# What is this about?

Network and database security is very important for our Mediawiki website. Security process involved from the start of the DevOps can help the security of the application when it reaches production. This can be things like automating attacks on the pre-production codes to find vulnerabilities and stop the release it if the attacks are successful. We want to add an automated encryption process, intrusion detection, configuration checks for each new instance added to the load balancer, and vulnerability checking.

# What context would it be useful?

This would be useful for banks or website holding valuable data. The encrypted network is required for a secure communication because websites have a greater risk of attack due to the value of the data they hold. The intrusion detection can help find attackers to minimize damage to the system and identifying the infected user, attacker, or stolen account. The vulnerability checking is used to give risk assessment in the system and code by providing codes that are at risk or can be vulnerable. The configuration checker can be used to find any changes made by malicious code or user to prevent backdoors or vulnerabilities being created.

# How does it relate to DevOps?

DevOps combines the development and operation teams, so this can include the Information Security team too. Security should be implemented as soon as possible to test the product before release to find weakness in the system. These should be things like automated configuration management, patching, code analysis, secret managements to scale with DevOps process. Automation lowers the chance of human error and associated downtime and vulnerabilities.

# What are the challenges?

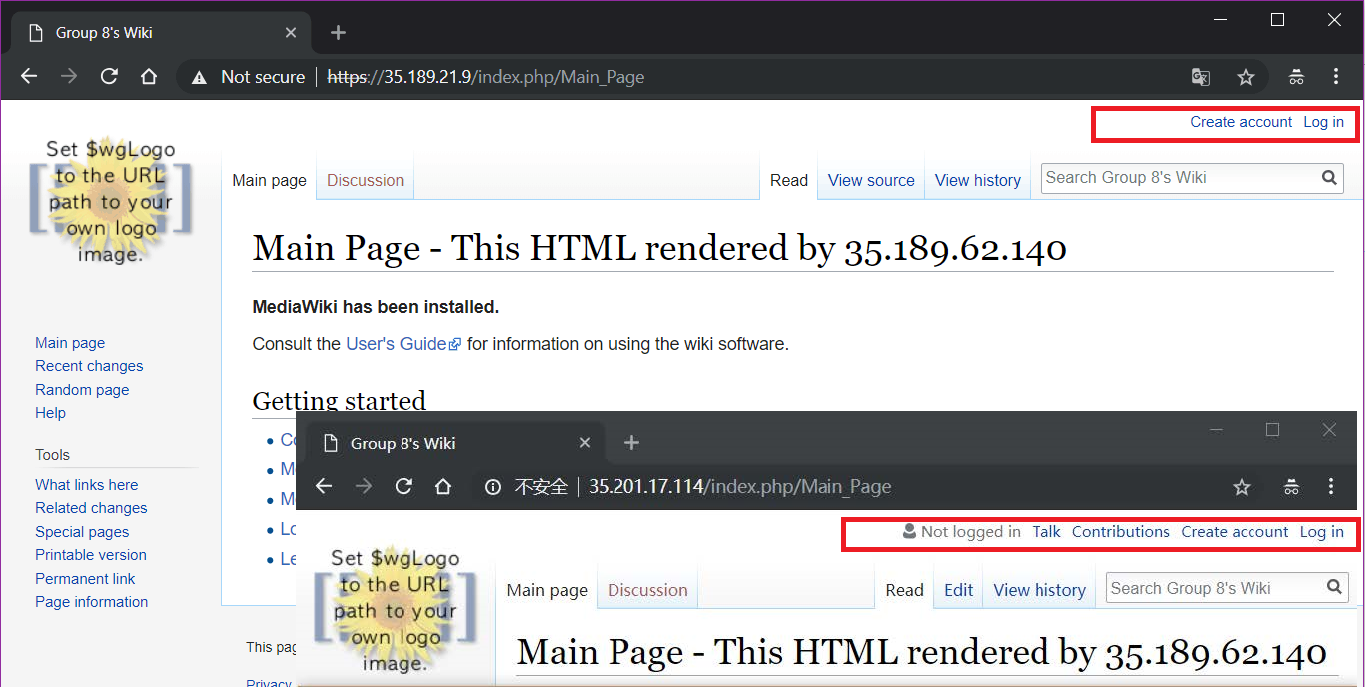
The security aspect faces many challenges in the DevOps cycle. This might not be the case in our small setup but in a bigger environment and company these challenges are more prevalent. If the IT security is not automated effectively then IT security will be behind which slows down the entire DevOps process or security not being up to standards. This can lead to things such as downtime because of the many outcomes that come from this.

The cloud environments used by DevOps lets us manage many server instances. In this environment simple mistakes can cause big problems. These can be things such as misconfigurations or bad security practices like sharing of secrets SSH keys. These things can spread causing a lot of exploitable security and compliance issues.

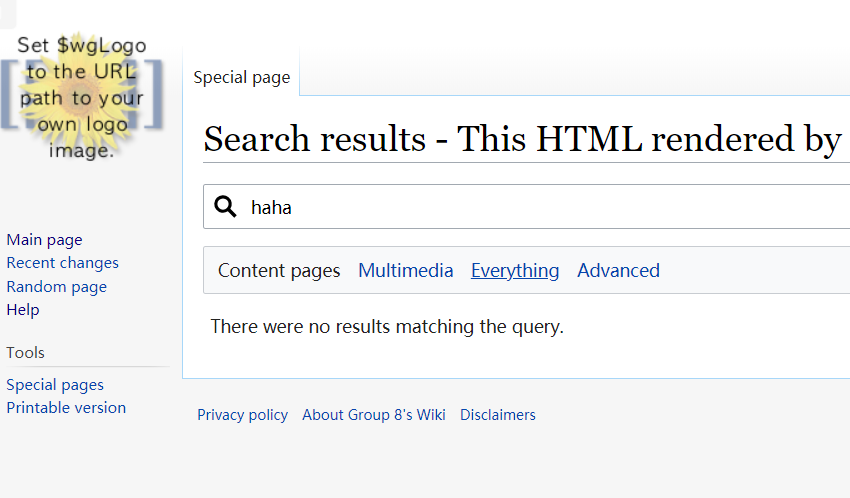
# What/how have you implemented?

For anonymous users, we change the variables in MediaWiki config file “LocalSetting.php” to forbid the anonymous users editing pages, creating new pages, creating a talk and writing APIs.

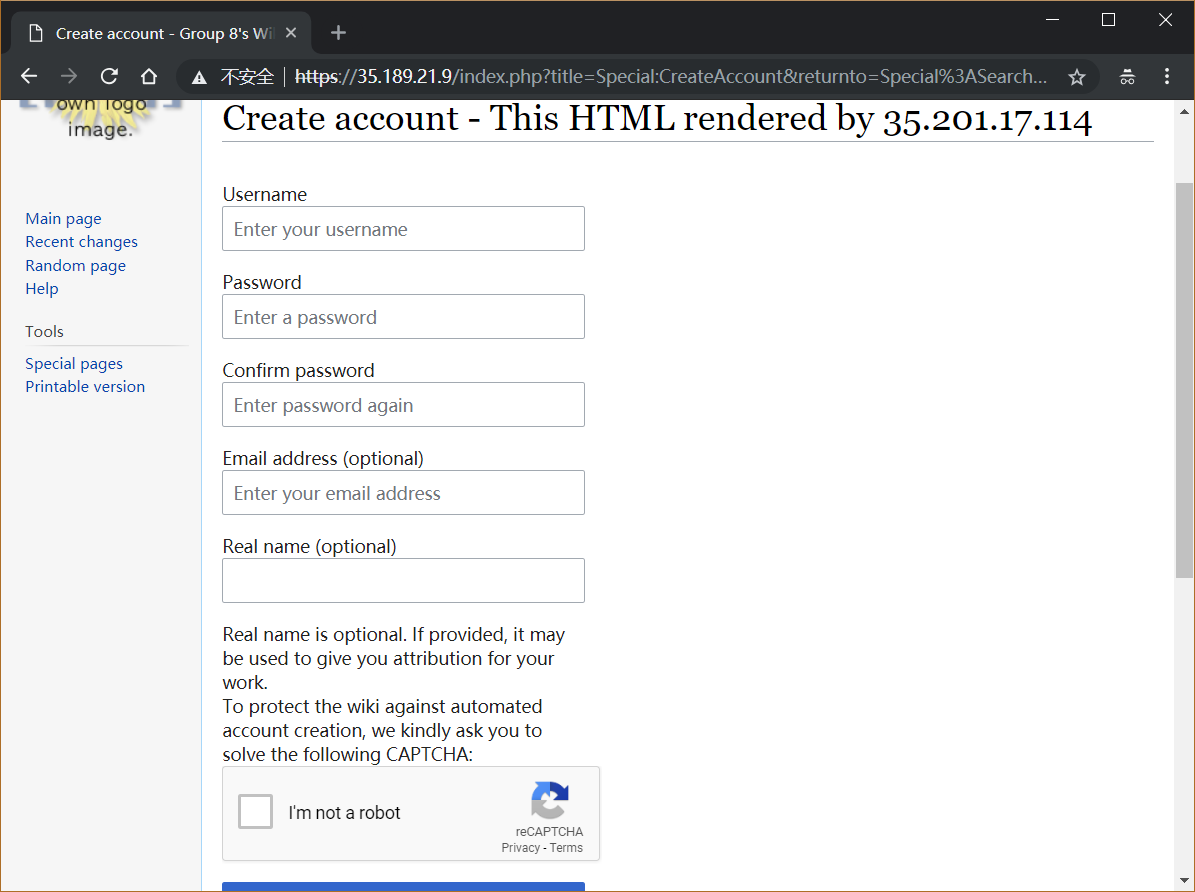
You can see the difference between two web pages, the former is the one added config variables, and the latter is not.



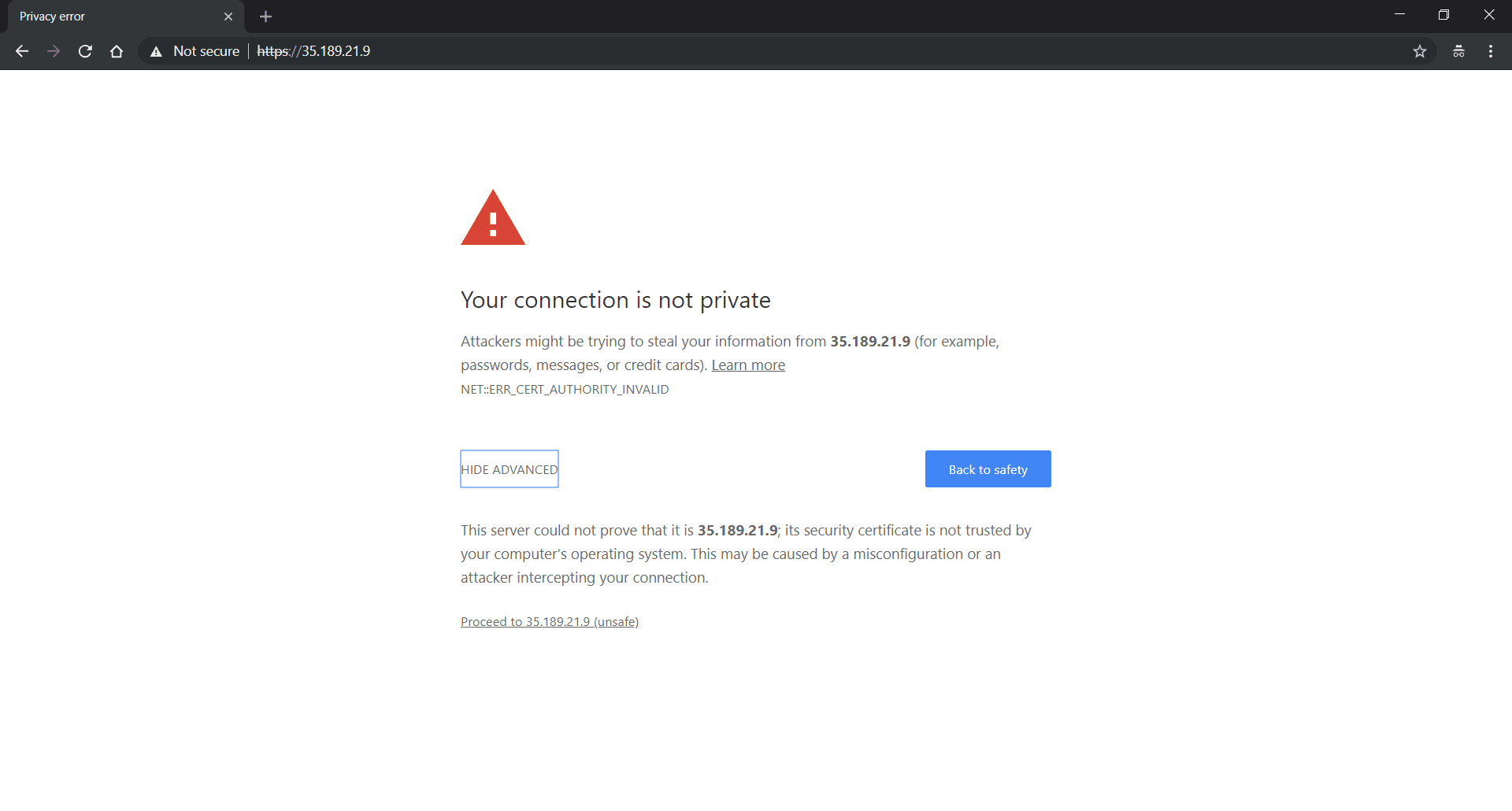
If you search for one page that does not exists it shows one line but no “create page” link;



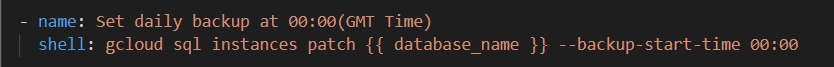
To avoiding bots registering, we add the google reCAPTCHA v2 to avoid bots or scripts signing up;



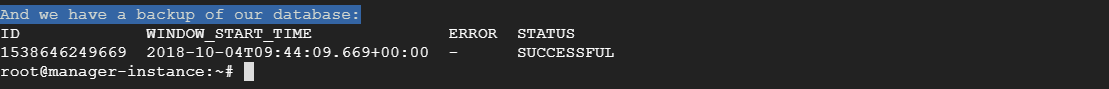
For internet security, we add the HTTPS(SSL/TLS) encryption (with a self-signed certification). But we used a self-signed Certification, so please press the “Proceed to \*\*.\*\*.\*\*.\*\* (unsafe)” to ignore the untrusted SSL notification.



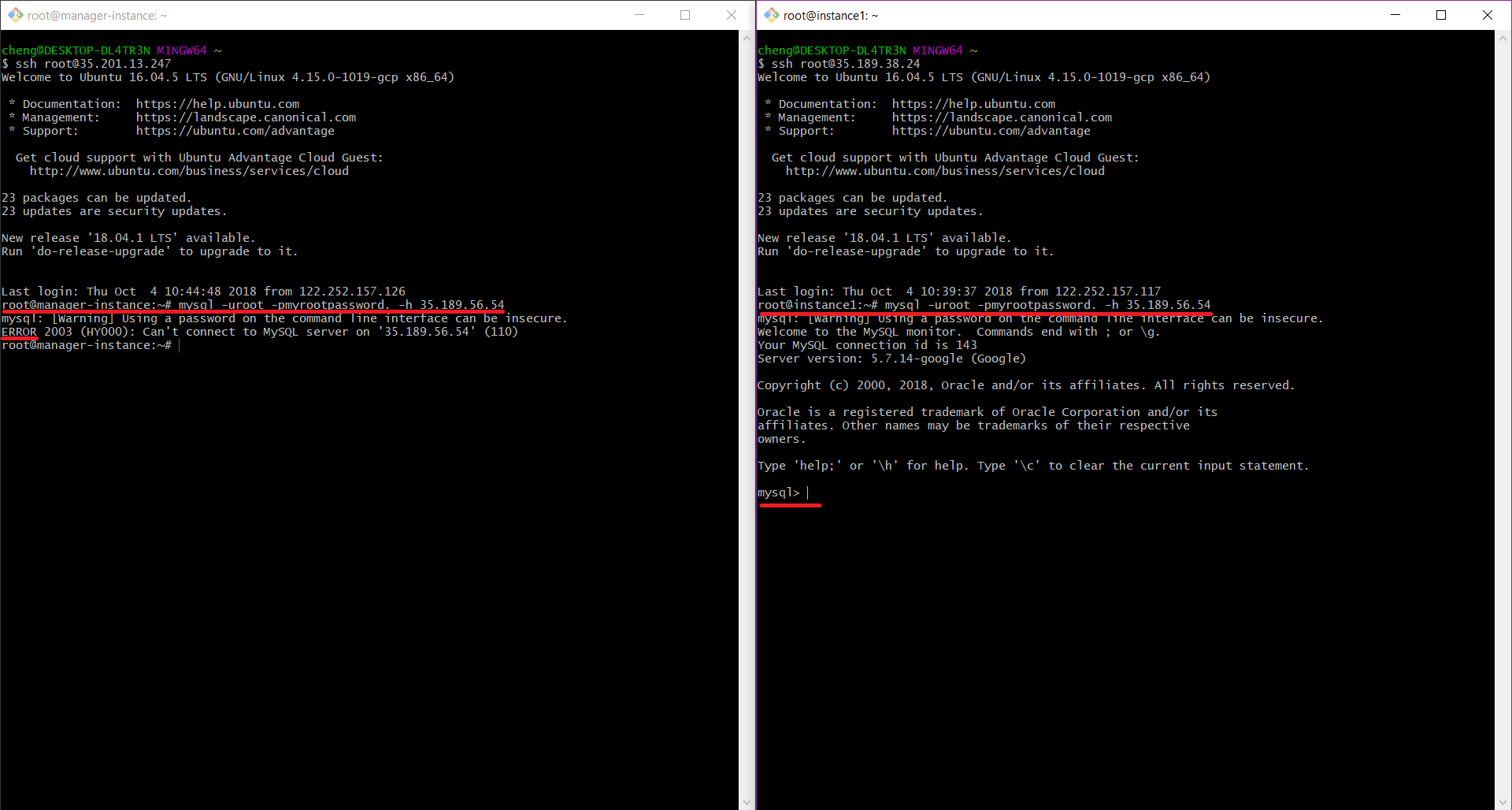
For database safety, we used Google Cloud SQL for the centralized Database system, which has better performance and stability than just install MySQL on an instance. We use Google Cloud SQL daily backup at 0:00(GMT)



And we print another backup which is created during implementation.



Another thing is that ip control of the database, we implemented it, and this is a test:



The left one does not have the permission, and the right one has the permission.