna cu versiunea fiecarui daemon ce este alocat unui port (exemplu SMTP – port 25, DNS port 53).

Cod	TSS04
Nume test	Identificarea porturilor deschise
Mod testare	Conectare la toate porturile ale unei masini pentru a verifica daca sunt deschise.
Rezultate asteptate	Lista cu porturi deschise

Identificarea serviciilor care ruleaza pe un anumit port

In urma identificarii porturilor deschise se va identifica fiecare serviciu ce ruleaza pe fiecare port

Cod	TSS05
Nume test	Identificarea serviciilor care ruleaza pe un anumit port
Mod testare	Determinarea serviciilor ce ruleaza pe anumite porturi
Rezultate asteptate	Lista de servicii identificate sau aplicatii pentru fiecare port ce este deschis pe server.

Determinarea vulnerabilitatilor cunoscute la nivelul serverelor de aplicatii

In urma identificarii tuturor serviciilor se vor stabili probleme de securitate ce trebuiesc remediate pentru fiecare serivciu in parte.

Cod	TSS06
Nume test	Determinarea vulnerabilitatilor cunoscute la nivelul serverelor de aplicatii
Mod testare	Identificarea masinilor ce contin aplicatii vulnerablie sau aplicatii pe care nu au fost aplicate pachurile de securitate eliberate de dezvoltator.
Rezultate asteptate	Lista de vulnerabilitati gasite la nivelul aplicatiilor

Determinarea vulnerabilitatilor cunoscute pentru bazele de date

In urma identificarii unei baze de date pe un anumit sistem de operare se va stabili numele si versiunea acesteia si se va determina toate problem de securitate pentru aceasta.

Cod	TSS07
Nume test	Determinarea vulnerabilitatilor cunoscute pentru bazele de date
Mod testare	Identificarea masinilor ce contin baze de date sau sunt configurate ca un server SQL . Identificarea versiunii a limbajului SQL (MS SQL , MySQL, etc.)
Rezultate asteptate	Lista de vulnerabilitati gasite la nivelul bazelor de date.

Determinarea vulnerabilitatilor cunoscute la nivelul serviciilor active identificate

In urma identificarii unor servicii active pe un anumit sistem de operare se va stabili numele si versiunea acestuia si se va determina toate problem de securitate pentru aceste servicii.

Cod	TSS08
Nume test	Determinarea vulnerabilitatilor cunoscute la nivelul serviciilor active identificate
Mod testare	Se verifica serviciile identificate pentru anumite vulnerabilitati specifice pentru versiunea de serviciu gasita pe sistemul de operare.
Rezultate asteptate	Lista specifica de vulnerabilitati pentru un anumit serviciu

Identificarea vulnerabilitatilor la nivel de transport intre servere si/sau modulele componente

In urma testari protocoalelor de securitate la nivel de transport se v-or identifica vulnerablitati ce pot afecta confidentialitatea sau integritatea informatiilor in tranzit.

Cod	TSS09
Nume test	Identificarea vulnerabilitatilor la nivel de transport intre servere si/sau modulele componente
Mod testare	Se testeaza modulele SSL instalate pe server pentru a asigura ca nu sunt folosite protocoale necorenspunzatoare sau certificate ce sunt slabe.
Rezultate asteptate	Transmitera datelor se face peste SSL

Identificarea problemelor de configurare a serviciilor active

Se verifica daca exista parole si conturi administrative implicite, date sensitive expuse, lipsa autentificarii si/sau a autorizarii

Cod	TSS010
Nume test	Identificarea problemelor de configurare a serviciilor active
Mod testare	Se verifica daca parolele pentru conturile implicite au fost schimbate
Rezultate asteptate	Parolele / conturile implicite nu functioneaza