CyberTest Project

System Request Statement / Planning Phase   
(Homework No.1A)

Student: Nargiz Heybatova

Instructor: Dr. Araz Yusubov

Submitted in partial fulfillment of the requirements of the INFT 2303: Systems Analysis and Design course project

|  |  |
| --- | --- |
| GitHub repository | https://github.com/ADA-SITE-INFT2303-2023-Spring/homework-1a-nargizh7 |
| Version date | Version Information |
| 9/2/2023 | Initial draft of the project (before the first draft, a research of the topic was conducted to collect and analyze all the needed materials) |
| 12/2/2023 | Final version of the project |

|  |
| --- |
|  |
| Project sponsor |
| Nargiz Heybatova, on behalf of Electronic Security Center of Ministry of Digital Development and Transport[[1]](#footnote-1). |
| Business Need |
| Recent research conducted in 2022 by the World Economic Forum shows that nowadays cybercrimes produce $1.5 trillion yearly revenues for illegal entities. Azerbaijan is one of the countries exposed to these illegal actions since the frequency of cyberattacks was increased by nearly four times.[[2]](#footnote-2) According to the National Cybersecurity Index ranking[[3]](#footnote-3), Azerbaijan holds 76th position among 160 countries when it comes to the Networked Readiness Index which implies that there should be changes in the way the economy is utilizing information systems to provide more sophisticated defense systems.  Moreover, as per NCSI Fulfilment Percentage, Azerbaijan holding only 20% for Cyber Crisis Management point proves the need for establishing proper mechanisms for managing cyber incidents[[4]](#footnote-4). Annually, approximate number of 6,000 corporate users in Azerbaijan experience cyberattacks leading to business disruption because of poorly established data protection mechanisms.[[5]](#footnote-5) In 2020, Azerbaijan became one of the top 10 countries exposed to the Ciphering-Trojan password-stealing malware attacks[[6]](#footnote-6). These issues resulted in Azerbaijan fulfilling 0% of NCSI criteria for proper protection of digital services and only 25% for protection of personal data3.  Besides, the high records of cyber-attacks during the Second Karabakh war as was reported by Director of the Electronic Security Service, Shahin Aliyev[[7]](#footnote-7), made the cybersecurity in Azerbaijan even more vulnerable. As there are still unresolved political issues, there should always be considered the potential risk of these attacks happening again.  Association Of Cyber Security Organizations of Azerbaijan (AKTA)[[8]](#footnote-8) underlines the importance to support research on the development of network security. [[9]](#footnote-9)2 Although the Ministry of Education is undertaking measures to boost the interest of more students to enroll into the field of cyber security, there is still a shortage of IT specialists in the country demand for whom grows at a tremendous pace. [[10]](#footnote-10)2  Hence, since one of main challenges in resolving above-mentioned issues is the lack of specialists in the cybersecurity field, there is a need to create a project that would increase the interest of people to join the IT field and accelerate research efforts to find ways to improve current defense mechanisms. For that reason, there is a business need to establish CyberTest Project that would organize VRP (vulnerability rewards program) by providing specific application where anyone interested in cyber security, can virtually test the defense system of the websites to exploit vulnerabilities. In case of finding software bugs, or successfully practicing SQL injections, the candidates must write a report of their research findings and submit their vulnerability assessment to receive rewards. |
| Business Requirements |
| The CyberTest system is represented by the application that provides virtual representation of the real governmental, organizational, and corporate websites based in Azerbaijan that demand high level security systems and are willing to be a part of the project to discover ways to improve their defense mechanisms.  The working process starts with candidates joining the application, and specifying their identification credentials: full name, age, occupation, email, phone, and passport number that can be used for registering one user only, description of their experience in IT field, certifications, skills, and education. Without properly completed registering phase and without agreeing to the Terms of Use of the system, it would be impossible to proceed and get access to the websites. These measures are necessary for controlling the users and their actions performed when using application.  The application can be accessed unlimited number of times, however, to avoid spam, each user will have limited attempts to report the found vulnerabilities. Since the application uses virtual machine upon which the copies of real websites are built, there is no need for candidates to get an organization’s consent to perform various techniques for finding security vulnerabilities such as SQL injections on its website. There will be no fixed number of websites available for testing on the application, depending on the need, more organizations will join the project if they are based in Azerbaijan.  Once the candidate uncovered the website’s vulnerabilities and identified how to fix them, a detailed report must be submitted through the application for further investigation. In case of approval from the Electronic Security Center1 the candidate will be rewarded, and the real website will change their defense system accordingly.  Besides, all the data of candidates’ actions will be collected to analyze the hackers’ behavior and perform statistical measures to identify common trends when trying to penetrate the website (how most of the candidates approach the problem, what tools do they use the most/least, how does their approach change throughout the whole time). The fact that users’ actions will be tracked will be specified in the Terms of Use agreement alongside with other important rules related to nondisclosure agreement all of which the candidates must follow.  To summarize, the application provides the following capabilities:   * Requires candidates to register and provide their personal data. * Requires candidates to attentively read and agree to the terms of use. * Provides instructions on the way to use the application. * Provides the application in three different languages (AZE/ENG/RUS). * Provides contact information in case of any questions. * Provides several websites available for virtual testing. * Allows to use the application unlimited number of times. * Restricts number of submissions depending on the tested website. * Tracks all the actions across the application. * Requires submitting reports only through the application itself. * Prohibits using the same identification credentials twice. * Prohibits neglecting the instructions and the terms of use. * Partners with Electronic Security Center1 when assessing the reports. * Contacts the organizations whose website were found to be vulnerable. * Provides rewards for successful analysis report. * Updates new versions of the websites on the application. |
| Business Value |
| Tangible benefits:   * Improved websites security systems. * Decreased financial losses. * Recovery operations cost savings. * Higher engagement of people in the IT field. * Valuable data collection for further research. * Ability to investigate more alternatives to the current IT systems. * Higher NCSI Fulfilment Percentage for Azerbaijan.   Intangible benefits:   * Lower chance of reputational damage for the organizations. * Increased customer trust when using the websites. * Increased compliance. * More opportunities for people to show their talents. |
| Special Issues or Constraints: |
| The implementation of such project at first might be considered to be too costly. However, it is an expense the committee should accept to do business well in the modern world[[11]](#footnote-11), in other words, improved security system will act as an insurance from dangerous threats that would lead to bigger financial losses in future.  Another potential issue is related to the hackers that may use the application specifically to better understand certain processes in the way the websites operate in order to find vulnerabilities but later use them to perform cyber-attacks rather than report them to receive rewards. For that reason, one of legislative requirements will be to track all the activities of the candidates to notice any suspicious behavior such as candidate analyzing a website for a long time but then stopping without submitting any reports. |

1. https://mincom.gov.az/en/view/organization/17/ [↑](#footnote-ref-1)
2. https://caliber.az/en/post/75039/ [↑](#footnote-ref-2)
3. https://ncsi.ega.ee/country/az/ [↑](#footnote-ref-3)
4. https://www.enisa.europa.eu/topics/cyber-crisis-management [↑](#footnote-ref-4)
5. https://en.trend.az/business/finance/3037874.html [↑](#footnote-ref-5)
6. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.dcaf.ch/sites/default/files/publications/documents/AzerbaijanCybersecurityGovernanceAssessment.pdf [↑](#footnote-ref-6)
7. https://www.azernews.az/business/194158.html [↑](#footnote-ref-7)
8. https://akta.az/ [↑](#footnote-ref-8)
9. [↑](#footnote-ref-9)
10. [↑](#footnote-ref-10)
11. https://www.vistainfosec.com/blog/why-cybersecurity-is-worth-the-cost-for-your-business/ [↑](#footnote-ref-11)