

Università degli Studi di Napoli “Federico II”
Corso di Laurea Magistrale in Ingegneria Informatica

Corso di System Security
Prof. Valentina Casola

Elaborato di System Security

Matteo Arnese - M63001837
Pietro Conte - M63001868

Indice

1 Homework 1 - OpenSSL	4
1.1 Esercizio 1	4
1.2 Esercizio 2	5
1.2.1 Appunto	5
1.3 Esercizio 3	6
1.4 Esercizio 4	8
1.5 Esercizio 5	12
2 Homework 2 - Java Cryptography Architecture	13
2.1 Esercizio 1	13
2.1.1 Primo esercizio	13
2.1.2 Secondo esercizio	14
2.1.3 Terzo esercizio	14
2.2 Esercizio 2	18
2.3 Esercizio 3	20
2.4 Esercizio 4	21
2.4.1 Firma di un PDF con la chiave privata di Alice	23
2.4.2 Firma di un PDF usando CMS (Cryptographic Message Syntax)	23
2.5 Esercizio 5	24
3 Homework 3 - Configurazione Apache/Tomcat con HTTPS	26
3.1 Esercizio 1	26
3.1.1 Primo metodo	26
3.1.2 Secondo metodo	27
3.2 Esercizio 2	28
3.2.1 Utilizzo di Docker	31
3.2.2 Analisi Statica	31
3.2.3 Analisi Dinamica	32
3.2.4 Apache2	33
3.2.5 Apache Tomcat	40
4 Homework 4 - Configurazione di un meccanismo di Identity Management e Access Control	45
4.1 Pay n' Go Next	45
4.2 Access Control	47
4.2.1 AC-1 – Policy and Procedures	47
4.2.2 AC-2 – Account Management	47
4.2.3 AC-3 – Access Enforcement	49
4.3 Analisi delle minacce	49
4.3.1 NextJS – Use up-to-date framework and well-tested routines and dependencies	50

4.3.2	NextJS – Implement SQLi protections, e.g., parameterized queries	50
4.3.3	Keycloak – Require https communication	51
4.3.4	Keycloak – Enable brute force detection	51
4.3.5	Keycloak – Use specific redirect URIs	52
4.3.6	Keycloak – Apply authorization checks to segregate and control access to user data	52
4.3.7	Keycloak – Limit client token scopes	52
4.3.8	Keycloak – Require authentication before presenting restricted data	53
4.3.9	Keycloak – Set short code validity periods	53
4.3.10	Keycloak – Shorten token lifespans and enable revocation	54
4.3.11	Keycloak – Use high-iteration PBKDF2 hashing	54
4.3.12	PostgreSQL – Use parameterized queries and validate inputs	55
4.3.13	PostgreSQL – Enforce TLS encryption for all connections	55
4.3.14	PostgreSQL – Apply authorization checks to segregate and control access to user data	55
4.3.15	PostgreSQL – Enforce secure file permissions on PostgreSQL database files	56
4.3.16	PostgreSQL – Implement rate limiting and resource throttling	56
4.3.17	PostgreSQL – Implement robust authentication and role-based access control	57
4.3.18	PostgreSQL – Regularly update postgresql to the latest secure version	57
4.3.19	PostgreSQL – Require authentication before presenting restricted data	58
4.3.20	PostgreSQL – Implement secure backup procedures with encryption and access controls	58
4.3.21	Docker container – Apply the principle of least privilege in your image builds	58
4.3.22	Docker container – Enhance the security posture of your container images	59
4.3.23	Docker container – Ensure content trust for Docker is enabled	59
4.3.24	Docker container – Ensure sensitive host system directories are not mounted on containers	60
4.3.25	Docker container – Harden the container runtime environment	60
4.3.26	Docker container – Implement a hardened container runtime configuration	61
4.3.27	Docker container – Mitigate resource exhaustion by setting strict resource limits and policies	61

4.3.28	Docker container – Remove sensitive information from Dockerfile or Docker-Compose files	62
4.3.29	Docker container – Strengthen network security and segmentation	62
4.3.30	Nginx – Implement appropriate security headers	63
4.3.31	Nginx – Implement modern SSL/TLS protocols and disable weak protocols	63
4.3.32	Nginx – Reconfigure NGINX with only necessary modules . .	64
4.3.33	Nginx – Regularly update NGINX	64
4.3.34	Nginx – Remove unnecessary server headers	65
4.3.35	Nginx – Restrict HTTP methods	65
5	Homework 5 - Protezione delle credenziali	67
5.1	Hashicorp Vault	67
5.2	Configurazione	67
5.3	Analisi delle minacce	68
5.3.1	Hashicorp Vault – Avoid running HashiCorp Vault as root .	68
5.3.2	Hashicorp Vault – Apply authorization checks to segregate and control access to user data	69
5.3.3	Hashicorp Vault – Disable swap on the system hosting HashiCorp Vault	69
5.3.4	Hashicorp Vault – Enforce TLS for HashiCorp Vault in production	70
5.3.5	Hashicorp Vault – Require authentication before presenting restricted data	70
6	Controlli implementati	71
7	Riepilogo controlli	82