SecurityEdu

by

Jacob, Tan, Quan, Rui, Nhat

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology AND/OR Cybersecurity

Jacob Gardner ____ 4/9/2023
STUDENT 1 Date

Tan Nguyen ____ 4/9/2023
STUDENT 2 Date

Quan Do ____ 4/9/2023
STUDENT 3 Date

Nhat Le ____ 4/9/2023
STUDENT 4 Date

Rui Zhou ____ 4/9/2023
STUDENT 5 Date

ADVISOR, Faculty Advisor Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Service

Table of Contents

LIST OF FIGURES

ABSTRACT

SecurityEdu was designed to gather information on the fast-growing world of cyber to help individuals who are new or sharpen the skills of a more experienced user in this area. The design of this project was to have information on how to properly secure your personal data whether this was through a personal device such as a laptop, smart phone, or securing your business and protecting your companies' data from potentially being stolen. Our site was designed to give information on how to secure all of these in the most updated ways from trusted sources such as Microsoft and was updated with new security vulnerabilities automatically.

INTRODUCTION

1.1 Introduction

Most people have multiple mobile devices and personal computers, which store a lot of personal information and personal data. But many people do not realize that this information is not so secure in the device, in other words, people may just need to do some learning to avoid most security information problems. What we want to do is to let people use our content, avoid some self-inflicted data leakage problems, and improve the security of personal computers and devices.

1.2 Problem

Many people leak their information because of a lack of understanding of security knowledge. For mobile phones, many people have given sufficient permissions to the app after downloading, and there is a possibility of data leakage. For example, 36% of apps downloaded on mobile devices will request access to your camera (Mikalauskas, 2022). If your account or data is compromised, then your camera may be accessed by a malicious user. This is also possible with your microphone and many other capabilities on mobile devices. Some bad developers will obtain user information, conduct data analysis, and even sell. For personal computers, many people do not know how to carry out a basic security configuration, or for some people, the need is to strengthen the defense of their personal computer. What we want to do is to let people use our content, avoid some self-inflicted data leakage problems, and improve the security of personal computers and devices.

1.3 Solution

SecurityEdu is a website to help users to reduce the possibility of information leakage and security issues by introducing information and specific steps to show users how to properly configure the settings using the controllable settings in mobile devices and PCs. The same is true for personal computers, but in addition, add defense mechanisms and methods on how to strengthen personal computers and small businesses.

1.4 Project Goals

The goal of our Securityedu project in the short term is to implement the groups around us, so that they can obtain the security configuration information and methods of mobile phones and personal PC devices by using the project products. And then through the proliferation of users, in the long-term goal, more users can participate in this project, and let these users learn how to improve the defense mechanism in the PC, and understand the basic configuration in the mobile phone, to improve people's awareness of Internet security and technology. In general, in the short term, it will be used by a small number of users, and in the long term, we hope that all users can get the help of security technology and improve their awareness of network security. Users can largely protect their mobile phones from unknown risks and improve the defense mechanism of computers or servers. We are even more looking forward to indirectly affecting developers through this product, enabling them to reduce unnecessary access to user permissions, information collection, and to increase the emphasis on users' personal privacy information.

1.5 Overview

Data leakage and lack security has been one of the most dangerous problems with technology implemented into all aspects of our daily lives. Our main goal is to help users to have a resource to educate themselves about information security in different types of devices and platforms. To achieve that, we create a website that has vulnerabilities and exploits for PCs, mobile devices, and Active Directory, so that users can use it as references to prevent cyber-attacks. This information can help users increase their knowledge to better understand and prevent threats that may occur when using mobile devices, computers, administering servers, and developing web applications. It can also allow more people to pay attention to current safety issues and learn how to prevent and deal with them.

DISCUSSION

2.1 Project Concept

Our inspiration for this project concept came from the large growth of cyber technology in the world and how it is becoming more important every day to secure your device and protect yourself and your information. For example, 36% of apps downloaded on mobile devices will request access to your camera (Mikalauskas, 2022). With the lack of cybersecurity knowledge for an average user, this is just one example of a potential security threat. There is plenty of data all over the internet, and if you take time to look in different places on how to secure different parts of each device it is very possible to find it. However, it takes time to look through all of that information, especially when you are new to the cyber realm. Our website will have all of this information laid out in an organized and up to date website that will pull real-time information from these trusted sources like Microsoft and Apple to help secure these devices.

2.2 Design Objectives

The primary objective of our application is to create an informational webpage to help end users secure their personal laptops, mobile devices, and active directory. Our website will host all of the necessary information that an end-user would be recommended to use to secure their personal device.

The website will automatically pull the latest updates and known vulnerabilities from online sources such as Microsoft or Apple. We will do this by scrapping their websites where these vulnerability patches come out and will have them linked and displayed under our site. This will create a way for end users to find all the information that they need in one organized layout.

The website will be easy to navigate, simplistic, and fluid as we expect our end users to be less experienced with this type of information.

2.3 Methodology and Technical Approach

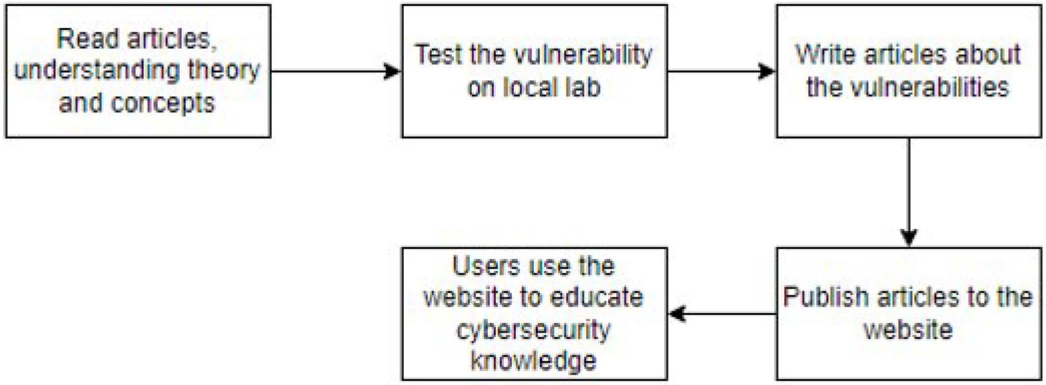

Read articles, understanding theory and concepts
Test the vulnerability on local lab
Write articles about the vulnerabilities
Publish articles to the website
Users use the website to educate cybersecurity knowledge

Figure 1: Research Process

We will research different vulnerabilities websites and databases to learn more about how hackers exploit vulnerabilities in PCs, mobile devices, and websites. After that, we will research deeply on how to perform those attacks and defend against those vulnerabilities to document different configurations that users can apply to their PCs or code to be more secure. References on where we get our data are:

a. Vulnerabilities and exploits

- https://book.hacktricks.xyz/

- https://attack.mitre.org/
- https://www.cvedetails.com/
- https://www.exploit-db.com/

b. Defense resources

- https://d3fend.mitre.org/
- https://adsecurity.org/
- https://owasp.org/

Our website is mainly for users researching security and want to make their system secure with different vulnerabilities related to mobile, PCs, and Active Directory. By using the content of SecurityEdu, users will be able to understand the concept of the vulnerability, how the exploit works, and how they can configure their system to prevent that vulnerability.

c. Article structure

Most of our articles are based on the same structure, which include:

- What are the concepts of vulnerability?
- How the vulnerability work?
- Practical examples of vulnerability on local lab
- Remediation/mitigation
- References

2.4 User Profiles/Personas

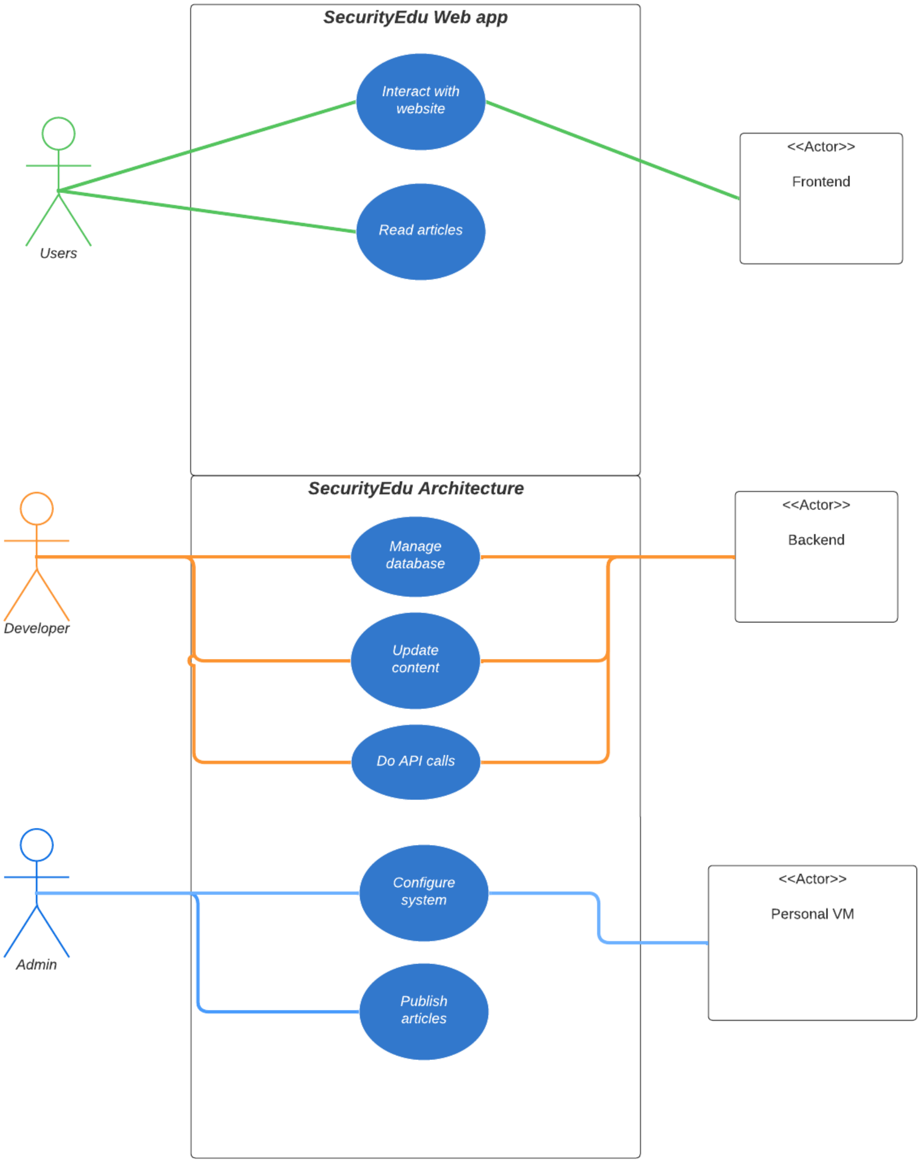
The primary users of SecurityEdu are people who wants to educate themselves about cybersecurity, including researchers, students, and teachers. Users can use data on our website to learn more about different types of cyber-attacks and how to defense against them. Moreover, the developers and administrators need to use the website to update new features and content.

User Profile 1
Application Github, Azure VMs, Django, Nextjs framework
Potential Users Developers and Cybersecurity Administrators.
Software and Interface Experience Users should have web development experience to create the web application with a decent interface. Additionally, users should know database management for constructing queries for website articles.
Experience with Similar Applications Users need to have experience with the fundamentals of web development such as: HTML, CSS, JavaScript, and database. Additionally, Cybersecurity Administrator needs to understand deeply with cybersecurity concepts to write and publish articles to the website.
Task Experience Task experience with web development and cybersecurity aspects listed above for the creation and maintenance of the application.
Frequency of Use Frequency of use will be high during the website development phase. Developers will create and update features, including the content and backend APIs. Cyber Administrators will research different topics in security and write articles for the site.

Key Interface Design Requirements that the Profile Suggests The web application needs to have ease of use, sufficient information about vulnerabilities.

User Profile 2
Application SecurityEdu web application
Potential Users Students, teachers, and cybersecurity researchers
Software and Interface Experience Users just need to be familiar with using web browsers to read through the content of our website.
Experience with Similar Applications Chrome, Firefox, Opera
Task Experience Navigate through website to read articles about specific topic.
Frequency of Use Anytime users need to research topics related to Mobile, PCs, and Active Directory security.
Key Interface Design Requirements that the Profile Suggests Easy to navigate and understand the articles' topic. Good instructions on how to configure the system securely.

2.5 Use Case Diagrams



Here is the use-case diagram of our project. The users will interact with the website to read articles. Our developer will manage the database to update the content and do API calls to update the vulnerability database. And our cybersecurity researcher in the team will research, build a lab environment to understand more about the vulnerability, write the articles about it and publish it to the website.

2.6 Technical Architecture

The product of our project is a web application consisting of the front-end and the back-end. For the front-end, we use NextJS as our framework after much consideration about ease of development, community adaptation and familiarity. The back-end makes use of the Django framework mainly because of our developer's experience using Python. Our project's vision for the application at first is simple so there aren't a lot of criteria to choose our frameworks on. But it is important to note that our framework choices here will not affect future expansion if needed.

For our database, our team is currently using the default database of Django. Our data will be stored in a file call db.sqlite3 and consists of 2 following tables:

- Categories: This table is for creating categories for different vulnerabilities, there's currently 3 categories: PCs/Laptops, Enterprises, and Mobile
- Articles: This table is for containing the articles' data: title, date created, content, and category

2.7 Testing

For the front-end, we test our website through three main types of testing. First, we have functional testing, which verifies that all links, buttons, and interactive elements are working correctly. Second, we have usability testing, which makes sure that the page layout stays the same and easy to navigate. Finally, we have cross-browser compatibility testing, which includes testing that the sites functionality works across multiple browsers like Chrome, and Firefox. Below, we will list the objectives of each test case which is followed by the conditions and results.

For the back-end testing, besides from testing with the console, we also use Postman, an app that can send request to our API, to test the response that the back-end send back after receiving a request.

OBJECTIVES	
FRONT END 1	Test functionality of buttons (function, animation)
FRONT END 2	Test functionality of links (function)
FRONT END 3	Test functionality of interactive elements (function, animation)
FRONT END 4	Test third-party APIs (Microsoft, CVS Detail)
FRONT END 5	Test search function
FRONT END 6	Test article display (image display, code display)
FRONT END 7	Test login for admin
FRONT END 8	Test post submission for admin
FRONT END 9	Test post deletion for admin

CONDITIONS	PASS	FAIL
FRONT END 1	Buttons work correctly	Buttons don’t work (no effect)
	Buttons show animation	Buttons no animation
FRONT END 2	Links redirect correctly	Links don't redirect
FRONT END 3	Interactive element work	Interactive element doesn’t work
	Show animation	Doesn’t show animation

FRONT END 4	Calls correct API API shows all information	Invalid API No information shown
FRONT END 5	Search shows correct posts	Search shows no post or doesn’t work correctly
FRONT END 6	Image + Code is displayed correctly	Image + Code displayed incorrectly
FRONT END 7	Admin can login	Login doesn’t work
FRONT END 8	Post submits correctly and database is updated	Post doesn’t submit or database doesn’t update
FRONT END 9	Post deletes correctly and database is updated	Post doesn’t delete or database doesn’t update

CONDITIONS	RESULT	FEEDBACK
FRONT END 1	Passed	N/A
FRONT END 2	Passed	N/A
FRONT END 3	Passed	N/A
FRONT END 4	Passed	N/A
FRONT END 5	Passed	N/A
FRONT END 6	Passed	N/A
FRONT END 7	Partial Pass	Login works fine using Firefox but doesn’t work on Chromium based browsers.
FRONT END 8	Passed	N/A
FRONT END 9	Passed	N/A

2.8 Budget

Our project will use Azure to host our web application. Our current plan will make use of Azure's free App Service option and host our application there. If the need arises later to scale our database/storage, we can migrate our project within the Azure system easily. Within Azure, the Virtual Machine option with lowest cost starts at $13.14 per month and consists of 1 Core, 0.75 GB RAM and 20 GB Storage. Other than the hosting solution, all our tools and applications used for development are freeware and do not count towards our budget.

2.9 Project Plan

Our project plan is to gather information on the most likely types of attacks/data leaks on these mobile or personal devices. We will do most of this manually by conducting research on these types of attacks and on how to prevent them. We also plan on adding to the backend of our project a tool that is able to pull public data relating to these attacks, so the user has updated/more information. We will have this updating website that shows these threats and how you can take steps to secure your personal device so users can take the best steps to secure their personal devices. Presented below is a timeline table of our tasks.

Task #	Task Name	Duration (days)	Start Date	End Date
1	**Project Management and Deliverables**	**232**	**8/25/22**	**4/13/23**
1.1	Team Building	7	8/25/22	8/31/22
1.2	Ideas and Brainstorming	7	8/25/20	8/31/22

1.3	Team Members and Project Name	1	8/25/20	8/25/22
1.4	Team Contract	7	8/25/20	8/31/22
1.5	Team Contract Resubmission	5	10/1/22	10/5/22
1.7	Research ways to configure personal device security	7	10/5/22	10/12/22
1.8	Research ways to configure applications security	7	10/5/22	10/12/22
1.9	Analyze methods for improving personal device security	7	10/5/22	10/12/22
2.0	Analyze methods for improving application security	7	10/5/22	10/12/22
2.1	Implement methods for improving personal device security	7	10/12/22	10/19/22
2.2	Implement methods for improving application security	7	10/12/22	10/19/22
2.3	Document findings for personal device security	7	10/12/22	10/19/22
2.4	Document findings for application security	7	10/12/22	10/19/22
2.5	Proofread the documents	7	10/20/22	10/21/22
2.6	Research on different web development stacks	14	09/19/22	10/02/12
2.7	Develop first draft of front-end using NextJS	14	10/03/22	10/16/22
2.8	Hosting the static front-end on Github Pages	7	10/17/22	10/23/22
	Adding placeholder functions to connect to back-end	7	10/24/22	11/06/22

	Connecting front-end with back-end	7	11/07/22	11/13/22
	Adding research data into database	14	10/27/22	11/09/22
2.8				11/15/22
	User Profile	40	10/5/22	11/14/22
	Use Case Diagram	40	10/5/22	11/14/22
	Draft Report	40	10/5/22	11/14/22
	Final Fall semester Report	40	10/5/22	11/14/22
	Fall Presentations	14	11/14/22	11/28/22
	Completed Alpha version of project	90	8/25/22	11/14/22
Spring				
	Test website's user experience	7	1/10	1/17/23
	Improve website user experience	7	1/10	1/17/23
	Code and implement scraper tool	20	1/10	1/30
	Host the website	13	1/17/22	1/30/22
	Present the project at IT Expo	1	4/11/22	4/11/22
	Refinement and finishing touches	7	4/11/22	4/18/22

2.10 Problems Encountered and Analysis of Problems Solved

One problem of our project is thinking of the structure of our website to display our data. We overcomplicate things and think of many complex structures that may confuse users to go through the articles. However, we discussed and decided to go with a simple option with just the vulnerability information and mitigation section.

Also, we have problems with our application architecture and website hosting. Which framework can be used for our backend and frontend? Which web hosting services are free for students? These are questions that we researched throughout the development process.

2.11 Recommendations for Improvement

We want our website to be very inviting for new users that want to learn about the cyber world and how to secure their device, so we will keep adjusting our code to give it a very comfortable feel and have the updated information as organized as we can have it going forward. If we had more time to make improvements, we would likely enhance user experience by giving each user an account so they can have a very personal experience being able to save certain articles to their account.

Despite having all our core functionalities, there are many other improvements that can be made in the future. First, we can improve our FAQ page to query our database instead of hard coding the questions and answers. Secondly, another improvement is in the search functionality once we have more posts. We can make the search function to be a back-end API and implement the logic in the back end, this will allow for better search like filters by categories instead of keywords. Other than functional improvements, we can also do visual improvements like adding in light mode, or displaying categories under post title, etc.

CONCLUSION

3.1 Lessons Learned

- Research and build virtual environments on VMWare to test different vulnerabilities.
- How to write a detailed project report.
- Working with members from different time zones.

3.2 Abilities and Skills Developed Throughout Project

Overall, we developed many skills through our time working on this project, as we all learned a bit of new skills with working with so many different software's. Working with Azure and API calls was very cool to research and learn. We also learned many cybersecurity concepts on our own during research time for our articles. We learned how to work in a group with members from different times zones and how to better our communication skills to make the time together more effective. and we learned how to search for relevant information and literature, summarize the content after reading, refine the content, and finally how to write user-oriented articles.

3.3 Plans for Future

Our plans for the future include us making improvements to the website and keeping it up for users to come and learn about the cyber world and submit new articles that are interesting to them. We will keep monitoring our site and answering any questions that come our way.

REFERENCES AND APPENDIX

4.1 References

Android Apps Are Asking for Too Many Dangerous Permissions ... - Cybernews.

https://cybernews.com/privacy/android-apps-are-asking-for-too-many-dangerous-permissions-heres-how-we-know/.