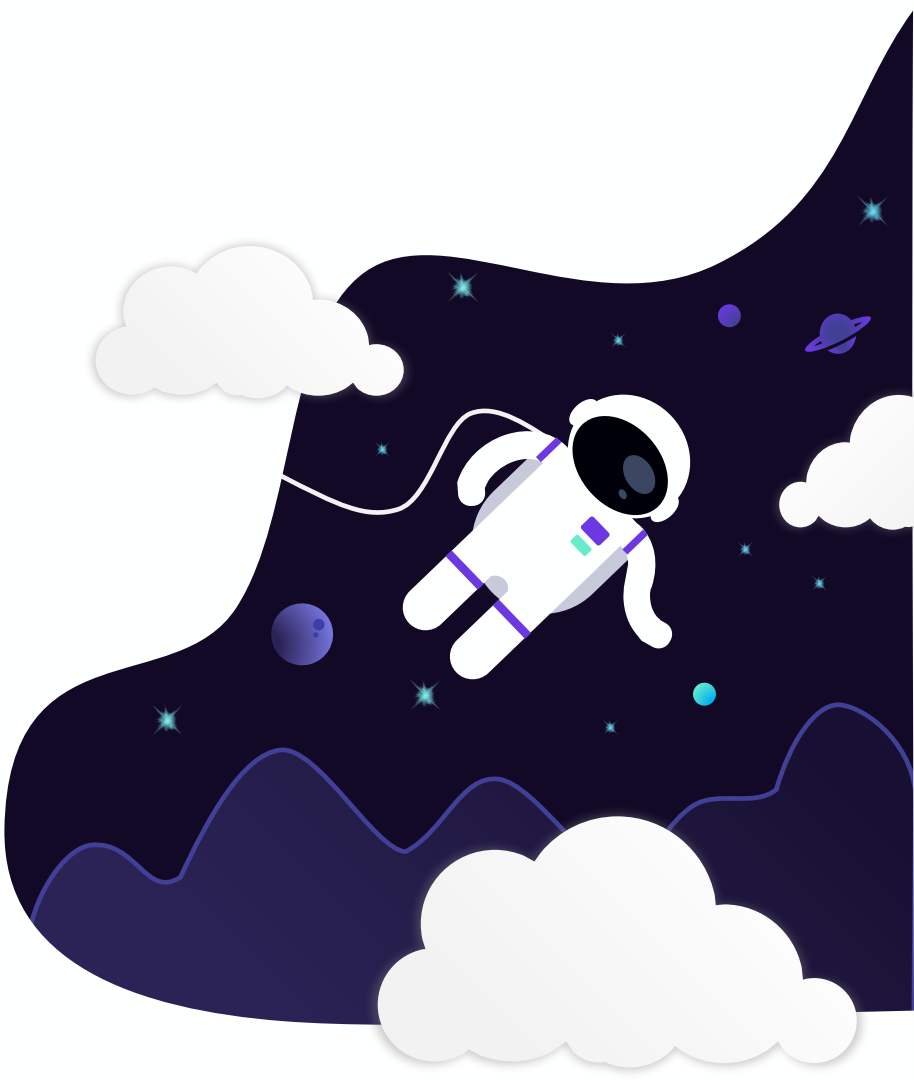
CYBER SECURITY
FOR NEWBIE DEVELOPERS

Yes, it's you!



WHO AM I ?

It doesn’t matter!
Let’s cut to the chase!

CYBER SECURITY PILLARS

3 TO 5 CONCEPTS

Information security is a discipline that aims to protect data and systems from threats and risks.

The definition of the pillars of information security can vary depending on the source and the approach adopted, which explains the dynamics of describing 3, 4 or 5 pillars.

LET'S PLAY A GUESSING GAME ?

!!1!!

@2@

#3#

4

%5%

It concerns the protection of information from unauthorized access.

CONFIDENTIALITY

!!1!!

It concerns the protection of information from unauthorized access.

@2@

It deals with ensuring that data has not been improperly altered during its life cycle.

#3#

4

%5%

INTEGRITY

!!1!!

It concerns the protection of information from unauthorized access.

@2@

It deals with ensuring that data has not been improperly altered during its life cycle.

#3#

It ensures that systems and data are always accessible when needed.

4

%5%

AVAILABILITY

!!1!!

It concerns the protection of information from unauthorized access.

@2@

It deals with ensuring that data has not been improperly altered during its life cycle.

#3#

It ensures that systems and data are always accessible when needed.

4

It involves ensuring that the origin of the information can be verified and that the information has not been falsified.

%5%

AUTHENTICITY

!!1!!

It concerns the protection of information from unauthorized access.

@2@

It deals with ensuring that data has not been improperly altered during its life cycle.

#3#

It ensures that systems and data are always accessible when needed.

4

It involves ensuring that the origin of the information can be verified and that the information has not been falsified.

%5%

It deals with the ability to prove that a person or system has carried out a specific action.

NON-REPUDIATION

WHAT CAN I DO ABOUT IT ?

In order to implement and ensure compliance with the pillars discussed so far it is necessary to adopt certain actions and processes.

Let's see some examples! ->

DON'T REINVENT THE WHEEL

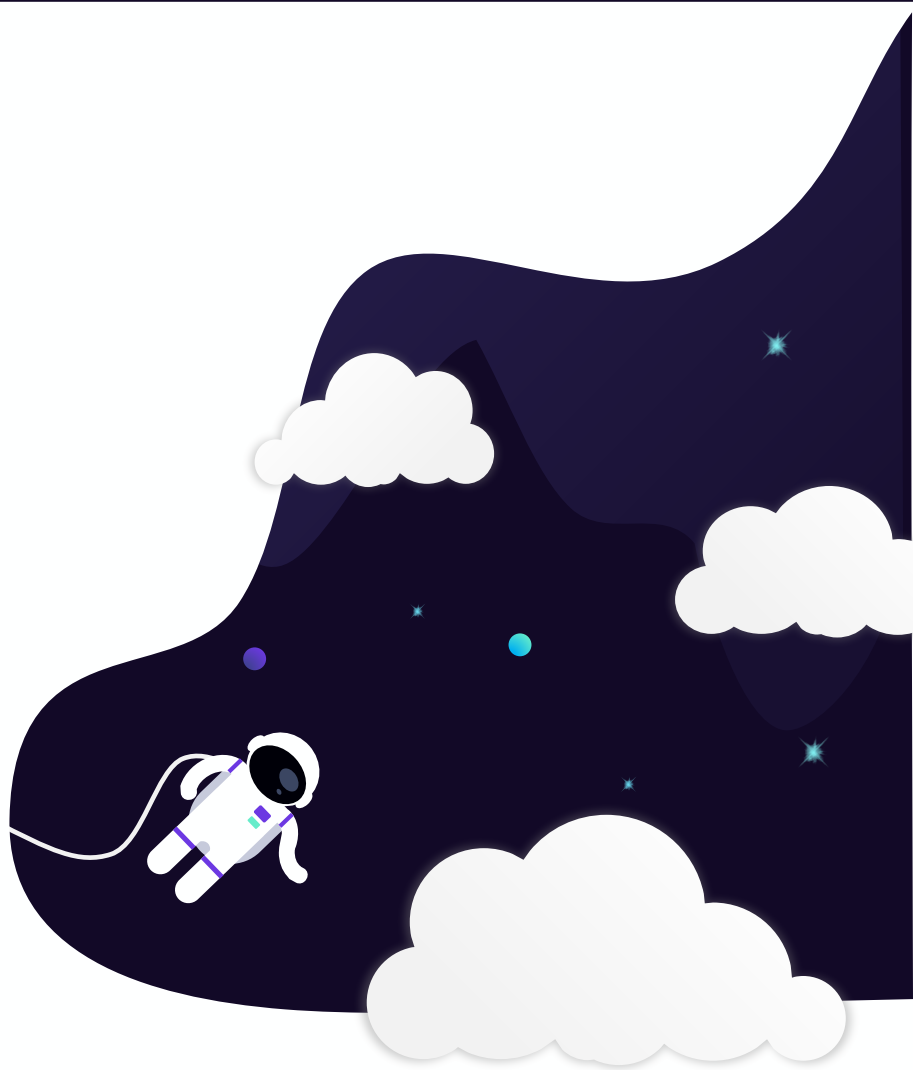
Prefer to use validated tools that are widely used by your community.

You're ***NOT*** building a f*ck!ng spaceship!

Don't risk making mistakes by implementing common tasks!

LAYERED SECURITY

A single security mechanism will never be enough to protect your application from existing threats.



VALIDATING INPUT DATA

Validation: Check what you want!

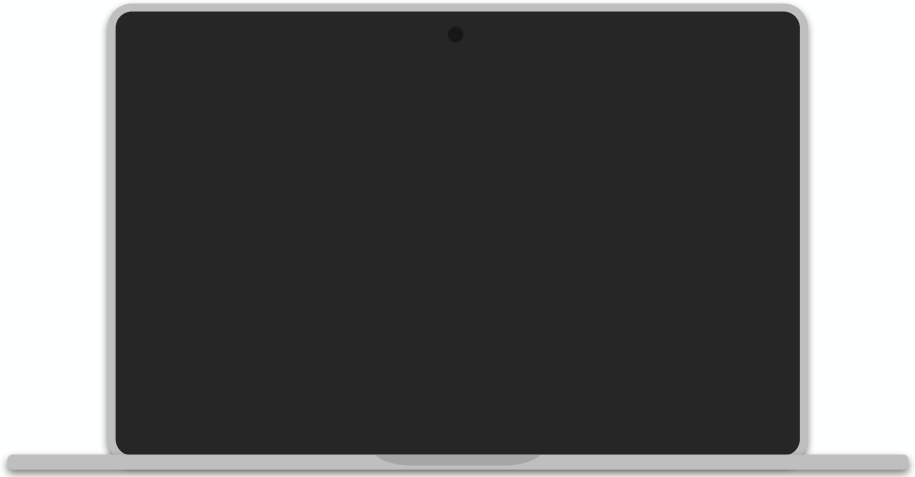
<>

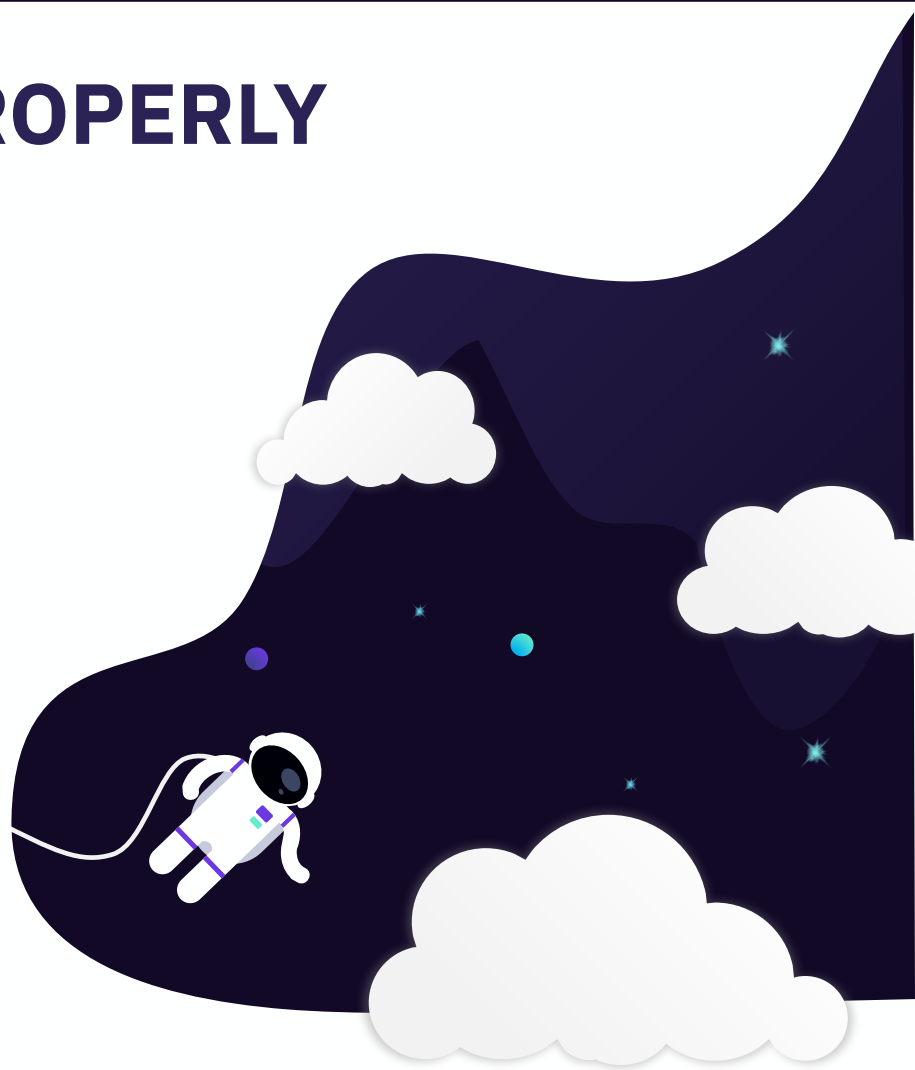
Sanitization: Remove what you do ***NOT*** want!

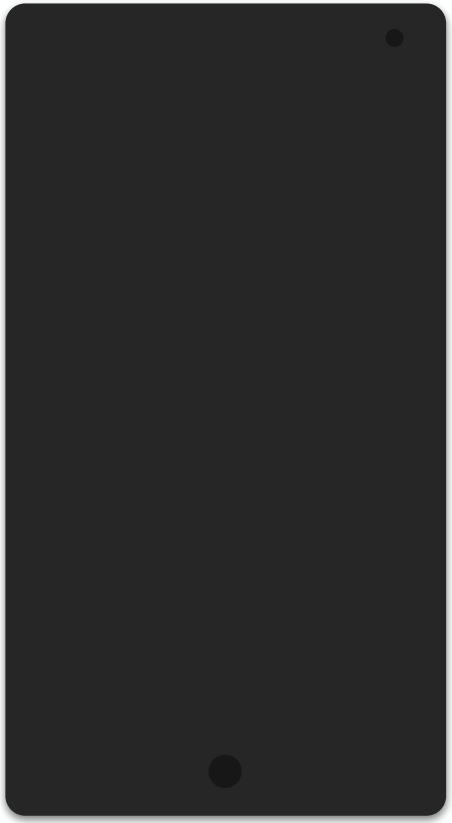
HANDLING ERRORS PROPERLY

You ***shouldn't*** expose sensitive data to common users!

Think about it!







AUTHENTICATION & AUTHORIZATION

Verify the identity of your users.

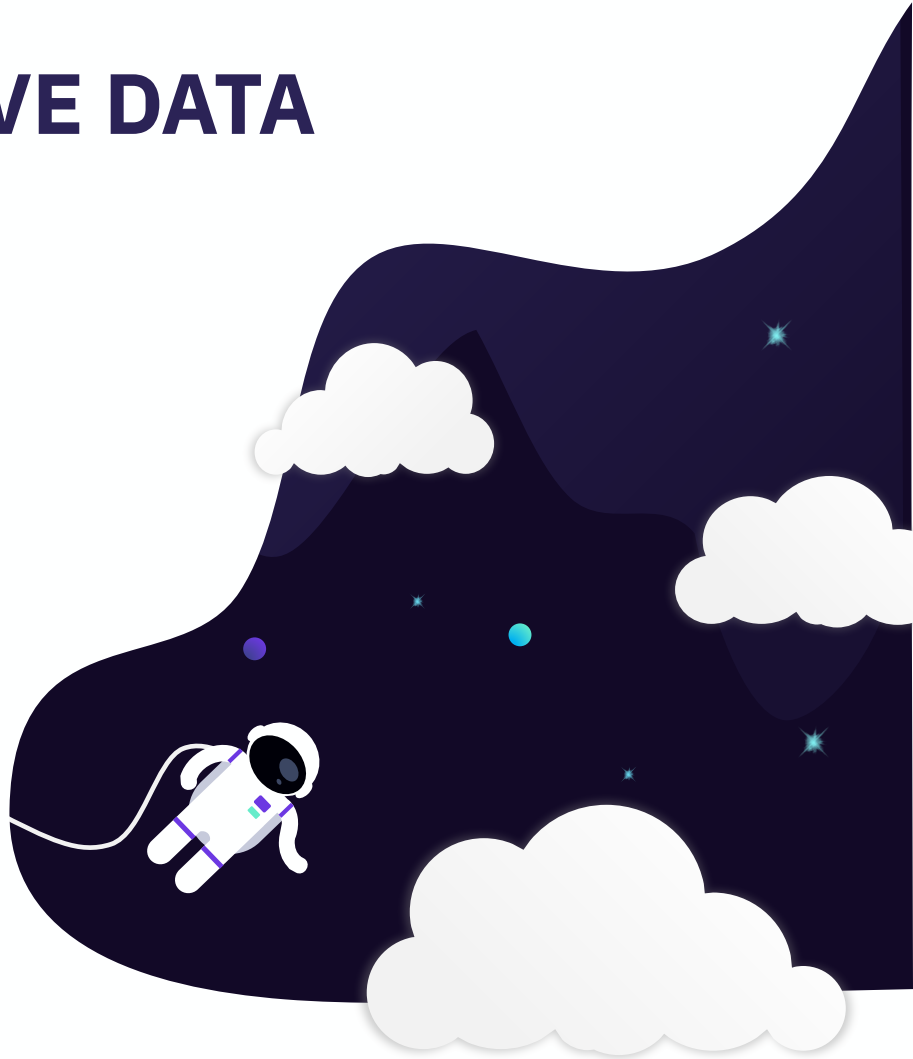
Grant only the necessary permissions to users and their roles.

Avoid giving administrative privileges to ordinary users.

ENCRYPTING SENSITIVE DATA

Private data probably shouldn’t be stored as plain text.

Implement password hashing and sensitive data protection using encryption techniques and strong keys.



THINK OUT OF THE BOX.

DON’T BE NAIVE!

Threats aren't

THAT'S NOT GOOD ENOUGH

Unfortunately, no system is completely safe! Yours won't be either!

Be prepared to react to emergencies and incidents!

This is just as important as protecting yourself against the threats that will inevitably come!

Have an incident response plan in place.

Don't ignore the importance of backups, rollback mechanisms and common security actions!

Do you have any questions?

Thank you!