BÁNKI KÖZLEMÉNYEK --- BÁNKI REPORTS
VI. ÉVFOLYAM 2. SZÁM --- VOLUME VI NO. 2

Using Challenge-based Tasks for Testing the Security of Web Applications

Zlatko Čović
Subotica Tech – College of Applied Sciences, Subotica, Serbia
chole@vts.su.ac.rs

***Abstract* — This paper explores the integration of challenge-based tasks in the education of cybersecurity and software engineers for the testing of the security of web applications. It provides an overview of security education and web application security, highlights the importance of challenge-based tasks, and details their implementation in the curricula. Specific tasks and their solutions are presented, along with future plans for improving these educational methods. The study emphasizes the critical role of hands-on, practical approaches in bridging the gap between theoretical knowledge and practical skills.**

***Keywords*:** challenge-based tasks, web security, web applications, owasp, code-entry challenges

1 INTRODUCTION

The rapid expansion and deep integration of web applications into everyday life have made securing these platforms more crucial than ever. Web applications are now omnipresent, enabling everything from online shopping and social interactions to banking services. This widespread use, however, also exposes them to numerous cyber threats, including data breaches and the exploitation of security vulnerabilities.

Traditional methods of security testing often fail to meet the demands posed by the complex and ever-evolving nature of modern web applications. These conventional approaches are typically static and predictable, lacking the ability to replicate real-world attack scenarios effectively. As a result, there is a pressing need for more innovative testing strategies that can more accurately assess and improve web application security.

In the education of software and/or cyber engineers, a gap often arises between theoretical and practical knowledge. It is essential to define and implement innovative educational methods that offer hands-on experience with real-world problems. The field of information security is one of the most critical aspects of modern life and communication. The vast amount of information we access and share through various services and tools forces the education of professionals who can create and maintain these systems securely.

Authors in the study [1] focus on the applicability of the hackathon method in training software engineers. The hackathon method, which is student-centered, uses a pedagogical approach based on constructivist theory. During a hackathon, programmers and other software development professionals collaborate intensively on projects with students. This method allows students to gain new knowledge and skills and develop key competences. The hackathon method is integrated into the Web programming course curriculum at Subotica Tech – College of Applied Sciences, aiming to assist students in building web applications. Upon completing the course, students will be able to work independently with multiple programming languages and technologies and manage databases in a client-server environment using appropriate security methods and techniques.

The application of the Challenge-Based Learning (CBL) methodology to cybersecurity education has been described in paper [2]. Challenges were formulated based on students' interest in securing information and systems, and solutions to meet these challenges were devised collaboratively by students working as a team. The knowledge learned was practiced by students in two cybersecurity competitions. Formative assessments showed that great benefits were derived from the CBL approach, though the extent of benefit varied among students. Computer skills, security knowledge, ability to teach others, and interest in cybersecurity were improved by the students. Although additional support resources and irregular meeting hours may be required, the increase in student learning justifies the extra effort [2].

Challenge-Based Learning (CBL) involves an external stakeholder (e.g., company, community, NGO) presenting a real-life complex problem. While CBL is gaining popularity in engineering education, its application in engineering ethics education lags due to specific design requirements. Although ethics CBL courses share similarities with general CBL courses, they necessitate unique design considerations [3]

A structured approach is needed to apply CBL in engineering ethics education, from both educational research and support perspectives. In [3] authors address this gap by exploring the particularities of CBL pedagogies in engineering ethics education using van den Akker's spider-web curriculum model and the Ethics Goal Model. The specificities for various course components in CBL engineering ethics courses are described, concluding that the balance between structured and open CBL approaches is crucial and warrants further research [3].

The design of defensive challenges for Capture the flag (CTF) in the industry is addressed in this [4] work. A challenge structure and six different challenge types were derived based on semi-structured interviews with security experts, a two-part survey, and informal discussions. Results indicate that security experts prefer traditional challenge types, such as Single-Choice and Multiple-Choice Questions, while Text-Entry Challenges are the least preferred. Additionally, Association Left-Right, Code-Entry Challenge, and Code-Snippet Challenge types were discussed. The Code-Entry Challenge, where players

submit code to the backend for validation, emerged as an unexpected yet promising type for secure coding challenges [4].

Further investigation is needed to detail the creation of Code-Entry Challenges. The results are based on feedback from security experts, and further work is required to validate the challenge structure and types in real CTF events within an industrial setting. Future publications will provide concrete examples of implementing the derived challenge types and will refine the structure based on feedback from CTF players [4].

For a web application or information system to be secure, the creators of these systems must test them using appropriate tests. It is also desirable to raise awareness about potential vulnerabilities and threats. The OWASP foundation created the OWASP Top 10 as a standard awareness document for developers and web application security. It reflects a wide consensus on the most critical security risks facing web applications [5].

This paper describes the usage of challenge-based tasks in the education of cyber security and software engineers. These tasks were implemented in two curricula: Security in e-business systems and Web programming. The challenges are defined to follow the OWASP Top 10 standard awareness document for developers and web application security.

This paper is organized as follows. Section 2 shortly introduces the education of security aspects and gives basic information about web applications security. In Section 3, the significance of challenge-based tasks is elucidated through several key arguments. The implementation of challenge-based tasks in education is described in Section 4. Some of the tasks and their possible solutions are also presented in detail. Future plans are outlined in the following section. The conclusion at the end of the paper summarizes the key points from the preceding sections.

2 Education of Security Aspects

In the education of cybersecurity and software engineers, it is very important to introduce new teaching methods to bridge the gap between practical and theoretical knowledge. Although practical topics are covered in lab exercises following theoretical knowledge, the traditional approach to assignments is not always sufficient.

At Subotica Tech – College of Applied Sciences, in most specialized subjects, students are required to complete homework assignments and a practical project, which often involves team collaboration. During the project, aspects of project-based learning (PBL) are applied. Digital tools are used for development as well as for collaboration. A newer method that has been tested after PBL is hackathon-based learning (HBL). This learning model also emphasizes teamwork but incorporates elements found in hackathons held outside of the university. Depending on the type of information system, whether it is a desktop program, mobile application, web application, or integrated web system students are required to test their software both functionally and for security within their projects. A strong emphasis is placed on simulating real-life situations.

During the hackathon, collaboration with local IT companies is encouraged, and these companies delegate their own programmers who join the teams as external mentors. Their task is to define additional functionalities for the project based on the project description provided by the course professors.

A strong focus is placed on various aspects of security within professional courses of study. In some of these courses, protection methods and techniques are taught through laboratory exercises, using diverse approaches to test information systems, web applications, mobile applications, and other types of software and networks.

It is crucial to provide students with opportunities to test their knowledge by assigning tasks in laboratory exercises and homework that are related to information security.

2.1 Web applications security

As part of information security, web application security specifically addresses the security of web applications, websites, web systems, and web services. Web application security is based on the principles of application security, combining and applying them separately to web systems and the internet.

Core issues in the development and use of web applications include insufficient knowledge and weak awareness of potential threats. Developers often fail to implement appropriate security techniques and methods, and do not conduct security checks of their applications.

Secure code has two aspects: develop code without bugs and security holes and develop code resistant to abuses and attacks. Current software engineering technology doesn't guarantee meeting both criteria. The best approach is dynamic or static testing to ensure code behavior matches user requirements. Functional testing checks if the code behaves as expected in various scenarios but can't guarantee the absence of errors. It can only show that errors are present. Additionally, traditional functional testing cannot confirm code security or immunity to attacks [6].

Developers and engineering students need to be able to identify security threats and vulnerabilities. The OWASP Top 10 standard document is the best resource for understanding these topics and for defining guidelines for security testing of software. It is also useful for creating challenge-based tasks in the education of software engineers and cybersecurity engineers.

3 Challenge-based tasks

Challenge-based tasks for assessing the security of web applications hold significant importance due to several key reasons:

- Realistic Cyberattack Simulations
- Thorough Vulnerability Testing
- Skill Verification
- Ongoing Skill Improvement
- Reducing Risks
- Meeting Compliance
- Affordable Security Testing

3.1 Realistic Cyberattack Simulations

These tasks mimic real cyberattacks, helping to evaluate how well an application's security can handle actual threats. By simulating authentic attack scenarios, these challenges provide a practical assessment of an application's defenses, enabling developers to identify and address potential weaknesses before they can be exploited by malicious actors.

3.2 Thorough Vulnerability Testing

These challenges cover various security issues like injection attacks (e.g., SQL injection, XSS), weak authentication, privilege escalation, and more, allowing testers to find weaknesses in different parts of the application.

3.3 Skill Verification

Overcoming these challenges requires a strong understanding of web security concepts and techniques, demonstrating testers' ability to identify and fix security risks effectively.

3.4 Ongoing Skill Improvement

These challenges can be set at different difficulty levels, helping testers advance from basic to advanced security testing skills and promoting continuous learning and skill growth within security teams.

3.5 Reducing Risks

By finding and fixing vulnerabilities through challenges, organizations can lower the chances of security breaches, protecting against data theft, system hacks, and damage to their reputation.

3.6 Meeting Compliance

Many industry standards and regulations require regular security testing. Challenge-based tasks help meet these requirements in an organized way.

3.7 Affordable Security Testing

Challenge-based tasks provide a cost-effective method to comprehensively assess an application's security posture. By simulating various threat scenarios in a controlled environment, organizations can efficiently identify and prioritize security weaknesses, thereby optimizing resource allocation for targeted remediation efforts. This approach not only helps mitigate potential risks but also promotes a proactive security culture, enabling continuous improvement of defenses without exceeding budgetary constraints.

4 IMPLEMENTATION OF CHALLENGE-BASED TASKS IN EDUCATION

Challenge-based tasks were first implemented in the education of cyber security and software engineers. These tasks were applied in two curricula: Security in e-business systems and Web programming.

The initial tasks were carried out with cybersecurity students from Obuda University who were participating in an Erasmus exchange program at Subotica Tech - College of Applied Sciences during one semester. These tasks were part of the mandatory curriculum within the subject of Security in e-business systems.

After successfully implementing these tasks and based on feedback from the students, the tasks were slightly modified and integrated into the Web Programming course with informatics students at Subotica Tech – College of Applied Sciences as the last class in the semester.

In the domain of information security and within various courses, students at Subotica Tech learn theoretically and practically about following terms:

- Filtering and validating user input data
- Secure file uploads and user management (registration, login)
- Secure use of sessions, cookies, and API endpoints
- Web server and directory protection
- Cryptography, crypto algorithms, and token authentication
- Security of IoT systems and networks
- Database protection and SQL injection prevention
- Mobile application security
- Restricting unsafe dynamic function calls and access to sensitive components
- Analyzing meta data in media files
- Avoiding legacy approaches, classes, and methods

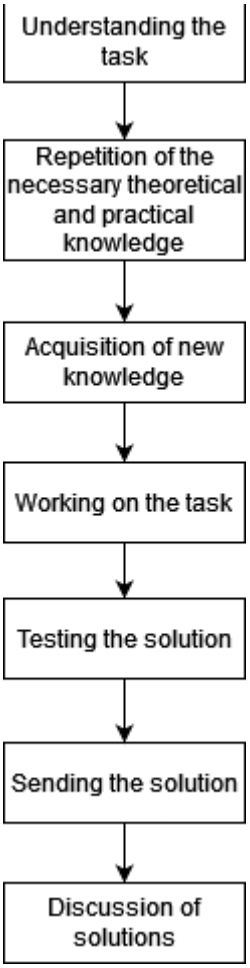
4.1 Task structure

After acquiring theoretical and practical knowledge in areas related to web programming and web security, students were given challenge-based tasks that they had to solve individually during laboratory exercises.

The tasks were designed to be based on challenges and to be related to the security of web applications. Each task was scheduled for a specific time. After that time, the students sent their material to the server that contained solution in the form of program code and textual file with information about their experiences during the work on task and, if necessary, detailed explanation of the solution. Also, in some tasks it is mandatory to write down what could be the potential security issues and vulnerabilities and how they can be avoided and what are the most suitable techniques or methods for that. A discussion followed where different approaches to solving tasks and encountered problems were discussed.

These are practical tasks that always required submitting created code or code snippets, so it can be said that these tasks have characteristics of code-entry challenges.

In the schema below, the general structure of flow of every task is presented.



1.figure: Structure of flow of every task

During each part of the task, students can ask the subject professor questions if something is unclear or if they need additional explanations. In the description of each task, web links to resources containing material for reviewing acquired knowledge and acquiring new knowledge have been added.

As can be seen in the schema, there is a section for testing the solution. This part is crucial because, in some tasks, additional information necessary for problem-solving cannot be obtained without testing.

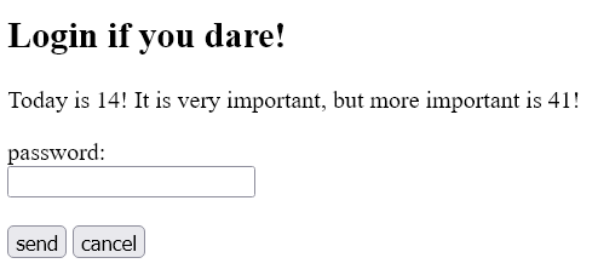
4.2 Examples of challenge-based tasks

In this section, some challenge-based tasks and their possible solutions will be presented. Some of them are easier and require less time to solve, but some require more testing attempts and more knowledge to be properly solved.

4.2.1 Finding the correct password

Task text: *Analyze html code of form on given url. Try to find the correct password. For getting password, you should write php code that will get important data. Write an explanation of your solution.*

Students were required to analyze the HTML code of a web page that contains text messages and a login form with a password input field and two buttons: one for submitting data and one for resetting the form.



2. figure: Web form of task 1

Below is the HTML code of the first task's webpage.

```
<!DOCTYPE html>
<html lang="en">
<body>
<h2>Login if you dare!</h2>
<p>Today is 14! It is very important, but more
important is 41!</p>

<form action="check.php" method="post">
<label for="password">password:</label><br>
<input type="password" id="password"
name="password"><br>
<input type="hidden" name="l1"
value="41rkPe3lA2fhgutijgkdkfjiti" >
<input type="hidden" name="l2"
value="ab0526ad3fc8bd9909482126d72deb432a0efbe54
a29ba0da3b64b" ><br>
<input type="submit" value="send">
<input type="reset" value="cancel">
</form>
</body>
</html>
```

When examining the source code of the HTML page, two hidden fields named l1 and l2 can be seen within the form. Each of these fields has an initial value assigned, consisting of a string of random numbers and letters. The length of the first field is 26 characters, and the second is 54 characters.

If the user refreshes the page multiple times or sends a new request to the server, they will notice that the value of the hidden field l2 changes, but only the first 14 characters. The remaining 40 characters stay the same.

Since the content is a random string of characters, a student might think it is a type of hash value. Knowing some hash algorithms, they might conclude that the SHA-1 algorithm generates a hash of 40 characters in length. By copying the 40 characters that do not change, they can use free online tools to try to find the plain text of the hash value. These tools contain many hash values and their corresponding plain text values. Some of these values are automatically generated, while others are manually added by volunteers. This type of service does not decrypt data in real-time but searches its own database based on the input provided. From an ethical standpoint, the purpose of these services is not to steal someone's password but to highlight the weakness of a password. Of course, some users of these services may have malicious intentions.

Entering the found hash value from the hidden field into an online tool will not result in finding the plain text version of the text. The student should continue analyzing the information on the web page. Above the web form, there is a message: *Today is 14! It is very important, but more important is 41!*

From this message, the student might deduce that the important information is that 41 is the reverse of 14. By using a programming language, such as PHP, to apply a built-in function or method to reverse a string, they can attempt to find the plain text value for the reversed string using an online service. In PHP, the function used for this purpose is *strrev*. For the reversed value, the student will easily find the plain text version of the password.

4.2.2 Uploading larger jpg and png files

Task text: *Analyze html code and try to upload jpg and png files that are bigger than 1MB. Don't forget to insert your index number from Subotica Tech. Write the explanation of your solution.*

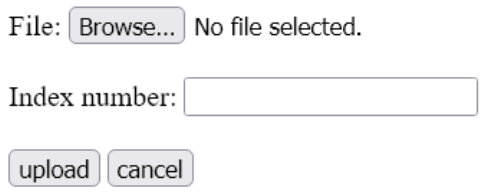
The HTML code of a web page contains file selection fields, a text field for entering an index number, and two buttons, one for submitting data and one for resetting the form.

Below is the HTML code of the second task's webpage.

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>File upload</title>
</head>
<body>
<form method="post" name="upload"
action="upload.php" enctype="multipart/form-
data">

    <input type="hidden" name="MAX_FILE_SIZE"
value="102400" >
    <label for="if">File:</label> <input
type="file" name="file" id="if"
accept="image/jpeg"><br><br>
    <label for="index">Index number:</label>
<input type="text" name="index"
id="index"><br><br>
    <input type="submit" name="sb" id="sb"
value="upload">
    <input type="reset" name="rb" id="rb"
value="cancel">
</form>

</body>
</html>
```



2. figure: Web form of task 2

By analyzing the HTML code, the following information can be obtained:

- the name of the page receiving submitted data through the form (action attribute),
- the value of the hidden field MAX_FILE_SIZE,
- and the value of the accept attribute.

In web forms, MAX_FILE_SIZE is a hidden input field that defines the maximum file size (in bytes) that the server will allow users to upload through that specific form. This ensures server-side restrictions on file size limits for uploads. The value of this field can be easily changed by a potential attacker.

The accept attribute in a file input type specifies the types of files that the file input element can accept for file selection. It assists browsers in filtering the files displayed in the file picker dialog to show only those files that match the specified types.

Based on the obtained values, the file size is limited to 100KB and selecting files of type jpg is preferred. The student can try changing the file type in the file picker to all types and select a png file instead. There are several solutions for uploading a png file larger than 1MB.

The first solution involves using the "Inspect element" option within the web browser to delete the hidden field MAX_FILE_SIZE. This action does not delete the original file on the server but changes the HTML code that is fetched and currently active in the web browser. Without this hidden field, there would be no size limit for the file. The student will only need to enter their index number and submit a png file larger than 1MB.

The second solution requires copying the entire HTML code into another HTML file and deleting the hidden field and the accept attribute. The newly created HTML file should be run locally in a web browser to test whether uploading a png file larger than 1MB will succeed. If the upload is successful, the student will receive confirmation of the file being sent.

It's notable here that there are several security vulnerabilities on the server side in program code. There is no verification of the size and type of the uploaded file or the origin domain from which the data is sent.

4.2.3 Try to find your own password

Text of task: *Try to get your password from hash. You can't remember the correct password, but you know that it contains 4 digits. Also, you find another hash or random string. Maybe it is connected to something with hash. Write php code and try to find the correct password.*

When looking at the length of the found hash, the result is 32 characters. A student familiar with hash algorithms can immediately conclude that the MD5 algorithm was used for hashing. Also, based on the string with random values, they might think that the SALT technique was used to obtain the hash value. SALT technique involves adding a unique, random value to a password before hashing it to ensure that identical passwords have different hash values and to protect against precomputed hash attacks. Since SALT can be added to the beginning, end,

or both ends of the password, the student must take all of this into account.

The password consists of 4 digits, but it is not yet known where the SALT is located within the password. The student can write program code that will hash values from 0000 to 9999 and check the obtained hash against the given hash. If they go through all combinations and do not find the password, the next step is to add the SALT value to the beginning of the potential password and perform the hashing with this data. If the result is still negative, the procedure is repeated by adding the SALT value to both the beginning and end, or only to the end of the potential password.

Some of the students tried to enter the hash into the search option available on some online services to obtain the plaintext based on that value. None of them succeeded. The reason is that these online services did not use SALT, which was generated randomly in this task, and therefore, even such a simple data of 4 digits cannot be found

5 Future plans

After the initial test implementation of tasks in the educational process and based on the feedback from students who worked on these tasks, future steps can be defined for the next implementation of these challenge-based tasks.

Solving certain tasks required more time and effort from some students. There were instances where some tasks were not successfully completed. One of the suggestions was to divide the tasks by difficulty level.

For this purpose, a control test (both theoretical and practical) would be conducted to determine the students' knowledge levels. Based on this level, tasks of the corresponding difficulty or tasks of the next level of difficulty could be assigned to the students.

Another suggestion was to categorize the tasks and have them completed after covering a larger teaching unit within the curriculum. This way, these types of tasks would be done multiple times throughout the semester.

Some students suggested that the tasks could be done in teams, because that think it could help them to solve problems more effectively.

Since many tasks require the input of certain data that were verified on the backend, the plan is to log all these attempts in a database. Based on this data, the students' thought processes and approaches to problem-solving can be determined.

A potential improvement in defining tasks would involve surveying industry experts to identify the areas where they see the most security vulnerabilities among developers in their companies, as well as the challenges that even they sometimes find problematic.

6 Conclusions

In educating software and cyber engineers, a gap often exists between theoretical and practical knowledge. Therefore, it is crucial to develop and apply innovative educational methods that provide hands-on experience with real-world challenges.

This paper has explored the integration of challenge-based tasks in the education of cybersecurity and software engineers. These tasks were implemented in two curricula: Security in E-Business Systems and Web Programming. The challenges were defined to follow the OWASP Top 10 standard for developers and web application security.

Section 2 provided a brief overview of the education of security aspects and fundamental information about web application security. The importance of challenge-based tasks was highlighted in Section 3 through key arguments. The implementation of these tasks in the curricula was detailed in Section 4, with specific tasks and their possible solutions presented. Based on feedback from students, future plans for the continued use and improvement of challenge-based tasks were discussed in the subsequent section. The key points from each section were summarized to emphasize the critical role of innovative, hands-on educational methods in bridging the gap between theoretical knowledge and practical skills in the field of cybersecurity and software engineering.

References

[1] Z. Čović, Z. Papp, H. Manojlović and J. Simon, "Hackathon-based Teaching Method in the Training of Software Engineers", Proceedings of the 12th International Conference on Applied Internet and Information Technologies AIIT 2022, Zrenjanin, Serbia, 2022, pp. 108-116

[2] Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). *Challenge based learning in cybersecurity education*. Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[3] G. Bombaerts, D. Martin and K. Doulougeri, "Structured and open Challenge-Based Learning in Engineering Ethics Education," 2022 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2022, pp. 1-8, doi: 10.1109/FIE56618.2022.9962652.

[4] Gasiba, T., Lechner, U., Pinto-Albuquerque, M., Zouitni, A. (2020). Design of Secure Coding Challenges for Cybersecurity Education in the Industry. In: Shepperd, M., Brito e Abreu, F., Rodrigues da Silva, A., Pérez-Castillo, R. (eds) Quality of Information and Communications Technology. QUATIC 2020. Communications in Computer and Information Science, vol 1266. Springer, Cham. https://doi.org/10.1007/978-3-030-58793-2_18

[5] Čović, Z. (2024). Threats and Vulnerabilities in Web Applications and How to Avoid Them. In: Kovács, T.A., Nyikes, Z., Berek, T., Daruka, N., Tóth, L. (eds) Critical Infrastructure Protection in the Light of the Armed Conflicts. HCC 2022. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-47990-8_9

[6] A. J. A. Wang, "Security testing in software engineering courses," 34th Annual Frontiers in Education, 2004. FIE 2004., Savannah, GA, USA, 2004, pp. F1C-13, doi: 10.1109/FIE.2004.1408561.