



**SECURE
CODE
WARRIOR**

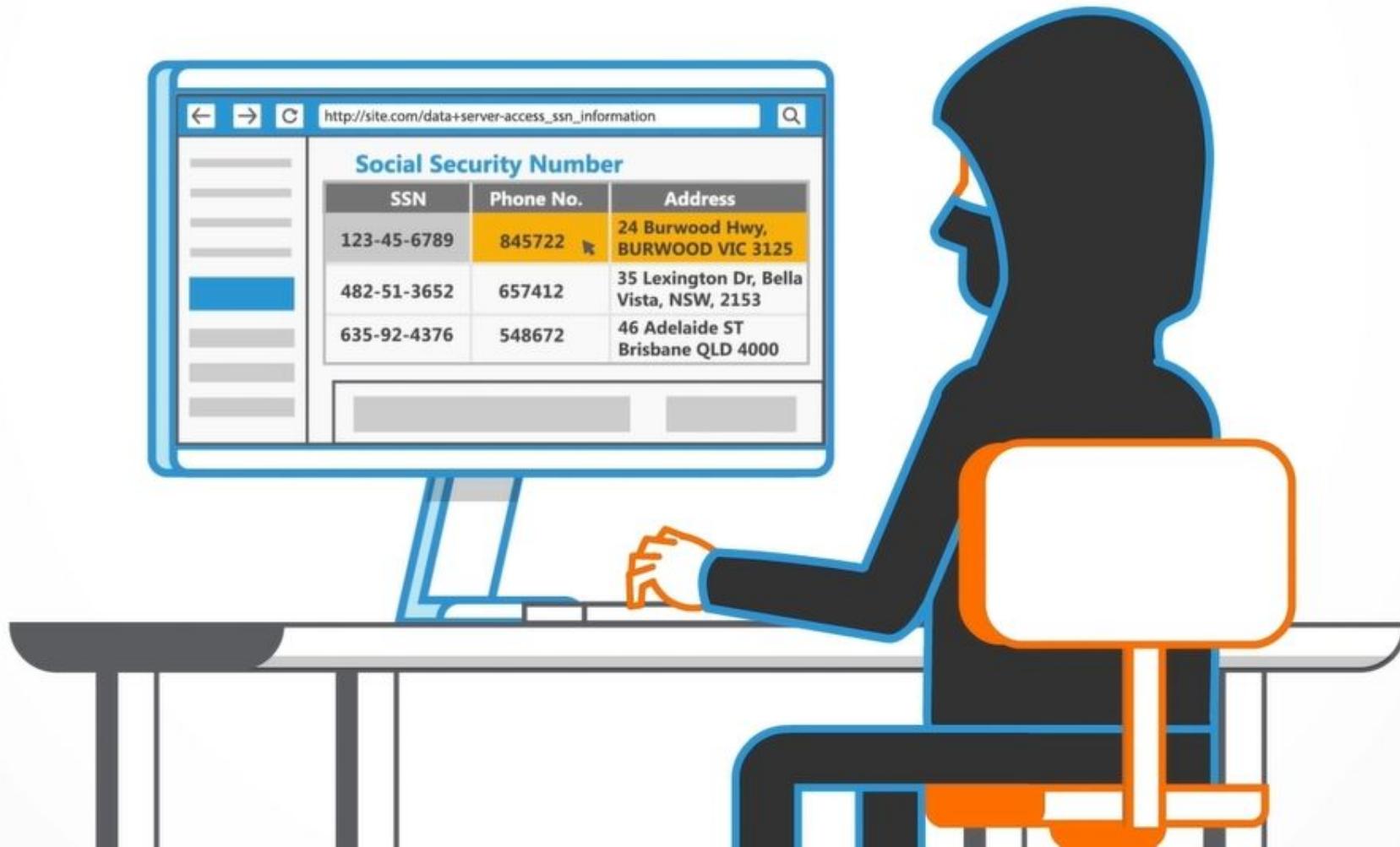
SENSITIVE DATA EXPOSURE

We'll explain

**What Sensitive Data Exposure is, its causes, preventions
and some potential hazards.**

WHAT IS SENSITIVE DATA EXPOSURE?

This is where sensitive data is exposed to actors that are not authorized to view that data.



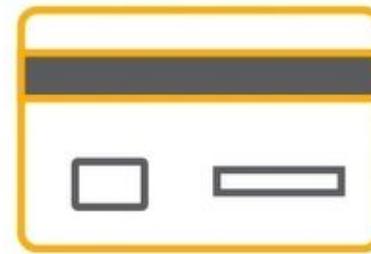
Such data could be user credentials, banking information, credit cards or personal information.



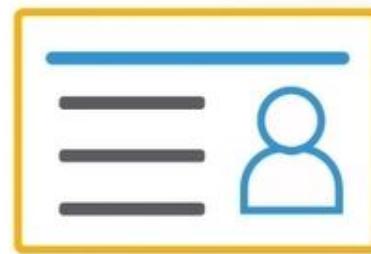
Credentials



Banking
Information



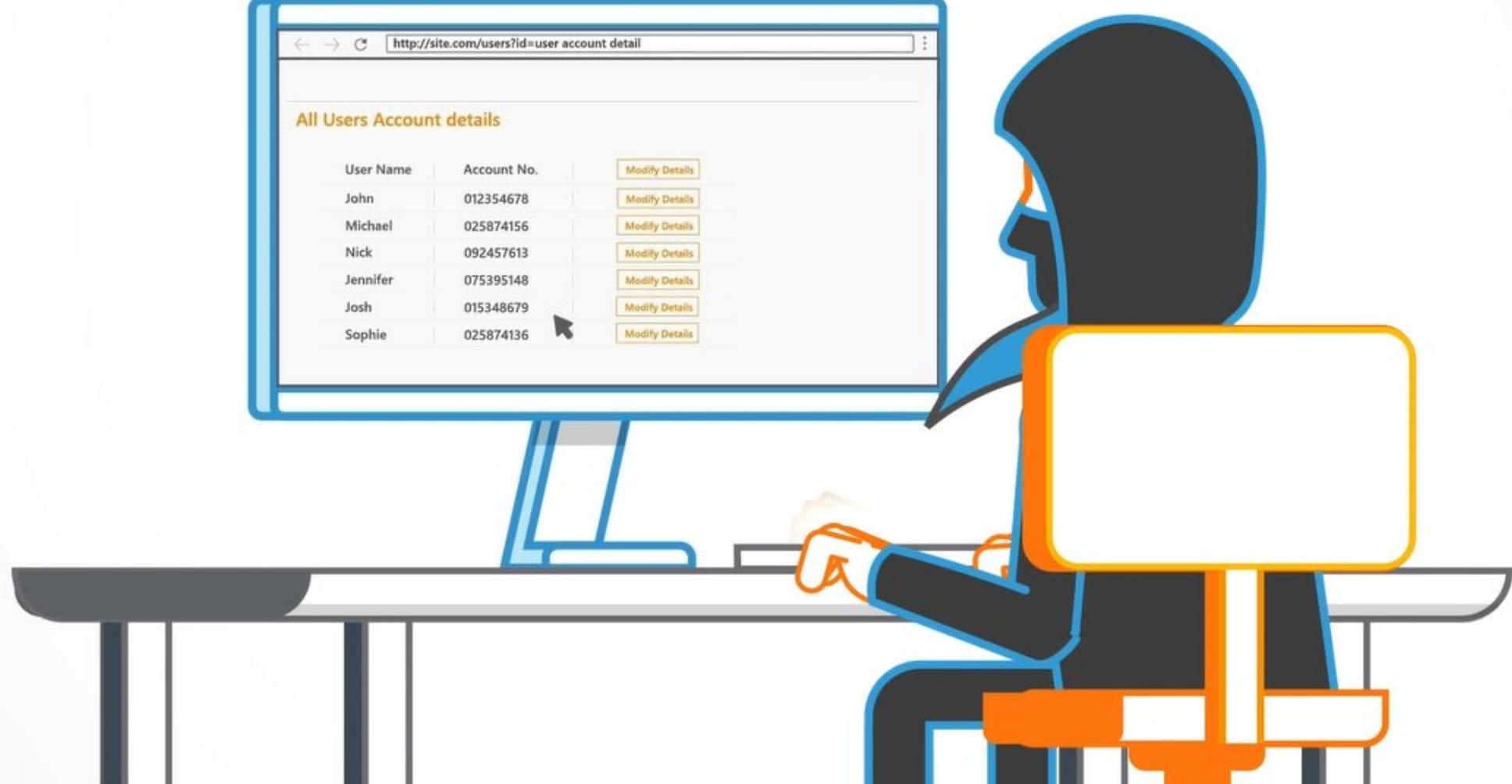
Credit cards



Personal
Information

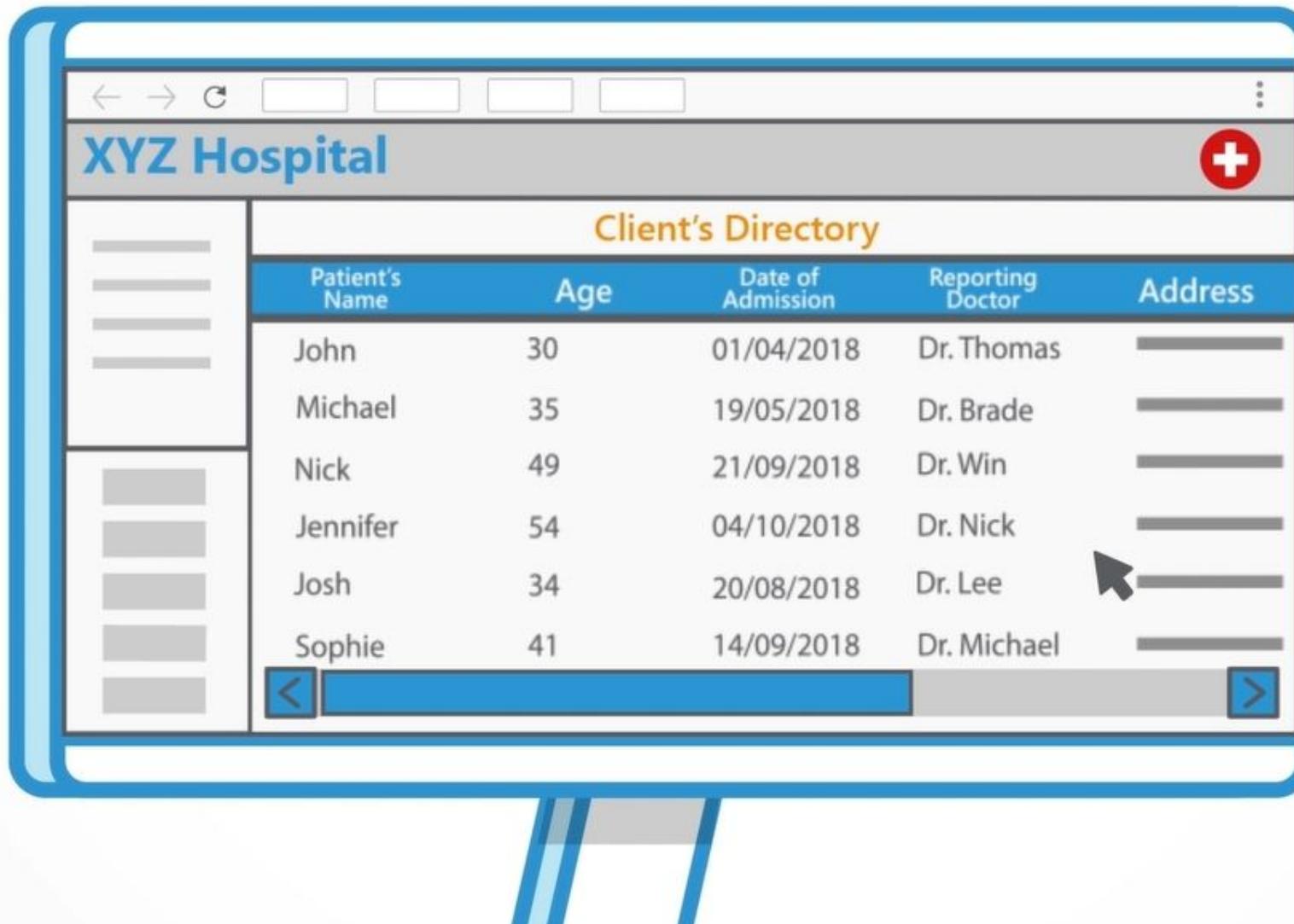
WHAT CAUSES SENSITIVE DATA EXPOSURE?

Sensitive data exposure vulnerabilities can occur when an application does not adequately protect sensitive information from being disclosed to attackers.



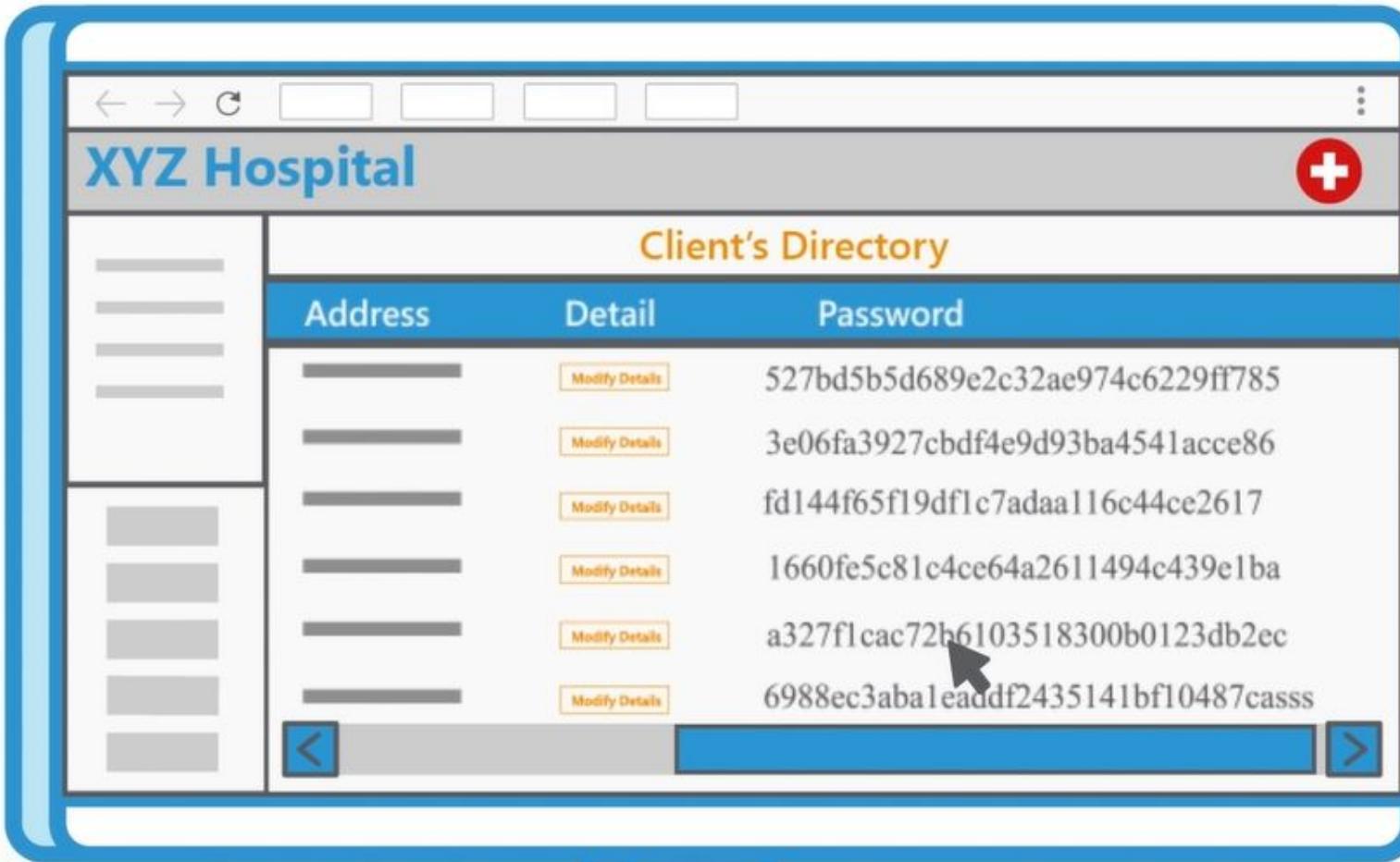
LET'S LOOK AT AN EXAMPLE

Let's say we have a dedicated computer with an application running that stores all medical information about clients from a hospital.



The password database for the application uses unsalted or simple hashes to store everyone's passwords.

UNsalted or Simple Hashes Password Encryption



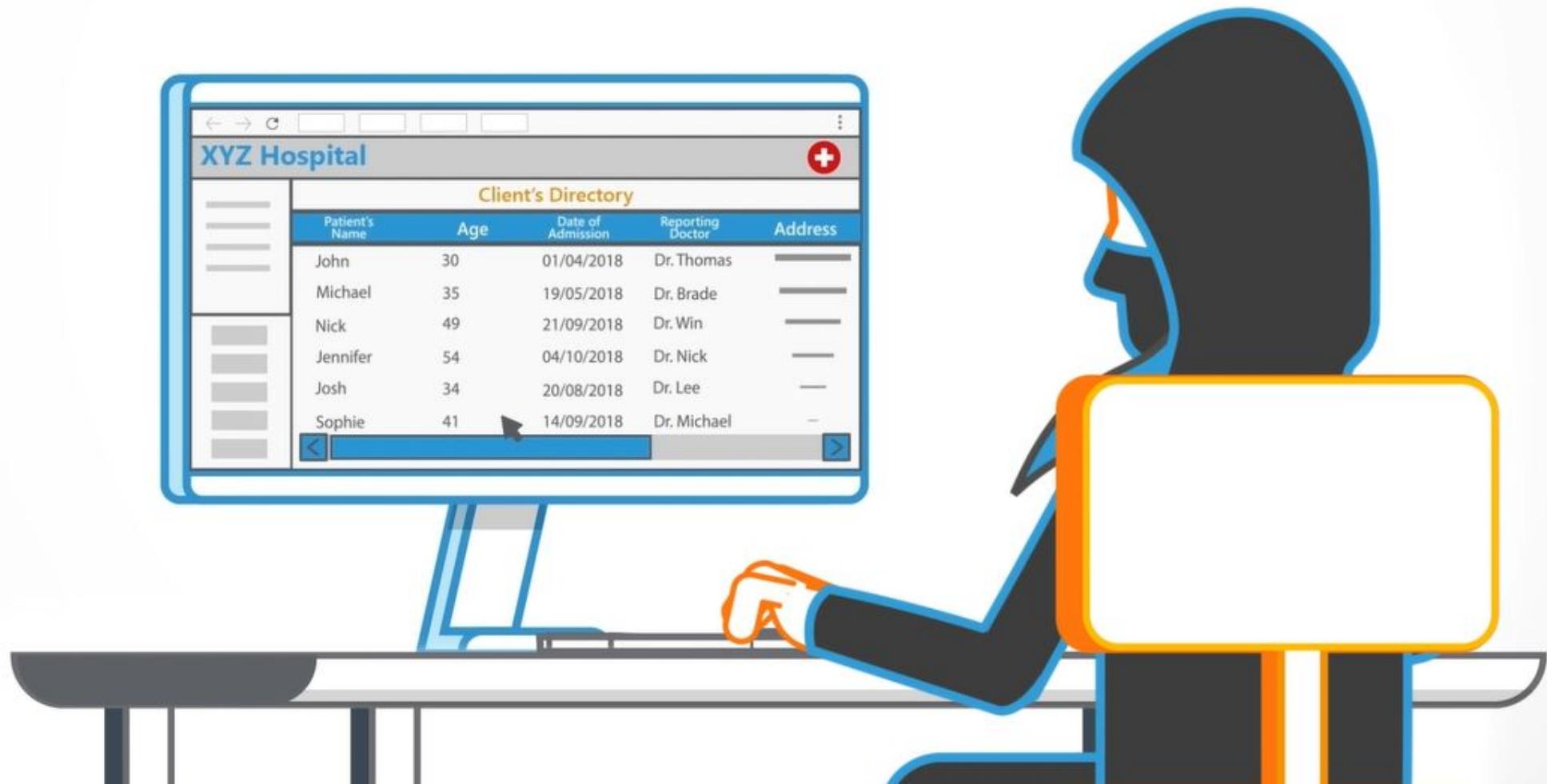
A screenshot of a web application interface titled "XYZ Hospital". The main section is labeled "Client's Directory" and displays a table with three columns: "Address", "Detail", and "Password". The "Address" and "Detail" columns contain redacted (grey) data, while the "Password" column lists various unsalted or simple hash values. Each row in the table includes a "Modify Details" button. A cursor arrow points to the fifth row's password hash, "a327f1cac72b6103518300b0123db2ec". The application has a navigation bar at the top with back, forward, and search icons, and a sidebar on the left.

Address	Detail	Password
[REDACTED]	[REDACTED]	527bd5b5d689e2c32ae974c6229ff785
[REDACTED]	[REDACTED]	3e06fa3927cbdf4e9d93ba4541acce86
[REDACTED]	[REDACTED]	fd144f65f19df1c7adaa116c44ce2617
[REDACTED]	[REDACTED]	1660fe5c81c4ce64a2611494c439e1ba
[REDACTED]	[REDACTED]	a327f1cac72b6103518300b0123db2ec
[REDACTED]	[REDACTED]	6988ec3aba1eaddf2435141bf10487casss

A file upload flaw allows an attacker to retrieve the password database.

- **Remote Access**

Now, all the unsalted hashes can be exposed with a rainbow table of pre-calculated hashes.



Hashes generated by simple or fast hash functions can also be cracked by GPUs, even if they were salted.

RAINBOW TABLE

Username	Password Hash	Password
John	527bd5b5d689e2c32ae974c6229ff785	john123
Michael	3e06fa3927cbdf4e9d93ba4541acce86	dragon
Nick	fd144f65f19df1c7adaa116c44ce2617	nick@1512
Jennifer	1660fe5c81c4ce64a2611494c439e1ba	123456
Josh	a327f1cac72b6103518300b0123db2ec	joshdoe123
Sophie	6988ec3abaleaddf2435141bf10487ca	password



As a result, all user credentials are now exposed.

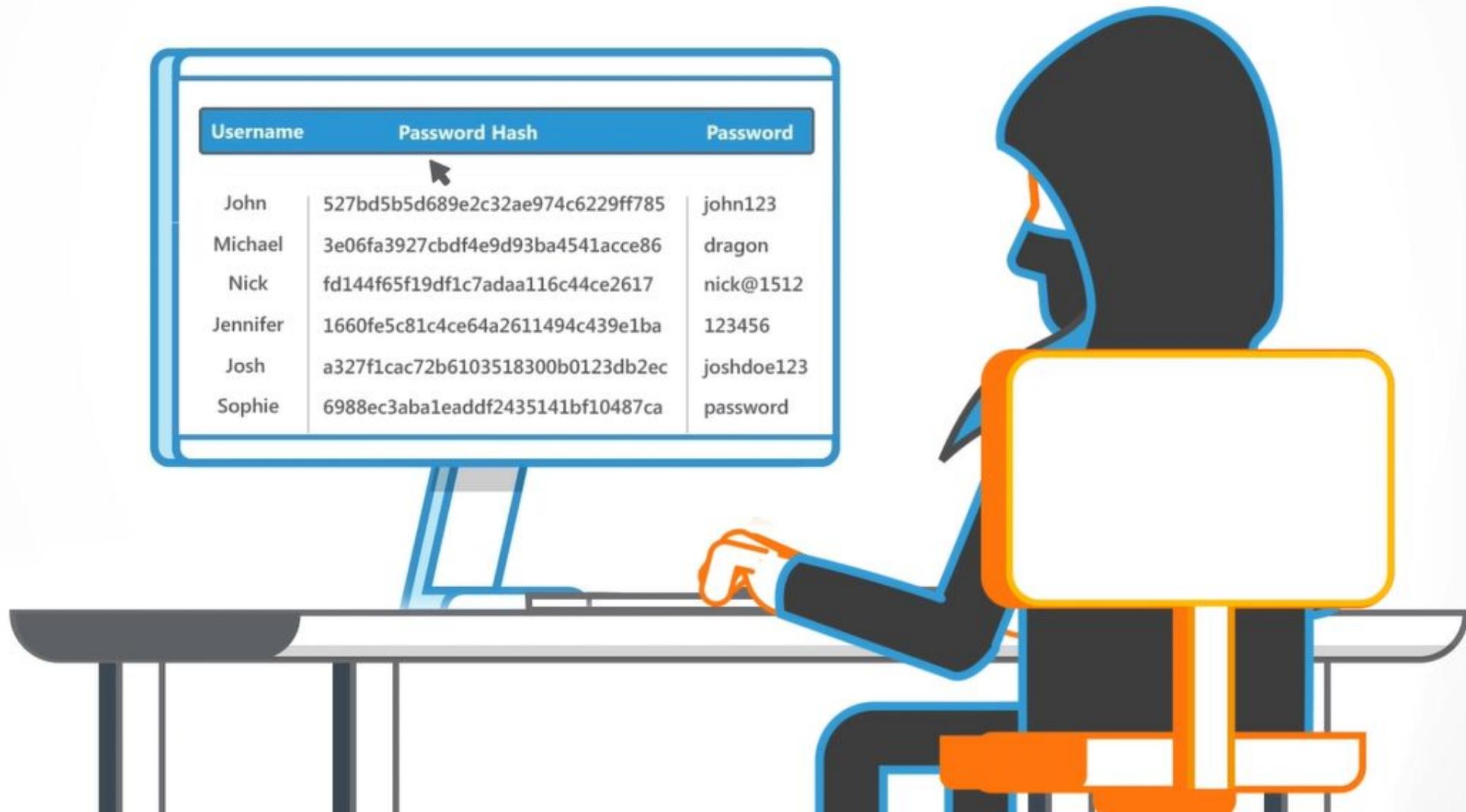


Username	Password Hash	Password
John	527bd5b5d689e2c32ae974c6229ff785	john123
Michael	3e06fa3927cbdf4e9d93ba4541acce86	dragon
Nick	fd144f65f19df1c7adaa116c44ce2617	nick@1512
Jennifer	1660fe5c81c4ce64a2611494c439e1ba	123456
Josh	a327f1cac72b6103518300b0123db2ec	joshdoe123
Sophie	6988ec3abaleaddf2435141bf10487ca	password

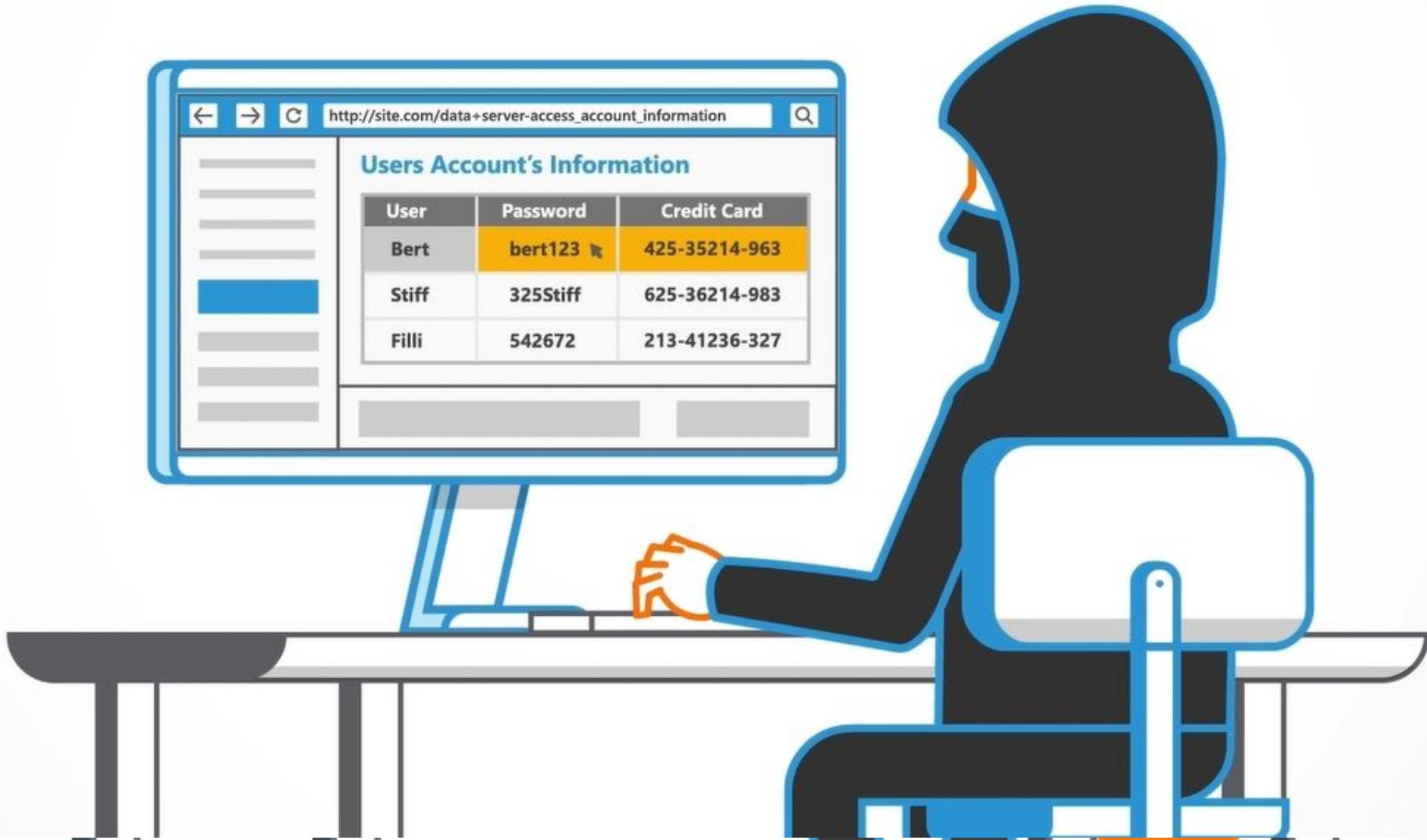


SENSITIVE DATA EXPOSURE COULD HAVE SIGNIFICANT IMPACT

Exposing sensitive data could lead to identity hijacking if credentials or personal information are being leaked.



If banking information or credit card numbers are exposed, this could lead to a financial loss.



To prevent Sensitive Data Exposure vulnerabilities:

- ④ Developers should encrypt data during transport and at rest, using the latest encryption algorithms.
- ④ Encrypt all data in transit with secure protocols such as TLS.
- ④ Don't store sensitive data unnecessarily.
- ④ Use a strong hashing or encryption algorithm where applicable.
- ④ When using a hashing algorithm be sure to use a salt and a pepper.
- ④ For data that doesn't need to be hashed, use symmetric encryption.
- ④ And finally, disable caching of sensitive data.

Congratulations, you have now completed this module, Sensitive Data Exposure!



**SECURE
CODE
WARRIOR**