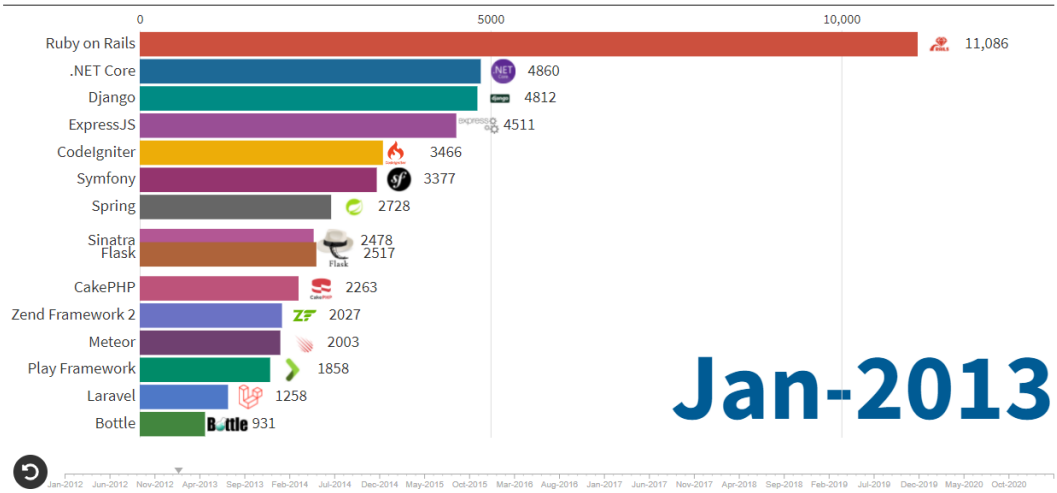
Phillip Yarbrough
S6 Assignment
A590

Web Frameworks, SQL Injection, and Race Condition

Developing web applications is an imperative tool in every information technology engineer's arsenal. Web apps can be developed for many different reasons such as communication between facilities, collaborating on projects on shared documents, also creating files, reports, and share information from anywhere and with any device necessary. Web applications is a heavily important field that many companies and small businesses owners need for our fast-paced economic growth. All communication, economic consumerism, and business is primary done now through some type of web application for ease, documentation, and low maintenance. Web applications are extremely important now and are growing at a tremendous pace.

According to Erikka Innes, "Bottle is a fast, micro web framework for Python. It has no dependencies besides the Python standard library and is so lightweight that the module for it is a single file. It handles everything you need to create small websites or applications. It's also async-friendly, allowing you to easily keep your application data continuously updated. Another nice feature is it comes with a built-in HTTP development server." [1] Bottle is a great choice for a user if they are building a web application that is small or you want to develop a prototype for an idea. The best part about using Bottle is that it is simple to use and a great tool for web application developers who are new or novices. The one downside for using Bottle is that is has a lot less documentation and support than Flask or Django. Bottle also does not have built-in are admin panel, ORM framework, NoSQL support, REST support, security, web forms, or authentication.

Below is a graph from StatisticsandData.org on the most popular backend frameworks [2]:

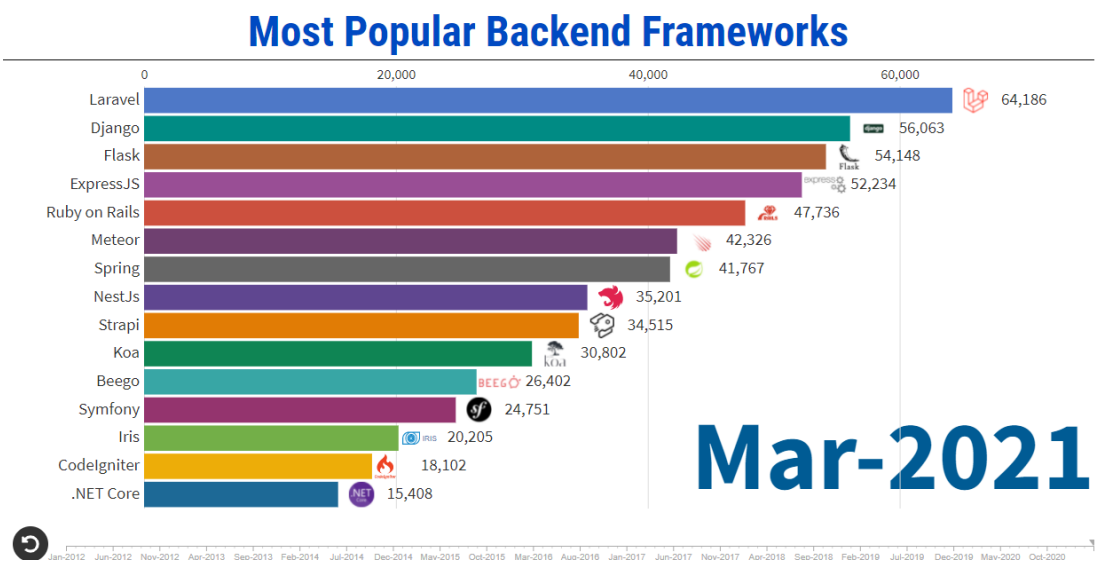


As you can see Bottle reached its popularity in January of 2013 and has dropped dramatically since then due to more popular backend frameworks being developed. Bottle seems like a great web application framework for beginners and learning opportunities to enhance one's skills.

According to fullstackpython.com, "Flask is considered more Pythonic than the Django web framework because in common situations the equivalent Flask web application is more explicit. Flask is also easy to get started with as a beginner because there is little boilerplate code for getting a simple app up and running." [3] There are countless developers that say Flask is a better choice than Bottle because Flask offers everything that Bottle has, but also adds countless new extensions, tools, and documentation. For a newer user who wants to do a more challenging web application, Flask would be a great choice. Someone out there has already documented a way to do whatever you are worming on is a great chance. Flask has a tremendous amount of content to support one's project.

Flask has fantastic extensions such as an admin panel, support REST, and a web form support. One major advantage of Flask is that it offers built-in security. A user can increase their security in Flask by purchasing Flask-Security. The only downside is that the user will have to stay up to date with security updates and patches as they are being discovered.

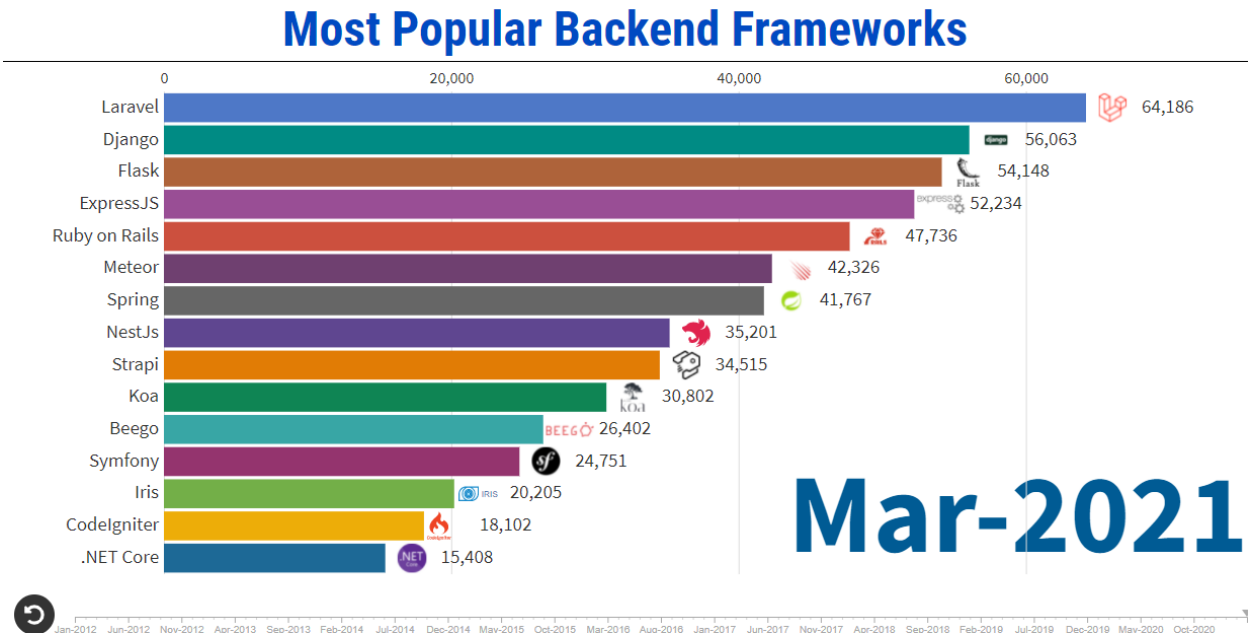
Below is a graph from StatisticsandData.org on the most popular backend frameworks:



As you can see, in March 2021 Flask was the third most popular backend framework right behind Django in second and Laravel in first.

According to djangoproject.com, "Django is a high-level Python web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of web development, so you can focus on writing your app without needing to reinvent the wheel. It's free and open source." [4] Django is fast and easy to develop web applications, but to do this a user must take time to learn the framework first. One of the best features of Django is its security. The primary purpose for Django was to be engineered to help protect your website for you. Some of the features of Django's security is it gives you a secure way to manage accounts and passwords and prevents you from making mistakes like putting session information in cookies. It enables protection against vulnerabilities like SQL injection, cross-site scripting, cross-site request forgery, and clickjacking.

Below is a graph from StatisticsandData.org on the most popular backend frameworks:



As you can see, in March 2021 Django was the second most popular backend framework right behind Laravel in first. A user should choose Django if you want to build a medium to large sized web application, make security a top priority, you are okay with an opiniated framework, and you have time to learn the framework.

SQL injection is one of the oldest vulnerabilities that is still present in modern day. This attack is in the OWASP top 10 for more than fifteen years! SQL injection allows a user to steal and modify information that is accessible in millions of databases throughout the world. SQL injection occurs when an attacker gets access to the data that is mistakenly treated as code by the SQL interpreter. Here is an example of SQL injection from cybersecure.com, "Take for example: the input field of a form (username/password combo) on a website, where an attacker enters "' OR 1=1;". This specific string is added at the end of an SQL query. When this query is executed, it allows the attacker to bypass authentication without knowledge of the password." [5] If this were to happen on a login page, this attack can return all user records that includes their usernames and passwords.

According to the image below, 29% of web applications are still vulnerable to SQL injections:

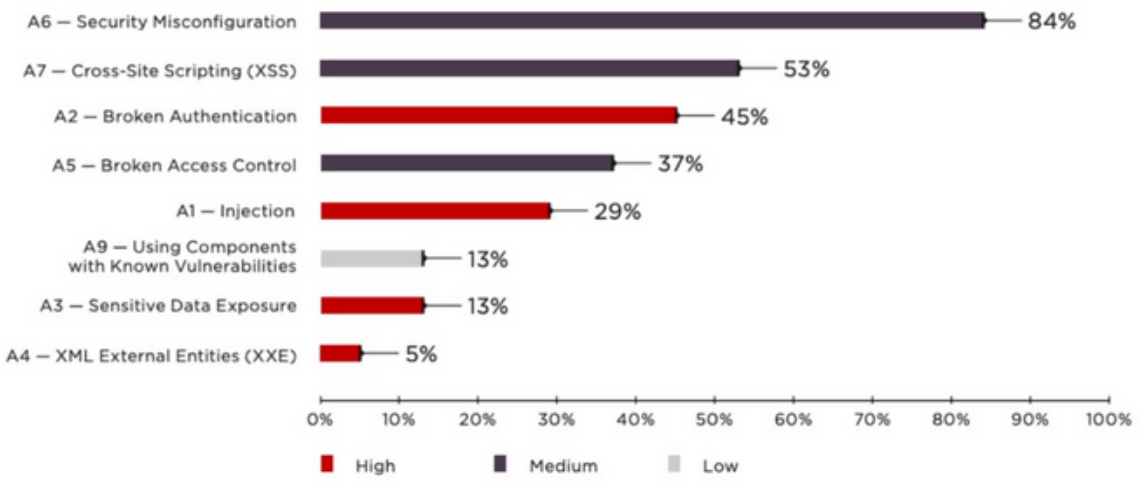


Image : *Most common OWASP Top 10 vulnerabilities* (percentage of web applications)
Credit : Web Application vulnerabilities and threats : statistics for 2019

We can confidently say that SQL injection attacks are still happening in 2021 and are continuing to be a huge problem with web applications.

According to searchstorage.techtarget.com, "A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but be cause of the nature of the device or system, the operations must be done in the proper sequence to be done correctly." [6] Race condition occurs when two computer program processes attempt to access the same resource at the same time. This can cause problems within the system and cause a computer to shutdown its applications.

One example of race condition is if a command is executed to read and write a large amount of data are received in the same instance. When this occurs, simultaneously another command is executed that attempts to overwrite some or all the old data while that old data is still being read. If all of this happens simultaneously the computer can crash or identify an illegal operation, an error can occur reading the data, and an error can occur writing the new data.

References

[1] Innes, E. (2021, May 25). *Bottle vs. Flask vs. Django-for python developers*. Medium. Retrieved October 30, 2021, from https://betterprogramming.pub/bottle-vs-flask-vs-django-for-python-developers-1f0be2f0e5d0.

[2] *Most popular backend frameworks – 2012/2021 - new update*. Statistics and Data. (2021, June 23). Retrieved October 30, 2021, from https://statisticsanddata.org/data/most-popular-backend-frameworks-2012-2021/.

[3] *Flask*. Full Stack Python. (n.d.). Retrieved October 30, 2021, from https://www.fullstackpython.com/flask.html.

[4] Django. (n.d.). Retrieved October 30, 2021, from https://www.djangoproject.com/.

[5] Ferradj, A. (2021, September 24). *SQL injection : Why is this attack still possible in 2021 ?* CyberSecura 2021. Retrieved October 30, 2021, from https://en.cybersecura.com/post/sql-injection-why-is-this-attack-still-possible-in-2021.

[6] Lutkevich, B., & Posey, B. (2021, June 16). *What is a race condition?* SearchStorage. Retrieved October 30, 2021, from https://searchstorage.techtarget.com/definition/race-condition.