OMEGA TRUST

ANEXA E – Model raport de securitate

Va rugam sa regasiti atasat modelul de raport pentru serviciile ce urmeaza sa fie prestate.

COSMIN-MATEI MACANEATA

Digitally signed by COSMIN-MATEI MACANEATA
DN: cn=COSMIN-MATEI MACANEATA, sn=MACANEATA, givenName=COSMIN-MATEI, serialNumber=201104209CMM11, email=cosmin.macaneata@omega-trust.ro, o=OMEGA TRUST SRL, l=BUCURESTI SECTORUL 2, st=BUCURESTI, c=RO, title=ADMINISTRATOR
Date: 2022.10.27 11:09:20 +03'00'

OMEGA TRUST

Raport de evaluare a securitatii sistemului informatic

Nume client

Data

INFORMATIILE PREZENTATE IN ACEST DOCUMENT SUNT TRICT CONFIDENTIALE SI TREBUIE TRATATE CORESPUNZATOR

Nota juridica:

- Acest raport poate contine date confidentiale si private cu privire la **Nume client** si la sistemul informatic al acesteia.
- Acest raport nu poate fi prezentat catre terte parti fara acordul formal al prestatorului.
- Utilizarea sau reproducerea neautorizata a acestui document este interzisa.
- Evaluarile si testele au fost realizate de catre expertii OMEGA TRUST S.R.L..
- Acest raport prezinta toate vulnerabilitatile relevante cunoscute la momentul redactarii acestuia.
- Avand in vedere descoperirea continua de noi vulnerabilitati si aparitia unor noi amenintari, este recomandat ca evaluarile de securitate sa fie realizate la orice modificare majora a sistemului sau la cel mult 1 an de zile.

Detalii document:

Tip	Raport de evaluare a vulnerabilitatilor de securitate
Client	
Consultant	OMEGA TRUST
Versiune	1.0
Data	

Cuprins

1 INTRODUCERE

La solicitarea **Nume client**, Omega Trust a evaluat securitatea aplicatiei _____ accesibile din reteaua _____. Scopul acestei evaluari a fost de a detecta vulnerabilitatile existente la nivelul acesteia, atat pe partea de server, cat si pe partea de client.

Evaluarea a fost realizata de catre o echipa de testare a Omega Trust, avand personal specializat in teste de penetrare. Echipa a simulat un atac extern asupra aplicatiei, fara a avea cunostinte despre arhitectura acesteia, pentru a detecta nivelul de securizare, pentru a descoperi slabiciunile si pentru a oferi o serie de recomandari in privinta tratarii vulnerabilitatilor identificate.

Acest exercitiu cuprinde testarea aplicatiei si a tuturor functionalitatilor acesteia. Astfel, pentru a evalua securitatea aplicatiei, Omega Trust a incercat sa obtina informatii confidentiale si sa determine nivelul de securitate prin utilizarea unei game largi de mecanisme de detectie automate si manuale a vulnerabilitatilor.

Concluziile acestui raport prezinta situatia din timpul testarii si nu reflecta in mod automat starea actuala.

Testarea a fost realizata de catre Omega Trust, in perioada _____.

In prezentul raport sunt detaliate toate vulnerabilitatile si riscurile de securitate descoperite, impreuna cu recomandari pentru rezolvarea acestora.

Analiza cuprinde atat identificarea vulnerabilitatilor cunoscute folosind unelte de scanare automate, cat si atacuri manuale personalizate pentru specificul sistemului tinta corelate cu listele de vulnerabilitati top ten OWASP, top twenty SANS.

2 NOTE

Acest raport contine informatii in ceea ce priveste vulnerabilitatile existente in cadrul infrastructurii evaluate, precum si metodele privind exploatarea acestora.

Omega Trust recomanda luarea unor masuri speciale de precautie pentru a proteja atat confidentialitatea acestui document, cat si a informatiilor pe care acesta le contine. Omega Trust a pastrat si a securizat o copie a acestui document din considerente comerciale. Toate celelalte copii ale acestui raport au fost predate catre **Nume client**.

Evaluarea securitatii este un proces care se bazeaza pe experienta anterioara, pe informatiile disponibile in prezent si pe amenintarile cunoscute. Trebuie luat in considerare faptul ca toate sistemele de informatii depind de fiinte umane, avand astfel un anumit grad de vulnerabilitate.

Analiza prezentata in acest document se bazeaza pe tehnologiile si amenintarile cunoscute la data realizarii acestui raport. O data cu trecerea timpului, tehnologia si riscurile evolueaza, iar vulnerabilitatile asociate cu functionarea sistemelor **Nume client** descrise in acest raport, precum si masurile necesare pentru a reduce expunearea la astfel de vulnerabilitati se vor modifica.

Omega Trust nu isi ia angajamentul de a completa sau actualiza acest raport, in baza modificarii unor fapte sau circumstante care au fost aduse la cunostinta dupa data realizarii acestui raport.

Acest raport a fost elaborat de Omega Trust pentru a fi utilizat exclusiv de catre **Nume client** si se supune dreptului de proprietate asupra informatiei.

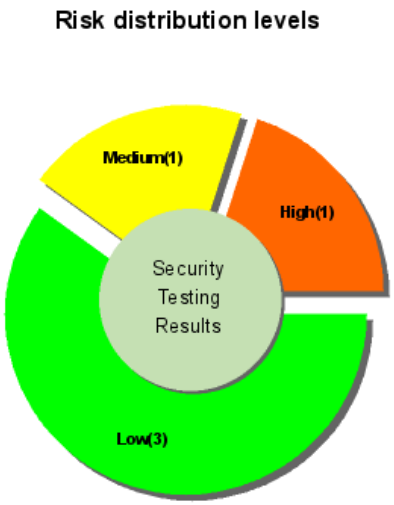
Contractul de confidentialitate dintre Omega Trust si **Nume client** reglementeaza divulgarea informatiilor din acest raport altor parti.

3 SUMAR EXECUTIV

Aplicatii in scop	
URLs	

3.1 VULNERABILITATI IDENTIFICATE

A fost detectat un numar de **5 vulnerabilitati** distribuite astfel pe nivele de risc: **1 vulnerabilitatate** cu **risc mare**, **1 vulnerabilitatate** cu **risc de nivel mediu** si **3 vulnerabilitati** cu nivel de **risc mic**. Nivelul de risc a fost estimat din punct de vedere al impactului tehnic asupra sistemului. Metodologia de calcul este prezentata in cap. 4.2 Metodologie evaluare nivel risc.



ID	Risc	Vulnerabilitate
1	**Mare**	Vulnerabilitate 1
2	**Mediu**	Vulnerabilitate 2
3	**Mic**	Vulnerabilitate 3
4	**Mic**	Vulnerabilitate 4
5	**Mic**	Vulnerabilitate 5

4 METODOLOGII UTILIZATE

4.1 METODOLOGII DE IDENTIFICARE A VULNERABILITATILOR

Tehnicile utilizate in identificarea si evaluarea vulnerabilitatilor se bazeaza pe cele mai bune practici in domeniu la nivel international:

- National Institute of Standards and Technology – NIST;
- Open Source Security Testing Methodology – OSSTM;
- Open Information Systems Security Group - OISSG;
- Open Web Application Security Project - OWASP.

4.2 METODOLOGIE EVALUARE NIVEL RISC

Riscul reprezinta probabilitatea ca o anumita amenintare-sursa sa exploateze o vulnerabilitate, precum si impactul acelui eveniment asupra organizatiei sau sistemului respectiv.

NIVEL RISC	VALOARE	ACTIUNI NECESARE
CRITIC	**75 – 125**	Actiune imediata pentru reducerea nivelului de risc.
MARE	**25 – 74**	Implementare de masuri corective cat mai curand posibil.
MEDIU	**5 - 24**	Implementare de masuri corective intr-o perioada rezonabila de timp
SCAZUT	**2 - 4**	Pot fi implementate anumite masuri corective sau se accepta riscul.
INFORMATIONAL	**1**	Reprezinta o observatie care nu determina un risc de securitate.

Nivelul de risc pentru fiecare vulnerabilitate este calculat folosind urmatoarea formula:

NIVEL RISC = VALOARE SEVERITATE (IMPACT) x VALOARE PROBABILITATE

VALOARE SEVERITATE (IMPACT TEHNIC)

Impactul negativ asupra informatiei gestionate de aplicatie si sistem, pierdere sau degradare sau o combinatie a acestora a urmatoarelor obiective ale securitatii: integritate, disponibilitate, confidentialitate.

NIVEL	SCOR	DESCRIERE
SCAZUT	**1 – 5**	Afectarea limitata a informatiilor sau sistemului; obtinerea de informatii utile pentru generarea unor atacuri.
MEDIU	**6 – 14**	Afectarea semnificativa a informatiilor sau sistemului; pierdere de informatii, indisponibilitate serviciu; acces limitat la sistem.
SEVER	**15 - 25**	Pierderi foarte importante ale informatiei, acces nelimitat la sistem; prejudicii la nivelul organizatiei

VALOARE PROBABILITATE

Probabilitatea ca o anumita vulnerabilitate sa fie exploatata de catre un atacator. La calcularea probabilitatii se are in vedere: motivatia atacatorului, nivelul de cunostinte necesar, usurinta in detectare si exploatare a vulnerabilitatii, nivelul de acces necesar si existenta unor masuri de detectie si prevenire.

NIVEL	SCOR	DESCRIERE
FOARTE MICA	**1**	Vulnerabilitatea nu este direct exploatabila
MICA	**2**	Vulnerabilitatea necesita un efort semnificativ si cunostinte avansate pentru a fi exploatata manual. Atacatorul ar putea avea nevoie de acces si cunostinte interne ale sistemului.
MEDIE	**3**	Vulnerabilitatea necesita cunostinte specifice si poate fi exploata cu instrumente disponibile public.
MARE	**4**	Vulnerabilitatea necesita anumite cunostinte si poate fi exploata fara instrumente speciale sau foarte usor de gasit si utilizat.
FOARTE MARE	**5**	Vulnerabilitatea necesita cunostinte foarte putine si poate fi exploata fara instrumente speciale.

5 TESTE EFECTUATE

In cadrul activitatii de evaluare a vulnerabilitatilor au fost efectuate urmatoarele tipuri de teste:

CODE	Test	Vulnerability	Status
Information Gathering			
SB-IG-001	Testing for Information Leakage though Search Engines	-	N/A
SB-IG-002	Testing for Metadata and Metafiles	-	PASS
SB-IG-003	Testing for Applications Version Disclosure	Vulnerabilitate 1	FAIL
SB-IG-004	Testing for Applications Discovery	-	PASS
SB-IG-005	Testing for Error Codes and Messages	Vulnerabilitate 2	FAIL
SB-IG-006	Testing for Sensitive Data Disclosure	Vulnerabilitate 3	FAIL
Configuration Management Testing			
SB-CM-001	Testing for Network and Infrastructure Configuration	-	PASS
SB-CM-002	Testing for Application Configuration Management	Vulnerabilitate 4	FAIL
SB-CM-003	Testing for Old Backup and Unreferenced Files	-	PASS
SB-CM-004	Testing for Admin Interfaces	-	PASS
SB-CM-005	Testing for HTTP Methods and XST	-	PASS
SB-CM-006	Testing for Browser Cache Management	-	PASS
SB-CM-007	Testing for HTTP Header Policies	-	PASS
SB-CM-008	Testing for Missing HSTS Header	-	PASS
SB-CM-009	Testing for RIA Cross Domain Policy	-	N/A
SB-CM-014	Testing For HTTP Host Header Poisoning	-	PASS
SB-CM-015	Testing For Web server directories and files enumeration	-	PASS
Identity Management			
SB-IM-001	Test Role Definitions	-	N/A
SB-IM-002	Test User Registration Process	-	N/A
SB-IM-003	Test Account Provisioning Process	-	N/A
SB-IM-004	Testing for Default or Guessable User Account	-	PASS
SB-IM-005	Testing for Weak or Unenforced Username Policy	-	N/A
Authentication Testing			
SB-AT-001	Testing for User Enumeration	-	PASS
SB-AT-003	Testing for Brute Force	-	PASS
SB-AT-004	Testing for Bypassing Authentication Schema	-	PASS
SB-AT-005	Testing for Password Caching	-	PASS
SB-AT-006	Testing for Captcha	-	N/A
SB-AT-007	Testing Multiple Factors Authentication	-	N/A
SB-AT-008	Testing for Race Conditions	-	PASS

SB-AT-009	Testing for Forceful Browsing	-	PASS
SB-AT-010	Testing for Authentication Logging	-	PASS
SB-AT-012	Testing for Weak Password Change or Reset Functionalities	-	PASS
SB-AT-013	Testing for Account Recovery functionalities	-	PASS
SB-AT-014	Testing for Remember Me functionalities	-	N/A
SB-AT-015	Testing for Username Uniqueness	-	N/A
SB-AT-016	Testing for Weak Password Policy	-	PASS
SB-AT-017	Testing for Weak Security Question Answer	-	N/A
SB-AT-018	Testing for Weaker Authentication in Alternative Channel	-	N/A
Authorization Testing			
SB-AZ-001	Testing for Path Traversal	-	PASS
SB-AZ-002	Testing for Bypassing Authorization Schema	-	PASS
SB-AZ-003	Testing for Privilege escalation	-	PASS
SB-AZ-004	Testing for Insecure Direct Object References	-	PASS
Session Management Testing			
SB-SS-001	Testing for Session Management Schema	-	PASS
SB-SS-002	Testing for Cookies Attributes	-	PASS
SB-SS-003	Testing for Session Fixation	-	PASS
SB-SS-004	Testing for Exposed Session Variables	-	PASS
SB-SS-005	Testing for Cross Site Request Forgery	-	PASS
SB-SS-006	Testing for Logout functionality	-	PASS
SB-SS-007	Testing Session Timeout	-	PASS
SB-SS-008	Testing for Session puzzling	-	PASS
Data Validation Testing			
SB-DV-001	Testing for Reflected Cross Site Scripting	-	PASS
SB-DV-002	Testing for Stored Cross Site Scripting	-	PASS
SB-DV-003	Testing for Local File Inclusion	Vulnerabilitate 5	FAIL
SB-DV-004	Testing for SQL Injection	-	PASS
SB-DV-005	Testing for LDAP Injection	-	N/A
SB-DV-006	Testing for ORM Injection	-	PASS
SB-DV-007	Testing for XML Injection	-	PASS
SB-DV-008	Testing for SSI Injection	-	PASS
SB-DV-009	Testing for XPath Injection	-	PASS
SB-DV-010	Testing for IMAPSMTP Injection	-	N/A
SB-DV-011	Testing for Code Injection	-	PASS
SB-DV-012	Testing for Command Injection	-	PASS
SB-DV-013	Testing for Buffer Overflow	-	PASS
SB-DV-015	Testing for HTTP Splitting Smuggling	-	PASS
SB-DV-016	Testing for URL Redirector Abuse	-	PASS
SB-DV-017	Testing for HTTP Verb Tampering	-	N/A
SB-DV-018	Testing for HTTP Parameter pollution	-	PASS
SB-DV-019	Testing for NoSQL injection	-	N/A
SB-DV-020	Testing for Remote File Inclusion	-	PASS
SB-DV-023	Testing for Format string	-	PASS
SB-DV-024	Testing for Insecure Deserialization	-	PASS
SB-DV-025	Testing for Server-Side Request Forgery	-	PASS
Cryptography			
SB-CR-001	Testing for Weak SSL TLS configuration	-	PASS
SB-CR-002	Testing for Padding Oracle	-	PASS

SB-CR-003	Testing for Sensitive information sent via Unencrypted Channels	-	PASS
Business Logic Testing			
SB-BL-001	Testing for Business Logic Data Validation	-	PASS
SB-BL-002	Test for Ability to Forge Requests	-	PASS
SB-BL-003	Test for Integrity Checks	-	N/A
SB-BL-004	Test for Process Timing	-	N/A
SB-BL-005	Test Number of Times a Function Can be Used Limits	-	PASS
SB-BL-006	Testing for the Circumvention of Work Flows	-	PASS
SB-BL-007	Test Defenses Against Application Misuse	-	PASS
SB-BL-008	Test Upload of Unexpected File Types	-	PASS
SB-BL-009	Test Upload of Malicious Files	-	PASS
Client Side Testing			
SB-CS-001	Testing for DOM based Cross Site Scripting	-	PASS
SB-CS-002	Testing for Cross Origin Resource Sharing CORS	-	PASS
SB-CS-003	Testing for Clickjacking	-	N/A
SB-CS-004	Testing for HTML Injection	-	PASS
SB-CS-005	Testing for CSS Injection	-	PASS
SB-CS-006	Testing for Client Side Resource Manipulation	-	PASS
SB-CS-007	Testing for Cross Site Flashing	-	N/A
SB-CS-008	Testing WebSockets	-	N/A
SB-CS-009	Test Web Messaging	-	N/A
SB-CS-010	Test Local Storage	-	PASS
Denial of Service			
SB-DS-001	Testing for SQL Wildcard Attacks	-	PASS
SB-DS-002	Testing for DoS Locking Customer Accounts	-	PASS
SB-DS-007	Testing for DoS Failure to Release Resources	-	PASS

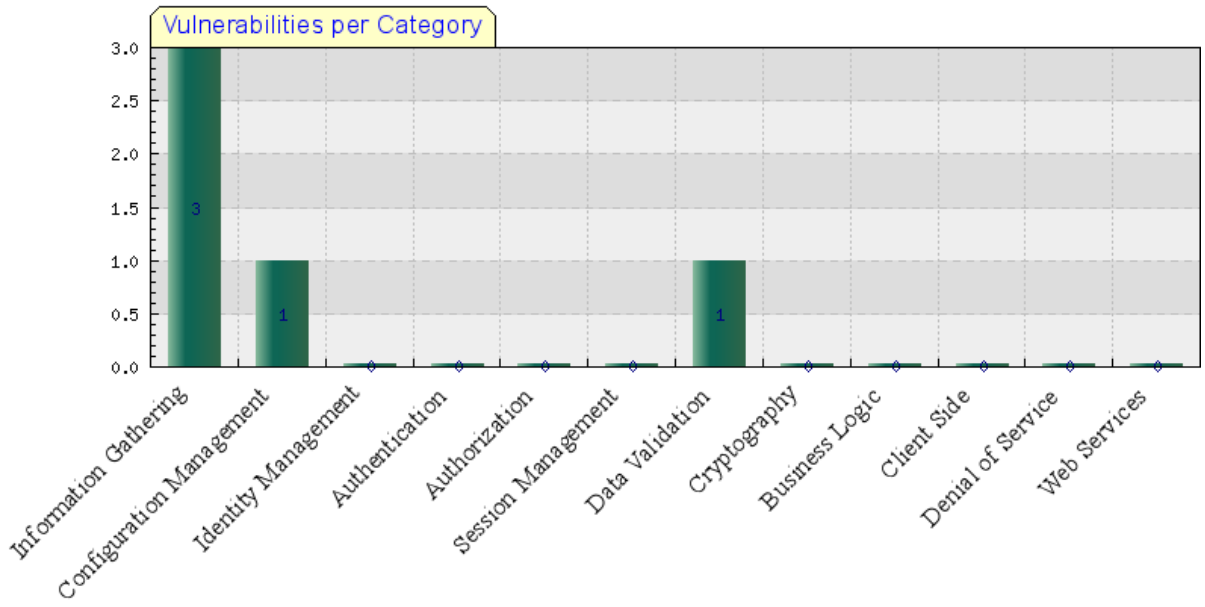
Legenda:
PASS: - Vulnerabilitate neconfirmata
FAIL: - Vulnerabilitate confirmata
N/A: - Vulnerabilitate netestata (nu se aplica)

6 VULNERABILITATI IDENTIFICATE LA NIVEL APLICATIE

6.1 LISTA VULNERABILITATI

Vid	Vulnerabilitate
1	Vulnerabilitate 1
2	Vulnerabilitate 2
3	Vulnerabilitate 3
4	Vulnerabilitate 4
5	Vulnerabilitate 5

6.2 DISTRIBUTIE VULNERABILITATI PE CATEGORII

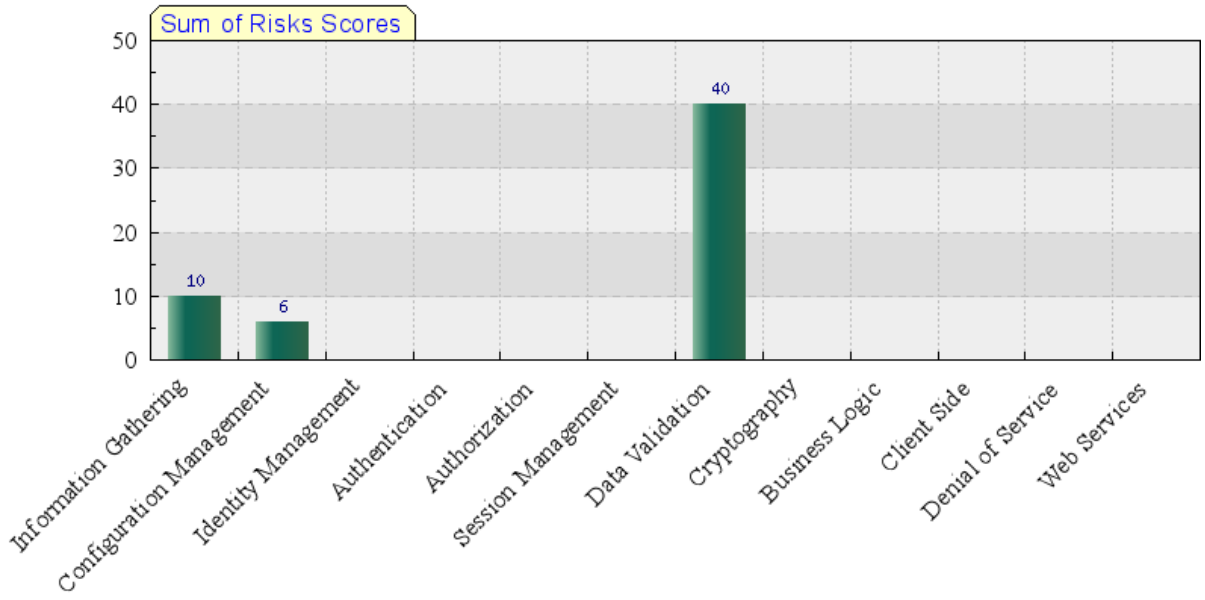


6.3 NIVELE RISC PER VULNERABILITATE

Nivelul de risc a fost estimat din punct de vedere al impactului tehnic asupra sistemului. Metodologia de calcul este prezentata in “cap. 4.2 Metodologie evaluare nivel risc”. Detalierea valorilor pentru fiecare vulnerabilitate se regaseste in “cap 6.4 Raport detaliat vulnerabilitati aplicatie”.

Level	Risk	ID	Vulnerability
High	40	1	Vulnerabilitate 1
Medium	6	2	Vulnerabilitate 2
Low	4	3	Vulnerabilitate 3
Low	3	4	Vulnerabilitate 4
Low	3	5	Vulnerabilitate 5

Graficul de mai jos prezinta nivelurile acumulate de risc pentru fiecare categorie. O valoare mare indica un risc crescut pentru o anumita categorie.



Nivele acumulate de risc

Categoria **Data Validation** are cel mai mare risc, cu o valoare cumulata de **40 puncte**.

6.4 RAPORT DETALIAT VULNERABILITATI APLICATIE

6.4.1 Vulnerabilitate 1

Sumar	
Risc	40 (Probabilitate: 4 | Severitate: 10)
Descrierea riscului	
Descrierea tehnica	
Mitigare	

6.4.2 Vulnerabilitate 2

Sumar	
Risc	6 (Probabilitate: 2 | Severitate: 3)
Descrierea riscului	
Descrierea tehnica	
Mitigare	

6.4.3 Vulnerabilitate 3

Sumar	
Risc	4 (Probabilitate: 2 | Severitate: 2)
Descrierea riscului	
Descrierea tehnica	
Mitigare	

6.4.4 Vulnerabilitate 4

Sumar	
Risc	3 (Probabilitate: 3 | Severitate: 1)
Descrierea riscului	
Descrierea tehnica	
Mitigare	

6.4.5 Vulnerabilitate 5

Sumar	
Risc	3 (Probabilitate: 3 | Severitate: 1)
Descrierea riscului	
Descrierea tehnica	
Mitigare	