Web Security Application

Becker, Joshua

Okereke, Uchechukwu Okpo

Shama, Muthuraman Venkatesan

Ulbrich, Damian

May 18, 2018

Contents

1 Introduction

Since the creation of the Internet, the world has seen it evolve with lots of practical applications. These include things like eCommerce, Instant Messaging, Video Streaming services and the likes. With this evolution and advancements, there has also been a rise in misuse and security concerns regarding identity theft, private data leaks etc.

One subset of eCommerce that is ever so popular is Online shopping, allowing consumers to directly buy goods or services from a seller over the Internet using a web browser. Consumers find a product of interest by visiting the website of the retailer directly or by searching among alternative vendors using a shopping search engine, which displays the same product's availability and pricing at different e-retailers. Customers must have access to the Internet and a valid method of payment in order to complete a transaction, such as a credit card, an Interac-enabled debit card, or a service such as PayPal. Hence, the element of security for user details is crucial.

In this project, we were tasked to create a simple eCommerce site called Webshop. We look to see how a user can interact with the online store and be able to make purchases with or without registering on the site while being safeguarded against security attacks. This report, documents the required specifications of the project, alongside how the requirements were implemented. Also, the challenges encountered during the course of the project.

2 Project Specification

2.1 Secure Session handling with Cookies and database

2.2 Timeout for Session and Tokens

2.3 Secure Storage of passwords

2.4 CSRF handling

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

2.5 XSS handling

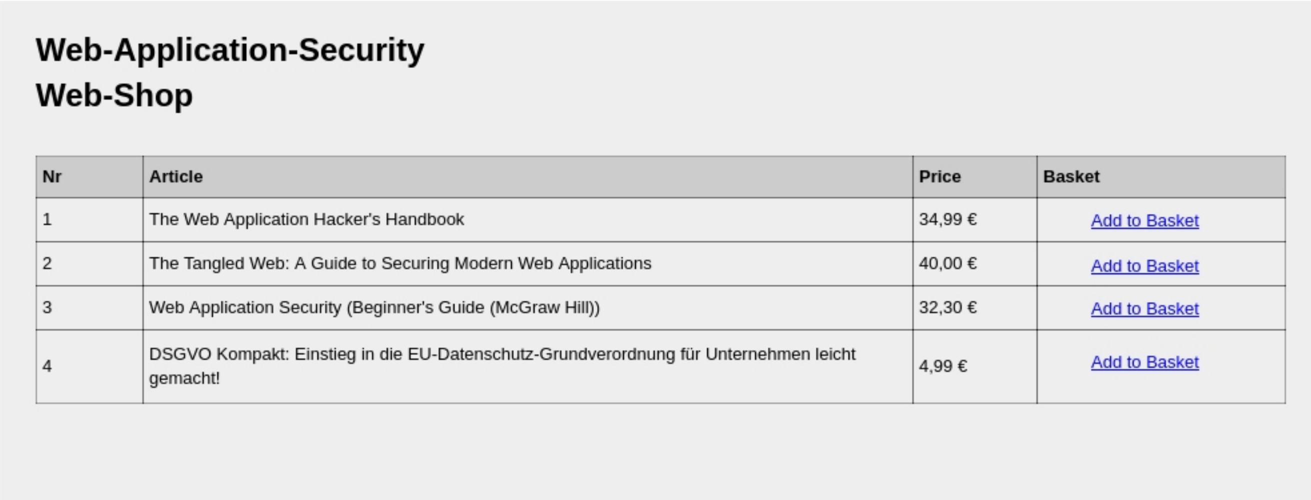
Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

2.6 SQL-injection handling

2.7 Secure logic design

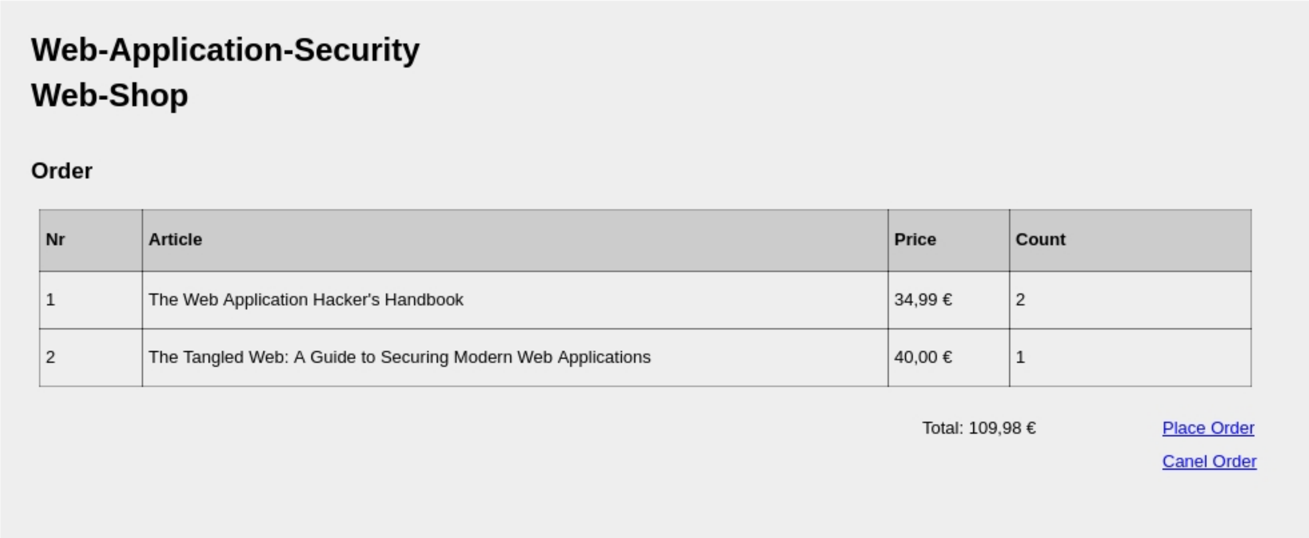
3 Problem Analysis

4 Implementation



Web-Application-Security
Web-Shop

Nr	Article	Price	Basket
1	The Web Application Hacker's Handbook	34,99 €	Add to Basket
2	The Tangled Web: A Guide to Securing Modern Web Applications	40,00 €	Add to Basket
3	Web Application Security (Beginner's Guide (McGraw Hill))	32,30 €	Add to Basket
4	DSGVO Kompakt: Einstieg in die EU-Datenschutz-Grundverordnung für Unternehmen leicht gemacht!	4,99 €	Add to Basket

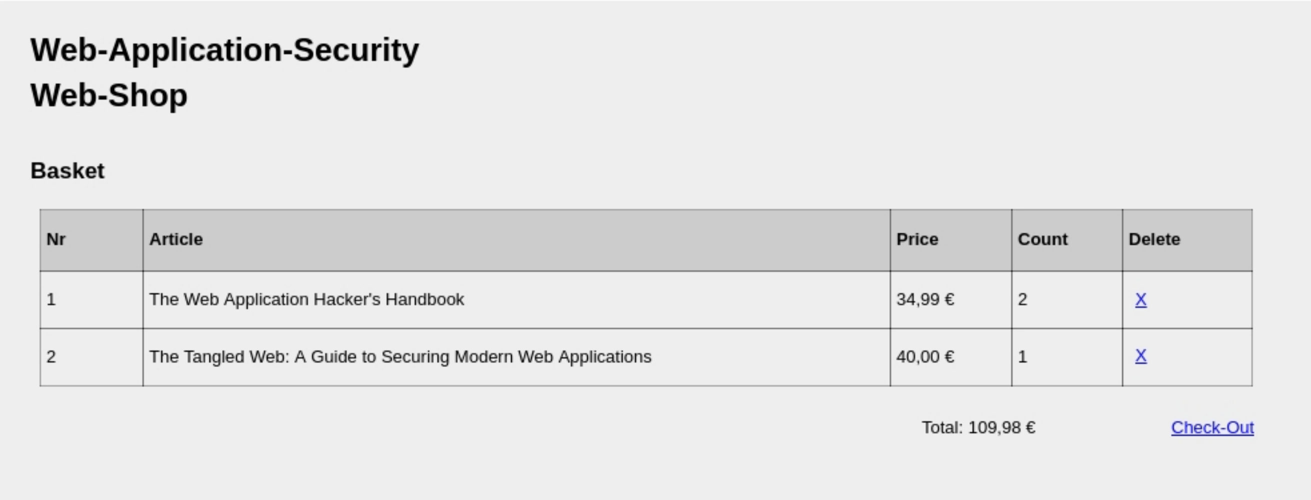


Web-Application-Security
Web-Shop

Order

Nr	Article	Price	Count
1	The Web Application Hacker's Handbook	34,99 €	2
2	The Tangled Web: A Guide to Securing Modern Web Applications	40,00 €	1

Total: 109,98 €



Web-Application-Security
Web-Shop

Basket

Nr	Article	Price	Count	Delete
1	The Web Application Hacker's Handbook	34,99 €	2	X
2	The Tangled Web: A Guide to Securing Modern Web Applications	40,00 €	1	X

Total: 109,98 €

5 Conclusion and Lessons Learnt