qrLogin
Керівництво для розробників
1.2

Зміст

qrLogin - опис системи. **2**

Як вбудувати систему на свій веб-ресурс. **2**

Основні функції 2

Стратегія впровадження системи qrLogin в веб-ресурс 2

Принцип роботи 2

Аутентифікація на веб ресурсі 3

Реєстрація нового користувача на веб-ресурсі і в мобільному додатку. 4

Методи аутентифікації. 4

Методи передачі даних. 4

Рівні безпеки передачі облікових даних 4

Формат QR-кодів реєстрації користувача 5

Новий користувач зі статичним паролем. 5

Новий користувач з ОТП паролем. 5

Новий користувач зі статичним паролем, який генерується в мобільному додатку 6

Новий користувач з OTP паролем, ключ для якого, генерується в мобільному додатку. 7

Прив'язка схеми “qrlogin://” до QR-коду аутентифікації. 7

Додатки **9**

Типи і методи авторизації використовуються в додатку qrLogin 9

Параметри ОТП пароля при реєстрації нового облікового запису 10

Приклади QR-кодів 10

Рекомендовані коди помилок 11

qrLogin - опис системи.

qrLogin - система аутентифікації, заснована на зчитуванні qr-коду мобільним телефоном і передачі даних аутентифікації по протоколу http/https у веб-ресурс.
Мобільний додаток qrLogin, методом зчитування спеціально сформованих qr-кодів, дозволяє:

- здійснити автентифікацію до веб-ресурсу;
- зчитати і зберегти дані облікового запису;
- зчитати ідентифікаційні дані нового облікового запису, згенерувати пароль або ключ, і відправити ці дані на веб-ресурс, для закінчення реєстрації цього облікового запису.

Як вбудувати систему на свій веб-ресурс.

Основні функції

Для роботи системи аутентифікації qrLogin Вам необхідно підтримати такі функції:

1. Функція аутентифікації, яка включає в себе:
    a. формування qr-коду аутентифікації на сторінці входу в веб-ресурс;
    b. отримання та перевірку запиту аутентифікації від мобільного пристрою, який прийде на URL вказаний в qr-коді аутентифікації;
    c. перевірку отриманих даних і автоматичний вхід на веб-ресурс з обліковими даними користувача за умови, що ці дані коректні.
2. Функція реєстрації нового користувача з підтримкою системи qrLogin, яка включає:
    a. формування qr-коду з даними облікового запису користувача на сторінці реєстрації та/або на сторінці налаштувань облікових даних. Цей код необхідний для поновлення даних бази облікових записів мобільного додатка.

Стратегія впровадження системи qrLogin в веб-ресурс

До вбудовування системи qrLogin в веб ресурс необхідно відповісти на 3 питання, які допоможуть однозначно вибрати які методи аутентифікації і реєстрації необхідно підтримати.

1. Який з типів http-запитів зручніше обробляти, POST з JSON об'єктом або POST з параметрами?
2. Який тип паролів повинна підтримувати система, статичний або OTP?
3. Який рівень безпеки передачі паролів з веб-ресурсу на мобільний додаток необхідний? Чи потрібно генерувати паролі або ключі в мобільному додатку або ці дані будуть передаватися в qr-коді реєстрації.

Відповівши на ці питання, стане ясно який тип qr-коду з описаних в розділі Формат QR-кодів реєстрації користувача необхідно буде підтримати в веб-ресурсі, які дані потрібно підготувати для формування цього коду і які запити від мобільного додатка потрібно обробляти.

Принцип роботи

Основний принцип роботи системи qrLogin:

- мобільний додаток зчитує qr-код аутентифікації веб-ресурсу і знаходить відповідний запис в локальній базі даних облікових записів;

- формує дані для аутентифікації, які включають ім'я користувача, пароль або одноразовий пароль і ідентифікатор сесії, отриманий з qr-коду авторизації;
- ці дані передаються на веб-ресурс. Методи і формат передачі даних описаний в розділі Методи передачі даних;
- веб-ресурс перевіряє актуальність сесійного ідентифікатора, а також валідність облікових даних і в разі позитивної перевірки здійснює автоматичний вхід на веб-ресурс зі сторінки аутентифікації відповідної переданому сесійної ідентифікатором;
- у відповідь на запит від мобільного пристрою в разі позитивної аутентифікації веб ресурс повинен повернути HTTP статус OK - 200;
- якщо запит обробився з помилкою веб-ресурс повинен повернути відповідний статус помилки. Рекомендовані коди помилок вказані в таблиці Рекомендовані коди помилок
- qrLogin рекомендовано використовувати як додаткову систему аутентифікації. У разі відсутності інтернет з'єднання на мобільному пристрої або неможливості його використовувати (роумінг) користувач може ввести як статичний так і OTP пароль вручну через форму аутентифікації веб-ресурсу.

Аутентифікація на веб ресурсі

Для аутентифікації на веб-ресурсі розмістіть на формі логіна QR-код, що містить наступну текстову інформацію:

Строка	Описание	Значение
1	qrLogin ідентифікатор. Це константне значення для всіх типів QR-кодів	**QRLOGIN**
2	Ідентифікатор функції. Це константне значення для даного типу функції.	**L:V1**
3	URL ресурса	*https://www.resources.com/sites/yousite*
4	Унікальний ідентифікатор сесії	*b7e3d7a5707806c17a380c31a56c*

1ій и 2ий рядок є константними значеннями. 1ий рядок - "**QRLOGIN**" - це ідентифікатор системи, який бере участь у всіх qr-кодах 1им рядком. Другий рядок - ідентифікатор, що позначає що даний код призначений для аутентифікації на ресурсі.
ВАЖЛИВО: Всі константи прописуються без змін, великими літерами.
3ій рядок - URL ресурсу. URL є ідентифікатором вашого ресурсу в базі мобільного додатка. URL ресурсу не повинен включати в себе якусь з сторінок ресурсу. Це або просто ім'я веб домену (наприклад: www.youname.com) або ім'я домену з шляхом до вашого додатку (наприклад: *www.resources.com/sites/yousite*). URL ресурсу може містити назву протоколу (наприклад: *https://www.resources.com/sites/yousite*) Якщо протокол зазначений не буде, мобільний додаток за замовчуванням додасть "http://"
4ий рядок - це унікальний ідентифікатор сесії користувача на веб-ресурсі. Для цього параметра можна використовувати як http-session ідентифікатор так і будь-який інший, згенерований на веб-ресурсі.

Головне щоб цей ідентифікатор був унікальний і однозначно ідентифікував сесію користувача веб-ресурсу.
Всі рядки в qr-кодах разделяються символом "новий рябок" (\n) - код 0x0A
Приклади qr-кодів дивіться в розділі Приклади QR-кодів

Реєстрація нового користувача на веб-ресурсі і в мобільному додатку.

Для реєстрації нового користувача веб-ресурс повинен розмістити на сторінці властивостей зареєстрованого користувача спеціально сформований qr-код, прочитавши який мобільним додатком, користувач додасть або оновить аккаунт в базі мобільного додатка.
QR-код реєстрації нового користувача має ряд параметрів настройки, які залежать від методу аутентифікації, за способом передачі даних на сервер і рівня безпеки передачі облікових даних в мобільний додаток.

Методи аутентифікації.

Система qrLogin в даний момент підтримує 2 методу аутентифікації:

- за допомогою статичного пароля.
- за допомогою ОТП пароля. В системі підтриманий сучасний алгоритм генерації одноразових паролів - TOTP (Time-based One Time Password Algorithm, RFC 6238). В реалізації даного алгоритму підтримані алгоритми SHA1, SHA256, SHA512 і можливість генерувати пароль до 8ми символів.

Методи передачі даних.

Для передачі даних на сторінку аутентифікації веб-ресурсу використовується 2 методу.

- HTTP POST запит з параметрами, де дані аутентифікації передаються як параметри POST запиту. Структура запиту має наступний вигляд: objectName=**qrLogin**&login=*username*&sessionid=*xxxxSESSIONIDxxxx*&password=*userpassword*
- HTTP POST запит з JSON об'єктом. В цьому випадку параметри аутентифікації передаються як JSON об'єкт в тілі POST запиту. Формат об'єкта має наступну структуру:

```
{
        "objectName":"qrLogin",
        "sessionid":"xxxxSESSIONIDxxxx",
        "password":"userpassword",
        "login":"username"
}
```

Подібним чином мобільний пристрій передає як дані для аутентифікації так і дані для реєстрації користувача на веб-ресурсі, в разі коли використовується метод генерації пароля на стороні мобільного додатка.

Рівні безпеки передачі облікових даних

При передачі облікових даних з веб ресурсу мобільному додатку, для реєстрації нового запису в мобільному додатку, існує 2 рівня безпеки:

- стандартний - всі дані облікового запису включаючи пароль або ключ для ОТР пароля включені в QR-код реєстрації.
- посилений - QR-код містить всі дані крім пароля або ключа ОТР пароля. В цьому випадку qr-код повинен також містити ідентифікатор поточної сесії користувача. Мобільний додаток

просканувавши даний код запропонує користувачеві згенерувати пароль або згенерує ключ для OTP пароля і відправить ці дані на веб ресурс, як зазначено в розділі Методи передачі даних

ВАЖНО: Для забезпечення прийнятного рівня безпеки передачі облікових даних, ми рекомендуємо використовувати для обміну між веб-ресурсом і мобільним додатком тільки HTTPS протокол. У мобільному додатку передбачений варіант, коли SSL сертифікат є самоподпісанного. Також, мобільний додаток коректно відпрацює переадресацію HTTP запитів на HTTPS, якщо така опція налаштована на вашому веб сервері.

Формат QR-кодів реєстрації користувача

Кожен qr-код містить 1им рядком ідентифікатор "**QRLOGIN**".
У 2му рядку прописується ідентифікатор операції додавання нового користувача "**NU:V1**" або "**NU:V2**".
3ій рябок - URL веб ресурсу, який буде ідентифікатором вашого ресурсу. URL може включати ідентифікатор протоколу, але не повинен включати якусь з сторінок вашого ресурсу.
Наприклад: *https://youdomain.com*, *https://hostersite.com/youapplication*, *yoursite.com/application1*
4ий рядок містить шлях і ім'я сторінки або частини URL який буде приймати запити від мобільного додатка. У мобільному додатку повний URL на який буде відправлятися запит формується як 3ий рядок qr-кода + 4ий рядок. Якщо в URL ресурсу не вказано протокол то мобільний додаток автоматично додасть "HTTP://"
Рядки розділяються символом "новій рядок" (\n) - код 0x0A
Приклади qr-кодів дивіться в розділі Приклади QR-кодів

Новий користувач зі статичним паролем.

Рядок	Опис	Значення
1	qrLogin ідентифікатор. Це константне значення для всіх типів QR-кодів	**QRLOGIN**
2	Ідентифікатор функції. Це константне значення для даного типу функції.	**NU:V1**
3	URL ресурсу	*https://www.resources.com/sites/yousite*
4	Сторінка для авторизації користувача з мобільного додатка	*/qrlogin.xhtml*
5	Ім'я користувача	*admin*
6	Пароль	*admin*
7	Тип і метод виклику функції. Доступні типи і їх коди вказані в таблиці нижче. дивіться таблицю Типи і методи авторизації використовуються в додатку qrLogin	*1*

Новий користувач з ОТП паролем.

Рядок	Опис	Значення

1	qrLogin ідентифікатор. Це константне значення для всіх типів QR-кодів	**QRLOGIN**
2	Ідентифікатор функції. Це константне значення для даного типу функції.	**NU:V1**
3	URL ресурсу	*https://www.resources.com/sites/yousite*
4	Сторінка для авторизації користувача з мобільного додатка	*/?actions=qrlogin*
5	Ім'я користувача	*admin*
6	Параметры ОТП пароля	*см. Параметры ОТП пароля при регистрации новой учетной записи*
7	Тип і метод виклику функції. Див: Типи і методи авторизації використовуються в додатку qrLogin	*4*

Новий користувач зі статичним паролем, який генерується в мобільному додатку

Рядок	Опис	Значення
1	qrLogin ідентифікатор. Це константне значення для всіх типів QR-кодів	**QRLOGIN**
2	Ідентифікатор функції. Це константне значення для даного типу функції.	**NU:V2**
3	URL ресурсу	*https://www.yousite.com*
4	Сторінка для авторизації користувача і передачі секретних даних облікового запису при реєстрації з мобільного додатка	*/qrlogin.php*
5	Ім'я користувача	*admin*
6	Парамтри генерації пароля розділений символом ";": 1 - мінімальна довжина пароля 2 - якщо 1 - в паролі повинні бути присутніми маленькі і великі літери 3 - якщо 1 - в паролі повинні бути присутніми цифрах 4 - якщо 1 - в паролі повинні бути присутніми спец символи	*8;1;1;0*
7	Тип і метод виклику функції. Див: Типи і методи авторизації використовуються в додатку qrLogin	*2*
8	Унікальний ідентифікатор сесії. необхідний для ідентифікації поточного користувача під час отримання пральних даних від мобільного додатка.	*c08596ad07f529e123e0f8e3223b*

Новий користувач з OTP паролем, ключ для якого, генерується в мобільному додатку.

Рядок	Опис	Значення
1	qrLogin ідентифікатор. Це константне значення для всіх типів QR-кодів	**QRLOGIN**
2	Ідентифікатор функції. Це константне значення для даного типу функції.	**NU:V2**
3	URL ресурсу	*https://www.yousite.com*
4	Сторінка для авторизації користувача і передачі секретних даних облікового запису при реєстрації з мобільного додатка	*/qrlogin.php*
5	Ім'я користувача	*admin*
6	Параметри ключа OTP пароля. У цьому виді коду параметри повинні починатися з символу ";" "30" - час дії пароля в секундах "SHA1" - алгоритм генерації ключа, підтримуються алгоритми SHA1, SHA256, SHA512 "6" - довжина пароля	*;30;SHA1;6*
7	Тип і метод виклику функції. Див: Типи і методи авторизації використовуються в додатку qrLogin	*4*
8	Унікальний ідентифікатор сесії. необхідний для ідентифікації поточного користувача під час отримання пральних даних від мобільного додатка.	*c08596ad07f529e123e0f8e3223b*

Прив'язка схеми “qrlogin://” до QR-коду аутентифікації.

Для підтримки аутентифікації за допомогою програми qrLogin на мобільному пристрої пропишіть в HTML коді web-ресурсу зображення QR-коду як вміст <a> тега, href-параметр якого відформатований наступним чином:
“qrlogin://”+”текстовий зміст QR-коду авторизації”+”qrlogin://”+”URL повернення в web browser для iOS додатку”.
Текстовий зміст QR-коду в qrLogin-URL переноситься без змін, роздільник рядків "\n" для коректного відображення в URL замінюється на "%0A", в кінці текстового вмісту QR-коду “новий рядок” \n не ставиться.

Приклад URL:

qrlogin://QRLOGIN%0AL:V1%0Aqrlogin.info/forum%0A2b6f237da373b639448a788ea18cf12fqrlogin://http%3A%2F%2Fqrlogin.info%2Fforum%2Findex.php

Приклад HTML кода:

<?xml

*version="1.0" encoding="utf-8"?> <img src="tmp/qrcode.png" width="100" height="100" alt="qrcode"> *

Користувач, зайшовши на web-ресурс з мобільного пристрою, на якому встановлено додаток qrLogin, натискає на зображення QR-коду. В результаті запускається додаток qrLogin, в якому користувач може авторизуватися за параметрами вказаними в URL на web-ресурсі і qrLogin поверне управління назад в browser.
Аналогічно, для зображення QR-коду реєстрації нового користувача потрібно прописати **<a>** тег у якого href параметр має наступний формат:
“qrlogin://”+”ттекстовий зміст QR-коду реєстрації нового користувача”
URL для повернення в web browser в даному випадку не потрібний.

Приклад URL:

qrlogin://QRLOGIN%0ANU:V1%0Aqrlogin.info/forum%0A/qrlogin%0Auser%0A%0A2

Приклад HTML кода:

* <img src="tmp/qrcode.png" width="100" height="100" alt="qrcode"> *

Додатки

Типи і методи авторизації використовуються в додатку qrLogin

Название	Описание	Код
Статичний пароль, HTTP(s) запит POST з параметрами	Мобільний додаток виконує POST запит для URL сторінки аутентифікації (наприклад: https://qrlogin.tcon.com.ua/qrLogin/?actions=qrlogin) що містить дані аутентифікації як параметри запиту, наприклад: objectName=qrLogin&login=admin&sessionid=bd54390368c40000b6dfae69bdbf&password=admin Порядок полів в параметрах пошуку можуть бути довільні. У разі успішної авторизації сервер повертає стандартний HTTP статус "OK" - 200	**1**
Статичний пароль, HTTP(s) запит POST з JSON	Мобільний додаток відкриває URL сайту зі сторінкою аутентифікації (наприклад: https://qrlogin.tcon.com.ua/qrLogin/loginsecret.xhtml) і методом POST посилає JSON об'єкт такого змісту: {"objectName":"**qrLogin**","sessionid":"*bdfa017358ee07403f77c564c2b0*","password":"*admin*","login":"*admin*"} Порядок полів в JSON об'єкті може бути довільні, формат такої як вказано в прикладі.	**2**
OTP пароль, HTTP(s) запит POST з параметрами	Мобільний додаток виконує POST запит для URL сторінки аутентифікації (наприклад: https://qrlogin.tcon.com.ua/qrLogin/?actions=qrlogin) що містить дані аутентифікації, наприклад: objectName=qrLogin&login=test&sessionid=be3ee6cf88573b767bccef0af0f4&password=737018 В якості пароля передається OTP пароль розрахований пристроєм згідно параметрам ОТП пароля при реєстрації. Порядок полів в параметрах пошуку можуть бути довільні. У разі успішної авторизації сервер повертає стандартний HTTP статус "OK" - 200	**3**
OTP пароль, HTTP(s) запит POST з JSON	Мобильное приложение открывает URL сайта со страницей аутентификации (например: https://qrlogin.tcon.com.ua/qrLogin/loginsecret.xhtml) і методом POST посилає JSON об'єкт такого змісту: {"sessionid":"be711d16882a90be0a5cba6cc3eb","password":"495655","objectName":"qrLogin","login":"test"} Порядок полів в JSON об'єкті може бути довільні, формат такої як вказано в прикладі. В якості пароля передається OTP пароль розрахований пристроєм згідно параметрам ОТП пароля при реєстрації.	**4**
Не показувати пароль після	Якщо немає необхідності показувати пароль користувача на екрані мобільного пристрою при помилки аутентифікації, добавте	**1XX**

помилки аутентифікації.	до коду - 100. Наприклад: 101, 102, 103, ...	

Параметри ОТП пароля при реєстрації нового облікового запису

Рядок ОТП пароля складається з наступних полів між якими ставиться крапка з комою (;):
OTPKey;ValidTime;Algorithm;PasswordLen

OTPKey - секретний ключ на базі якого розраховується ОТП пароль, повинен відповідати обраному алгоритму і передається як рядок hex-значення ключа;
ValidTime - час дії ОТП пароля в секундах;
Algorithm - алгоритм розрахунку ОТП пароля. Підтримані: SHA1, SHA256, SHA512
PasswordLen - Довжина пароля в символах, діапазон значень 1 - 8.

Приклад:
43ACCFA77B3620735D6D6E0068AFE2BA1059EE0A8D366A2150ED47B167BE32A393613F02A089F496C0CE8FA5FFA106436D2FDDA72E0684D4A80E4F58520FCB7E;300;SHA1;6

Приклади QR-кодів

Функция	**Пример**
Авторизація Вміст QR-коду: *QRLOGIN* *L:V1* *qrlogin.tcon.com.ua/qrLogin* *b7e3d7a5707806c17a380c31a56c*	
Реєстрація нового користувача зі статичним паролем в мобільному додатку Вміст QR-коду: *QRLOGIN* *NU:V1* *qrlogin.tcon.com.ua/qrLogin* */loginsecret.xhtml* *admin* *admin* *1*	
Реєстрація нового користувача з ОТП паролем. Ключ в QR-коді. Вміст QR-коду: *QRLOGIN* *NU:V1* *qrlogin.tcon.com.ua/qrLogin* */loginsecret.xhtml*	

admin *43ACCFA77B3620735D6D6E0068AFE2BA1059EE0A8D366A2* *150ED47B167BE32A393613F02A089F496C0CE8FA5FFA1064* *36D2FDDA72E0684D4A80E4F58520FCB7E;30;SHA1;6* *4*	
Реєстрація нового користувача зі статичним паролем який генерується в мобільному додатку і передається на сервер. Вміст QR-коду: *QRLOGIN* *NU:V2* *qrlogin.tcon.com.ua/qrLogin* */loginsecret.xhtml* *admin* *8;1;1;0* *2* *c08596ad07f529e123e0f8e3223b*	
Реєстрація нового користувача з ОТП паролем ключ для якого генерується в мобільному додатку і передається на сервер. Вміст QR-коду: *QRLOGIN* *NU:V2* *qrlogin.tcon.com.ua/qrLogin* */loginsecret.xhtml* *admin* *;30;SHA1;6* *4* *c08596ad07f529e123e0f8e3223b*	

Рекомендовані коди помилок

Мобільний додаток qrLogin визначає результат виконання команди по HTTP-статусу який веб-ресурс повертає на http-запит.

Код	Обозначение	Назначение
200	OK	Успішне виконання запиту
400	BAD_REQUEST	Невірно сформований запит
403	FORBIDDEN	Доступ заборонено. Аутентифікація пройшла неуспішно.
406	NOT_ACCEPTABLE	Запит поновлення пароля або ключа при реєстрації нового користувача з генерацією пароля / ключа на мобільному пристрої не виконано
408	REQUEST_TIMEOUT	Таймаут виконанню внутрішніх операцій веб-ресурсу.