UN UNEA EUROPEANĂ

Programul Operațional Capacitate Administrativă
Competența face diferența!

Instrumente Structurale 2014-2020

Sorin-Valentin Cirjan

Digitally signed by Sorin-Valentin Cirjan
Date: 2021.03.01 14:00:05 +02'00'

PLATFORMA INTEGRATA DE SERVICII ELECTRONICE DIN CADRUL PROIECTULUI „SOLUTII INFORMATICE INTEGRATE PENTRU SIMPLIFICAREA FURNIZARII SERVICIILOR CATRE CETATENI SI MEDIUL DE AFACERI SI OPTIMIZAREA PROCEDURILOR ADMINISTRATIVE LA NIVELUL MUNICIPIULUI RAMNICU-SARAT”, COD SMIS 129270

RAPORT DE TESTARE DE SECURITATE

Remis spre publicare către AM POCA

SIPOCA 647
SMIS 129270

Proiect finanțat din POCA

Versiunea 1.0

Număr exemplar: _____

CUPRINS

Precizări

- Acest raport prezinta toate vulnerabilitățile cunoscute la data elaborării lui
- Deoarece vulnerabilități noi sunt descoperite continuu și apar noi amenințări, se recomandă efectuarea unor evaluări de securitate la orice schimbare majoră a sistemului sau cel mult după un an.

Detalii ale documentului

Tip	Raport de testare de securitate
Versiunea	V1
Data	12.02.2021

1. Introducere

La solicitarea Furnizorului, IT Embassy a evaluat securitatea Portalului web de servicii pentru cetățeni al Primăriei Râmnicu Sărat, care poate fi accesat la adresa http://eservicii-eprimarie.primariermsarat.ro . Scopul evaluării este identificarea potențialelor vulnerabilități și a riscurilor de Securitate, alături de propunerea de recomandări și soluții tehnice menite să remedieze.

Acest exercițiu include testarea sistemelor identificate și a funcționalităților acestora. Am încercat să obținem informații confidențiale și să determinăm nivelul de securitate utilizând o gamă largă de mecanisme de detectare automată și manuală a vulnerabilităților

Concluziile acestui raport prezintă situația în timpul testării și nu reflectă automat starea actuală.

Testarea a fost efectuată de IT EMBASSY, în perioada 10 Februarie – 12 Februarie.

În acest raport, toate vulnerabilitățile și riscurile de securitate descoperite sunt detaliate împreună cu recomandări pentru a le rezolva.

Analiza include atât identificarea vulnerabilităților cunoscute utilizând instrumente de scanare automată, cât și atacuri manuale personalizate pentru specificul sistemului țintă legate de listele de amenințări Top Ten OWASP, Top Twenty SANS

2. Conținutul livrabilului

Acest document conține informații cu privire la vulnerabilitățile existente ale aplicației și infrastructurii evaluate și metodele de exploatare a acestora.

IT Embassy recomandă luarea de precauții speciale pentru a proteja confidențialitatea acestui document și a informațiilor din acesta.
Evaluarea securității este un proces bazat pe experiențe anterioare, informații disponibile și amenințări cunoscute. Trebuie luat în considerare faptul că toate sistemele informaționale sunt configurate si administrate de oameni, având astfel anumite grade de vulnerabilitate.

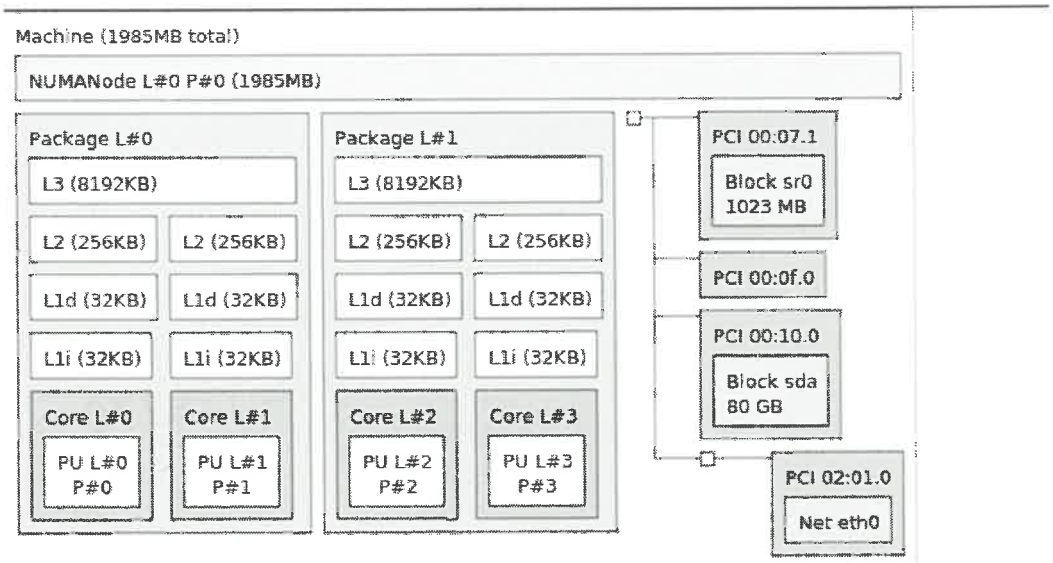
3. Rezumat

În cursul evaluării au fost verificate următoarele sisteme:

Aplicație web	Portal web de servicii pentru cetățeni al Primăriei Râmnicu Sărat
URL	http://eservicii-eprimarie.primariermsarat.ro

Pentru punerea in aplicare a planului de testare a securitatii, au fost folosite urmatoarele echipamente si software:

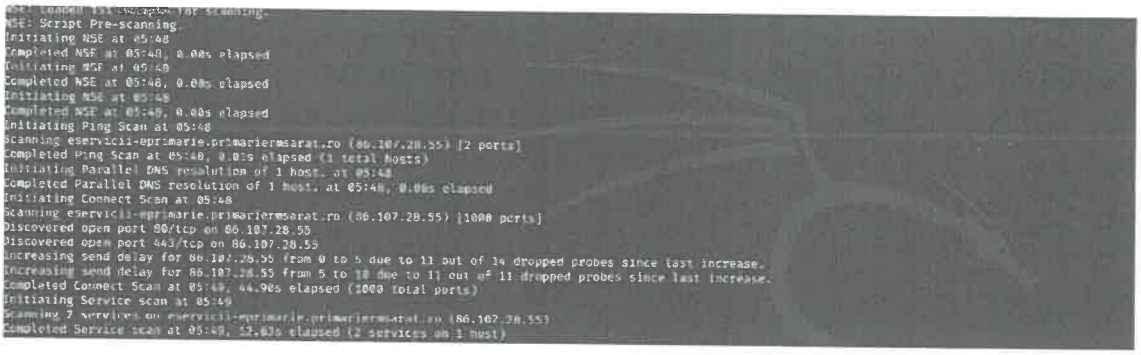
Mașină virtuala Vmware Workstation 16
OS: Kali Linux VMware 2020.4
Used RAM: 2 GB
Hardware: HP EliteBook 850 G6
Procesor: Intel Core i7-8565U@1.8 GHz
IP Address: 5.2.155.76



Au fost efectuate teste exploratorii pentru a înțelege sistemul care nu poate fi obținut prin cunoștințe publice sau documente de specificații. Apoi a fost creat un model de amenințare pentru a explora activele, amenințările, vectorii de atac și condițiile necesare pentru un atac cu succes. În cele din urmă, a fost dezvoltat un plan de testare pentru a ghida atacul și procesul de execuție a testelor, asigurându-se că fiecare cale de atac a fost acoperită cu atenție.

VULNERABILITĂȚI

Scanarea host-ului extern, folosind nmap, a identificat 2 porturi deschise catre exterior, permitand consultarea unor informatii referitoare la tipul de servere utilizate:




```
NSE: Script scanning 86.107.28.55.
Initiating NSE at 05:49
Completed NSE at 05:49, 8.33s elapsed
Initiating NSE at 05:49
Completed NSE at 05:49, 0.37s elapsed
Initiating NSE at 05:49
Completed NSE at 05:49, 0.00s elapsed
Nmap scan report for eservicii-eprimarie.primariermsarat.ro (86.107.28.55)
Host is up (0.019s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Microsoft IIS httpd 10.0
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-IIS/10.0
|_http-title: ePrimarie R\xC3\xA2mnicu S\xC4\x83rat
443/tcp open  ssl/http Fortinet security device httpd
|_http-favicon: Fortinet
| http-methods:
|   Supported Methods:  GET HEAD
|_  Potentially risky methods:
|_http-server-header: xxxxxxxx-xxxxx
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=FGT81ETK19005677/organizationName=Fortinet/stateOrProvinceName=California/countryName=
| Issuer: commonName=support/organizationName=Fortinet/stateOrProvinceName=California/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-08-29T07:05:19
| Not valid after:  2038-01-19T03:14:07
| MD5:   9f08 db31 ec01 ac14 9623 486f aec6 f904
|_SHA-1: 8a8f 7225 bb4f f29f 1b96 01c8 8867 daa2 4119 4d13
|_ssl-date: TLS randomness does not represent time
Service Info: OS: Windows; Device: security-misc; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 05:49
Completed NSE at 05:49, 0.00s elapsed
Initiating NSE at 05:49
Completed NSE at 05:49, 0.00s elapsed
Initiating NSE at 05:49
Completed NSE at 05:49, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.79 seconds
```

Nu au fost identificate vulnerabilități Nivelul de risc a fost estimat pe baza impactului tehnic asupra sistemului și a probabilității de exploatare. Metodologia de calcul este prezentată în capitolul. Metodologia de evaluare nivelurilor riscului.

4. Metodologii folosite

METODOLOGII PENTRU IDENTIFICAREA VULNERABILITATILOR

Tehnicile utilizate în identificarea și evaluarea vulnerabilităților se bazează pe cele mai bune practici din industrie la nivel internațional: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.

NIVELURI DE EVALUARE A RISCURILOR

Riscul reprezintă probabilitatea ca o anumită sursă de amenințare să exploateze o vulnerabilitate și impactul evenimentului respectiv asupra organizației sau sistemului respectiv.

RISK LEVEL	VALUE	REQUIRED ACTION
CRITICAL	75 – 125	Immediate action to reduce risk level.
HIGH	25 – 74	Implementation of corrective actions as soon as possible.
MEDIUM	6 - 24	Implementation of corrective actions in a certain period.
LOW	2 - 5	Implementation of certain corrective actions or accepting the risk.
INFORMATIONAL	1	An observation that does not determine a level of risk.

Nivelul de risc al vulnerabilităților este calculat utilizând următoarea formulă:

RISK LEVEL = SEVERITY VALUE (IMPACT) x PROBABILITY VALUE

SEVERITY VALUE	LEVEL	SCORE	DESCRIPTION

(TEHNICAL IMPACT)

Impactul negativ asupra aplicației gestionate și a informațiilor de sistem, pierderea sau degradarea sau o combinație a acestora cu următoarele obiective de securitate: integritate, disponibilitate, confidențialitate.

LOW	**1 – 5**	Damage limited of information or system, obtain useful information for generating attacks.
MEDIUM	**6 – 14**	Significant damage of information or system, loss of data, unavailability of service, limited access to the system.
SEVERE	**15 - 25**	Very important losses of information, unlimited access to the system, harm to the organization.

PROBABILITY VALUE

Probabilitatea ca o anumită vulnerabilitate să fie exploatată de un atacator. Calculul probabilității pe care îl are cu atenție: motivația atacatorului, nivelul la cunoștințele necesare, ușurința detectării și exploatării vulnerabilității, nivelul de acces necesar și existența măsurilor de detectare și prevenire.

LEVEL	SCORE	DESCRIPTION
VERY LOW	**1**	The vulnerability is not exploitable directly
LOW	**2**	The vulnerability requires a significant effort and advanced knowledge to be exploited manually. The attacker would need access and knowledge of the internal system.
MEDIUM	**3**	The vulnerability requires specific knowledge and can be exploited with available public exploit tools.
HIGH	**4**	The vulnerability requires some knowledge and can be exploited without special tools or tools can be easily found and used.
VERY HIGH	**5**	The vulnerability requires very few knowledge and can be exploited without special tools.

5. Teste efectuate

Au fost efectuate un număr de 86 de teste specifice bazate pe cele mai bune practici din domeniu. Nu au fost identificate vulnerabilitati.

COD	Test	Vulnerabilitate	Status
Information Gathering			
STI-IG-001	Testing for Information Leakage though Search Engines	-	PASS
STI-IG-002	Testing for Metadata and Metafiles	-	PASS
STI-IG-003	Testing for Applications Fingerprint	-	PASS
STI-IG-004	Testing for Applications Discovery	-	PASS
STI-IG-005	Testing for Error Codes and Messages	-	PASS
STI-IG-006	Testing for Sensitive Data Disclosure	-	PASS
Configuration Management Testing			
STI-CM-001	Testing for Infrastructure Configuration Management	-	PASS
STI-CM-002	Testing for Application Configuration Management	-	PASS
STI-CM-003	Testing for Old Backup and Unreferenced Files	-	PASS
STI-CM-004	Testing for Admin Interfaces	-	PASS
STI-CM-005	Testing for HTTP Methods and XST	-	PASS
STI-CM-006	Testing for Browser Cache Management	-	PASS
STI-CM-007	Testing for HTTP Header Policies	-	PASS
STI-CM-008	Testing for Missing HSTS Header	-	PASS
STI-CM-009	Testing for RIA Cross Domain Policy	-	PASS

Authentication Testing			
STI-AT-001	Testing for User Enumeration	-	PASS
STI-AT-002	Testing for Default or Guessable User Account	-	PASS
STI-AT-003	Testing for Brute Force	-	PASS
STI-AT-004	Testing for Bypassing Authentication Schema	-	PASS
STI-AT-006	Testing for Captcha	-	N/A
STI-AT-007	Testing Multiple Factors Authentication	-	N/A
STI-AT-008	Testing for Race Conditions	-	PASS
STI-AT-009	Testing for Forceful Browsing	-	PASS
STI-AT-010	Testing for Authentication Logging	-	N/A
STI-AT-012	Testing for Weak Password Change or Reset Functionalities	-	N/A
STI-AT-013	Testing for Account Recovery functionalities	-	PASS
STI-AT-014	Testing for Remember Me functionalities	-	PASS
STI-AT-015	Testing for Username Uniqueness	-	PASS
STI-AT-016	Testing for Weak Password Policy	-	PASS
STI-AT-017	Testing for Weak Security Question Answer	-	N/A
STI-AT-018	Testing for Weaker Authentication in Alternative Channel	-	N/A
Authorization Testing			
STI-AZ-001	Testing for Path Traversal	-	PASS
STI-AZ-002	Testing for Bypassing Authorization Schema	-	PASS
STI-AZ-003	Testing for Privilege escalation	-	PASS
STI-AZ-004	Testing for Insecure Direct Object References	-	PASS
Session Management Testing			
STI-SS-001	Testing for Session Management Schema	-	PASS

STI-SS-002	¤ Testing for Cookies Attributes	-	PASS
STI-SS-003	Testing for Cross Site Request Forgery	-	PASS
STI-SS-004	Testing for Logout functionality	-	PASS
STI-SS-005	Testing Session Timeout	-	PASS
STI-SS-006	Testing for Session puzzling	-	PASS
Data Validation Testing			
STI-DV-001	Testing for Reflected Cross Site Scripting	-	PASS
STI-DV-002	Testing for Stored Cross Site Scripting	-	PASS
STI-DV-003	Testing for Local File Inclusion	-	PASS
STI-DV-004	Testing for SQL Injection	-	PASS
STI-DV-005	Testing for LDAP Injection	-	PASS
STI-DV-006	Testing for ORM Injection	-	PASS
STI-DV-007	Testing for XML Injection	-	PASS
STI-DV-008	Testing for SSI Injection	-	PASS
STI-DV-009	Testing for XPath Injection	-	N/A
STI-DV-010	Testing for IMAPSMTP Injection	-	N/A
STI-DV-011	Testing for Code Injection	-	PASS
STI-DV-012	Testing for Command Injection	-	PASS
STI-DV-013	Testing for Buffer Overflow	-	PASS
STI-DV-015	Testing for HTTP Splitting Smuggling	-	PASS
STI-DV-016	Testing for URL Redirector Abuse	-	PASS
STI-DV-017	Testing for HTTP Verb Tampering	-	PASS
STI-DV-018	Testing for HTTP Parameter pollution	-	PASS
STI-DV-019	Testing for NoSQL injection	-	N/A

Cryptography			
STI-CR-001	Testing for Weak SSL TLS configuration	-	PASS
STI-CR-002	Testing for Padding Oracle	-	PASS
STI-CR-003	Testing for Sensitive information sent via Unencrypted Channels	-	PASS
Business Logic Testing			
STI-BL-001	Testing for Business Logic Data Validation	-	PASS
STI-BL-002	Test for Ability to Forge Requests	-	PASS
STI-BL-003	Test for Integrity Checks	-	N/A
STI-BL-004	Test for Process Timing	-	N/A
STI-BL-005	Test Number of Times a Function Can be Used Limits	-	PASS
STI-BL-006	Testing for the Circumvention of Work Flows	-	N/A
STI-BL-007	Test Defenses Against Application Misuse	-	N/A
STI-BL-008	Test Upload of Unexpected File Types	-	N/A
STI-BL-009	Test Upload of Malicious Files	-	N/A
Client Side Testing			
STI-CS-001	Testing for DOM based Cross Site Scripting	-	PASS
STI-CS-002	Testing for Cross Origin Resource Sharing CORS	-	PASS
STI-CS-003	Testing for Clickjacking	-	PASS
STI-CS-004	Testing for HTML Injection	-	PASS
STI-CS-005	Testing for CSS Injection	-	PASS
STI-CS-006	Testing for Client Side Resource Manipulation	-	PASS
STI-CS-007	Testing for Cross Site Flashing	-	N/A

STI-CS-008	Testing WebSockets	-	N/A
STI-CS-009	Test Web Messaging	-	N/A
STI-CS-010	Test Local Storage	-	PASS
Denial of Service			
STI-DS-001	Testing for SQL Wildcard Attacks	-	PASS
STI-DS-002	Testing for DoS Locking Customer Accounts	-	N/A
STI-DS-007	Testing for DoS Failure to Release Resources	-	PASS

PASS: - Unconfirmed vulnerability
FAIL: - Confirmed vulnerability
N/A - Untested vulnerability (not applicable)

6. Concluzii

Analiza întreprinsă de echipa IT Embassy se bazează pe cele mai bune practici din acest domeniu. În timpul testării, au fost utilizate metodologii și tehnologii recunoscute la nivel mondial. Echipa a funcționat din exterior, având cunoștințe minime despre infrastructura testată și folosind tehnici utilizate de hackerii de astăzi.

Recomandarea echipei IT Embassy este să fie aplicate update-urile de securitate, ori de câte ori acestea sunt disponibile.