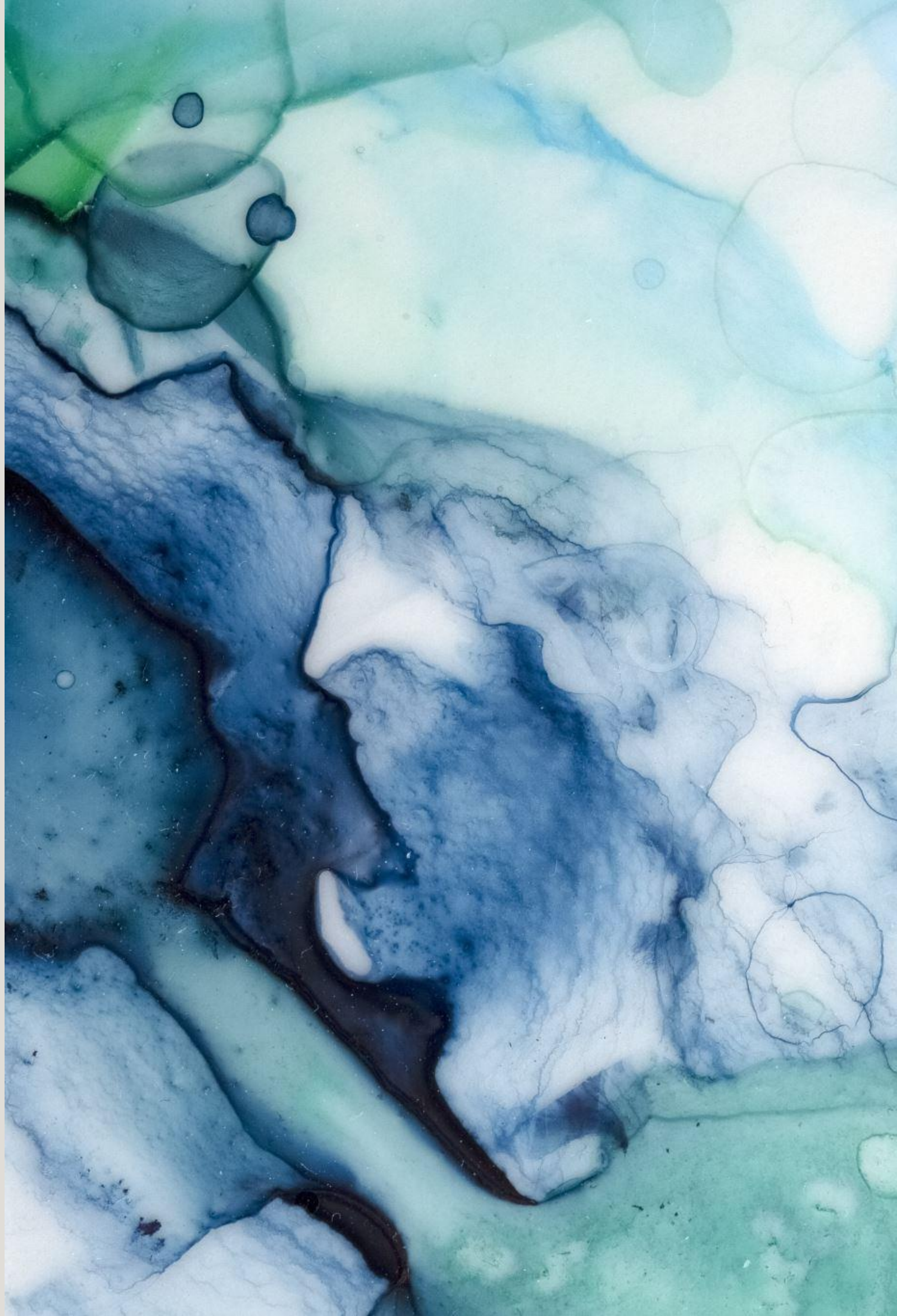
INSECURE CRYPTOGRAPHIC STORAGE- CWE 327

Sanad Masannat



WHAT IS INSECURE CRYPTOGRAPHIC STORAGE

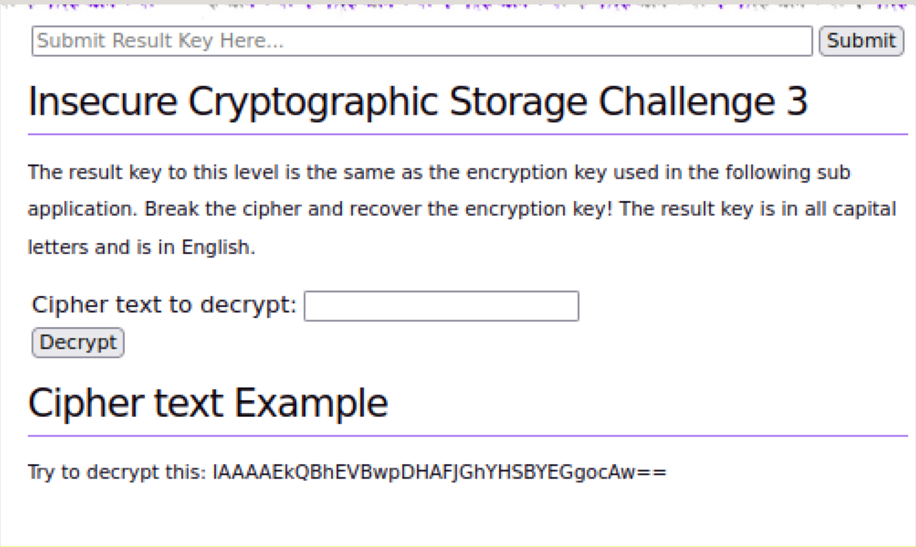
- Weak or outdated cryptography algorithms are used
- Improper Key Handling
- No hashing and/or salting used on passwords

WHAT WAS TESTED

- Security Shepherd Web Application
- Insecure Cryptography Challenge 3
- VM Environment

WHAT WAS USED

- Python Code
- Burp Suite



Insecure Cryptographic Storage Challenge 3

The result key to this level is the same as the encryption key used in the following sub application. Break the cipher and recover the encryption key! The result key is in all capital letters and is in English.

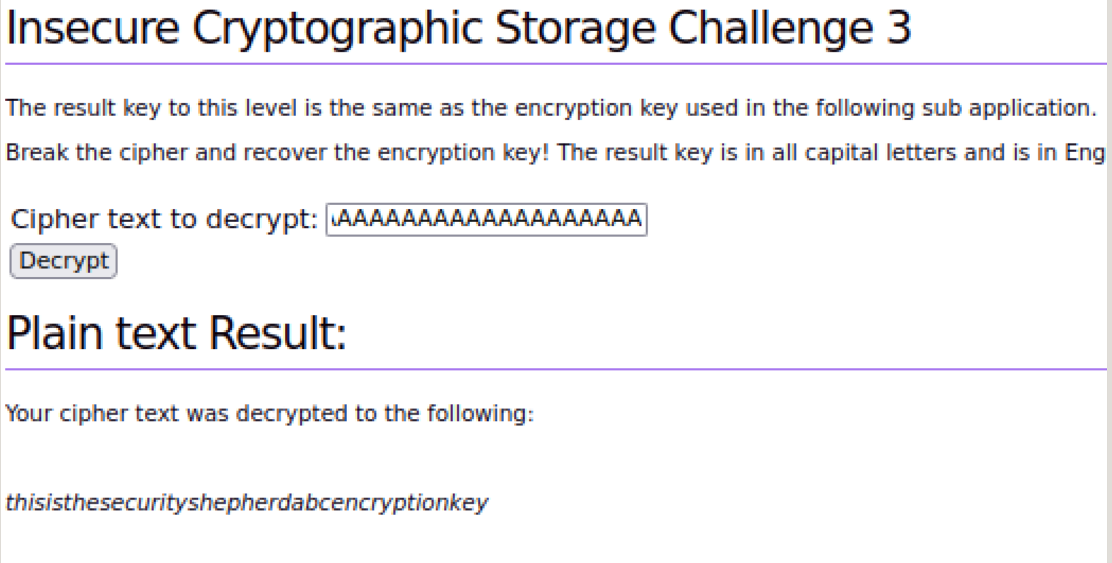
Cipher text to decrypt:

Cipher text Example

Try to decrypt this: IAAAAEkQBhEVBwpDHAFJGhYHSBYEGgocAw==

TEST PROCESS

- Input given cipher text and make note of output
- Put it through base64 decode on BurpSuite
- Run python code to compare plaintext and cipher text
- Input various strings and characters to see what is output
- Input 55 A's to get encryption key



Insecure Cryptographic Storage Challenge 3

The result key to this level is the same as the encryption key used in the following sub application.

Break the cipher and recover the encryption key! The result key is in all capital letters and is in Eng

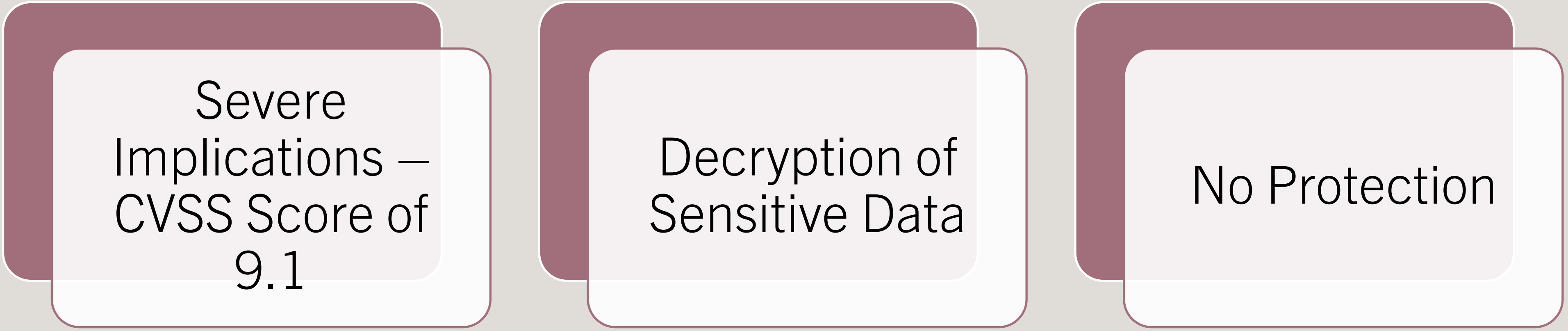
Cipher text to decrypt: AAAAAAAAAAAAAAAAAAA

Plain text Result:

Your cipher text was decrypted to the following:

thisisthesecurityshepherdabcencryptionkey

IMPLICATIONS OF THIS VULNERABILITY



Severe Implications – CVSS Score of 9.1

Decryption of Sensitive Data

No Protection

MITIGATION RECOMMENDATIONS

- Avoid using XOR and cyclic keys
- Avoid custom encryption
- Use more secure encryption algorithms
- Transient Keys
- Proper Key Management
- Use Salt and Hashes