SECURE CODE WARRIOR

WEAK CRYPTO ALGORITHM

We'll go through

some preventions steps for
vulnerabilities in this category

To understand

The Insecure Cryptographic storage vulnerability, let's look at some examples

IN THE FIRST SCENARIO WE'LL TAKE A LOOK AT "THE MALICIOUS INSIDER"

Let's say the database contains sensitive user information such as personal data, payment information or passwords.

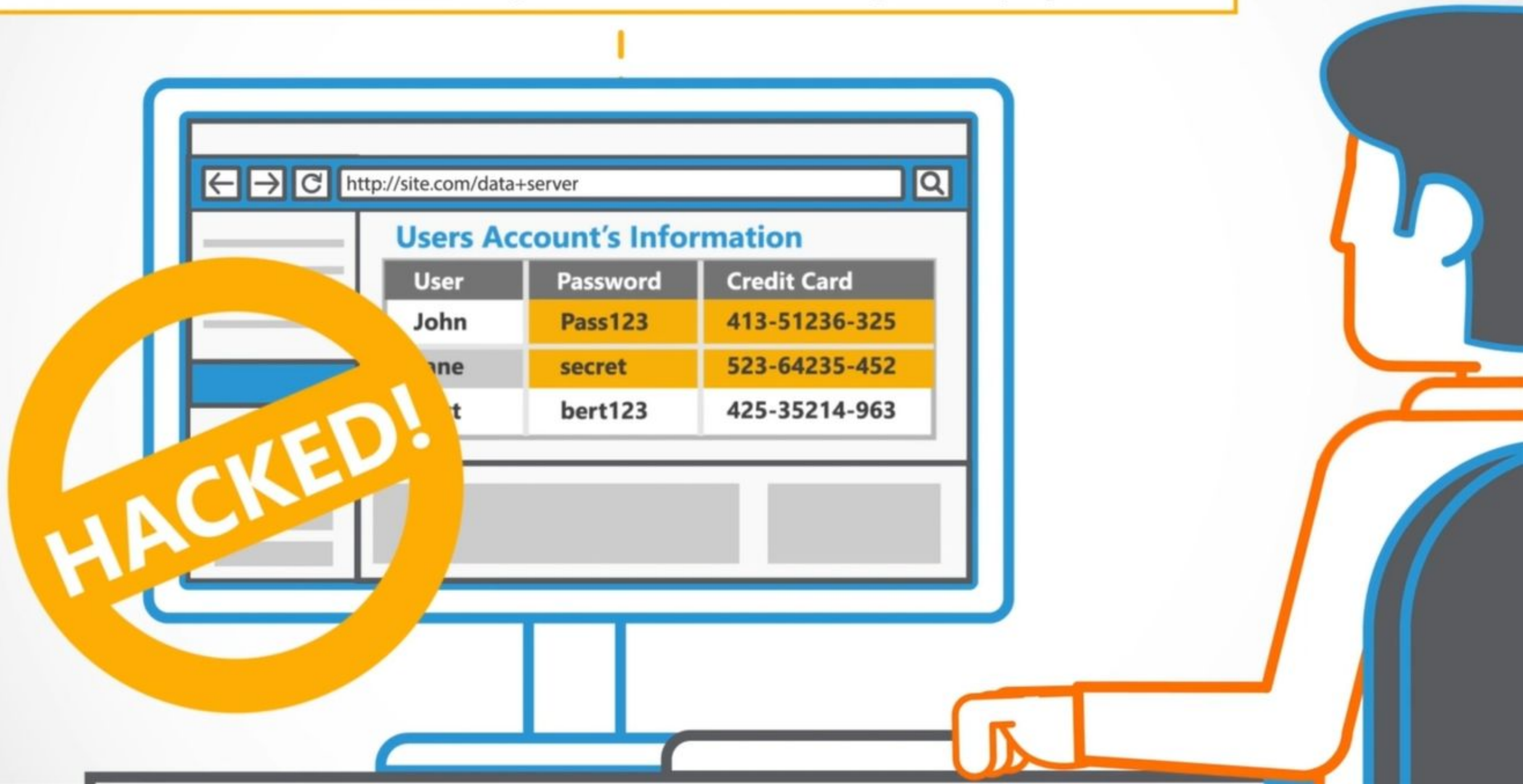
User	Password	Credit Card
John	Pass123	413-51236-325
Jane	secret	523-64235-452
Bert	bert123	425-35214-963

No crypto scheme, or a weak crypto scheme, has been used to store this sensitive data.

User	Password	Credit Card
John	Pass123	413-51236-325
Jane	secret	523-64235-452
Bert	bert123	425-35214-963

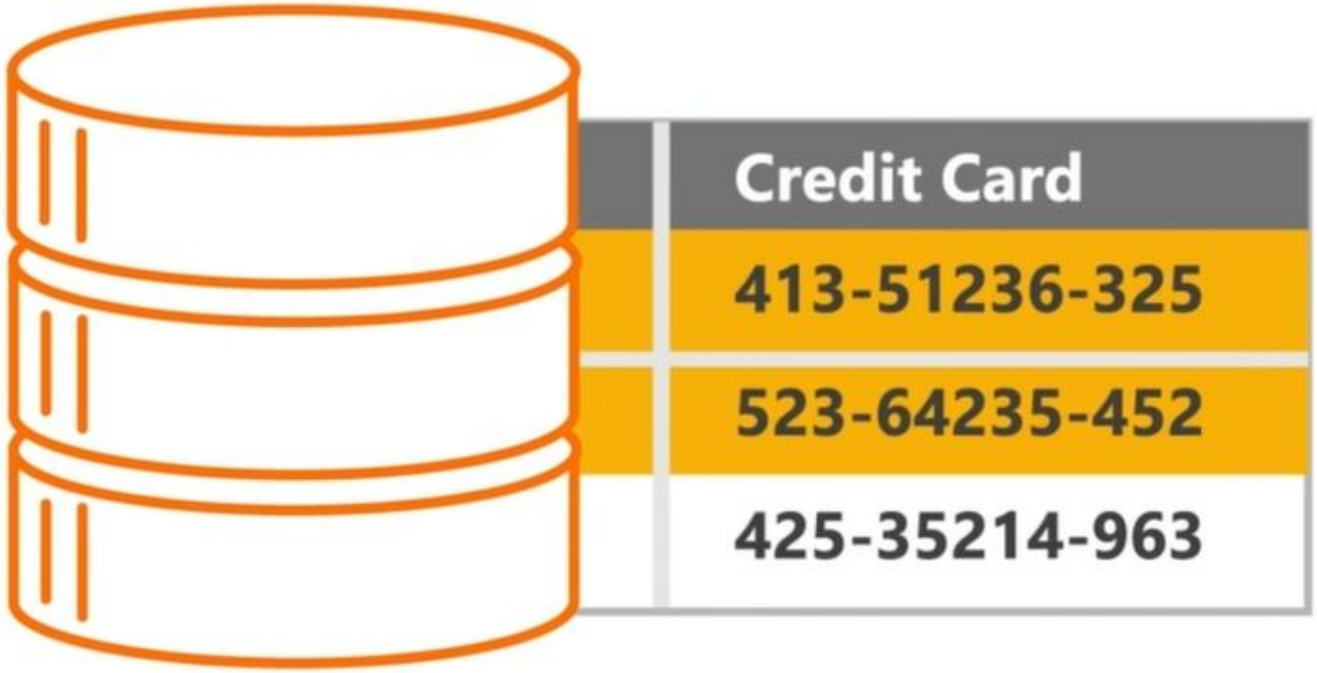
The malicious employee easily obtains unauthorised access to the database server.

Now, sensitive information can be easily extracted and abused by the employee.



LET'S LOOK AT ANOTHER SCENARIO THIS TIME, "THE EXTERNAL ATTACKER"

Again, the database contains sensitive user information such as passwords to protect accounts.



	Credit Card
	413-51236-325
	523-64235-452
	425-35214-963

As with the first example, no crypto scheme, or a weak crypto scheme, is used to store this data.

User	Password	Credit Card
John	kpio123	F23-E36G5-R3G
Jane	tfdsfu	3ED-8R2JK-3B6
Bert	cfsu123	R67-B77GH-E36

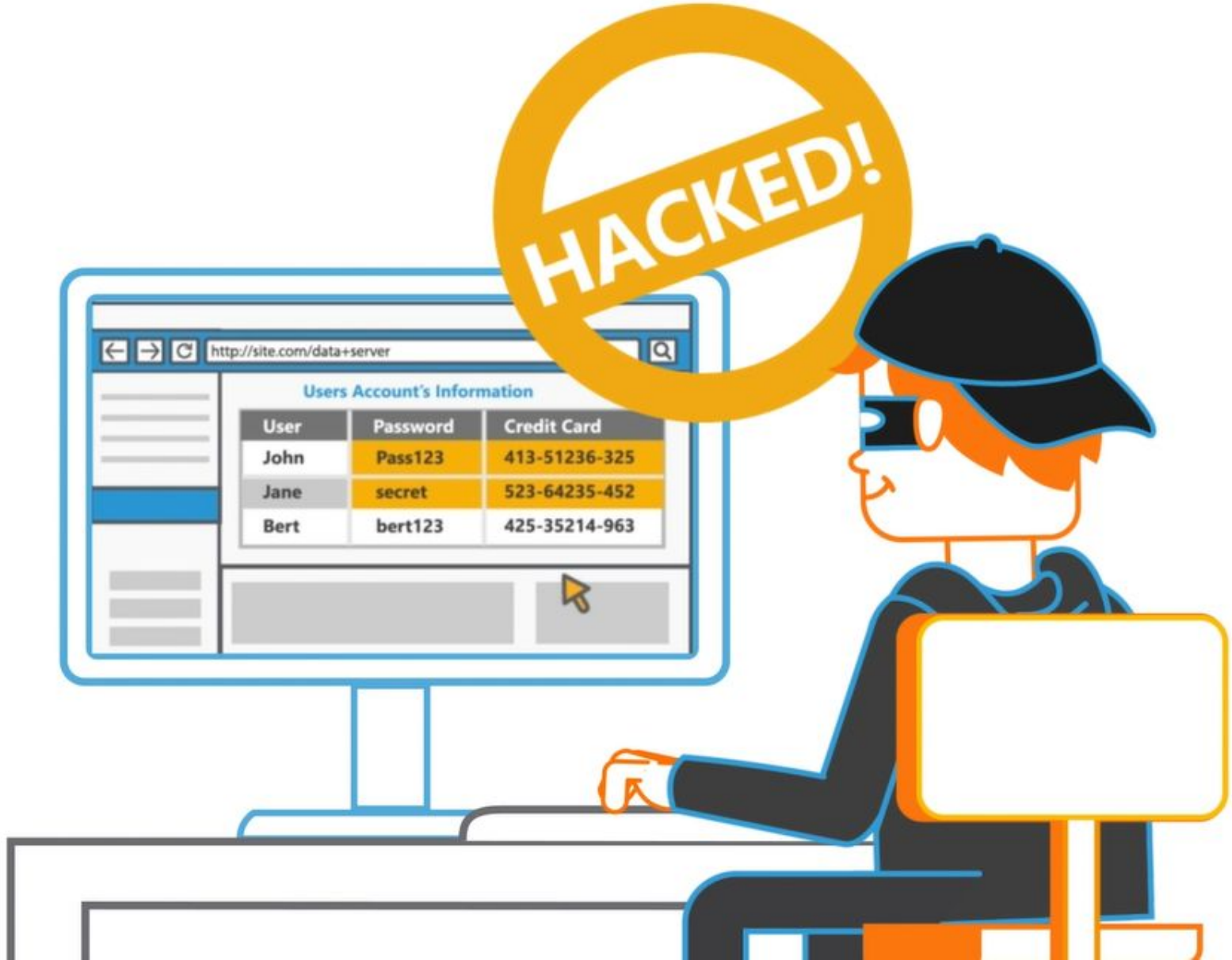
So the external attacker can use other vulnerabilities in the application to obtain unauthorised access to the database.

SQL Injections

XML Injections

Brute Force

Now, the attacker can steal usernames and passwords and impersonate a normal user.



PREVENTING INSECURE STORAGE OF DATA IS CRITICAL

- Developers should firstly identify sensitive data, which needs protection.
- Then, ensure appropriate strong standard algorithms, and strong keys, are used.
- And, application wide key management is in place.
- Ensure passwords are hashed with a strong standard algorithm and an appropriate salt is used.
- And always make sure all keys and passwords are protected from unauthorized access.

Congratulations, you have now completed this module!

SECURE
CODE
WARRIOR