21HT-2DV702 - Internet Security
Assignment 3 - Web Security

LNU Student Shop - A Vulnerable Web Application

Faculty of Technology
Department of Computer Science

This document builds on the work by:
Uraz Odyurt

Instructor: Kristoffer Björklund & Nikolaos Papadopoulos
kb222wa@student.lnu.se
np222fc@student.lnu.se
2021-09-16

INTRODUCTION

For this assignment you will be working in a group of 2 people. The purpose of the third practical work is to get an insight in how a malicious entity might work when conducting an attack. By doing this you will hopefully see how you can better protect yourself, your potential business or employer against exploitation in the future. You will be faced with a number of challenges of different types, where some are easy, while others are really tough to solve. You get to try out a variation of challenges to test your skills and will have a lot of freedom in choosing the attacks you want to learn more about. In the second part, you will work with and learn about some of the tracking techniques on the Internet. You will also learn how to counter them

You are free to use any platform for this lab, as separate instances of the web application will be served to each of you on LNU's *CScloud* infrastructure. You will only need to access the URL designated to you. Practically speaking, the main (and maybe only) tool you need to negotiate this lab, is the developer tools of a capable web browser.

DEADLINE & SUBMISSION

The deadline for the third assignment is **Sunday the 24th of October, 23:55**. The group report should be limited to 10 pages and should clearly describe how you have solved the given challenges. For each challenge, you should discuss what could have been done to prevent you from realising the attack, i.e., from an administrator or developer's perspective. What would you do?

Submission of the report is done on *MyMoodle*; **observe that you must upload the report before the deadline as the system will not accept your file after this time**. Do not forget to put your names, group and student id on the front page of the Report Template and to convert it to `.pdf` before sending it in.

THE PLATFORM

This practical work takes place in a virtual system, *LNU Student Shop*, which is a vulnerable web application, hosted on LNU's *CScloud* infrastructure. As a result, you cannot have access to the source code as you would have on a local system. We have selected a number of relatively less complex challenges for this lab. The web application is written in JavaScript.

INSTRUCTIONS

You will be able to access your personal instance of the shop with the provided URLs on the course page. So where should you start? The first step is to follow a so-called *happy path* and get familiar with how different parts of the web application work. You will use browser developer tools to study underlying interactions and code. For this, we strongly recommend you to have a capable web browser, e.g., *Mozilla Firefox*. We will be providing hints about different challenges during the tutoring sessions. You are specifically required to use *John the Ripper* when solving task 13.

Do not forget, *for each challenge, you should discuss what could have been done to prevent you from realising the attack*. If you were the system administrator/developer, what would you do? You should add this after each task's solution, clearly separated.

Finally, you should familiarise yourself with *OWASP Top 10* classification of vulnerabilities from 2013 and from 2017. After going through the list, for each challenge you have solved, try to find which category applies and mention your reasoning. The category column in the scoreboard will almost provide this. We care about your reasoning.

As you will observe after solving the kick-starter challenge, LNU Student Shop has many vulnerabilities with different levels of exploitation difficulty. Feel free to choose and solve more challenges if you wish. However, you should limit your solution descriptions to 16 in your report, i.e., up to three extra challenges are allowed to be included in your report for bonus points. These three extra tasks will either compensate for missing tasks from section V, or will be considered as extra bonus points for the whole assignment. The rest, you can solve for fun and for your own learning.

You will be reading material, mostly online I presume, to get familiar with the concepts and tools for this lab. It is not allowed to take any provided solutions from the Internet. Try your best and ask for hints during the tutoring sessions. While we encourage you to share ideas with your classmates, at the same time, it is not allowed to share solutions.

At the end of the report you need to include a section describing what each person in the group has contributed to. If we feel that it is necessary, we will have a video meeting with both members to follow up on the work.

1. CHALLENGES

Kick-starter challenge

1. *Find the carefully hidden scoreboard page:*
   There is a hidden scoreboard present on this website, which will provide you an overview of available challenges, as well as the solved/unsolved status of them.

And the rest …

2. *Behave like any "white hat" should before getting into the action:*
   Read about this proposed standard from IETF and other resources. Can you check the security policy of LNU Student Shop?

3. *Access a confidential document:*
   There seems to be an unintended trade secret document left alongside other documents for this website. The "About Us" section might give you some clues.
4. *Use a deprecated B2B interface that was not properly shut down:*
   There are mechanisms on the website, allowing customers to communicate with the business owner. There might be a way to send a forbidden file type …

5. *Provoke an error that is neither very gracefully, nor consistently handled:*
   There are many ways to achieve this. Any bad request to a web server will be considered an error and the user will be notified, either in a proper manner, or in a way that would reveal the system's internals. You should be aiming for the latter.
6. *Let us redirect you to one of our cryptocurrency addresses, which are not promoted any longer:*
   This challenge is all about payments, so you know where to start. Take a look at the payment and merchandise section. What is happening to links?
7. *Perform a DOM XSS attack with*
   `<iframe src="javascript:alert(`xss`)">`*:*
   Challenges 7 and 8 will result in identical output for the average user. Knowing the difference will enable you to choose the right place for this type of XSS.
8. *Perform a reflected XSS attack with*
   `<iframe src="javascript:alert (`pwned`)">`*:*
   Challenges 7 and 8 will result in identical output for the average user. Knowing the difference will enable you to choose the right place for this type of XSS.
9. This is a theoretical task. Explain the difference between DOM-based and reflected XSS that you had to deal with in the above two challenges. How can you observe the difference?
10. *Follow the DRY principle while registering a user:*
    Study what the DRY principle is. Try to apply it to the user registration process and exploit a vulnerability.

11. *Give a devastating zero-star feedback to the store:*
    The website has a mechanism for rating the shop. It will not accept a zero-star feedback, or maybe it does…?
12. *View another user's shopping basket:*
    Try adding an item into your own basket. Observe what type of client-side association exists to a user's basket. Can you manipulate it?

13. *Log in with the administrator's user credentials:*
    Luckily, someone has leaked a piece of information that seems to be some form of admin password, *"0192023a7bbd73250516f069df18b500"*. Can you crack it?

2. CHECK YOUR ONLINE FINGERPRINT

1. Start by directing your web browser to this link. This is your online fingerprint. Explain the information included in this fingerprint and whether it poses any threat to your privacy or not. As the list is long, try to focus on important fields and explain the risks. If you were in an intruder's shoes, which items would have been more useful for you?

2. Search for different ways to change your online fingerprint. Now use the same link again. Perform the following changes:
   (a) The link should show that you are from *Russia*, *Moscow* region.
   (b) Click on the link once more. This time your operating system and browser should appear as *Microsoft Windows XP* and *AOL version 9*, respectively.

3. Explain what *Canvas Fingerprinting* is and check if different web-browsers are vulnerable against the practice or not, by browsing to this link. You should consider Firefox, Chromium and Tor Browser. How does the Tor Browser handle it? How about your everyday web browser? Is it vulnerable against the practice? You can read more on the topic here and here.

Include screenshots from your results and explain the steps you have taken, along with the tools you have used. Do not forget to reference your sources, online tools, etc according to IEEE.