qrLogin
Руководство для разработчиков
1.2

Оглавление

qrLogin - описание системы.

qrLogin - система аутентификации, основанная на считывании qr-кода мобильным телефоном и передаче данных аутентификации по протоколу http/https в веб-ресурсе.
Мобильное приложение qrLogin, методом считывания специально сформированных qr-кодов, позволяет:

- аутентифицироваться на веб-ресурсе;
- вычитать и сохранить данные учетной записи;
- вычитать идентификационные данные новой учетной записи, сгенерировать пароль или ключ, и отправить эти данные на веб-ресурс, для окончания регистрации данной учетной записи.

Встраивание системы в ваш веб-ресурс.

Основные функции

Для работы системы аутентификации qrLogin Вам необходимо поддержать следующие функции:

1. Функция аутентификации, которая включает в себя:
    a. формирование qr-кода аутентификации на странице входа в веб-ресурс;
    b. получение и проверку запроса аутентификации от мобильного устройства, который придет на URL указанный в qr-коде аутентификации;
    c. проверку полученных данных и автоматический вход на веб-ресурс с учетными данными пользователя при условии, что эти данные корректны.
2. Функция регистрации нового пользователя с поддержкой системы qrLogin, которая включает:
    a. формирование qr-кода с данными учетной записи пользователя на странице регистрации и/или на странице настроек учетных данных. Этот код необходим для обновления данных базы учетных записей мобильного приложения.

Стратегия внедрения системы qrLogin в веб-ресурс

До встраивания системы qrLogin в веб ресурс необходимо ответить на 3 вопроса, которые помогут однозначно выбрать какие методы аутентификации и регистрации необходимо поддержать.

1. Какой из типов http-запросов удобнее обрабатывать, POST с JSON объектом или POST с параметрами?
2. Какой тип паролей должна поддерживать система, статический или OTP?
3. Какой уровень безопасности передачи паролей с веб-ресурса на мобильное приложение необходим? Нужно ли генерировать пароли или ключи в мобильном приложении или эти данные будут передаваться в qr-коде регистрации.

Ответив на эти вопросы, станет ясно какой тип qr-кода из описанных в разделе Формат QR-кодов регистрации пользователя необходимо будет поддержать в веб-ресурсе, какие данные нужно подготовить для формирования этого кода и какие запросы от мобильного приложения нужно обрабатывать.

Принцип работы

Основной принцип работы системы qrLogin следующий:

- мобильное приложение считывает qr-код аутентификации веб-ресурса и находит соответствующую запись в локальной базе данных учетных записей;
- формирует данные для аутентификации, которые включают имя пользователя, пароль или одноразовый пароль и идентификатор сессии, полученный из qr-кода авторизации;
- эти данные передаются на веб-ресурс. Методы и формат передачи данных описан в разделе Методы передачи данных;
- веб-ресурс проверяет актуальность сессионного идентификатора, а также валидность учетных данных и в случае положительной проверки осуществляет автоматический вход на веб-ресурс со страницы аутентификации соответствующей переданному сессионному идентификатору;
- в ответ на запрос от мобильного устройства в случае положительной аутентификации веб ресурс должен вернуть HTTP статус OK - 200;
- если запрос обработался с ошибкой веб-ресурс должен вернуть соответствующий статус ошибки. Рекомендованные коды ошибок указаны в таблице Рекомендуемые коды ошибок
- qrLogin рекомендовано использовать как дополнительную систему аутентификации. В случае отсутствия интернет соединения на мобильном устройстве или невозможности его использовать (роуминг) пользователь может ввести как статический так и OTP пароль вручную через форму аутентификации веб-ресурса.

Аутентификация на веб ресурсе

Для аутентификации на веб-ресурсе разместите на форме логина QR-код, содержащий следующую текстовую информацию:

Строка	Описание	Значение
1	qrLogin идентификатор. Это константное значение для всех типов QR-кодов	**QRLOGIN**
2	Идентификатор функции. Это константное значение для данного типа функции.	**L:V1**
3	URL ресурса	*https://www.resources.com/sites/yousite*
4	Уникальный идентификатор сессии	*b7e3d7a5707806c17a380c31a56c*

1ая и 2ая строка являются константными значениями. 1ая строка - "**QRLOGIN**" - это идентификатор системы, который присутствует на всех qr-кодах 1ой строкой. Вторая строка - идентификатор, обозначающий что данный код предназначен для аутентификации на ресурсе.
ВАЖНО: Все константы прописываются без изменений, большими буквами.
3я строка - URL ресурса. URL является идентификатором вашего ресурса в базе мобильного приложения. URL ресурса не должен включать в себя какую либо из страниц ресурса. Это либо просто имя веб домена (например: www.youname.com) или имя домена с путем к вашему приложению (например: *www.resources.com/sites/yousite*). URL ресурса может содержать название протокола (например: *https://www.resources.com/sites/yousite*) Если протокол указан не будет, мобильное приложение по умолчанию добавит "http://"

4ая строка - это уникальный идентификатор сессии пользователя на веб-ресурсе. Для этого параметра можно использовать как http-session идентификатор так и любой другой, сгенерированный на веб-ресурсе. Главное чтобы этот идентификатор был уникальный и однозначно идентифицировал сессию пользователя веб-ресурса.
Все строки в qr-кодах разделяются символом “перевод строки” (\n) - код 0x0A
Примеры qr-кодов смотрите в разделе Примеры QR-кодов

Регистрация нового пользователя на веб-ресурсе и в мобильном приложении.

Для регистрации нового пользователя веб-ресурс должен разместить на странице свойств зарегистрированного пользователя специально сформированный qr-код, считав который мобильным приложением, пользователь добавит или обновит аккаунт в базе мобильного приложения.
QR-код регистрации нового пользователя имеет ряд параметров настройки, которые зависят от метода аутентификации, метода передачи данных на сервер и уровня безопасности передачи учетных данных в мобильное приложение.

Методы аутентификации.

Система qrLogin в данный момент поддерживает 2 метода аутентификации:

- с помощью статического пароля.
- с помощью ОТП пароля. В системе поддержан современный алгоритм генерации одноразовых паролей - TOTP (Time-based One Time Password Algorithm, RFC 6238). В реализации данного алгоритма поддержаны алгоритмы SHA1, SHA256, SHA512 и возможность генерировать пароль до 8ми символов.

Методы передачи данных.

Для передачи данных на страницу аутентификации веб-ресурса используется 2 метода.

- HTTP POST запрос с параметрами, где данные аутентификации передаются как параметры POST запроса. Структура запроса имеет следующий вид: objectName=**qrLogin**&login=*username*&sessionid=*xxxxSESSIONIDxxxx*&password=*userpassword*
- HTTP POST запрос с JSON объектом. В этом случае параметры аутентификации передаются как JSON объект в теле POST запроса. Формат объекта имеет следующую структуру:

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

Подобным образом мобильное устройство передает как данные для аутентификации так и данные для регистрации пользователя на веб-ресурсе, в случае когда используется метод генерации пароля на стороне мобильного приложения.

Уровни безопасности передачи учетных данных

При передаче учетных данных от веб ресурса мобильному приложению, для регистрации новой записи в мобильном приложении, существует 2 уровня безопасности:

- стандартный - все данные учетной записи включая пароль или ключ для OTP пароля включены в QR-код регистрации.
- усиленный - QR-код содержит все данные кроме пароля или ключа OTP пароля. В этом случае qr-код должен также содержать идентификатор текущей сессии пользователя. Мобильное приложение просканировав данный код предложит пользователю сгенерировать пароль или сгенерирует ключ для OTP пароля и отправит эти данные на веб ресурс, как указано в разделе Методы передачи данных.

ВАЖНО: Для обеспечения приемлемого уровня безопасности передачи учетных данных, мы рекомендуем использовать для обмена между веб-ресурсом и мобильным приложением только HTTPS протокол. В мобильном приложении предусмотрен вариант, когда SSL сертификат является самоподписанным. Также, мобильное приложение корректно отработает переадресацию HTTP запросов на HTTPS, если такая опция настроена на вашем веб сервере.

Формат QR-кодов регистрации пользователя

Каждый qr-код содержит 1ой строкой идентификатор "**QRLOGIN**".
Во 2ой строке прописывается идентификатор операции добавления нового пользователя "**NU:V1**" или "**NU:V2**".
3я строка - URL веб ресурса, который будет являться идентификатором вашего ресурса. URL может включать идентификатор протокола, но не должен включать какую либо из страниц вашего ресурса.
Например: *https://youdomain.com*, *https://hostersite.com/youapplication*, *yoursite.com/application1*
4ая строка содержит путь и имя страницы или части URL который будет принимать запросы от мобильного приложения. В мобильном приложении полный URL на который будет отправляться запрос формируется как 3я строка qr-кода + 4ая строка. Если в URL ресурса не указан протокол то мобильное приложение автоматически добавит "HTTP://"
Строки разделяются символом "перевод строки" (\n) - код 0x0A
Примеры qr-кодов смотрите в разделе Примеры QR-кодов

Новый пользователь со статическим паролем.

Строка	Описание	Значение
1	qrLogin идентификатор. Это константное значение для всех типов QR-кодов	**QRLOGIN**
2	Идентификатор функции. Это константное значение для данного типа функции.	**NU:V1**
3	URL ресурса	*https://www.resources.com/sites/yousite*
4	Страница для авторизации пользователя с мобильного приложения	*/qrlogin.xhtml*
5	Имя пользователя	*admin*
6	Пароль	*admin*
7	Тип и метод вызова функции. Доступные типы и их коды указаны в таблице ниже. Смотрите таблицу Типы и методы авторизации используемые в	*1*

	приложении qrLogin	

Новый пользователь с ОТП паролем.

Строка	Описание	Значение
1	qrLogin идентификатор. Это константное значение для всех типов QR-кодов	**QRLOGIN**
2	Идентификатор функции. Это константное значение для данного типа функции.	**NU:V1**
3	URL ресурса	*https://www.resources.com/sites/yousite*
4	Страница для авторизации пользователя на мобильном приложении	*/?actions=qrlogin*
5	Имя пользователя	*admin*
6	Параметры ОТП пароля	*см. Параметры ОТП пароля при регистрации новой учетной записи*
7	Тип и метод вызова функции. См. Типы и методы авторизации используемые в приложении qrLogin	*4*

Новый пользователь со статическим паролем, который генерируется в мобильном приложении

Строка	Описание	Значение
1	qrLogin идентификатор. Это константное значение для всех типов QR-кодов	**QRLOGIN**
2	Идентификатор функции. Это константное значение для данного типа функции.	**NU:V2**
3	URL ресурса	*https://www.yousite.com*
4	Страница для авторизации пользователя и передачи секретных данных учетной записи при регистрации с мобильного приложения	*/qrlogin.php*
5	Имя пользователя	*admin*
6	Парамтры генерации пароля разделенный символом “;”: 1 - минимальная длинна пароля 2 - если 1 - в пароле должны присутствовать маленькие и большие буквы 3 - если 1 - в пароле должны присутствовать цыфры 4 - если 1 - в пароле должны присутствовать спец символы	*8;1;1;0*

7	Тип и метод вызова функции. См. Типы и методы авторизации используемые в приложении qrLogin	*2*
8	Уникальный идентификатор сессии. необходим для идентификации этого пользователя во время получения учетных данных от мобильного приложения.	*c08596ad07f529e123e0f8e3223b*

Новый пользователь с OTP паролем, ключ для которого, генерируется в мобильном приложении.

Строка	Описание	Значение
1	qrLogin идентификатор. Это константное значение для всех типов QR-кодов	**QRLOGIN**
2	Идентификатор функции. Это константное значение для данного типа функции.	**NU:V2**
3	URL ресурса	*https://www.yousite.com*
4	Страница для авторизации пользователя и передачи секретных данных учетной записи при регистрации с мобильного приложения	*/qrlogin.php*
5	Имя пользователя	*admin*
6	Параметры ключа OTP пароля. В этом виде кода параметры должны начинаться с символа “;” “30” - время действия пароля в секундах “SHA1” - алгоритм генерации ключа, поддерживаются алгоритмы SHA1, SHA256, SHA512 “6” - длина пароля	*;30;SHA1;6*
7	Тип и метод вызова функции. См. Типы и методы авторизации используемые в приложении qrLogin	*4*
8	Уникальный идентификатор сессии. необходим для идентификации текущего пользователя во время получения парольных данных от мобильного приложения.	*c08596ad07f529e123e0f8e3223b*

Привязка схемы qrlogin:// к QR-коду аутентификации.

Для поддержки аутентификации с помощью приложения qrLogin на мобильном устройстве пропишите в HTML коде web-ресурса изображения QR-кода как содержимое **<a>** тега, href-параметр которого отформатирован следующим образом:
“qrlogin://”+”текстовое содержание QR-кода авторизации”+”qrlogin://”+”URL возврата в web browser для iOS приложения”.
Текстовое содержание QR-кода в qrLogin-URL переносится без изменений, разделитель строк “\n” для корректного отображения в URL заменяется на “%0A”, в конце текстового содержания QR-кода перевод строки не ставится.

Пример URL:

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

Пример HTML кода:

```
<a href="qrlogin://QRLOGIN%0AL:V1%0Aqrlogin.info/forum%0A28724a2b649681934471740b8c399ae8qrlogin://http%3A%2F%2Fqrlogin.info%2Fforum%2Findex.php" title="Scan in qrLogin"><?xml version="1.0" encoding="utf-8"?> <img src="tmp/qrcode.png" width="100" height="100" alt="qrcode"> </a>
```

Пользователь, зайдя на web-ресурс с мобильного устройства, на котором установлено приложение qrLogin, нажимает на изображение QR-кода. В результате запускается приложение qrLogin, в котором пользователь может авторизоваться по параметрам указанным в URL на web-ресурсе и qrLogin вернет управление обратно в browser.
Аналогично, для изображения QR-кода регистрации нового пользователя нужно прописать **<a>** тег у которого href параметр имеет следующий формат:
“qrlogin://”+”текстовое содержание QR-кода регистрации нового пользователя”
URL для возврата в web browser в данном случае не нужен.

Пример URL:

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

Пример HTML кода:

```
<a href="qrlogin://QRLOGIN%0ANU:V1%0Aqrlogin.info/forum%0A/qrlogin%0Amorry%0A%0A2" title="Scan for save account qrLogin"> <img src="tmp/qrcode.png" width="100" height="100" alt="qrcode"> </a>
```

Приложения

Типы и методы авторизации используемые в приложении qrLogin

Название	Описание	Код
Статический пароль, HTTP(s) запрос POST с параметрами	Мобильное приложение выполняет POST запрос для URL страницы аутентификации (например: https://qrlogin.tcon.com.ua/qrLogin/?actions=qrlogin) содержащий данные аутентификации как параметры запроса, например: objectName=qrLogin&login=admin&sessionid=bd54390368c40000b6dfae69bdbf&password=admin Порядок полей в параметрах запроса могут быть произвольные. В случае успешной авторизации сервер возвращает стандартный HTTP статус “OK” - 200	**1**
Статический пароль, HTTP(s) запрос POST с JSON	Мобильное приложение открывает URL сайта со страницей аутентификации (например: https://qrlogin.tcon.com.ua/qrLogin/loginsecret.xhtml) и методом POST посылает JSON обьект следующего содержания: {"objectName":"**qrLogin**","sessionid":"*bdfa017358ee07403f77c564c2b0*","password":"*admin*","login":"*admin*"} Порядок полей в JSON обьекте может быть произвольные, формат такой как указан в примере.	**2**
OTP пароль, HTTP(s) запрос POST с параметрами	Мобильное приложение выполняет POST для URL страницы аутентификации (например: https://qrlogin.tcon.com.ua/qrLogin/?actions=qrlogin) содержащий данные аутентификации, например: objectName=qrLogin&login=test&sessionid=be3ee6cf88573b767bccef0af0f4&password=737018 В качестве пароля передается OTP пароль рассчитанный устройством согласно параметрам ОТП пароля при регистрации. Порядок полей в параметрах запроса могут быть произвольные. В случае успешной авторизации сервер возвращает стандартный HTTP статус “OK” - 200	**3**
OTP пароль, HTTP(s) запрос POST с JSON	Мобильное приложение открывает URL сайта со страницей аутентификации (например: https://qrlogin.tcon.com.ua/qrLogin/loginsecret.xhtml) и методом POST посылает JSON обьект следующего содержания: {"sessionid":"be711d16882a90be0a5cba6cc3eb","password":"495655","objectName":"qrLogin","login":"test"} Порядок полей в JSON обьекте может быть произвольные, формат такой как указан в примере. В качестве пароля передается OTP пароль рассчитанный устройством согласно параметрам ОТП пароля при регистрации.	**4**
Не показывать пароль после	Если нет необходимости показывать пароль пользователя на экране мобильного устройства при ошибки аутентификации,	**1XX**

ошибки аутентификации.	добавте к коду - 100. Например: 101, 102, 103,...	

Параметры ОТП пароля при регистрации новой учетной записи

Строка ОТП пароля состоит из следующих полей разделенных точкой с запятой (;):
OTPKey;ValidTime;Algorithm;PasswordLen

OTPKey - секретный ключ на базе которого рассчитывается ОТП пароль, должен соответствовать выбранному алгоритму и передается как строка hex-значения ключа;
ValidTime - время действия ОТП пароля в секундах;
Algorithm - алгоритм расчета ОТП пароля. Поддержаны: SHA1, SHA256, SHA512
PasswordLen - Длина пароля в символах, диапазон значений 1 - 8.

Пример:
43ACCFA77B3620735D6D6E0068AFE2BA1059EE0A8D366A2150ED47B167BE32A393613F02A089F496C0CE8FA5FFA106436D2FDDA72E0684D4A80E4F58520FCB7E;300;SHA1;6

Примеры QR-кодов

Функция	Пример
Авторизация Содержимое QR-кода: *QRLOGIN* *L:V1* *qrlogin.tcon.com.ua/qrLogin* *b7e3d7a5707806c17a380c31a56c*	
Регистрация нового пользователя со статическим паролем в мобильном приложении Содержимое QR-кода: *QRLOGIN* *NU:V1* *qrlogin.tcon.com.ua/qrLogin* */loginsecret.xhtml* *admin* *admin* *1*	
Регистрация нового пользователя с ОТП паролем. Ключ в QR-коде. Содержимое QR-кода: *QRLOGIN* *NU:V1* *qrlogin.tcon.com.ua/qrLogin* */loginsecret.xhtml*	

admin *43ACCFA77B3620735D6D6E0068AFE2BA1059EE0A8D366A2* *150ED47B167BE32A393613F02A089F496C0CE8FA5FFA1064* *36D2FDDA72E0684D4A80E4F58520FCB7E;30;SHA1;6* *4*	
Регистрация нового пользователя со статическим паролем который генерируется в мобильном приложении и передается на сервер. Содержимое QR-кода: *QRLOGIN* *NU:V2* *qrlogin.tcon.com.ua/qrLogin* */loginsecret.xhtml* *admin* *8;1;1;0* *2* *c08596ad07f529e123e0f8e3223b*	
Регистрация нового пользователя с ОТП паролем ключ для которого генерируется в мобильном приложении и передается на сервер. Содержимое QR-кода: *QRLOGIN* *NU:V2* *qrlogin.tcon.com.ua/qrLogin* */loginsecret.xhtml* *admin* *;30;SHA1;6* *4* *c08596ad07f529e123e0f8e3223b*	

Рекомендуемые коды ошибок

Мобильное приложение qrLogin определяет результат выполнение команды по HTTP-статусу который веб-ресурс возвращает на http-запрос.

Код	Обозначение	Назначение
200	OK	Успешное выполнение запроса
400	BAD_REQUEST	Неверно сформирован запрос
403	FORBIDDEN	Доступ запрещен. Аутентификация прошла не успешно.
406	NOT_ACCEPTABLE	Запрос обновления пароля или ключа при регистрации нового пользователя с генерацией пароля/ключа на мобильном устройстве не выполнен
408	REQUEST_TIMEOUT	Таймаут выполения внутренних операций веб-ресурса.