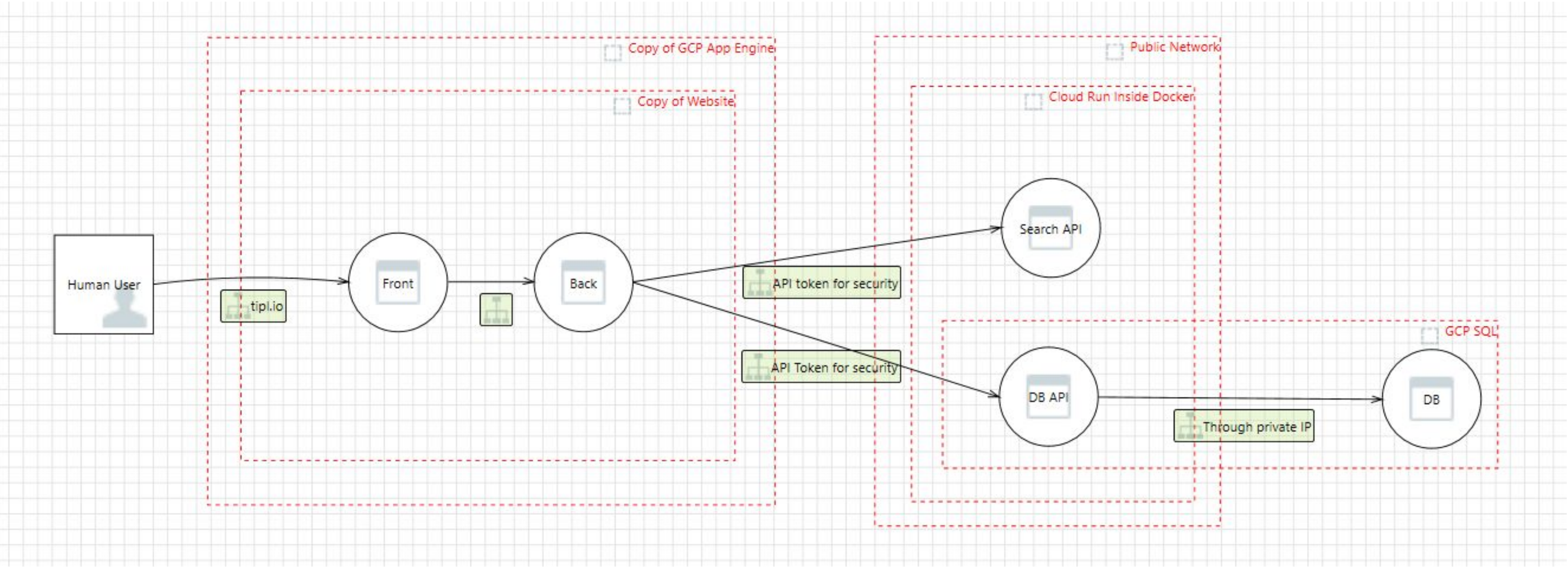
TIPL Security Assessment

By Giancarlo Betti

What is TIPL?

TIPL is a search engine powered by the powerful GPT3 AI. It allows the user to gather the most relevant information about a stock, such as price to earning ratio, debt to equity, stock performance, public image, and other important factors. It will also tell the user whether its favorable to invest or not.

Data Flow Diagram



Overview

1. Compliance: There are a plethora of rules and policies that must be followed.
2. Secure Code Review: I went through all our lines of code and tried to identify any security flaws
3. Google Cloud Platform: This is one of our most important assets, since everything is being hosted here. Any breaches to GCP could be fatal to our company. .
4. Vulnerability Scan: I utilized a wide variety of tools to scan TIPL for any possible security flaws.
5. Penetration Testing: After running multiple scans, i attempted to exploit any vulnerabilities I could find

My Roles

I was the only member of the purple team for the TIPL project. I conducted both offensive and defensive activities.

I started by focusing on secure code development. I communicated clearly with the developers to ensure that they were following security best practices. This was crucial, as it is much more efficient and effective to focus on security early on.

Next, I secured Google Cloud Platform (GCP). I configured the services running on GCP, such as the MySQL database and the firewall. I made sure that the database was not accessible to anyone other than the services that needed access. I also used stored procedures to reduce the risk of SQL injections.

I then set up IAM permissions for GCP. I created roles for each service account to ensure that each account had only the permissions it needed. This would limit the attack surface if an account was breached.

Finally, I secured the web application. I implemented a WAF, input validation, and X-XSRF-Tokens. I also ran a penetration test, which the site passed.

I am proud of the work I did on the TIPL project. I believe that my efforts helped to make the project more secure.

Compliance

Compliance

Under GDPR guidelines, any website that collects user information must have a privacy policy that clearly states the information that is being recollected. It must also include how the data will be processed and who will have access to it. At TIPL, we strongly believe in transparency, and do not sell or distribute private information to anyone. Here are the main points of our privacy policy:

Privacy Policy

Under GDPR guidelines, any website that collects user information must have a privacy policy that clearly states the information that is being recollected. It must also include how the data will be processed and who will have access to it. Here are the main points of our privacy policy:

Personal data we collect

We collect only the username and email address of our users. We do not collect any other personal data.

How we use your personal data

We use your personal data to create and manage your account on our website. We do not use your personal data for any other purpose.

How we protect your personal data

We take appropriate technical and organizational measures to protect your personal data from unauthorized access, use, or disclosure. We limit access to your personal data to those employees who have a need to know.

Your rights

You have the right to access, correct, and delete your personal data. You can do this by logging in to your account and making the necessary changes.

Secure Code Review

What is SCR?

Secure code review is the process of reviewing and analyzing software code for potential security vulnerabilities and weaknesses. The goal of a secure code review is to identify and address security issues early in the software development lifecycle, before they can be exploited by attackers.

At TIPL, we are strong believers in security by design. We believe that the best way to keep our data and assets safe is to incorporate security principles into the software development process from the start. This helps us to prevent security vulnerabilities from being introduced into the code in the first place, and it also makes it easier and quicker to identify and fix security vulnerabilities when they do occur.

The Four Cores of SCR

Failures in Identification, Authentication, and Access Control

Mishandling of identification and authentication can lead to serious repercussions. With proper access control policies and by implementing zero trust, each account is limited to access only what they need.

Potential Exposure of Sensitive Data

Potential exposure of sensitive data occurs when a company unknowingly exposes sensitive data or when security incident leads to the data being compromised. This could potentially ruin a company, since data such as PII and SPII is heavily protected by the government, and if company IP is exposed, it could spell the end.

The Four Cores of SCR

Inadequate error handling

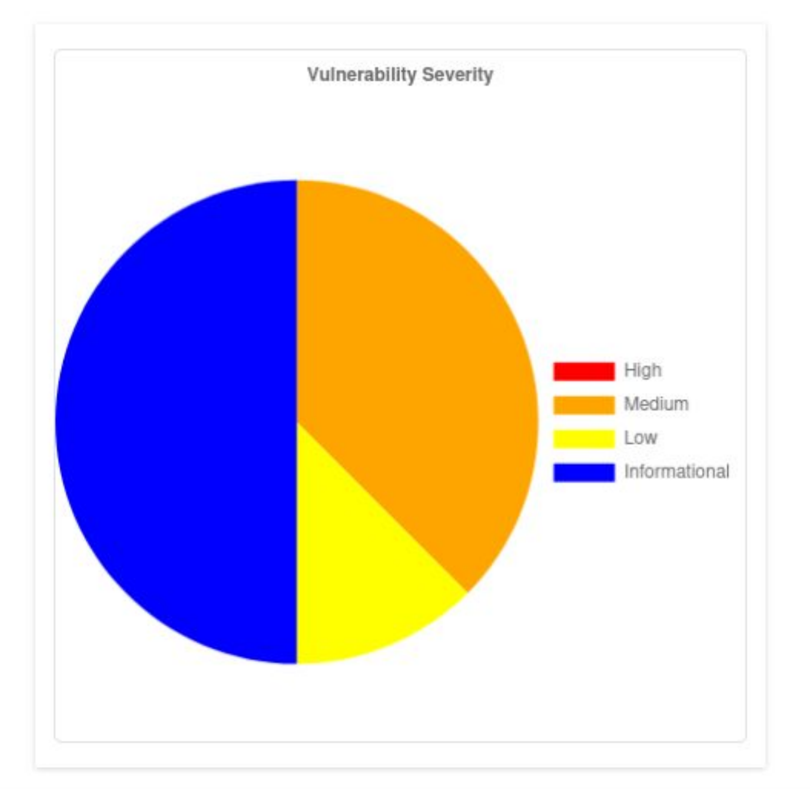
By itself, inadequate error handling won't cause too much damage. However, displaying too much information regarding an error could provide an attacker with the necessary data to carry out an attack. Rather than providing lengthy error messages, we display error codes with minimal information.

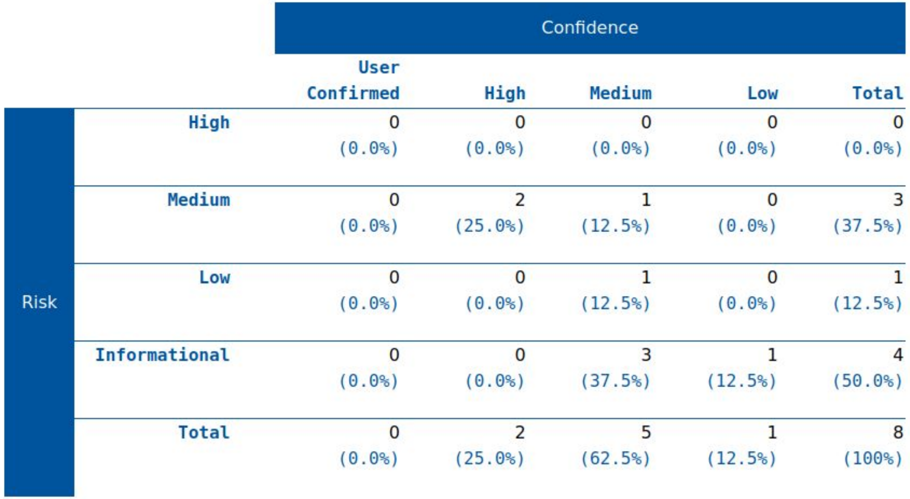
Injection Flaws

Injections occur when an attacker supplies malicious input into the site. This could lead to a plethora of attacks, such as leaking private data, modifying information stored in databases, injecting malware, and other nefarious activities. By implementing proper measurements such as input validation and keeping our internal services and processes secure, we can greatly reduce the risk of a successful injection.

Vulnerability Scan

OWASP ZAP





		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (25.0%)	1 (12.5%)	0 (0.0%)	3 (37.5%)
	Low	0 (0.0%)	0 (0.0%)	1 (12.5%)	0 (0.0%)	1 (12.5%)
	Informational	0 (0.0%)	0 (0.0%)	3 (37.5%)	1 (12.5%)	4 (50.0%)
	Total	0 (0.0%)	2 (25.0%)	5 (62.5%)	1 (12.5%)	8 (100%)

OWASP ZAP Vulnerabilities

Content Security Policy Header not set

Risk: Medium

Confidence: High

Description: CSP is a security measure that prevents attacks like XSS and data injection by letting website owners specify which sources of content their website can load.

Solution: In order to fix this vulnerability, I configured the web server to return the Contest Security Policy HTTP header.

Missing Anti-clickjacking Header

Risk Medium

Confidence Medium

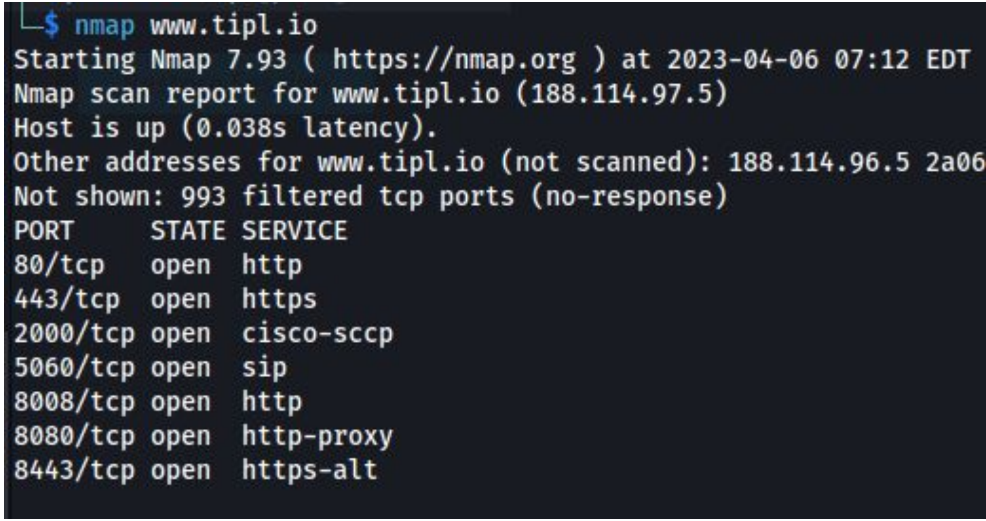
Description: The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

Solution: This issue was resolved by setting the CSP header in the previous vulnerability.

NMAP

Nmap is an open-source tool that allows us to map networks, scan for vulnerabilities, port-scanning, and much more. In this case, I utilized nmap -Sv -Sc to try and find open ports and information about the services that are running on the system.

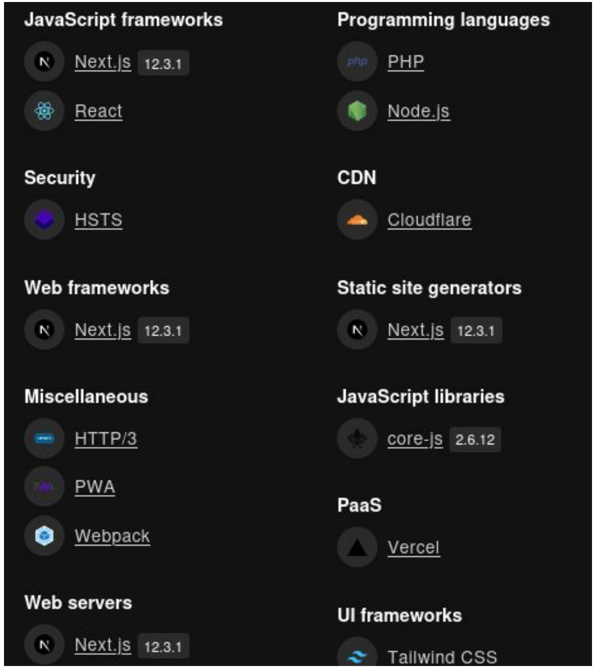
- -sV option enables version detection, which
- -sC option enables the default script scan, in which Nmap will run a set of pre-configured scripts



```
└─$ nmap www.tipl.io
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 07:12 EDT
Nmap scan report for www.tipl.io (188.114.97.5)
Host is up (0.038s latency).
Other addresses for www.tipl.io (not scanned): 188.114.96.5 2a06
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8008/tcp open  http
8080/tcp open  http-proxy
8443/tcp open  https-alt
```

Server Software and technology found

By utilizing Wappalyzer,a web browser extension that can identify the technologies used by a website, I found the following information regarding the site.Knowing what technologies the website is using allows us to identify potential vulnerabilities or attack vectors that may be found in those technologies.



JavaScript frameworks

Next.js 12.3.1

React

Security

HSTS

Web frameworks

Next.js 12.3.1

Miscellaneous

HTTP/3

PWA

Webpack

Web servers

Next.js 12.3.1

Programming languages

PHP

Node.js

CDN

Cloudflare

Static site generators

Next.js 12.3.1

JavaScript libraries

core-js 2.6.12

PaaS

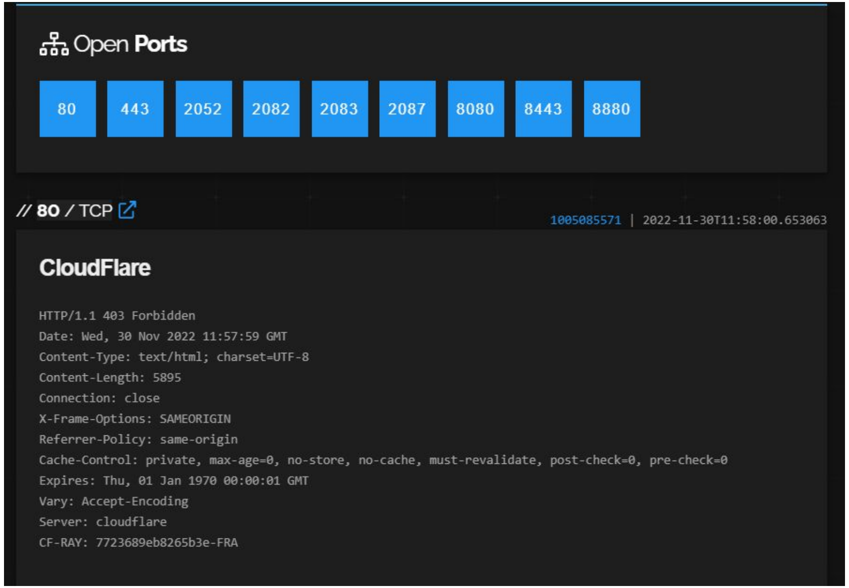
Vercel

UI frameworks

Tailwind CSS

Shodan Network Scanner

Shodan is a tool that helps to pen test web applications by identifying possible vulnerabilities and attack routes. It scans for exposed devices and services, detects known vulnerabilities, uncovers poorly secured systems, and maps the attack surface of the target application. This provides valuable information to identify entry points and potential attack vectors for compromising the application.



Open Ports

// 80 / TCP

1005085571 | 2022-11-30T11:58:00.653063

CloudFlare

```
HTTP/1.1 403 Forbidden
Date: Wed, 30 Nov 2022 11:57:59 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 7723689eb8265b3e-FRA
```

OWASP TOP 10

OWASP Top 10 is a list of the most critical security risks to web applications. The list is compiled by the Open Web Application Security Project (OWASP), a nonprofit organization that focuses on improving the security of software.

The OWASP Top 10 list provides a ranking of the top 10 security risks based on their prevalence and potential impact on web applications. The list is updated periodically to reflect new threats and changes in the security landscape.

I made a list addressing the vulnerabilities on the list that could possibly affect TIPL.

Crypto failure

Cryptographic failure occurs whenever a web application exposes sensitive data due to a weak or a non-existent cryptographic algorithm.

TIPL avoids cryptographic failure by using Google authentication, which does not store sensitive user information like passwords or PII in their databases. Only emails, tokens, and query histories are stored, and they are encrypted using the AES-256 bit encryption algorithm and a secure symmetric key.

We also have a valid https certificate, which provides confidentiality, integrity, authentication, and trust.

Authentication and Identification Failure

Users sign in through Google Authentication, which is a widespread login method that is highly secure, since Google handles the data storage as well as the encryption. We don't directly store any passwords, so using Google Authentication significantly reduces our workload.In the scenario that a hacker manages to acquire the google sign on for a user, they wouldn’t be able to do much besides having access to the user's tokens and previous queries.

Security Misconfiguration

To reduce risks, we only included necessary functionalities on our website and implemented automated updates to ensure the latest security patches. Vulnerabilities were patched, including one that revealed detailed error codes. Another vulnerability allowed attackers to list directories, but we ensured that no directories besides the necessary ones could be accessed through the site to further establish a foothold.

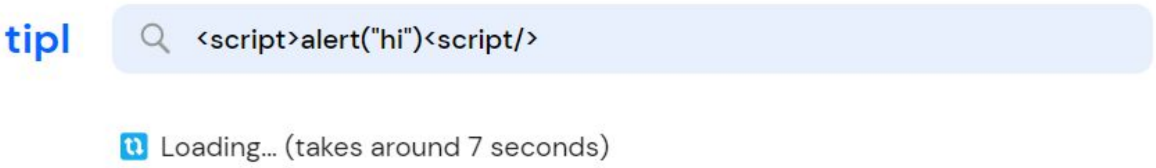
Software and data Integrity Failure

Using public libraries provides benefits, but also poses potential vulnerabilities from malicious or existing libraries. We mitigate this by removing unused libraries, thoroughly researching chosen libraries, and constantly updating them. Digital signatures or similar mechanisms verify software or data is from the expected source and has not been altered, ensuring trustworthy software use.

Exploitation

Cross Site Scripting (XSS)

Cross site scripting is a type of attack where the hacker inputs a malicious script into the site in an attempt to have it executed. Usually the best places to attempt this are search boxes and contact us request forms. Tipl only has the search function, which could be used to execute an XSS attack. However, since we implemented input sanitization, the code removes any unwanted characters before running the query. This way, hackers are unable to run scripts on our site. Here is an example.



```
<script>alert("hi")<script/>
```

Loading... (takes around 7 seconds)

Denial of Service (DOS)

A Denial of Service (DoS) attack is a type of cyber attack in which an attacker attempts to make a network or website unavailable to its intended users. This is typically done by overwhelming the target system with a flood of traffic or requests, which can cause the system to become slow or unresponsive.

In this case, I chose to attempt a basic synflood attack. This targets the TCP protocol, which is used to establish connections between devices over the internet. In a SYN flood attack, the attacker sends a large number of TCP connection requests (SYN packets) to the target device, with fake or spoofed source IP addresses.

GCP provides automated DDoS protection for all projects, including protection against SYN flood attacks, through the Google Cloud Armor service. Cloud Load Balancing is also available to protect against SYN flood and other DDoS attacks. Third-party DDoS protection solutions can also be integrated with GCP services.

Directory Traversal

Directory traversal is a technique in which the attacker attempts to access files and directories that are not meant to be accessed. This can be accomplished by manipulating the path used to access files by adding special characters like ".." or "../" in order to traverse up the directory tree and access files outside the current directory.

In this case, to facilitate the process, I utilized a directory buster. It is a tool specialized in making directory traversal much faster. Directory busters work by sending a large number of HTTP requests to the target server, using a wordlist of common file and directory names as input. The tool then analyzes the HTTP responses to determine if the requested file or directory exists on the server.

There are no real ways of keeping an attacker from utilizing these tools. At TIPL, we covered this vulnerability by ensuring there were no accessible directories of files through the website besides the necessary ones, as well as strict access control. We also have a robust firewall which constantly monitors for any malicious traffic.

Google Cloud Platform

Why did we choose GCP

Google Cloud Platform (GCP) is a cloud computing platform offered by Google. It provides a variety of services, including computing, storage, networking, data analytics, machine learning, and more, all delivered over the internet.

It is designed to provide security through the entire information processing lifecycle. This infrastructure ensures secure deployment and storage of services and data, prioritizing end-user privacy. It enables secure communication between services, maintains confidentiality and privacy of customer communication over the internet, and ensures safe operation by administrators.

Roles

Security leader: It's essential to comprehend Google's core principles for cloud security and their practical application to secure the organization's deployment.

Security engineer: needs to understand how to configure and operate multiple different security controls so that they seamlessly interact with each other.

Risk and compliance officer: it's vital to be familiar with the controls offered by Google Cloud to ensure they align with your business requirements. Must know how to deploy these controls automatically and monitor any control drift or areas that require additional attention to meet the business's regulatory needs.

Core Security Principles

We adopted three security principles that are the core of Google security

- Executing defense in depth, at scale, by default.
- Adopting the BeyondProd approach to infrastructure and application security.
- De-risking cloud adoption by moving toward a shared fate relationship.

Defense in depth

The principle of defense in depth emphasizes the importance of having multiple layers of protection between a potential attacker and a valuable target.

To ensure maximum data protection, multiple layers of defense are implemented by default, including policies and controls configured across various services such as networking, encryption, IAM, detection, logging, and monitoring. Additionally, IAM and access context levels are employed to further enhance data protection through multiple levels of access control.

BeyondProd

The BeyondProd framework operates on the principle of zero trust, recognizing that perimeter-based security models are insufficient in preventing system breaches By breaking down large, monolithic applications into microservices, BeyondProd increases segmentation and isolation, thereby reducing the affected area in the event of a breach.

Each microservice runs independently within their own container, and proper rights and permissions are assigned. Services may only interact with other trusted services. This impedes an attacker from running untrusted code.

Shared Fate

Google Cloud Platform has transitioned from a shared responsibility model to a shared fate model, which significantly reduces the workload for us. In the shared responsibility model, TIPL (the customers) and GCP are responsible for different assets, whereas in the shared fate model, the focus is on meeting TIPL's needs. This approach leverages the cloud provider's expertise to help TIPL achieve optimal security in the cloud.

The shared fate approach allows TIPL to manage risks by utilizing secure-by-default configurations, secure blueprints, secure policy hierarchies, consistent availability of advanced security features, and high assurance attestation of controls. By tapping into these resources, TIPL can more effectively address their security needs without becoming overwhelmed by the responsibility.

Safe Browsing

1. Always keep your passwords secure. Make sure they are at least 8 characters long and include uppercase letters, lowercase letters, numbers, and special characters.
2. If possible, use a VPN to keep your data encrypted and safe.
3. Ensure that the TIPL website you are using has a valid HTTPS certificate. This will prove that the site is reliable and that the communication is being encrypted.
4. Always double-check the URL to avoid typosquatting.