OULUN AMMATTIKORKEAKOULU

Tapio Pelkonen

KYBEROPPI – TIETOTURVAN KOULUTUSPALVELU

KYBEROPPI – TIETOTURVAN KOULUTUSPALVELU

Tapio Pelkonen
Opinnäytetyö
Kevät 2017
Tietotekniikan koulutusohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietotekniikan koulutusohjelma, ohjelmistokehityksen suuntautumisvaihtoehto

---

Tekijä: Tapio Pelkonen
Opinnäytetyön nimi: Kyberoppi – tietoturvakoulutuksen koulutuspalvelu
Työn ohjaaja: Teemu Korpela
Työn valmistumislukukausi ja -vuosi: Kevät 2017
Sivumäärä: 37 + 2 liitettä

Opinnäytetyön aiheena oli suunnitella ja toteuttaa selainpohjainen tietoturvan koulutuspalvelu. Palvelu rakentuu tuotantoyhtiön toteuttaman TV-minisarjan ympärille, jossa käsitellään kuvitteellisen yrityksen kohtaamia tietoturvaan liittyviä jokapäiväisiä tilanteita.

Palvelulle tuli toteuttaa pilvipalvelin, tietokanta sekä selainkäyttöliittymä. Palvelu toteutettiin JavaScript- ja PHP-ohjelmointikielillä, HTML-kuvauskielellä sekä CSS-tyyliohjeilla. Lisäksi palvelussa hyödynnettiin jQuery-, Mustache- ja RestServer-kirjastoja sekä Ajaxia.

Opinnäytetyö alkoi perehtymisellä TV-minisarjaan sekä palvelusta kiinnostuneen asiakkaan toiveisiin. Tämän jälkeen tehtiin määrittely palvelukokonaisuudesta. Palvelulle suunniteltiin tietokanta sekä palvelimen rajapinta, jonka avulla käyttöliittymän ja tietokannan välille muodostettiin tiedonsiirtoyhteys. Lopuksi suunniteltiin ja toteutettiin käyttöliittymä sekä tarvittavat rajapintafunktiot.

Asiasanat: tietoturva, koulutus, verkkosivut, palvelin, JavaScript, PHP, MySQL

ALKULAUSE

Opinnäytetyö oli haastava: en ollut kirjoittanut riviäkään JavaScript- tai PHP-ohjelmointikielillä ennen projektiin ryhtymistä. Lisäksi minun tuli suunnitella palvelun graafinen käyttöliittymä sekä käyttökokemus.

Tämä oli projekti, jonka aikana sain vahvistuksen sille, että olen omimmillani silloin kun pitää ymmärtää monimutkainen kokonaisuus ja samalla tehdä kaikkensa, jotta se olisi mahdollisimman yksinkertainen käyttää ja ylläpitää.

Haluan kiittää työnantajaani, Second Nature Security Oy:tä luottamuksesta ja tuesta. Erityiskiitokset Jani Manniselle ja Jussi-Pekka Erkkilälle selvien linjojen vetämisestä sekä Henri Sikiölle asiakkaan näkökulman esilläpidosta.

Lämmin kiitos myös rakkaalle vaimolleni, Johannalle, kaikesta tuesta.

Klaukkalassa 30.5.2017

Tapio Pelkonen

SISÄLLYS

Liite 1. Kyberopin rakennekaavio

Liite 2. Kyberopin ERD-kaavio

1 JOHDANTO

Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa selainpohjainen tietoturvan koulutuspalvelu. Koulutuspalvelu koostui verkkosivuista, palvelimesta ja tietokannasta. Verkkosivuilla tavoitteena oli luoda mahdollisimman yksinkertainen oppimisympäristö, jonka käyttäminen ei vaatisi erillistä koulutusta. Oppimisympäristön lisäksi luotiin sisäänkirjautumisprosessi, jonka kautta pääsi hallintapaneeliin. Hallintapaneelin tarkoitus oli tukea asiakkaan itsenäistä toimintaa ja vähentää palveluntarjoajan ylläpitotoimia, kuten henkilötietojen säännöllistä päivittämistä. Palvelimen tehtävänä oli vastaanottaa verkkosivuilta kerätyt tiedot ja tallentaa ne tietokantaan, josta ne voitaisiin edelleen hakea hallintapaneeliin ja oppimisympäristöön katsottavaksi.

Asiakkaalta oli tullut pyyntö koulutusympäristöstä videoiden ympärille toteutettuna. Ideaa työstettiin ja sen pohjalta suunniteltiin käyttöliittymä ja käytettävyys. Seuraavassa vaiheessa suunniteltiin palvelun ja tietokannan rakenteet ja valittiin käytettävät ohjelmointikielet. Harkinnan alla oli myös valmiita oppimisympäristöjä, mutta kaikista vaihtoehdoista löytyi liikaa ominaisuuksia tai käyttöliittymä oli liian sekava. Kun suunnitelmat ja luonnokset olivat valmiina, siirryttiin toteuttamaan palvelu.

Jokainen oppimisjakso oli rakenteeltaan samanlainen: ensin aiheesta oli lyhyt esittelyteksti, sitten video, jota seurasi tiivistelmä videolla nähdystä tietoturva-aiheesta. Tiivistelmän jälkeen oli kolme kysymystä ja jokaiselle kysymykselle oli laadittu kolme vastausvaihtoehtoa. Vastauksesta riippumatta näkyviin tuli aina selitys, joka avasi oikeaa vastausta lisää. Kun vastasi kaikkiin kysymyksiin oikein, sai oppimisjaksosta ”suoritettu”-merkinnän.

Lopputuloksena saatiin toimiva kokonaisuus, joka toimitettiin asiakkaalle ja jonka palautteesta palvelua on kehitetty eteenpäin ja tarjottu myös muille yrityksille.

2 KÄYTETYT TEKNOLOGIAT

2.1 JavaScript

JavaScript on pääasiassa web-ympäristössä käytettävä dynaaminen komentosarjakieli (kuva 1). Sen tärkein sovellus on mahdollisuus lisätä web-sivuille dynaamista toiminnallisuutta. JavaScript on sukua C-ohjelmointikielelle, mutta on syntaksiltaan löyhä: muuttujatyyppiä ei tarvitse määrittää missään vaiheessa, sen voi vaihtaa haluamassaan kohtaa täysin eriksi ja muuttujan määrittelyn voi tehdä senkin jälkeen, kun muuttujaa on jo käytetty. (1.)

JavaScript valittiin koulutuspalvelun käyttöliittymän ohjelmointikieleksi, koska sen ja jQuery-kirjaston avulla oli tehokasta ja nopeaa muokata DOM (Data Object Model) -elementtejä. Koska palvelusta oli tarkoitus tehdä mahdollisimman yksinkertainen, niin suunnitteluvaiheessa ei nähty tarpeelliseksi käyttää pitkälle kehitettyjä ohjelmistokehyksiä, kuten Reactia tai Angjular 2:ta. Mitä enemmän kerroksia perinteisen JavaScriptin päällä, sitä raskaampaa sen käyttö, ylläpitö ja jatkokehitys.

```
/* Set UNIX timestamps to dd.mm.yyyy format */
function setTimestampToDate(ts) {

        var date = new Date(ts*1000);
        // getMonth() is zero indexed and getYear() starts from 1900
        var formatted = date.getDate() + '.' + (date.getMonth() + 1) + '.' + (date.getYear() + 1900);

        return formatted;
}
```

KUVA 1. *Funktio, jonka avulla parametrina annettu UNIX aikaleima (millisekunteja) muutetaan muotoon dd.mm.yyy.*

2.2 jQuery

jQuery on kaikille selaimille soveltuva, avoimeen lähdekoodiin perustuva JavaScript-kirjasto (kuva 2). jQuery:n syntaksi on tehty erittäin helposti ymmärrettäväksi ja sitä on nopeampi kirjoittaa kuin JavaScriptin omaa syntaksia. Sen käyttämisessä oli tärkeää huomioida selaimen käyttömuistiin

kohdistuva kuormitus, sillä kaikki JavaScriptin päälle tulevat kerrokset kasvattivat nopeasti selaimeen kohdistuvaa kuormaa. (2.)

```
function hideCheckboxes() {

        var alpha = ["a", "b", "c"];
        for (var i in alpha) {
                $("#option_" + alpha[i]).css("display", "none");
        }
}
```

KUVA 2. *jQueryn avulla tekee nopeasti muutoksia DOM-elementteihin.*

2.3 Mustache

Mustache on logiikaton mallipohjien syntaksi. Koulutuspalvelussa mustache-tageja käytettiin käytännössä kaikissa HTML-mallipohjissa (kuva 3). Mustache.js:n avulla HTML-mallipohjien täyttäminen halutulla tiedolla oli selkeää ja nopeaa (kuva 4). (3.)

```
<div class="settings">
        <div id="user_name">{{logged}} {{> username}}</div>

        <a href="admin/admin.html"><i class="fa fa-user-circle-o fa-lg" aria-hidden="true" id="user_icon"></i></a>
        <!-- Languages -->
        <ul id="languages">
                {{#languages}}
                <li class="language" id=language_{{.}}>{{.}}</li>
                {{/languages}}
        </ul>
</div>
```

KUVA 3. *Mustache-tageja HTML-mallipohjassa.*

```
// Fetch main.html
var main_template = window.templateCaller.fetchTemplate("main");
// Add languages to JSON object
window.json.main.languages = window.languages;
// Render the template with given values
var main_rendered = Mustache.render(main_template, window.json.main, {
        // partials, {{> placeholder}} in HTML
        username: userData.fname + ' ' + userData.lname
});
// Place the rendered template into div-element
$("#course_container").html(main_rendered);
```

KUVA 4. *Mustache-renderöinti JavaScript-tiedostossa.*

2.4 AJAX

AJAX (Asynchronous JavaScript And XML) on tekniikka, jonka tarkoituksena on vaihtaa pieniä määriä dataa palvelimen kanssa taustalla niin, ettei koko verkkosivua tarvitse ladata uudelleen joka muutoksen kohdalla (kuva 5). Toisin kuin nimi antaa ymmärtää, XML (Extensible Markup Language) -merkkauksen sijaan koulutuspalvelussa käytettiin yksinkertaisempaa JSON (JavaScript Open Notation)-merkkausta. (6.)

```
AjaxCaller.prototype.getCourses = function() {
    return ($.ajax({
        url: this.protocol + '://' + this.hostname + '/' + this.api + '/episodes',
        headers: {'X-Access-Token': this.accessToken},
        async: true,
          dataType: 'json',
        type: 'GET'
    }));
};
```

KUVA 5. *AjaxCaller-luokan funktio, joka palauttaa AJAX-kutsuna kaikkien kurssien yleistiedot.*

2.5 PHP

PHP on ohjelmointikieli, jota käytetään erityisesti web-palvelinympäristöissä dynaamisten sivujen luonnissa (4). Vuoden 2017 toukokuussa ohjelmointikielien suosiota arvioiva TIOBE Index sijoitti PHP:n 9. suosituimmaksi kieleksi, pari sijaa JavaScriptin alapuolelle (5). Koulutuspalveluun PHP valittiin mm. seuraavista syistä:

1. Suuri ohjelmoijien yhteisö helpottaa tiedon saannissa
2. On suosituin ohjelmointikieli palvelinpuolella
3. PHP 7.x-versiot ovat tuoneet uusia, nykyaikaisia ominaisuuksia
4. Suuret tunnetut palvelut, kuten Facebook ja WordPress, on kirjoitettu PHP:llä
5. PHP löytyy vanhoistakin palvelimista valmiina, joten palvelun siirto onnistuu tarvittaessa helposti

2.6 RESTServer

RESTServer on Jacob Wrightin kirjoittama kevytrakenteinen PHP REST-palvelin, joka on nopea ottaa käyttöön. Tietoturvan kannalta tärkein ominaisuus on sen riippumattomuus muista kirjastoista ja ohjelmistokehyksistä. Se tukee myös HTTP-autentikointia eli käyttäjän tunnistautumista. Kontrollereiden (kuva 6) avulla ohjelmointirajapintafunktioiden (API-funktioiden) kirjoittaminen oli nopeaa ja helposti ymmärrettävää sekä ylläpidettävää ensikertalaisellekin. (7.)

```php
/**
 * Fetch admin's organization
 *
 * @url GET /org
 */
public function getAdminsOrg() {

    $conn = $this->initConnection();

    /* Fetch org */
    $st = $conn->prepare('SELECT name FROM offices WHERE id = :org');
    $st->bindParam(':org', $this->org);
    $st->execute();

    $org = $st->fetch(PDO::FETCH_COLUMN, 0);
    return utf8_encode($org);
}
```

KUVA 6. *Kontrollerifunktio, jonka avulla järjestelmänvalvojan toimipisteen sijainti haetaan tietokannasta.*

2.7 MySQL

MySQL on maailman suosituin (kuva 7) vapaan lähdekoodin tietokanta, jota käytetään paljon web-palveluiden tietokantana. MySQL on suorituskykyinen, luotettava ja helppokäyttöinen. Koulutuspalveluun se valittiin hyvin pitkälti samoilla perusteilla kuin ohjelmointikieli PHP: se on todettu hyväksi, sillä on iso yhteisö ja se tulee olemaan käytössä vielä vuosikymmeniä eteenpäinkin. Lisäksi siirto palvelimelta toiselle on laajan tuen myötä helppoa. (8.)

KUVA 7. *Muutama tunnettu MySQL-tietokantaa käyttävä yritys.*

2.8 Apache HTTP

Koko koulutuspalvelu toteutettiin Amazonin pilvipalveluna (AWS) ja sen ohjelmakokoelmaksi (nk. stack) valittiin LAMP-malli: Linux, Apache, MySQL ja PHP. Palvelimena oli siis avoimen lähdekoodin Apache http (kuva 8), joka ohjelmakokoelman muiden komponenttien tavoin on vuosia olemassa ollut ja hyväksi todettu ratkaisu.

Apache pyrkii olemaan tehokas, turvallinen ja laajennettavissa oleva vapaan lähdekoodin HTTP palvelin. (9.)

```
# Apache needs to let you overrite this (AllowOverride Indexes or AllowOverride All)
DirectoryIndex index.php
<IfModule mod_rewrite.c>
        # Turn Rewrite Engine on
        RewriteEngine On
        # Send all requests to index.php (index.php will parse the request url and routes accordingly)
        RewriteRule ^.*$ index.php [QSA,L]
</IfModule>
```

KUVA 8. *.htaccess-tiedosto ohjaa pyynnöt oikean tiedoston luo.*

3 PALVELUN SUUNNITTELU

Tässä pääluvussa esitetään palvelun vaatimusmäärittely sekä kuvataan sen pääosilta vaadittavat toiminnot.

3.1 Vaatimusmäärittely

Käyttäjävaatimukset

Käyttäjävaatimuksilla tarkoitetaan toimia, jotka käyttäjän tulee pystyä toteuttamaan sovellusta käyttäessä. Selainpohjaisen palvelun käyttäjävaatimuksia ovat

koulutuspalvelussa:

- palveluun siirtyminen henkilökohtaisen linkin avulla
- aktiivisten, aktiivisten suoritettujen sekä ei-aktiivisten oppimisjaksojen näkeminen
- oppimisjakson esittelytekstin lukeminen
- videon katsominen
- tiivistelmän lukeminen
- kysymyksien lukeminen ja vastausvaihtoehdon valitseminen
- vastausvaihtoehtoihin liittyvän palautteen lukeminen
- oppimisjakson suorittamisesta saadun palautteen lukeminen.

hallintapaneelissa:

- salasanan asettaminen sisäänkirjautumista varten
- unohtuneen salasanan palauttaminen
- sisäänkirjautuminen
- käyttäjien etsiminen nimen tai henkilönumeron mukaan
- toimipaikan yleisen suoritusprosentin näkeminen
- henkilölistan päivittäminen
- käyttäjän lisääminen ja poistaminen
- käyttäjän suoritusmerkintöjen lisääminen, tallentaminen ja poistaminen
- käyttäjän henkilökohtainen ja kaikkien käyttäjien muistuttaminen

- suoritusmerkintöjen lataaminen CSV-tiedostona
- uloskirjautuminen.

Toiminnalliset vaatimukset

Toiminnalliset vaatimukset ovat sovelluksen toimimiseen edellytettäviä vaatimuksia palvelulta. Toiminnallisia vaatimuksia ovat

koulutuspalvelussa:

- käyttäjän ja oppimisjaksoihin liittyvien tietojen hakeminen tietokannasta
- käyttäjän antamien vastausten tallentaminen tietokantaan
- kaksisuuntainen ja salattu tiedonsiirto selaimen ja palvelimen välillä.

hallintapaneelissa:

- käyttäjien ja suoritettujen oppimisjaksojen tietojen hakeminen tietokannasta
- uusien tai muokattujen tietojen tallentaminen tietokantaan
- kaksisuuntainen ja salattu tiedonsiirto selaimen ja palvelimen välillä.

Ei-toiminnalliset vaatimukset

Ei-toiminnalliset vaatimukset liittyvät sovelluksen käytettävyyteen. Ei-toiminnallisia vaatimuksia ovat

- palvelun tulee toimia kaikissa yleisimmissä selaimissa selaimessa (Internet Explorer, Edge, Firefox, Chrome ja Safari)
- palvelun käyttö vaatii mahdollisimman vähän koulutusta, jos ollenkaan
- palveluun pääsee vain henkilökohtaisella linkillä, joka on jokaisella käyttäjällä yksilöllinen ja käytännössä mahdoton arvata.

3.2 Tietokannan määrittely

Palvelussa käytettävä käyttäjädata sijaitsee tietokannassa olevissa tauluissa. Tietokannasta tulee löytyä tallennusmahdollisuus seuraaville tiedoille:

- käyttäjätiedot

- käyttäjän vastaukset
- suoritetut oppimisjaksot

Palvelun tietokanta koostuu seuraavista tauluista:

- answers
- completed_episodes
- correct_answers
- episodes
- organizations
- users

Answers-taulu sisältää jokaisen oppimisjakson kaikki kolme oikeaa vastausvaihtoehtoa (a, b tai c). Completed_episodes-taulu sisältää käyttäjän tietokanta-id:tä vastaavat hyväksytysti suoritetut oppimisjaksot. Correct_answers-taulu sisältää oikeat vastausvaihtoehdot kaikkiin oppimisjaksoihin. Episodes-taulu sisältää oppimisjaksojen nimet, upotuskoodien linkit sekä oppimisjaksojen alkamis- ja päättymisajankohdat. Offices-taulu sisältää asiakkaan kaikki toimipisteet. Users-taulu sisältää kaikki käyttäjän perustiedot sekä kirjautumistiedot palveluun. Opinnäytetyön Liitteet-osiosta löytyy tarkka kuvaus tietokannan rakenteesta (liite 2).

3.3 Palvelimen rajapinnan määrittely

Palvelimen rajapinta käsittelee kaiken tiedon selainkäyttöliittymän ja tietokannan välillä. Koulutuspalvelun rajapinnalta vaaditaan seuraavat toiminnot

koulutuspalvelussa:

- käyttäjän tullessa henkilökohtaisella linkillä oppimisympäristöön, rajapinta tunnistaa käyttäjän ja palauttaa selainkäyttöliittymälle sen tarvitsemat tiedot käyttäjästä sekä oppimisjaksoista
- oppimisjakson nimi, videon upotuskoodi ja sulkeutumisajankohta haetaan tietokannasta. Jokaisen oppimisjakson sivupohjat (esittely, tiivistelmä sekä kysymykset ja vastaukset) haetaan oppimisjakson

järjestysnumeron (episodes-taulun id) mukaan erillisestä hakemistosta (/var/www/app)
- suorittaessaan oppimisjaksoa, käyttäjän vastaukset tallentuvat tietokantaan.

hallintapaneelissa:

- järjestelmänvalvojan asettaessa salasanaa, palauttaessa unohtunut salasana ja hallintapaneeliin sisään kirjautuessa rajapinnan on pystyttävä tunnistamaan käyttäjä ja palauttamaan tarvittava tieto.
- rajapinnan on pystyttävä tallentamaan järjestelmänvalvojan tekemät muutokset hallintapaneelissa.
- rajapinta pystyy päivittämään järjestelmänvalvojan tekemät muutokset hallintapaneelissa.

3.4 Selainkäyttöliittymän määrittely

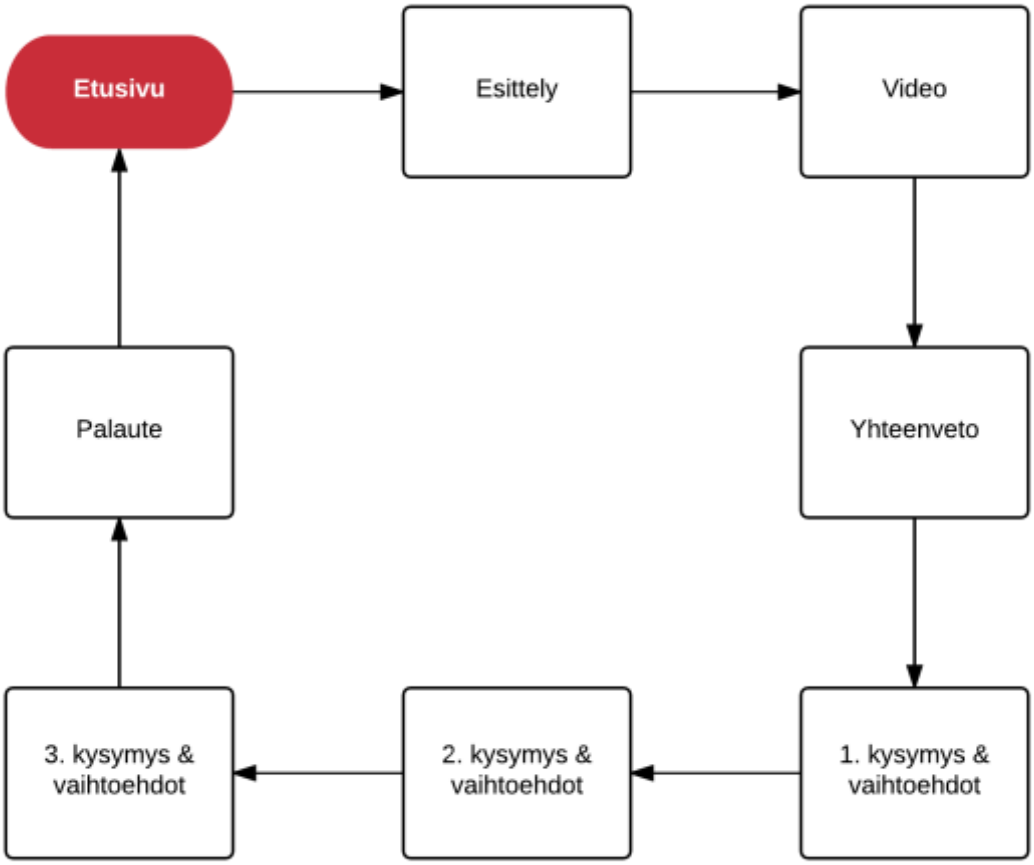
Selainkäyttöliittymältä vaaditaan seuraavat toiminnot:

- henkilökohtaisella linkillä oppimisympäristöön kirjautuminen
- oppimisjakson valinta
- oppimisjakson esittelyn näyttäminen
- oppimisjakson videon näyttäminen
- oppimisjakson tiivistelmän näyttäminen
- oppimisjakson kysymysten ja vastausvaihtoehtojen näyttäminen
- käyttäjän vastausten taustalla tallentaminen
- oppimisjakson yhteenvedon näyttäminen
- järjestelmänvalvojan salasanan asettaminen
- järjestelmänvalvojan salasanan palauttaminen
- hallintapaneeliin sisäänkirjautuminen
- järjestelmävalvojan toimipaikan työntekijöiden tietojen ja suoritusten näyttäminen listana
- listassa olevien henkilöiden suoritusmerkintöjen muuttaminen

- listassa olevien henkilöiden massamuistuttaminen suorittamattomasta kurssista
- listassa olevan henkilön poistaminen ja muistuttaminen suorittamattomasta kurssista
- uuden henkilön lisääminen
- toimipaikan tietojen tallentaminen CSV-tiedostoon, jonka voi tallentaa koneelle
- hallintapaneelista kirjautuminen ulos.

4 PALVELUN TOIMINNAN KUVAUS

Palvelusta luotu vuokaavio (kuva 9) antaa peruskäsityksen palvelun rakenteesta.



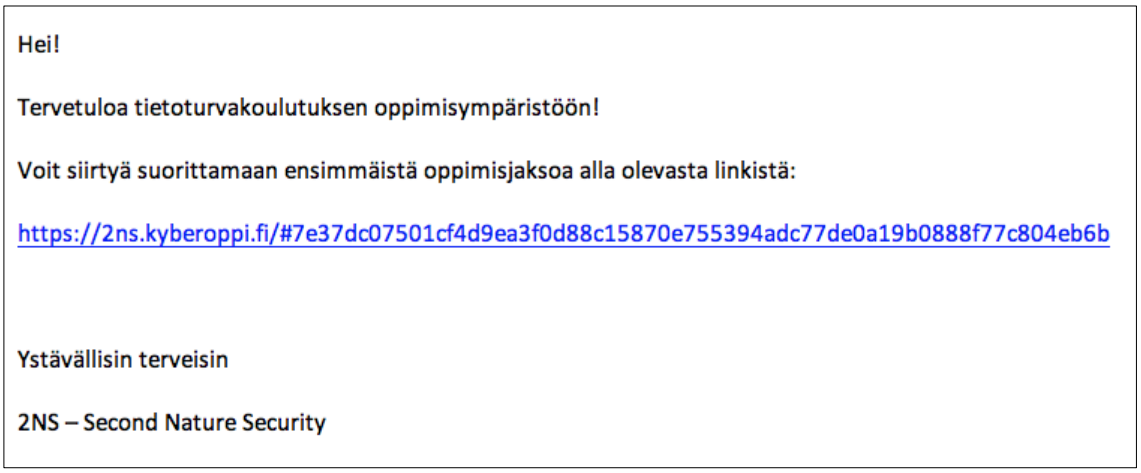
KUVA 9. *Vuokaavio koulutuspalvelusta.*

4.1 Palvelun toiminta yleisesti

Jokaiselle asiakkaalle luodaan oma instanssi, johon tarvitaan logo, pääväri ja nimilista käyttäjistä seuraavilla tiedoilla:

- koko nimi
- sähköpostiosoite
- henkilönumero
- toimipaikka.

Työntekijöiden tiedot luetaan saadusta CSV-tiedostosta ja ajetaan tietokantaan PHP-skriptillä. Kun on todettu, että tiedot ovat menneet tietokantaan oikein ja koulutusympäristö toimii halutusti, jokaiselle käyttäjälle lähetetään aloitussähköposti (kuva 10) ajamalla sitä varten tehty PHP-skripti. Sähköpostissa käyttäjä toivotetaan tervetulleeksi käyttämään palvelua ja se sisältää henkilökohtaisen linkin palveluun.


Hei!

Tervetuloa tietoturvakoulutuksen oppimisympäristöön!

Voit siirtyä suorittamaan ensimmäistä oppimisjaksoa alla olevasta linkistä:

https://2ns.kyberoppi.fi/#7e37dc07501cf4d9ea3f0d88c15870e755394adc77de0a19b0888f77c804eb6b

Ystävällisin terveisin

2NS – Second Nature Security

KUVA 10. *Aloitussähköposti.*

Päästäkseen oppimisympäristöön käyttäjä tarvitsee toimivan tietoliikenneyhteyden ja selaimen. Oppimisympäristössä (kuva 11) käyttäjä voi suorittaa kaikki avoinna olevat oppimisjaksot. Kun oppimisjakso on kerran suoritettu hyväksytysti, tulevat suoritukset eivät muuta tulosta. Jokaisen hyväksytyn suorituskerran myötä käyttäjä saa sähköpostiin tiivistelmän käydystä oppimisjaksosta. Tuotantokauden viimeisen oppimisjakson suorittamisen jälkeen käyttäjä saa sähköpostin, jossa on kaikkien kuuden oppimisjaksojen tiivistelmät allekkain, kollektiivisena muistilistana.

KUVA 11. *Oppimisympäristön päänäkymä.*

Oppimisjaksojen avautumisajankohdat määritellään ennalta ja tiedot niistä syötetään tietokantaan. Ei-aktiivinen oppimisjakso näkyy harmaana ja sen nimen alla näkyy avautumisajankohta. Avautuneen oppimisjakson ajankohtana ajetaan PHP-skripti, joka lähettää käyttäjille sähköpostilla ilmoituksen avautuneesta oppimisjaksosta. Sähköposti (kuva 12) sisältää lisäksi henkilökohtaisen linkin oppimisympäristöön.

Hei!

Oppimisympäristössä on avautunut uusi oppimisjakso.

Voit siirtyä suorittamaan oppimisjaksoa alla olevasta linkistä:

https://2ns.kyberoppi.fi/#7e37dc07501cf4d9ea3f0d88c15870e755394adc77de0a19b0888f77c804eb6b

Ystävällisin terveisin

2NS – Second Nature Security

KUVA 12. *Uuden oppimisjakson avautumisesta ilmoittava sähköposti.*

4.2 Palvelimen rajapinta

Palvelimen rajapinnan tehtävänä on käsitellä ja välittää tietoa palvelun ja tietokannan välillä. Koulutuspalvelussa rajapintafunktioita on useita. Ne on jaettu osa-alueiden mukaan eri kontrollereihin: esimerkiksi hallintapaneelia koskevat rajapintafunktiot löytyvät AdminController-luokasta, oppimisjaksoja koskevat rajapintafunktiot EpisodeController-luokasta.

RestServer-kirjasto tukee käyttäjän tunnistautumista authorize()-metodilla (kuva 13), joka tarkistaa, että käyttäjän tunnistava hash palauttaa tietokannasta vain ne tiedot, jotka tälle käyttäjälle kuuluvat. Koska käyttäjä tulee palveluun henkilökohtaisella linkillä, jossa hash on, palvelu tietää joka tilanteessa kenestä on kyse ja kenen tietoja pitää tuoda tai päivittää tietokantaan.

```
public function authorize() {
    $conn = $this->initConnection();

    $st = $conn->prepare('SELECT id FROM users WHERE login_hash = :hash');
    $headers = getallheaders();
    if (isset($headers['X-Access-Token'])) {
        $this->token = $headers['X-Access-Token'];
    } else {
        return false;
    }
    $st->bindParam(':hash', $this->token);
    $st->execute();
    $user_id = $st->fetch(PDO::FETCH_COLUMN, 0);
    if ($user_id) {
        $this->userId = $user_id;
        return true;
    }
    return false;
}
```

KUVA 13. *UserController-luokan authorize()-metodi.*

4.3 Koulutuspalvelun käyttöliittymä

Tässä osiossa kuvataan koulutuspalvelun käyttöliittymä osa-alue kerrallaan.

Aloitusviesti

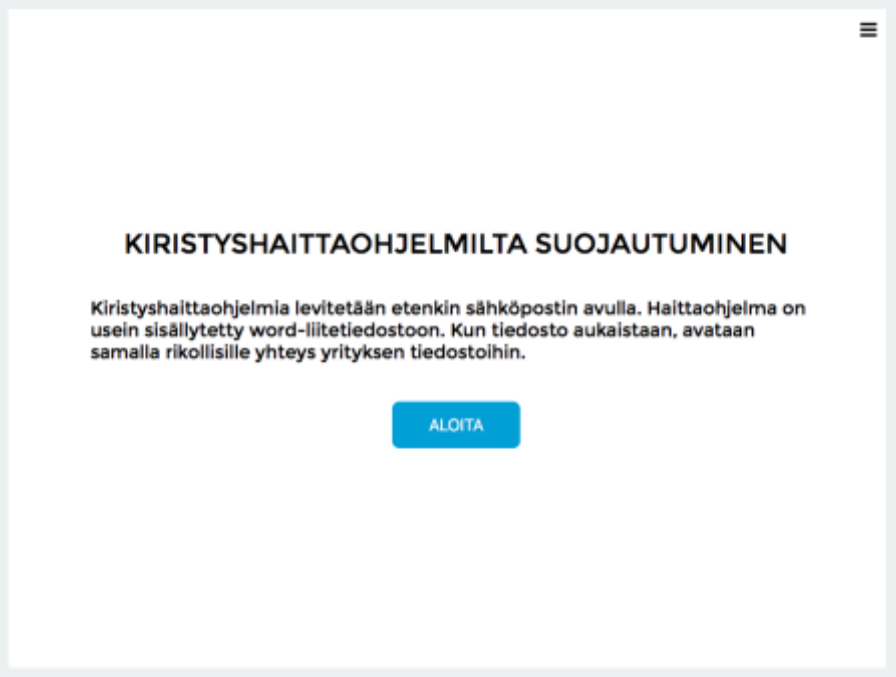
Jokainen käyttäjä saa oppimisympäristön avaamisen yhteydessä aloitussähköpostin. Koska jokainen käyttäjä siirtyy palveluun henkilökohtaisen linkin avulla, tunnistautuminen voidaan tehdä, ennen kuin oppimisympäristön sisältö lataantuu ja erillistä kirjautumista ei tarvita. Näin työntekijöiden ei tarvitse opetella yhtä salasanaa lisää.

Avoimen oppimisjakson valinta

Käyttäjä valitsee oppimisympäristöstä avoimen oppimisjakson, joka erottautuu selkeästi harmaista, lukituista oppimisjaksoista. Avoinna oleva oppimisjakso on yrityksen päävärin mukainen. Oppimisjakson nimen alla näkyy ”suoritettu”-merkintä, jos käyttäjä on vähintään kerran suorittanut kyseisen oppimisjakson hyväksytysti.

Oppimisjakson esittelytekstin lukeminen

Oppimisjakso alkaa esittelytekstillä (kuva 14), jossa hyvin yleisellä tasolla kerrotaan oppimisjakson aiheesta.

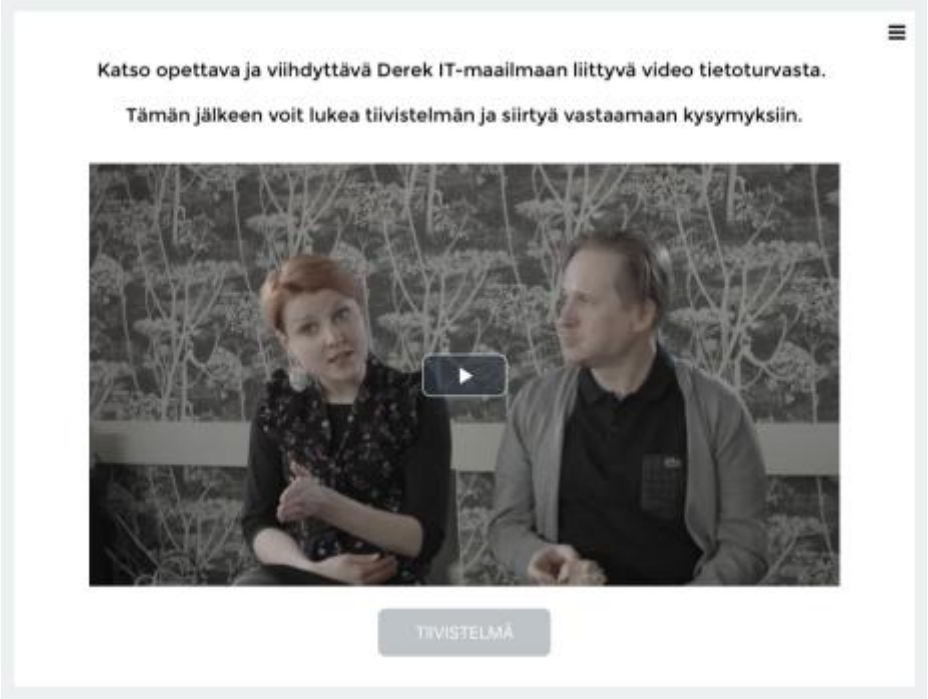


KUVA 14. *Oppimisjakson esittelyteksti.*

Videon katsominen

Oppimisjakso on rakennettu videon (kuva 15) ympärille: video on noin neljä minuuttia pitkä ja kertoo kuvitteellisesta Derek IT-nimisestä yrityksestä arkipäiväisissä tilanteissa. Joka oppimisjaksossa video keskittyy yhteen tietoturvaan liittyvään asiaan.

Videosta pääsee seuraavalle sivulle vasta, kun on odottanut kymmenen sekuntia, jotta painike tulee aktiiviseksi. Tällä ohjataan käyttäjää katsomaan video ennen tiivistelmään siirtymistä.



KUVA 15. *Oppimisjakson video viivepainikkeella.*

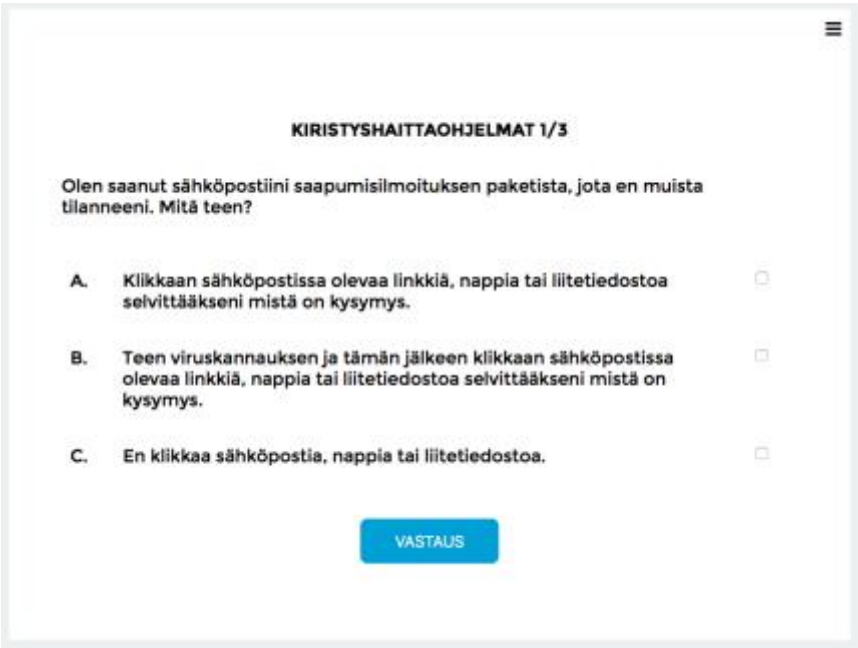
Tiivistelmän lukeminen

Videon jälkeen luetaan tiivistelmä (kuva 16), johon on kiteytetty koko oppimisjakson keskeisin tieto. Tämä tiivistelmä on sama teksti, joka lähetetään käyttäjälle sähköpostilla joka kerta, kun oppimisjakso on suoritettu hyväksytysti.

KUVA 16. *Tiivistelmä.*

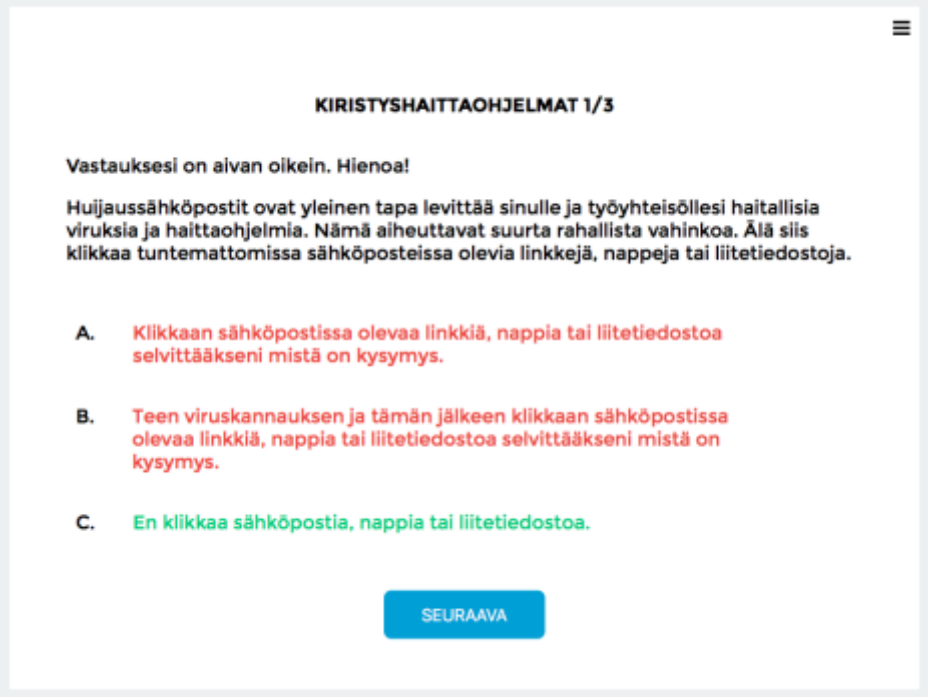
Kysymyksiin vastaaminen

Oppimisjaksossa on kolme kysymystä, joihin jokaiseen on kolme vastausvaihtoehtoa (kuva 17). Vain yhden vaihtoehdon voi valita. Muissa tapauksissa käyttäjää huomautetaan alert()-metodilla.



KUVA 17. *Kysymys ja kolme vastausvaihtoehtoa.*

Kun käyttäjä painaa ”Vastaus”-painiketta, näkyviin tulee selkeästi erotettuna oikea vastaus (kuva 18) ja lisäksi sitä avataan laajemmin vastausvaihtoehtojen yläpuolella.

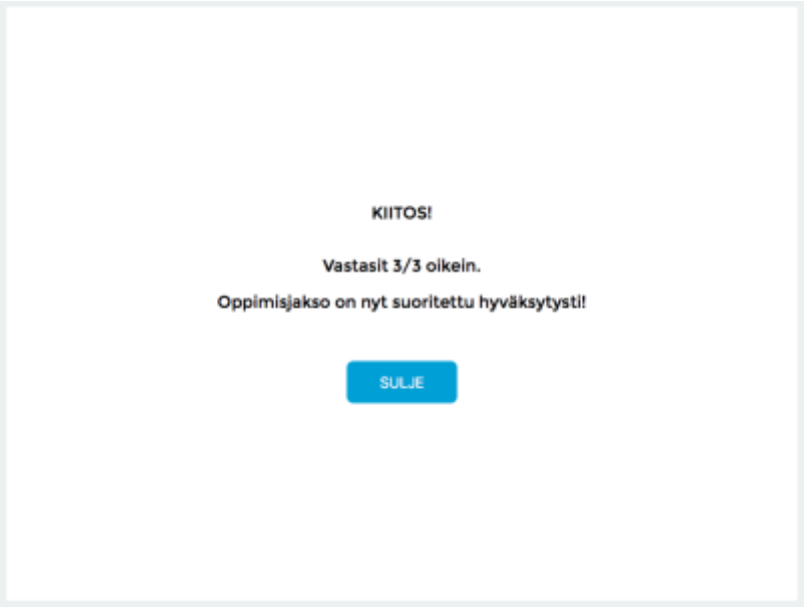


KUVA 18. *Oikea vastaus näkyy vihreänä.*

Oppimisjakson hyväksytty suoritus

Viimeisellä sivulla näkyy oikeiden vastausten määrä suhteessa kysymysten määrään. Kun käyttäjä vastaa kaikki oikein (kuva 19), hänelle lähtee sähköposti, jossa on oppimisjakson tiivistelmä. Tähän sähköpostiin käyttäjä voi palata palvelun loppumisen jälkeenkin.

Painamalla ”sulje”-painiketta käyttäjä siirtyy takaisin oppimisympäristön päänäkymään. Hyväksytysti suoritetun oppimisjakson nimen alle ilmestyy nyt ”suoritettu”-merkintä.



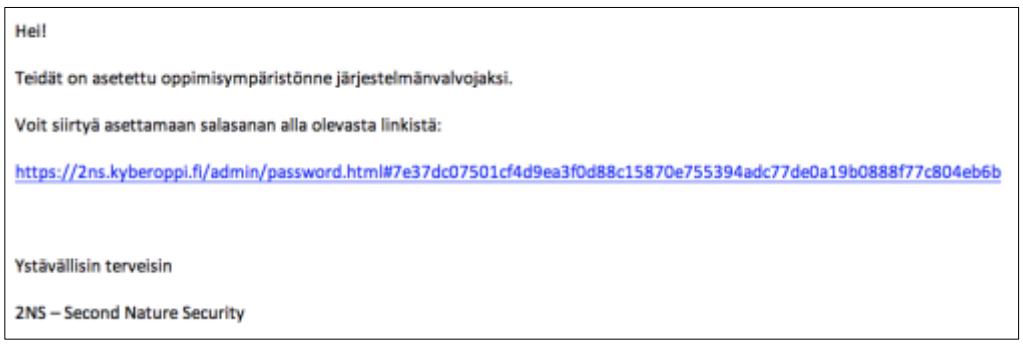
KUVA 19. *Oppimisjakso on suoritettu hyväksytysti.*

4.4 Hallintapaneelin käyttöliittymä

Hallintapaneeliin voivat kirjautua vain erikseen määritellyt järjestelmänvalvojat. Hallintapaneelissa järjestelmänvalvoja näkee oman toimipaikkansa käyttäjät ja näiden suoritukset listana. Käyttäjiä voi hakea nimen ja henkilönumeron mukaan.

Järjestelmävalvojan aloitusviesti

Järjestelmänvalvoja saa aloitusviestin (kuva 20), josta tämä pääsee asettamaan salasanan. Salasanan asettamissivulle ohjaavassa linkissä on henkilökohtainen hash, jonka avulla järjestelmä tunnistaa, että kyseessä on oikea henkilö.

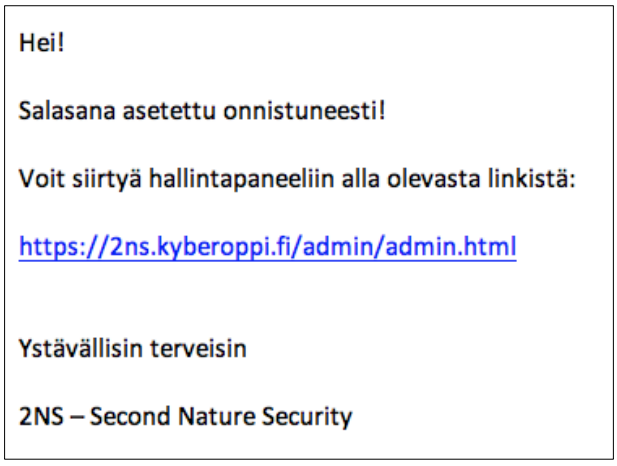


KUVA 20. *Salasanan asettamissähköposti.*

Salasanan asettaminen

KUVA 21. *Salasanan asettaminen.*

Salasanan hyväksytyn asettamisen (kuva 21) jälkeen järjestelmänvalvoja saa sähköpostin (kuva 22), jossa on suora linkki hallintapaneelin kirjautumissivulle.


Hei!

Salasana asetettu onnistuneesti!

Voit siirtyä hallintapaneeliin alla olevasta linkistä:

https://2ns.kyberoppi.fi/admin/admin.html

Ystävällisin terveisin

2NS – Second Nature Security

KUVA 22. *Salasana asennettu onnistuneesti.*

Salasanan unohtaminen

Jos järjestelmänvalvoja unohtaa salasanan, hän voi kirjoittaa uuden salasanan asettamissivulla kenttään oman sähköpostiosoitteensa. Jos käyttäjän sähköpostiosoite löytyy tietokannasta ja hänet on merkitty järjestelmänvalvojaksi, hänelle lähetetään sähköposti, jonka kautta pääsee asettamaan uuden salasanan.

Löytyy käyttäjää tietokannasta tai ei, oikean mittaisen salasanan asettamisen jälkeen kaikille tulee näkyviin sama teksti (kuva 23), jotta kukaan ei pysty tarkistamaan, kuka toimii yrityksessä järjestelmänvalvojana.

KUVA 23. *Steve ei saa koskaan sähköpostia.*

Kirjautuminen

Järjestelmänvalvoja kirjautuu hallintapaneeliin omalla sähköpostilla ja asettamallaan salasanalla (kuva 24). Hallintapaneelissa näkyvät tiedot haetaan tietokannasta vasta sitten, kun käyttäjä on kirjautunut hyväksytysti.

KUVA 24. *Kirjautuminen hallintapaneeliin sähköpostilla ja salasanalla.*

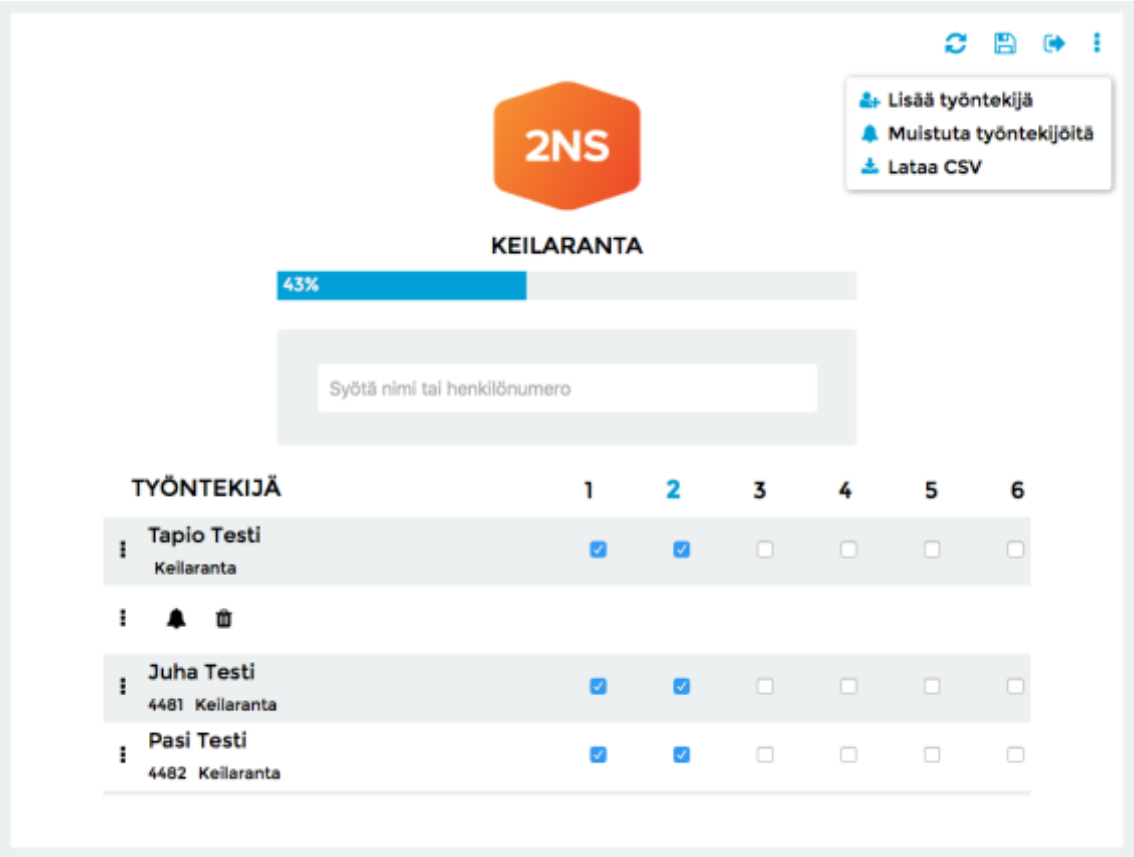
Oppimisympäristön käyttäjään liittyvät toiminnallisuudet

Hallintapaneelissa (kuva 25) järjestelmänvalvoja voi poistaa yksittäisen käyttäjän, lähettää tälle muistutuksen suorittamattomasta viimeksi auenneessa oppimisjaksosta ja muuttamaan tämän oppimisjaksojen suoritusmerkinnät.

Järjestelmänvalvoja voi yhdellä napin painalluksella lähettää sähköpostimuistutuksen kaikille niille toimipaikan työntekijöille, jotka eivät ole suorittaneet viimeksi auennutta oppimisjaksoa.

Hallintapaneelissa järjestelmänvalvoja voi tallentaa omalle koneelle CSV-tiedoston, joka sisältää selkeästi merkittynä kaikkien toimipaikan työntekijöiden nimet ja suoritusmerkinnät. Tämä ominaisuus on tehty yrityksen HR-osastoa varten.

Järjestelmänvalvoja voi lisätä uuden työntekijän ja lisäksi määrittää, onko tämä oman toimipaikkansa järjestelmänvalvoja. Hyväksyttyään uuden käyttäjän tiedot tälle lähtee automaattinen aloitusviesti sähköpostilla (kuva 10).



KUVA 25. *Hallintapaneelin kaikki toiminnallisuudet.*

5 PALVELUN TIETOTURVATESTAUS

Koska projektiin osallistuneet olivat jäävejä testaamaan tekemänsä palvelun tietoturvaa, projektin ulkopuolinen työntekijä auditoi oppimisympäristön ja hallintapaneelin kahden työpäivän aikana.

Auditoinnilla pyrittiin etsimään niin monta haavoittuvuutta kuin mahdollista ja raportoimaan niistä. Tietoturvatestauksessa käytettiin samoja sovelluksia, kuin 2NS:n normaalisti suorittamissa tietoturva-auditoinneissa, joiden avulla löydettiin muutama matalan tason haavoittuvuus.

Kaikki raportoidut huomautukset korjattiin ja tämän jälkeen koko palvelu käytiin näiltä osin vielä kertaalleen läpi. Kun auditoija oli todennut palvelun tietoturvan puolesta turvalliseksi, olimme valmiita pystyttämään ensimmäisen asiakkaan instanssin oikeilla henkilötiedoilla.

6 PALVELUN KEHITTÄMINEN TULEVAISUUDESSA

Tässä pääluvussa esitellään ne mahdolliset kehittämistarpeet, jotka nousivat esille palvelua luodessa ja sen käytettävyyttä testatessa.

6.1 Selain

Palvelun luominen oli tasapainottelua helpon käytettävyyden ja selainmuistin kuormittumisen välillä. Koska ensimmäinen asiakas oli lähes neljän tuhannen työntekijän yritys, nähtiin heti, että tavallisen käyttäjän käyttämä data ei hidasta perustoiminnollisuuksia. Muutamalta järjestelmänvalvojalta tuli palautetta hakukentän käytön hitaudesta. Hakunopeutta parannettiin luomalla muuttuja, josta haettiin tarvittavat tiedot haun perusteella ja ne päivitettiin listanäkymään. Näin saatiin karsittua tietokantahaku kokonaan.

Hakunopeutta voidaan jatkossa parantaa mm. optimoimalla kaikki for-loopit. Juuri for-loopeissa suuren tietomäärän käsittely hidastaa toimintaa huomattavasti; etenkin jos siihen liittyy yhtään rajapintafunktion käsittelyä.

6.2 Palvelin ja tietokanta

Palvelu luotiin alun perin suomenkielisille käyttäjille ja palvelun luomista helpottamaan päädyttiin tekemään joka oppimisjaksosta omat sivupohjat kiinteillä teksteillä. Nyt palvelua on alettu tarjoamaan ulkomaille ja erikielisiä käännöksiä on alettu toivomaan. Jotta ylläpito olisi mahdollisimman selkeää ja nopeaa, niin kaikille teksteille voisi luoda oman JSON-tiedoston. Tähän datarakenteeseen voi sitten viitata aina samalla tavalla kielestä riippumatta. Käyttäjälle tulee lisätä kielelle oma sarake tietokantaan ja oppimisympäristön käyttämän kieliversion saa asetettua automaattisesti tämän mukaan.

Hallintapaneelin nimilista täyttyy loppupäästä uusilla käyttäjillä. Tämä saadaan aakkosjärjestykseen korvaamalla users-taulun name-sarake uusilla fname- ja lname-sarakkeilla (etunimi ja sukunimi). Tämän jälkeen tietokantahaun voi tehdä sukunimen (lname) mukaan laskevassa järjestyksessä (ORDER BY lname ASC).

6.3 Käyttöliittymä

Käyttöliittymä on selkeä ja yksinkertainen (kuva 26). Koska tulevaisuudessa oppimisjaksoja tulee olemaan enemmän kuin kuusi, on luotava järkevä tapa selata kahden tai useamman tuotantokauden välillä päänäkymässä. Mahdollinen ratkaisu tähän on laittaa oppimisjaksojen ja logon väliin vaakariviin välilehtiä, joissa tuotantokaudet on nimetty.

KUVA 26. *Käyttöliittymään liitetty tuki eri kielille ja useammalle tuotantokaudelle.*

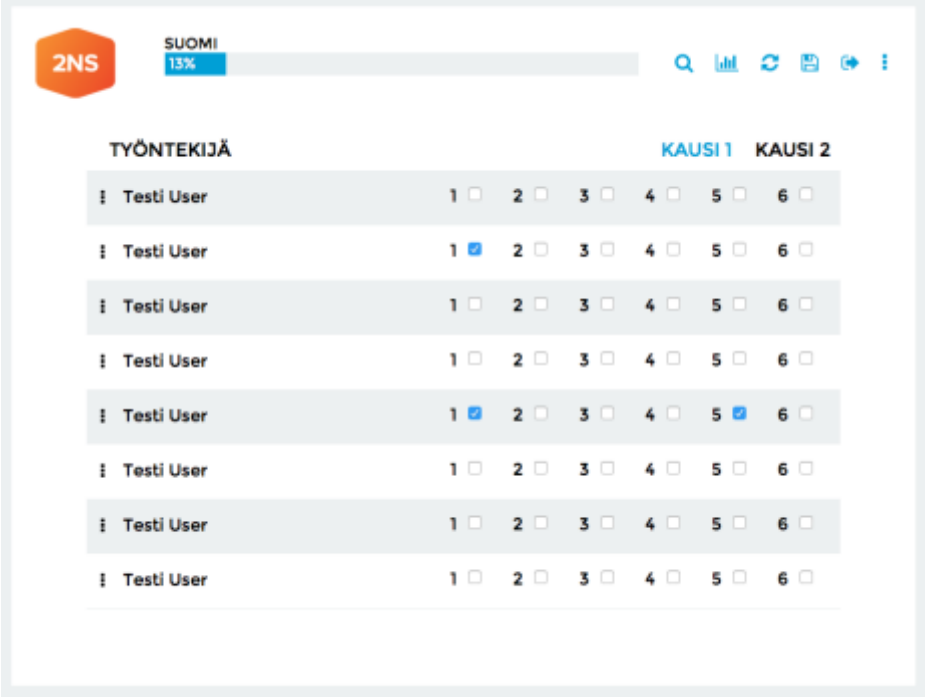
6.4 Käytettävyys

Käytettävyydeltään palvelu on helppo: hiiren liike kuvaruudulla on pyritty minimoimaan, painettavista objekteista on tehty mahdollisimman isoja ja koko koulutuspalvelu on yksi iso putki, jonka läpi mennään alle kymmenessä minuutissa ja lopuksi palataan aina samaan paikkaan.

Palautetta on saatu siitä, että kysymyksistä ei voi palata edelliseen näkymään. Palvelun avaamisen jälkeen lisäsin oikeaan yläkulmaan ikonin, josta pääsee suoraan oppimisympäristön päänäkymään ja siihen astiset oikeat merkinnät eivät vaikuta oppimisjakson suoritusmerkintään. Paluu-painiketta ei ole lisätty,

koska oppimisjaksot ovat lyhyitä ja kertaus on hyvästä. Uskon, että jatkossakin pysymme tässä kannassa.

Hallintapaneelissa (kuva 27) tulee miettiä uusiksi nimilistan näkymä. Siinä näkyy neljä työntekijää kerrallaan ja isossa yrityksessä listan selaaminen on työlästä. Tämän apuna on dynaaminen hakukenttä, mutta kokonaisuuden kannalta on hyvä, että myös listaa olisi mahdollisimman helppo käyttää.



KUVA 27. *Uusittu näkymä on rakennettu iso ja selkeä nimilista huomioiden.*

7 YHTEENVETO

Peter Sondegaard on todennut, että nykyään jokainen yritys on teknologiayritys: kaikilta aloilta löytyy ainakin tiedon siirtoa sähköisessä muodossa. Tämä altistaa jokaisen yrityksen haavoittuvuuksille ja tietomurroille. (10.)

On todettu myös, että työntekijän inhimillinen virhe on yleisin syy tietomurtoon. Tästä johtuen on tärkeää, että jokaiselle työntekijälle koulutetaan tietoturvan perusteet. Mitä nopeammin tietoturvauhkiin ja -haavoittuvuuksiin osataan reagoida, sitä pienemmäksi todelliset ja taloudelliset vahingot jäävät. (11.)

Koska koulutus on jo sanana luotaan työntävä, niin halusimme luoda koulutuspalvelun, josta kehtaa puhua lounastauolla muiden työntekijöiden kanssa. Tärkeintä oli tehdä käyttäjän näkökulmasta helposti lähestyttävä ja käytettävä kokonaisuus, joka tarjoaa eväitä myös yksityiselämän tietoturvaan.

Asetimme kolme kuukautta projektin valmistumisajaksi ja julkaisuajankohtaa siirrettiin asiakkaan toiveesta vielä kahdella viikolla. Siihen mennessä kaikki sovittu oli valmista.

Koulutuspalvelun julkaisun myötä olen saanut rauhassa keskittyä jatkokehittämiseen ja ylläpitoon. Paras palaute on saatu aina asiakkailta: sen pohjalta on hyvä jatkaa palvelun kehittämistä edelleen.

LÄHTEET

1. JavaScript. 2017. Wikipedia. Saatavissa: https://fi.wikipedia.org/wiki/JavaScript. Hakupäivä 18.4.2017.

2. jQuery. 2017. Wikipedia. Saatavissa: https://fi.wikipedia.org/wiki/JQuery. Hakupäivä 18.4.2017.

3. Mustache.js. 2016. GitHub. Saatavissa: https://github.com/janl/mustache.js/. Hakupäivä 18.4.2017.

4. PHP. 2017. Wikipedia. Saatavissa: https://fi.wikipedia.org/wiki/PHP. Hakupäivä 18.4.2017.

5. AJAX. 2017. W3Schools. Saatavissa: https://www.w3schools.com/xml/ajax_intro.asp. Hakupäivä 18.4.2017.

6. TIOBE Index for May 2017. 2017. TIOBE. Saatavissa: https://www.tiobe.com/tiobe-index/. Hakupäivä 16.5.2017.

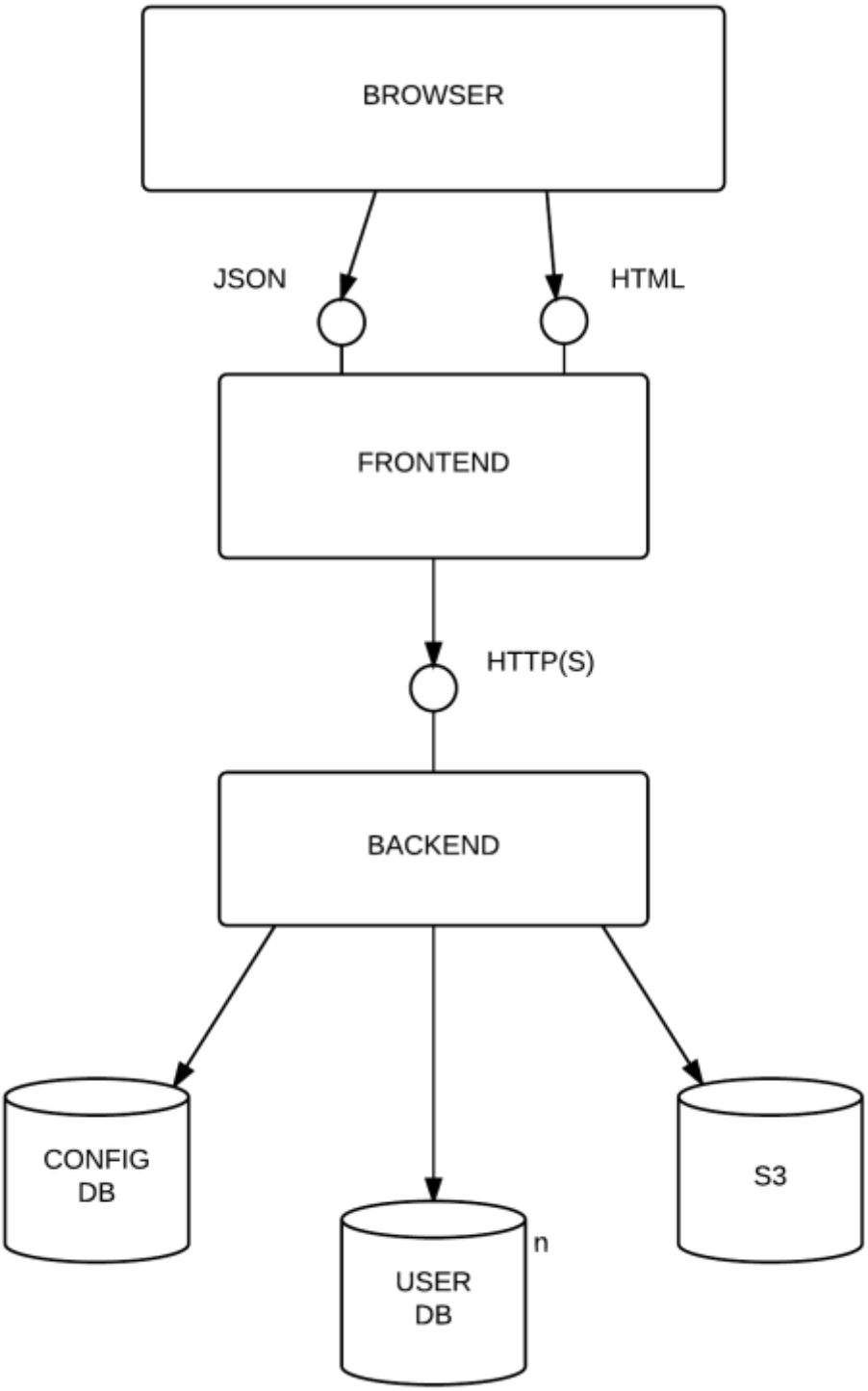
7. Jacwright RESTServer v1.0.1. 2016. GitHub. Saatavissa: https://github.com/jacwright/RestServer. Hakupäivä 16.5.2017.

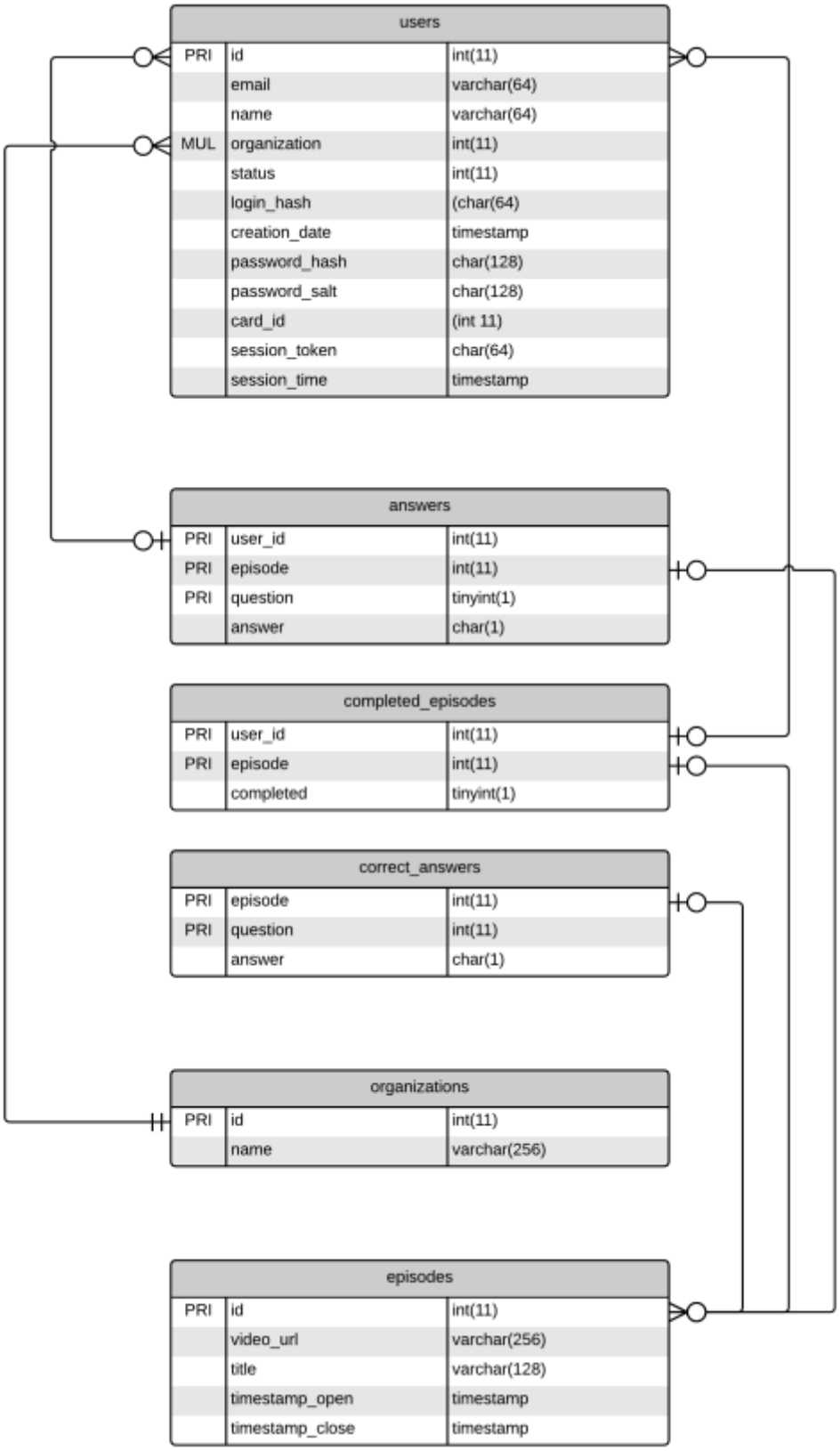
8. 1.3.1 What is MySQL? 2017. MySQL 5.7 Reference Manual. Saatavissa: https://dev.mysql.com/doc/refman/5.7/en/what-is-mysql.html. Hakupäivä 23.5.2017.

9. Apache HTTP Server Project. 2017. Apache. Saatavissa: https://httpd.apache.org/. Hakupäivä 23.5.2017.

10. Everyone is a Technology Company. 2013. Gartner Blog Network. Saatavissa: http://blogs.gartner.com/peter-sondergaard/everyone-is-a-technology-company/. Hakupäivä 16.5.2017.

11. Employees Are the Weakest Link in Computer Security. 2016. Fortune. Saatavissa: http://fortune.com/2016/06/20/employees-computer-security/. Hakupäivä 16.5.2017.


BROWSER
JSON
HTML
FRONTEND
HTTP(S)
BACKEND
CONFIG
DB
USER
DB
n
S3


users
PRI id int(11)
email varchar(64)
name varchar(64)
MUL organization int(11)
status int(11)
login_hash (char(64)
creation_date timestamp
password_hash char(128)
password_salt char(128)
card_id (int 11)
session_token char(64)
session_time timestamp
answers
PRI user_id int(11)
PRI episode int(11)
PRI question tinyint(1)
answer char(1)
completed_episodes
PRI user_id int(11)
PRI episode int(11)
completed tinyint(1)
correct_answers
PRI episode int(11)
PRI question int(11)
answer char(1)
organizations
PRI id int(11)
name varchar(256)
episodes
PRI id int(11)
video_url varchar(256)
title varchar(128)
timestamp_open timestamp
timestamp_close timestamp