Website Penetration Report

http://infoseckma.usic.org.ua:1019

Tuesday, January 2, 2024

Prepared by Olesia Shevchuk

Introduction

The aim of this web penetration test is to help the technical personnel of the company to make the website more secure. Although this report contains technical terms, a non-technical explanation of the content - which can be found in the appendices - is given along with the test report, for the technical personnel and security consultant to review. This also makes it possible for them to reproduce the tests. Should the reader find it difficult to understand the penetration test report, go directly to the "Recommendations and Conclusions" section. This section contains executive information. For future help, we continue to be available to answer any of your questions.

Scope and approach

A security review was conducted internet-shop penetration test.

- gain unauthorized access to the systems, individual functions or critical internet-shop components,
- read or falsify data without authorization.

To do so, we have tested the internet-shop for the following issues:

- Cross-site scripting (XSS)
- SQL injection
- Path traversal
- OS command injection
- PHP insecure deserialization
- XML external entities

This was done to simulate as closely as possible the viewpoint of a completely external hacker. We tried to penetrate the website, specifically focusing on transactions and events happening in the internet-shop's front-end and back-end.

Tools

Manual testing activities	***Checking all application vulnerabilities by hand***
Burpsuite	Used to sniffer the parameters of application and URL
Manual testing	Checking all vulnerabilities of server by hand

Risk Classification

HIGH	The high-risk level indicates maximum risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to successfully exploit the underlying application and its data to modify application behavior to become other than it is, and is recommended to be handled with utmost priority.
MEDIUM	The medium risk level indicates considerable risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to exploit the underlying application and its data to a particular level so that the hacker can gain low-level information about the application. Such information can be used by a hacker to craft more specific attacks based on the information collected. The vulnerability marked with "Medium" should be mitigated at the earliest or soon after "High" risk vulnerabilities are mitigated.
LOW	The low-risk level indicates lowest risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to gain important information to the underlying application and its data to an informative level. Such vulnerability should be mitigated soon after the high and medium risk vulnerabilities are mitigated

HIGH	MEDIUM	LOW
2	0	0

Executive Summary

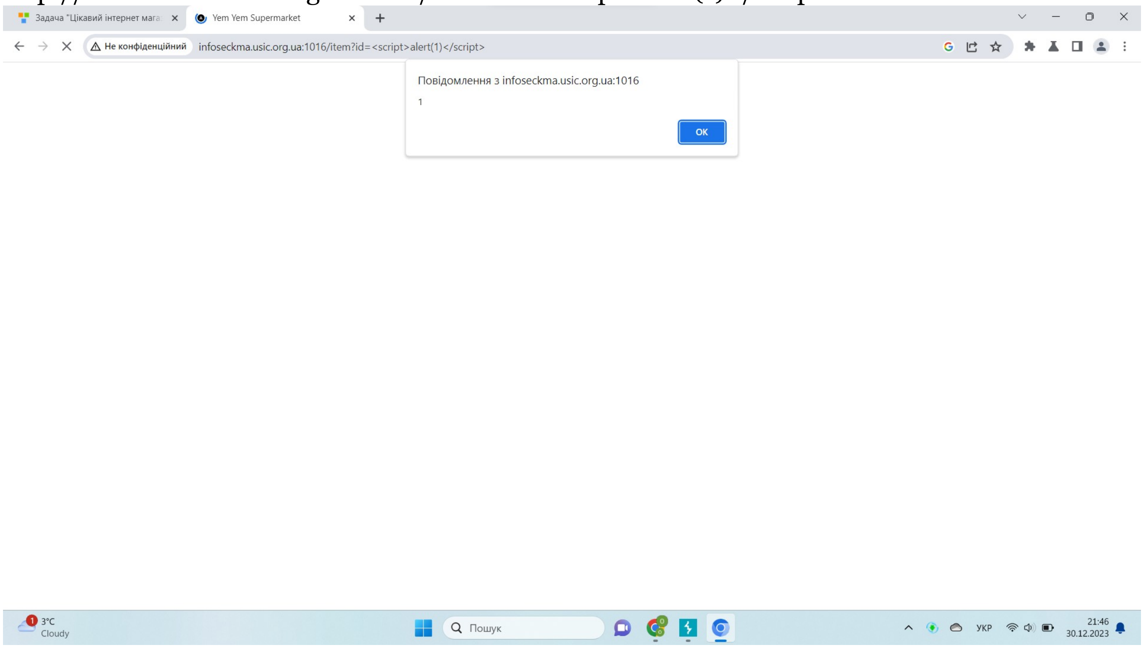
The level of danger is high. When testing the online store, it was possible to display a pop-up message, log in on behalf of the administrator, thanks to which access to the site's user lists, change the price of goods and its description.

Tech contact / report prepared by	Olesia Shevchuk
Release date	02.01.2024
Target domain name(s)	http://infoseckma.usic.org.ua:1019
Document classification	Confidential

Document control and details on scope

Description of vulnerability

When testing the online store, the following vulnerabilities were identified:
- an alert-message was triggered when a cross-scripting attack was carried out
http://infoseckma.usic.org.ua:1016/item?id=<script>alert(1)</script>


Задача "Цікавий інтернет мага
Yem Yem Supermarket
Не конфіденційний
infoseckma.usic.org.ua:1016/item?id=<script>alert(1)</script>
3°C
Cloudy
Пошук
УКР
21:46
30.12.2023

Повідомлення з infoseckma.usic.org.ua:1016

1

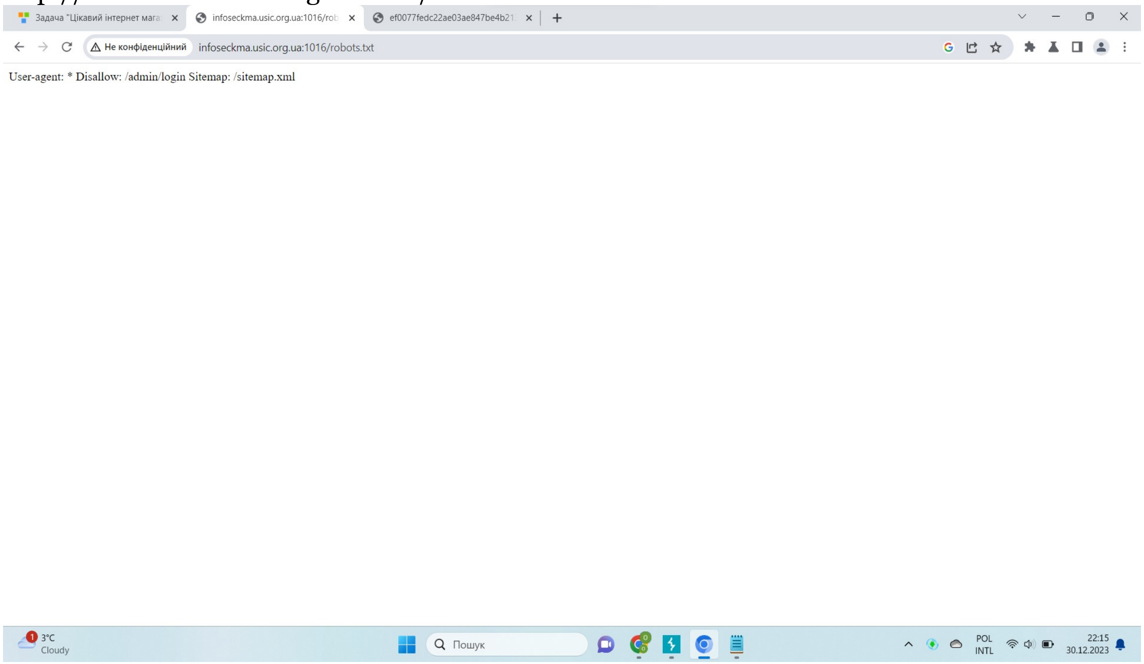
OK

- an SQL injection was attempted to gain access to the database. Access to the database was not obtained:

http://infoseckma.usic.org.ua:1016/item?id='ÚNION+SELECT+NULL –
http://infoseckma.usic.org.ua:1016/item?id='ÚNION+SELECT+NULL, NULL –
http://infoseckma.usic.org.ua:1016/item?id='ÚNION+SELECT+NULL,NULL,NULL--

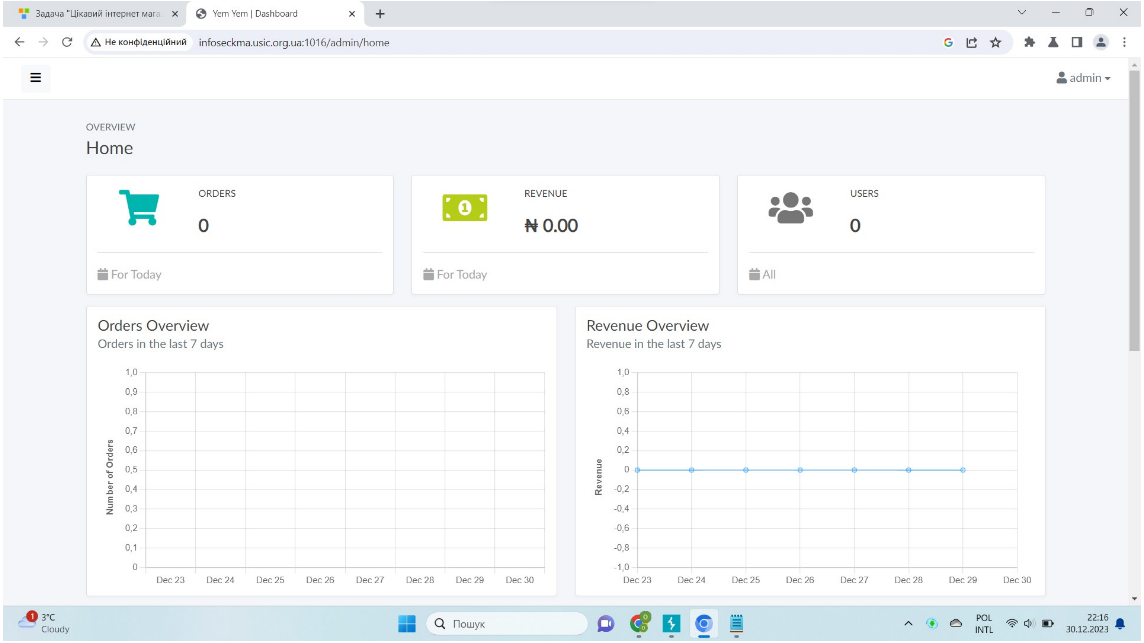
- access to robox.txt was obtained, as a result it was possible to gain access to the data of the admin-user, and therefore, in fact, access to the data of users of the internet-shop, the database of products and prices, sending messages to users of the internet-shop.

http://infoseckma.usic.org.ua:1016/robots.txt


Задача "Цікавий інтернет мага
infoseckma.usic.org.ua:1016/rob
ef0077fedc22ae03ae847be4b21
Не конфіденційний
infoseckma.usic.org.ua:1016/robots.txt
3°C
Cloudy
Пошук
POL
INTL
22:15
30.12.2023

User-agent: * Disallow: /admin/login Sitemap: /sitemap.xml

http://infoseckma.usic.org.ua:1016/admin/home



Obtaining the specified information by a real attacker can lead to serious financial losses for the owner of the internet-shop and for the users of the internet-shop, loss of reputation, etc.

Risk: HIGH

Client-Side Testing

OWASP Checklist and results

Test Name	Description	Tools	Result
Review Webserver Metafiles for Information Leakage	Analyze robots.txt and identify <META> Tags from website.	Browser, Burpsuite	Failed
Identify application entry points	Identify from hidden fields, parameters, methods HTTP header analysis	Browser, Burpsuite	Passed
Testing for Account Enumeration and Guessable User Account	Generic login error statement check, return codes/parameter values, enumerate all possible valid users	Browser, Burpsuite	Failed
Testing for Weak or unenforced username policy	User account names are often highly structured and valid account names can easily guessed.	Browser, Burpsuite	Failed
Testing for bypassing authentication schema	Force browsing, Parameter Modification, Session ID prediction, SQL Injection	Browser, Burpsuite	Passed
Testing for Bypassing Session Management Schema	SessionID analysis prediction, unencrypted cookie transport, brute-force.	Browser, Burpsuite	Failed
Testing for Exposed Session Variables	Encryption of session Tokens vulnerabilities, Send sessionID with GET method	Browser, Burpsuite	Passed
Testing for Cross Site Request Forgery	URL analysis, Direct access to functions without any token.	Browser, Burpsuite	Failed
Testing for Reflected Cross Site Scripting	Check for input validation, Replace the vector used to identify XSS, XSS with HTTP Parameter Pollution.	Browser, Burpsuite	Failed

Testing for SQL Injection	Union, Boolean, Error based.	Browser, Burpsuite	Failed
Testing for XPath Injection	Check for XML error enumeration by supplying a single quote (‘) Username: admin Password: admin	Browser, Burpsuite	Failed
Testing for Code Injection	Enter OS commands in the Input field. ?arg= 1, system (‘id’)	Browser, Burpsuite	Passed