The preview shows how the test is presented to participants. You can also see the correct answers for all questions except free text answers. No correct answers are shown to participants when they complete the test.

Total max score: 30

Start by reading through all questions. Peter will visit the room 45 minutes after the exam has started to clarify the questions you do not understand. Max score is 30 points.

- For grade 3, 40% of max score (12 points) is required.
- For grade 4, 60% of max score (18 points) is required.
- For grade 5, 80% of max score (24 points) is required.

You are not allowed to use the computer for anything else but answering the questions on this page.

Write your answers in either English or Swedish. If you write your answers in Swedish, make sure to not introduce any translation confusement. Write proper sentences (spelling, upper/lower case characters, punctuation, etc.). Answers that do not do this good enough/are vague/are ununderstandable cannot receive full score on the questions.

Good luck!

What is the querystring in the URI? What is it used for? Give an example.

Max score: 1

In an HTTP request, clients can send data to the server both in the querystring and in the body of the request. Explain when they should use which one.

Max score: 1

Explain what the HTTP headers `Accept`, `Content-Type` and `Location` are used for/represents respectively. Which of them can be used in requests and responses respectively?

Max score: 1.5

Pair each HTTP response code with its corresponding reason phrase.

Correct answer

200	OK
400	Bad Request
404	Not Found

500	Internal Server Error
201	Created
401	Unauthorized

Max score: 1

Explain how middlewares work in Express and what a middleware is.

Max score: 2

A REST architencture consists of a set of *architectural constraints*, as described by Roy Thomas Fielding. Explain what an architectural constraint is.

Max score: 1

Name and describe each architectural constraint REST consists of.

Max score: 3

Here is a short story:

Alice is going on semester to Australia. To do this she needs a passport and a visa ("visium" in swedish). She orders this and later picks them up at the police station. When she do this, she needs to show the police officer at the station her driver license (so not anyone else can pick them up). Then she goes to the air port and takes an air plane to Australia. In Australia she needs to show her passport and her visa for them to let her off the airport and go to the rest of Australia.

In this story, we have one identity and places where authentication and authorization takes place. Which are them? You only need to mention those that are explicitly mentioned in the text.

The identity in the story:

The place(s) where authentication takes place:

The place(s) where authorization takes place:

Max score: 1.5

Who/What follows the Same-Origin Policy?

Max score: 1.5

An Android application can send HTTP requests to any website it wants, even if that website doesn't support *Cross-Origin Resources Sharing*. Explain why this is not a security issue.

Max score: 2.5

Explain what a JWT token is and how they work/are structured internally. Is it safe to store any infromation you want in it? When the server receives back a JWT token it has previously sent to a client, can it really trust that the client hasn't modified it? Justify your answers.

Max score: 3

Does it make sense to put the user's favorite color in a JSON Web Token? Justify your answer.

Max score: 2

OAuth 2.0 defines four different ways a client can obtain an access token. Explain how each of them works and when you are supposed to use which one.

Max score: 4

OpenID Connect is an authentication layer built on top of OAuth 2.0. Describe how OpenID Connect works and what you can use it for that you can't do with OAuth 2.0. You can presume the reader already knows how OAuth 2.0 works.

Max score: 2

What is a foreign key constraint? Why should you use them, and what can happen if you don't use them? Give an example.

Max score: 2

The code below is taken from an Express application making use of an SQLite database.

```
app.get("/humans", function(request, response){
   db.all("SELECT * FROM humans", function(error, humans){
      if(error){
         console.log(error)
      }else{
         response.json(humans)
         return
      }
   })
   response.json({"error": "Got an error from the database :("})
})
```

When receiving a GET request for `/humans`, it should send back all human resources stored in the database, or an error message if it for some reason can't fetch them from the database, but the code does not work as intended. Why? Also, explain what needs to be done do make the code work as intended.

Max score: 1