OWASP TOP 10

A6 Sensitive Data Exposure

A6-Sensitive Data Exposure

- The Sensitive Data of the users such as passwords, Credit Card Details, SSN or Bank Details are generally exposed to an attacker due to the lack of implementation of Security Measures.
- The most commonly seen flaw is not encrypting the sensitive data, especially while transmitting and storing.

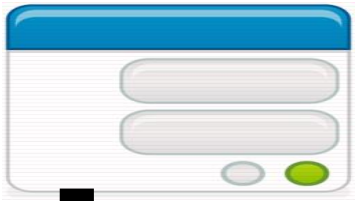
Causes:

- Sensitive Data either stored or sent in the plain text format.
- Implementation of obsolete/outdated cryptographic algorithms.
- Missing of required browser headers while such Sensitive Information is sent to the browser.
- Implementation of faulty key management.
- Lack of Implementation of Input Sanitization.

Insecure Cryptographic Storage

User

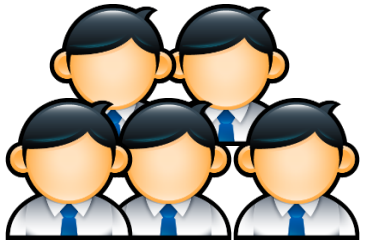
Enter the Credentials onto the form



Form

Log Files

Malicious Insider



IT Team

The logs are available to the IT Team for Debugging purposes.

As the merchant gateway is unavailable, the error handler logs the User's Credentials.

Consequences

- Sensitive data being misused by the attackers.
- Leading to compromise of the user accounts and data.
- Financial loss to the Users and to the Company as well.
- Legal liabilities as the sensitive data is exposed.
- Company Reputation would also get affected.

Mitigations

- Ensure that the PHP Implementation being used has a proper working mhash extension so as to incorporate SHA 256
- Ensure that the PHP Implementation being used has a proper working mcrypt extension in order to incorporate AES
- Avoid Vulnerable PHP Libraries.
- Ensure that Stable version of PHP is used instead of the beta version.
- To ensure that proper key management is implemented.
- To ensure that the passwords are stored with proper algoritms implemented such as scrypt or bcrypt.

Mitigations cont’d

- To ensure that the auto complete feature is disabled on forms that collect sensitive data.
- Encrypting all the Sensitive Data at all levels of Data transfer and storage.
- To ensure strong ciphers such as AES 128 is implemented.
- To ensure strong standard algorithms are implemented.

Real World Attacks

- http://nakedsecurity.sophos.com/2012/06/06/linkedin-confirms-hack-over-60-of-stolen-passwords-already-cracked/

DEMO