"If you want, I can store the encrypted password." A Password-Storage Field Study with Freelance Developers

Supplementary Material

Alena Naiakshina
University of Bonn
naiakshi@cs.uni-bonn.de

Anastasia Danilova
University of Bonn
danilova@cs.uni-bonn.de

Eva Gerlitz
University of Bonn
gerlitz@uni-bonn.de

Emanuel von Zezschwitz
University of Bonn, Fraunhofer FKIE
zezschwitz@cs.uni-bonn.de

Matthew Smith
University of Bonn, Fraunhofer FKIE
smith@cs.uni-bonn.de

ACM Reference Format:
Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, Emanuel von Zezschwitz, and Matthew Smith. 2019. "If you want, I can store the encrypted password." A Password-Storage Field Study with Freelance Developers: Supplementary Material. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3290605.3300370

1 SECURITY SCORE

We based the evaluation of participants' submissions on the security score of Naiakshina et al. [5].

(1) The end-user password is salted (+1) and hashed (+1).
(2) The derived length of the hash is at least 160 bits long (+1).
(3) The iteration count for key stretching is at least 1 000 (+0.5) or 10 000 (+1) for `PBKDF2` and at least $2^{10} = 1\,024$ for `bcrypt` (+1).
(4) A memory-hard hashing function is used (+1).
(5) The salt value is generated randomly (+1).
(6) The salt is at least 32 bits in length (+1).

2 STATISTICS

Due to the adjusted study design, we were able to test only three of the seven main hypotheses from [6]:

H-P1 Priming has an effect on the likelihood of participants attempting security.[1]
H-G1 Years of Java experience have an effect on the security scores.
H-G2 If participants state that they have previously stored passwords, it affects the likelihood that they store them securely.

Table 1 shows a summary of our statistical analysis results.

3 PLAY-BOOK

To keep the communication with freelancers consistent, we used a uniform question/answer catalog. *P* indicates the question of the participant and *R* indicates the answer of the researcher.

Project Offer

- 1st Message: *R: Hi xyz, I noticed your profile and would like to offer you my project. We can discuss any details over chat.*
- 2nd Message: *R: Hey, we are developing a social networking website to share pictures with family and friends. People need to register to this website in order to be able to share their pictures. Your task would be to program the registration functionality for this website in the back-end. The project is in Java and uses Hibernate and JSF, our database uses postgreSQL. The front-end and some parts of the program logic are already developed. What do you think? Kind regards, ...*
- Over project bidding: *R: Hi. We are happy that you want to work on our project. We would like to give you the code as a ZIP file. *sending files**

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5970-2/19/05.
https://doi.org/10.1145/3290605.3300370

[1] While we were able to track security attempts in a lab setting, in a field study this information was not accessible. We did, though, consider the subset *secure = 1* for our analysis.

H	Sub-sample	IV	DV	Test	OR	CI	p-value	$cor-p$-value
Omnibus test	-	Payment, Prompting	Secure	FET	-	-	0.02*	-
H-P1#	-	Prompting	Secure	FET	6.55	[1.44, 37.04]	0.01*	0.03*
H-G1#	-	Java experience	Security Score	Kruskal-Wallis	-	-	0.21	-
H-G2#	-	Stored Passwords Before	Secure	FET	0	[0, 8.91]	0.52	0.52
H-G4	-	Payment	Secure	FET	2.29	[0.56, 10.20]	0.22	0.44
E-A1	Prompted = 1	Payment	Task Acceptance	FET	0.24	[0.058, 0.90]	0.02*	-
E-A2	Prompted = 0	Payment	Task Acceptance	FET	0.56	[0.07, 3.42]	0.69	-
E-A3	-	Security Request	Security Score	Wilcoxon rank sum	-	-	0.83	-
E-A4	Prompted = 0	Sample (Students, Freelancer)	Secure	FET	0	[0,1.89]	0.12	-

Table 1: Summary of Statistical Analysis

IV: Independent variable, **DV**: Dependent variable, **OR**.: Odds ratio, **CI**: Confidence interval, **E-A**: Exploratory analysis
All tests were conducted on security values before participants received a *security request* except for E-A3.
H-P1, H-G2 and H-G4 are corrected with Bonferroni-Holm correction (cor-p value).
= Hypothesis of Naiakshina et al. [6]
* = Significant Tests

- When participant accepts project: *R: Happy to hear that!*

Deadline

- *P:* What is the final delivery? *R:* What do you think how long you need to solve the task? *P:* *** *R:* Ok, that's fine. Thank you
- Deadline exceeded: *R:* Hi, could you give us a status update?

Password-related Questions

- *P:* Should I implement security/secure password storage? *R:* Yes, please!
- Participant handed in insecure code: *R:* I saw that the password is stored in clear text. Could you also store it securely?
- *P:* Is *** fine? *R:* Whatever you would recommend/use!
- *P:* "I have so much experience on Java/Hibernate/what you mentioned..." *R:* Perfect, sounds good!
- *P*: Cannot find password encryption in the requirements, can you tell me where it is written? I might have missed it." *R:* It is not in there, that is true. But could you add it?

General Questions

- *P:* Is it homework? *R:* No, does it look like it is?
- *P:* Can I build it from scratch? *R:* You can solve the task as you prefer.
- *P:* Do I have to use Eclipse? *R:* You can use an IDE of your choice.
- *P:* If I have some questions for your project, can I ask to you? *R:* Sure!
- *P:* Do you use Skype/...? *R:* No, sorry!
- About the budget: *R:* Unfortunately our budget is only .. euro right now. If not enough: *R:* But I'll keep you in mind, if we cannot find somebody else. Sorry!
- *P:* Is it one time development. or are there any future jobs? *R:* For this project it would be one time development, but if you like working with us, we might ask you to help us in the future as well.
- *P:* What happened to your previous developer? *R:* Unfortunately for us, he got a very good job offer.
- P wants email for communication. *R:* If you have any questions, you can just leave them here and I will answer as soon as I see them, if that is ok for you?
- *P:* I have seen your living site with your url *R:* Yeah, we put that online (even though it is not finished yet), so you get to know us a little bit and know who we are.
- *P:* Do you have server where we can upload this code for you to test. *R:* None that I have access to. Would it be possible for you to send me a video or screen-shots so I can see that it is working on your computer?
- *P:* I have a suggestion. Can't I access to your site source directly? As you know, local environment is different from server environment. and if I work there, we can check it online. / etc. *R:* Unfortunately, I do not have access to the source code right now. Is it ok for you to work on your local environment?
- *P:* Do you want me to build Registration on your website or should I do it locally on my machine and hand over it to you? *R:* It would be great if you could do it locally on your machine and hand it over!
- *P:* May I check the code and get back to you tomorrow/later/... *R:* Yes, sure! Take your time.
- P did not work on our db: *R:* Could you also make it work on our database?

- *P:* Once user registers, do we need to send verification email also and once he clicks on that, we will make user status as Active. *R:* No, we only need the data to be stored in our database for now!
- *P:* Which version control service do you use? *R:* Not any yet, as we are still at the beginning of the project.
- *P:* I need to see the ER diagram *R:* We do not have that yet. Is it necessary? *P:* .. *R:* Could you please create a single table for now and I will talk to my colleagues about the rest?
- *P:* Do you require the login functionality as well? Should I implement it as a further task? What else except registration will be needed? *R:* No, thank you!/Please only program the registration functionality.
- *P*: Password is in database, so users wont be able to access it" *R:* And what if somebody get access to the database?

Implementation and Technical Questions

- *P:* Are you using a SSL/TLS server? *R:* Yes.
- *P:* In java there is servlet or jsp? *R:* Yes!
- *P:* There are errors in compile *R:* The errors occur, because the files are not complete, that's what we would need you to do
- *P:* How do I install the project? *R:* Our developer worked with Eclipse, it should be possible to import the files as existing maven project.
- *P:* Can I use additional APIs/frameworks? *R:* Yes, you can use any additional APIs or framework you like.
- *P:* What exactly do I need to do? *R:* All fields in the registration form should be stored in a database.
- *P:* Can you provide me db credentials? *R:* You can find all relevant information in the task sheet, which is included in the ZIP file.

Review for Participants

- *R:* Very good communication, delivered on time. It was nice working with him!

Survey Request

Hello,
thank you very much for completing the task. We have one further request for you. We are researchers from the University of Bonn. The task you worked on is part of a scientific study we are conducting to help developers write more secure code. For an additional 20 euro we would like to invite you to fill out a survey related to the task you worked on. It will take roughly 20 to 30 minutes. The data will be processed pseudonymously. After the survey is complete all data will be anonymized and and there will be no identifying information published in any form. If you wish we can inform you concerning the results of our research. In this case please supply us with an email address under which we can reach you. We would be grateful if you can complete the survey here: [Link] Your study id is: [...]
Thank you again!
With kind regards,...

4 SURVEY

We adapted the exit survey of Naiakshina et al. [6] to the freelance context and expanded it by the following questions:

- Did you create the code on your own or in a team? *[I worked on my own; I worked in a team.]*
- Can you please fill out this questionnaire together with all people who did the coding? *[Ok, my team is here; Sorry, I can't get my team right now, but I was involved in the coding process; Sorry, I can't get my team right now and I was not involved in the coding process.]*
- Which IDE did you use to solve the task?*[free text]*
- Why did you not implement your suggestions? *[free text]*
- At any point, did you think this task could be part of a scientific study? *[Yes, No]*
  - If yes: When did you think this task could be part of a scientific study? *[free text]*
  - If yes: Why did you think this task could be part of a scientific study? *[free text]*
- What is your current main occupation? *[Freelance developer, Industrial developer, Industrial researcher, Academic researcher, Undergraduate student, Graduate student, Other]*
- Do you have a university degree?*[Yes, No]*
- At which university/universities were/are you enrolled? *[free text]*
- What was/is your subject? *[free text]*
- Were/Are you taught about IT-security at university? *[Yes, No, I don't recall.]*
- Were/Are you taught about IT-security extramural?*[Yes, No]*
  - If yes: Where were/are you taught about IT-security extramural? *[free text]*
- What was your main source of learning about IT-security? *[free text]*
- How did you gain your IT skills? *[free text]*
- How did you gain your IT-security skills?*[free text]*
- What type(s) of software do you develop? *[Web applications, Mobile applications, Desktop applications, Embedded applications, Enterprise applications, Other (please specify)]*
- How many years of experience do you have with Java development? *[Integer]*
- How many years of experience do you have with software development in general? *[Integer]*

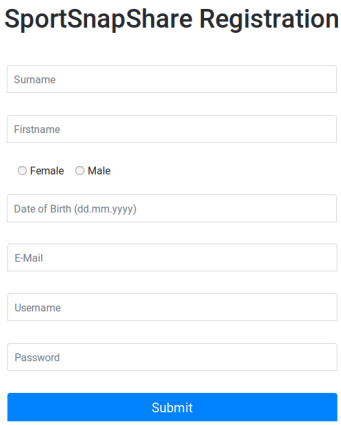
- What country do you live in? *[free text]*
- Are you in contact with other freelancers working on freelancer.com? *[Yes, No]*
  - If yes: How do you communicate with other freelancers working on freelancer.com? *[free text]*
- How do you rate the payment of the implementation task? *[Way too little, Too little, Just right, Too much, Way too much]*
- How do you rate the payment of the survey? *[Way too little, Too little, Just right, Too much, Way too much]*
- If you wish to be contacted by our research group to be informed about the study results, you can provide us your email address. The email address will be stored separately from the study data. *[free text]*
- If you wish to be contacted by our research group for further studies in the future, you can provide us your email address. The email address will be stored separately from the study data. *[free text]*

5 TASK (NON-)PRIMED

Hello,

thank you so much for helping us finishing our project!

We are developing a social networking website to share pictures with family and friends. People need to register (email, name, gender, birth date, username and password) to this website in order to share their pictures. As we already wrote in the project description, we need help with finishing the registration logic for our social networking website. You can find our website here: Link



The front-end is already developed. Another developer started to implement the program logic (MVC), but left the team recently. **We need you to complete the partially available implementation by programming the registration functionality in the back-end.** ***(Please ensure that the user password is stored securely.)***

According to our former developer, the following things have to be done:

Setting up the environment:
The following software will be needed:
1. Tomcat server
2. Optional: Eclipse IDE for Java EE Developers
3. Optional: pgAdmin

Prepare the project & the database:
If you use Eclipse, it could look the following way:

1. Import the existing project as Existing Maven Project.
2. Add Maven Dependencies to the project in Eclipse: Right mouse click on the project/Properties/Deployment Assembly/Add/Java Build Path Entries → choose Maven Dependencies → Finish→ Apply

3. Connect to database (For example in pgAdmin: File/Add Server…)
You will find all necessary information (host, port, DB Name, username and password) in the *hibernate.cfg.xml* file (src/main/resources).

Implementing the registration process:
This was our developer's TODO list, it might not be complete, but hopefully it will help you understand what already was developed and what is left to be done. Figure 1 shows how the different parts are communicating with each other.

In order to test/start your application: Right mouse click on the project/Run As/Run on Server

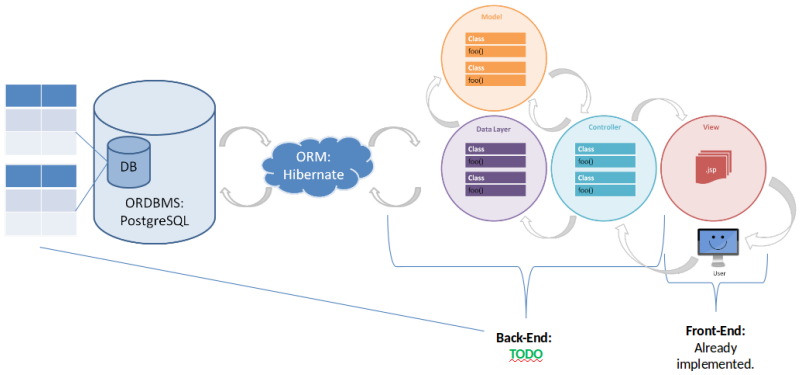


Figure 1

Util:

1. Done: Hibernate configuration
2. Done: Implement method: getSessionFactory()

View:

1. Done: Create registration.xhtml
2. Done: Create successRegistration.xhtml

Database:

1. TODO: Add table *appuser* in the database

Model – Appuser.java

1. TODO: Add user properties (see registration.xhtml)
2. TODO: Add getters & setters

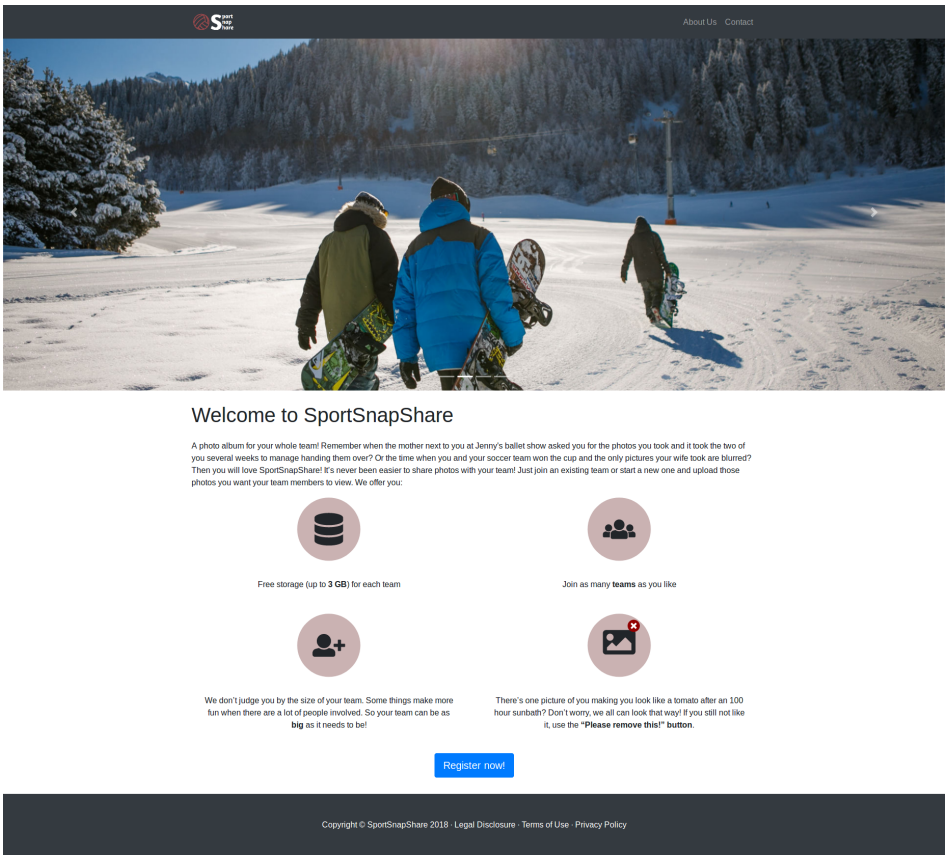
DAO – UserDAO.java

1. Done: Implement mehtod: validateUsername()
2. Done: Open session
3. TODO: Implement method: save()

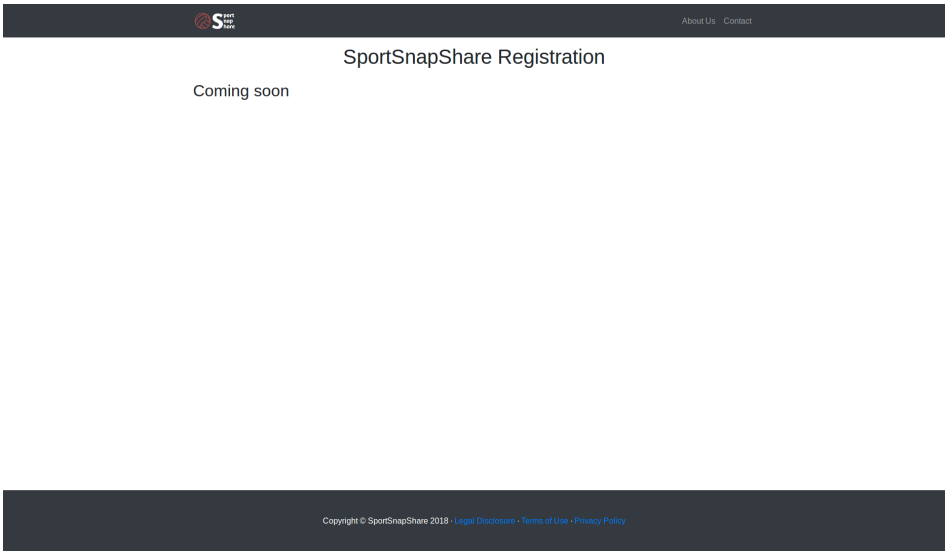
Controller – AppController.java

1. TODO: Add variables for properties
2. TODO: implement method: saveUser()

*(Please ensure that the **user password is stored securely.**)*

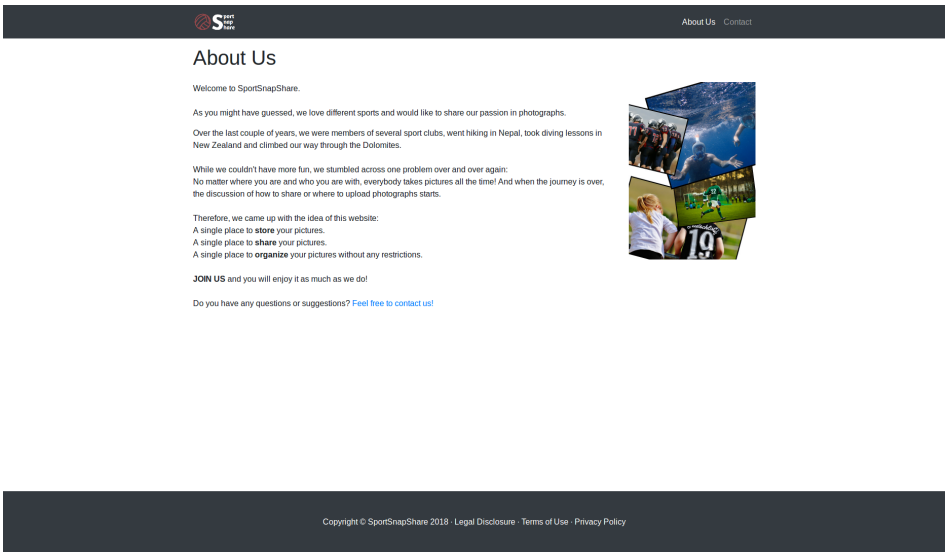


(a) Index Page
Sport Picture: ©Visit Almaty [2]



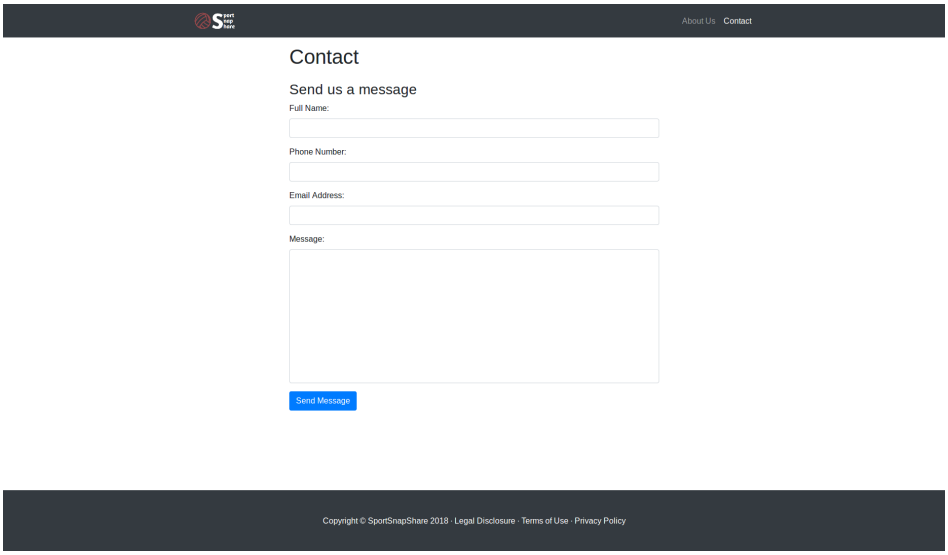
(b) Registration Form

Figure 1: Our Web Presence



(a) About Us

Sport Pictures: ©Alexandra [1], ©Teodor Andersson [3], ©Keith Johnston [4], ©Noz Urbina [7]



(b) Contact Form

Figure 2: Our Web Presence (Cont.)

REFERENCES

[1] Alexandra. [n. d.]. Retrieved January 02, 2019 from https://pixabay.com/en/girl-gate-curious-play-out-nature-1424937/

[2] Visit Almaty. [n. d.]. Retrieved January 02, 2019 from https://www.pexels.com/photo/three-person-holding-bubble-jacket-carrying-snowboards-848594/

[3] Teodor Andersson. [n. d.]. Retrieved January 02, 2019 from https://pixabay.com/en/football-boy-youth-teen-run-shoes-2395754/

[4] Keith Johnston. [n. d.]. Retrieved January 02, 2019 from https://pixabay.com/de/american-football-1465510/

[5] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. 2017. Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. ACM, New York, NY, USA, 311–328. https://doi.org/10.1145/3133956.3134082

[6] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, and Matthew Smith. 2018. Deception Task Design in Developer Password Studies: Exploring a Student Sample. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, USA, 297–313. https://www.usenix.org/conference/soups2018/presentation/naiakshina

[7] Noz Urbina. [n. d.]. Retrieved January 02, 2019 from https://www.pexels.com/photo/photo-of-people-snorkeling-underwater-734725/

Phase	*Category*	*Code*	*Participant*
Request	**Dependent Security & Requirements**	Security dependent on task	$N2_{100}$
		Security dependent on client requirements	$N6_{100}$, $N10_{100}$, $P9_{200}$, $P7_{100}$
		Security dependent on requirements	$P5_{100}$, $N11_{100}$, $N7_{100}$
		Security dependent on application	$N4_{100}$
		Task complexity	$N7_{100}$
		If you want security ask for it.	$P2_{200}$, $P7_{200}$, $N5_{200}$
		Meet all criteria.	$N11_{100}$,$N9_{200}$, $N5_{200}$
	Security Awareness	Needed confirmation.	$N10_{200}$
		Do you need security?	$N10_{100}$
Implementation	**Misconceptions**	Password Security Misconception	$P5_{200}$, $N5_{100}$, $P1_{200}$, $P2_{100}$, $P6_{200}$, $N7_{100}$, $N9_{200}$, $N11_{100}$, $N6_{100}$, $P2_{200}$, $N10_{100}$, $P3_{200}$, $N12_{100}$
		Do not update knowledge	$N11_{100}$, $P2_{200}$, $N8_{100}$, $N10_{100}$
		Believes stored password securely	$N6_{100}$, $N10_{100}$, $P9_{200}$, $P7_{100}$, $N3_{100}$, $N1_{200}$, $P10_{200}$,$P4_{200}$, $P1_{200}$, $P6_{200}$,$N7_{100}$, $N12_{100}$, $N7_{200}$, $N9_{200}$
		Base64 is secure	$N3_{100}$, $N6_{100}$, $N7_{200}$, $P10_{200}$, $N12_{100}$
		Believe used optimal security	$N6_{100}$, $N1_{200}$, $N10_{100}$, $N12_{100}$, $N9_{200}$
		Threat model	$P10_{200}$, $N11_{100}$, $N5_{200}$
		Synonym hash encryption	$N10_{200}$, $N10_{100}$, $N5_{200}$,$N4_{200}$,$P7_{100}$,$N3_{200}$,$P5_{100}$,$P8_{200}$,$P4_{100}$,$N8_{100}$,$N2_{200}$,$P4_{200}$,$P3_{200}$,$P9_{200}$, $N6_{200}$
	Functionality first	Task complexity	$N7_{100}$
		Security one separate part of application	$N3_{200}$
	Security costs extra	Security costs money	$N11_{100}$
		Security needs time	$P9_{100}$
	Information source	Easy documentation	$P4_{100}$, $P9_{200}$
		Examples and tutorials available	$N4_{100}$
		Documentation available	$N6_{200}$, $N8_{200}$
	Library usability	Available methods	$P5_{100}$, $N10_{200}$, $P11_{200}$
		Easy to use	$N1_{100}$, $N10_{100}$,$N3_{200}$, $N6_{200}$, $P4_{200}$
		Few code	$P8_{100}$, $P11_{200}$
		Automatic security	$N10_{200}$
		Javax.crypto hard to use	$P2_{100}$, $N7_{100}$
Reflection	**Self-reflection**	Cocky	$N1_{100}$, $N4_{200}$, $P11_{200}$
		Missing knowledge	$P3_{100}$, $P7_{200}$, $N8_{200}$
		Missing knowledge of parameters	$N8_{200}$
		Aware solution is not best	$P3_{100}$, $P9_{100}$, $P10_{200}$
		Code can always be improved	$P10_{200}$, $N6_{100}$
		Nobody wants insecurity	$N6_{200}$
	Standards	Industry standard	$P8_{100}$, $P9_{200}$
		Standards	$N11_{100}$, $P3_{200}$, $N2_{100}$, $P2_{100}$, $N4_{100}$, $P12_{200}$
	Experience	Experienced no security issues	$P4_{200}$, $N9_{100}$
	Tests	Conducted tests	$N9_{100}$, $N9_{200}$, $P7_{200}$
	Trust in APIs	Trusts third parties	$P6_{100}$, $P9_{200}$, $N11_{100}$, $P11_{200}$
	Social desirability vs. reality	Indicated to be security aware (needed security hint)	$P6_{200}$, $N1_{100}$, $N1_{200}$, $N3_{200}$, $N8_{200}$, $N10_{100}$, $N10_{200}$, $N11_{100}$, $N9_{200}$, $P4_{100}$, $P6_{200}$, $N7_{100}$, $N8_{100}$, $N4_{200}$

Table 2: Coding of Open Questions