

Использование двухэтапной аутентификации в приложении на Django Framework

Киселева Елизавета Александровна

Приамурский государственный университет им. Шолом-Алейхема

Студент

Аннотация

В момент рассвета информационных технологий, с особой скоростью растет популярность использования веб-приложений. На текущий момент существует множество веб-приложений, которые приносят крупным и даже мелким компаниям большие деньги. Таким образом, в ходе работы описан способ защиты учетных записей с помощью двухэтапной авторизации. После чего подробно раскрыто внедрение двухэтапной авторизацию в приложении разработанного на Framework Django.

Ключевые слова: веб-приложение, Framework Django, двухэтапной аутентификации.

Using 2-step authentication in an application on the Django Framework

Kiseleva Elizaveta Alexandrovna

Sholom-Aleichem Priamursky State University

Student

Abstract

At the dawn of information technology, the popularity of using web applications is growing with particular speed. Currently, there are many web applications that bring large and even small companies a lot of money. Thus, in the course of work, a method of protecting accounts using two-step authorization is described. After that, the implementation of two-stage authorization in an application developed on Framework Django is described in detail.

Keywords: web application, Framework Django, 2-step verification.

В настоящее время, веб-приложения развиваются с особой скоростью. На текущий момент существует множество языков программирования и фреймворков для разработки веб-приложений, которые приносят крупным и даже мелким компаниям большие деньги. Из-за роста конкурентов вырастает и количество злоумышленников, которые хотят сделать вред путем взлома учетной записи.

Цель данной статьи организация защиты учетной записи при авторизации на сайте, разработанном на Framework Django.

Многие ученые занимались проблемой, связанной с разработкой веб приложений. Ученые Р. И. Баженов и О. Ю. Пронина [1] описали разработку

информационной системы учета и контроля брусита с помощью Framework Yii2. Размахнина А. Н. [2] произвела обзор PHP фреймворков для разработки веб-приложений. S. Sano [3] в своей работе описал способ работы reCaptcha. З.А. Арсаханова [4] привел пример двухэтапной авторизации сайта на языке PHP.

Framework разрабатывается для облегчения разработки приложений за счет готовых функций, за счет чего уменьшается порог вхождения и время на разработку веб-приложений. Но не один Framework в полной мере не может обезопасить сайт от злоумышленников. Таким образом, было решено использовать двухэтапную авторизацию для более надежной защиты.

Для безопасности учетной записи на приложении разработанном на Framework Django было решено использовать двухэтапную авторизацию.

Двухэтапная аутентификация или двухфакторная – это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж – это логин и пароль, второй – специальный код, приходящий по SMS или электронной почте. Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя.

Двухэтапную аутентификацию часто называют двухфакторной, не делая особой разницы между понятиями. Двухфакторная аутентификация может быть двухэтапной, но обратное верно не всегда. Граница между этими понятиями очень тонкая, поэтому их часто и не различают. Двухэтапная аутентификация (Two-Step Verification, 2SV). Вход выполняется в два этапа – например, сначала вы вводите пароль к учетной записи, а потом код из SMS.

На первом этапе, требуется установить библиотеку, которая позволит организовать двойную двухтактную авторизацию. Для этого потребуется использовать команду:

```
pip install django-two-factor-auth.
```

Далее в файле `settings.py` добавить следующий код:

```
INSTALLED_APPS = (  
    'django_otp',  
    'django_otp.plugins.otp_static',  
    'django_otp.plugins.otp_totp',  
    'two_factor',  
)  
MIDDLEWARE = (  
    ...  
    'django.contrib.auth.middleware.AuthenticationMiddleware',  
    'django_otp.middleware.OTPMiddleware',  
)
```

В файле `urls.py` добавить роутер для второй авторизации:

```
from two_factor.urls import urlpatterns as tf_urls
urlpatterns = [
    path(include(tf_urls))
]
```

Далее требуется зарегистрировать на официальном сайте сайт, на котором планируется организовать двойную аутдификацию. После регистрации сайта пользователь получит штрихкод, благодаря которому сможет в мобильном приложении Google Authenticator привязать сайт. На рисунке 1 изображена страница привязки сайта.

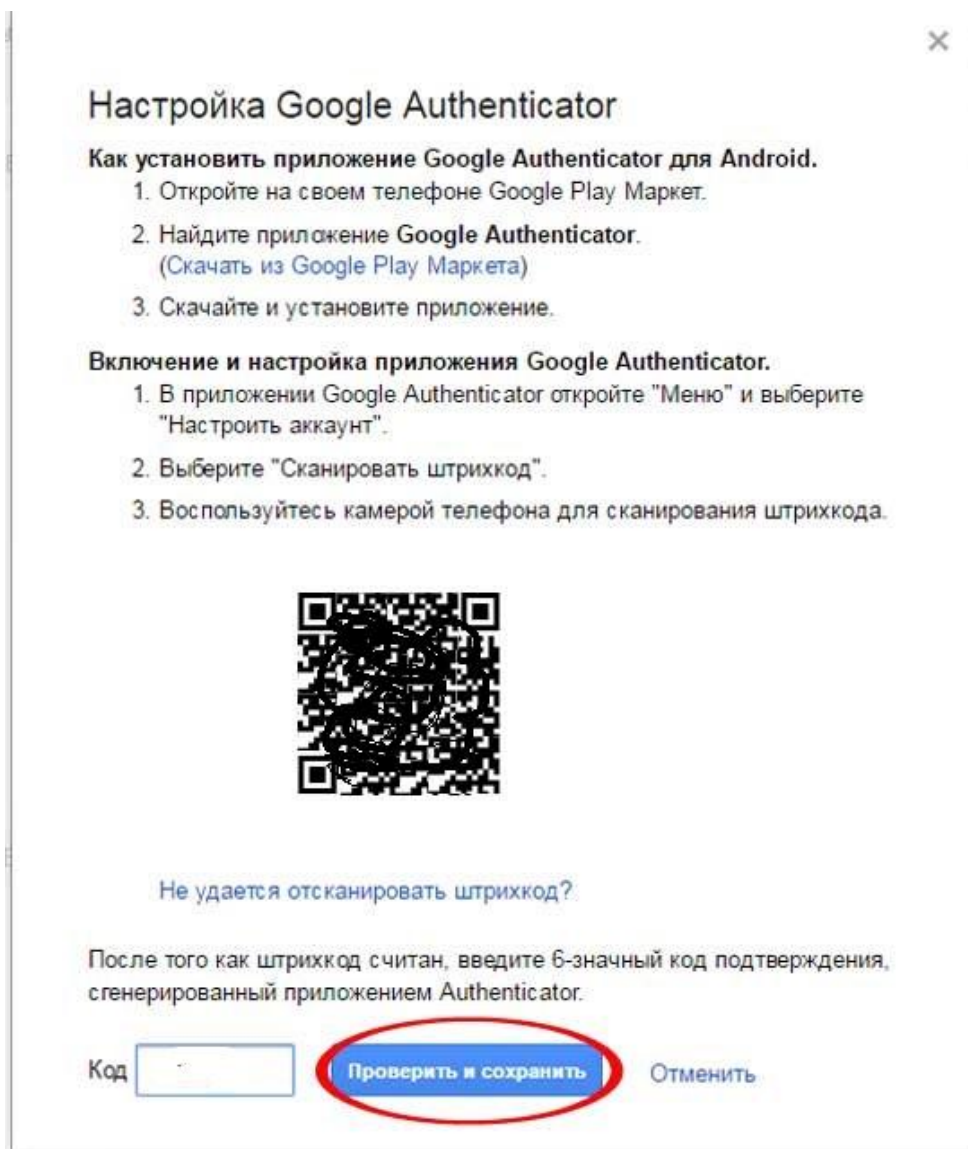


Рисунок 1 – Страница привязки сайта

После привязки сайта к программе, каждую минуту изменяется одноразовый пароль, который требуется вводить. На рисунке 2 изображен одноразовый пароль.

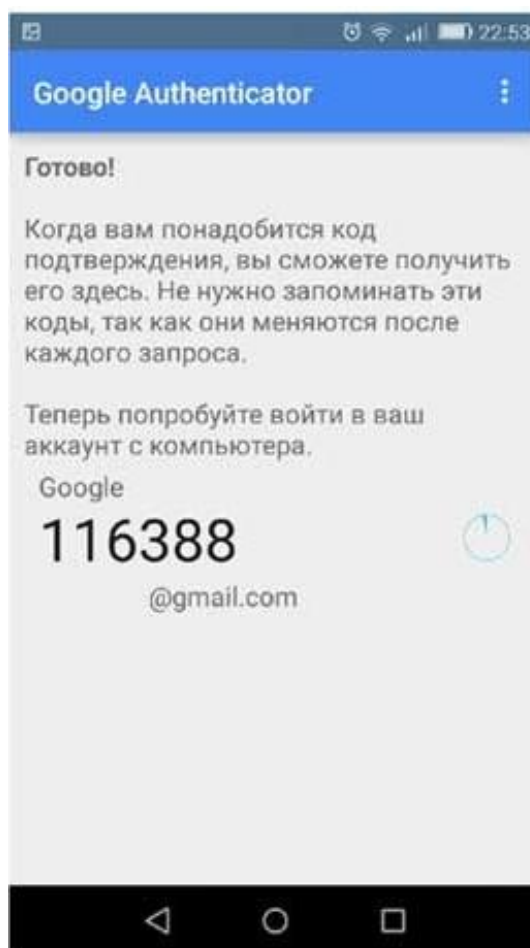


Рисунок 2 – Одноразовый пароль

Таким образом, после ввода логина и пароля пользователя перенаправляет на страницу ввода второго кода, где требуется ввести одноразовый код и только после этого происходит авторизация.

Заключение

В ходе работы для защиты учетной записи при авторизации на сайте было решено использовать двухэтапную аутентификацию. Вследствие чего, была успешно внедрена двойная аутентификация на сайте разработанном на Framework Django, которая обезопасит сайт от злоумышленников.

Библиографический список

1. Баженов Р. И., Пронина О. Ю. Разработка на фреймворке yii информационной системы учета и контроля брусита //Информационные технологии в экономике и управлении. 2016. С. 100-103.
2. Размахнина А. Н. Обзор PHP фреймворков //Постулат. 2018. №. 1
3. Sano S. et al. HMM-based Attacks on Google's ReCAPTCHA with Continuous Visual and Audio Symbols //Journal of Information Processing. 2015. Т. 23. – №. 6. С. 814-826.
4. Арсаханова З. А. Авторизация и аутентификация клиента банка //Современные условия взаимодействия науки и техники. 2017. С. 27.