# Contents

[Unit 1. REPLACE TEMPLATE TEXT – EXAMPLE ONLY Error! Bookmark not defined.](#_Toc27743478)

[1.1 Introduction to Magento Cloud Error! Bookmark not defined.](#_Toc27743479)

[Quiz Question 1.1.1 **Error! Bookmark not defined.**](#_Toc27743480)

[Exercise 1.1.1 **Error! Bookmark not defined.**](#_Toc27743481)

# Unit 2.3 - Defensive PHP Coding

### Exercise 2.3.1

Review the provided customer facing form for security vulnerabilities

> exercise\_1.php

If you have php installed on your machine, you can run this form on your local machine with the following command

> php -S localhost:8080 ./example\_1.php

Then visit:

> <http://localhost:8080>

**Solution**:

* Line 10 – XSS Vulnerability – Unescaped User Input to HTML Output
* Line 15 – XSS Vulnerability – Unescaped User Input to HTML Output
* Line 22 – XSS Vulnerability – Unescaped User Input to HTML Output
* Line 26 – XSS Vulnerability – Unescaped User Input to HTML Output
* Line 30 – XSS Vulnerability – Unescaped User Input to HTML Output
* Line 48 – RCE Vulnerability – Unescaped User Input to Shell Command

### Exercise 2.3.2

Review the provided admin facing form for sucurity vulnerabilities

> exercise\_2.php

If you have php installed on your machine, you can run this form on your local machine with the following command

> php -S localhost:8080 ./example\_2.php

Then visit:

> [http://localhost:8080](http://localhost:8080/)

**Solution**:

* Line 22 – XSS Vulnerability – Unescaped User Input to HTML Output
* Line 41 – XSS Vulnerability – Unescaped User Input to HTML Output
* Line 42 – XSS Vulnerability – Unescaped User Input to HTML Output