1.	Record Nr.	UNINA9910624378903321
Autore	Baker Matthew
Titolo	Secure Web Application Development : A Hands-On Guide with Python and Django / / by Matthew Baker
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2022
ISBN	9781484285961 1484285964
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (471 pages)
Disciplina	004.6
Soggetti	Internet programming Python (Computer program language) Web Development Python
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	1. Introduction -- 2. The Hands-On Environment -- 3. Threat Modelling -- 4. Transport and Encryption -- 5. Installing and Configuring Services -- 6. APIs and Endpoints -- 7. Cookies and User Input -- 8. Cross-Site Requests -- 9. Password Management.-10. Authentication and Authorization -- 11. OAuth2 -- 12. Logging and Monitoring -- 13. Third-Party and Supply Chain Security -- 14. Further Resources.
Sommario/riassunto	Cyberattacks are becoming more commonplace and the Open Web Application Security Project (OWASP), estimates 94% of sites have flaws in their access control alone. Attacks evolve to work around new defenses, and defenses must evolve to remain effective. Developers need to understand the fundamentals of attacks and defenses in order to comprehend new techniques as they become available. This book uses a hand-on approach to teach you how to write secure web applications and will highlight how hackers attack applications along with a broad arsenal of defenses. You'll see how to Implement the right defenses in Python/Django applications to prevent such attacks. Secure Web Application Development is your guide to picking the appropriate techniques to close vulnerabilities and ensuring you still provide users

with their needed functionality. You will: Understand common coding vulnerabilities and how to avoid them Configure services, such as databases and web servers, to minimize the risk of attack Implement secure methods for password management, authentication, and authorization Safely manage requests to and from external web sites Establish a framework for modelling and assessing risks.