# Chapter twenty (OWASP)

- SQL Injection
- Cross Site Scripting
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

358



# OWASP Introduction

- **OWASP** or **O**pen **W**eb **A**pplication **S**ecurity **P**roject is a non-profit charitable organization focused on improving the security of software and web applications.
- The organization publishes a list of top web security vulnerabilities based on the data from various security organizations.
- The web security vulnerabilities are prioritized depending on exploitability, detectability and impact on software.

359

- **OWASP**أواقلم**دبليو**يب**أ**تطبيق**س**الأمن**ص**.هي منظمة خيرية غير ربحية تركزعلى تحسين أمان البرامج وتطبيقات الويب roject
- تنشرالمنظمة قائمة بأهم الثغرات الأمنية على شبكة الإنترنت استناداً إلىالبيانات الواردة من مؤسسات الأمان المختلفة.
- يتمتحديد أولويات الثغرات الأمنية على الويب بناءً على قابلية الاستغلالوقابلية الاكتشاف والتأثير على البرامج.

# OWASP Introduction-cont.

- **Exploitability –**
  - What is needed to exploit the security vulnerability? Highest exploitability when the attack needs only web browser and lowest being advanced programming and tools.
- **Detectability –**
  - How easy is it to detect the threat? Highest being the information displayed on URL, Form or Error message and lowest being source code.
- **Impact or Damage –**
  - How much damage will be done if the security vulnerability is exposed or attacked? Highest being complete system crash and lowest being nothing at all.

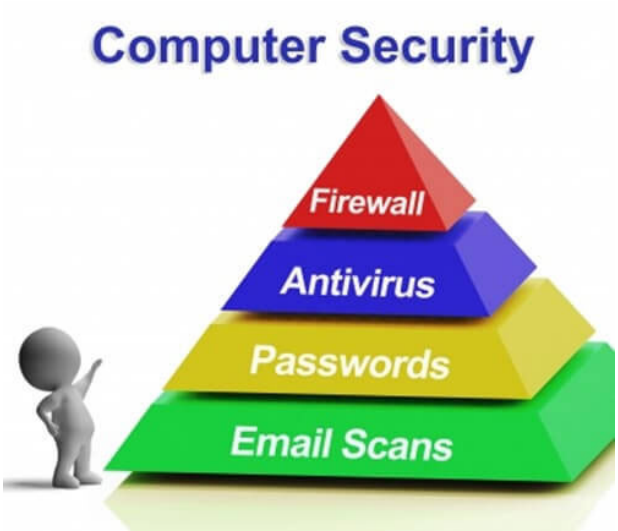
360

- **القابليةللاستغلال -**
  - ماهو المطلوب لاستغلال الثغرة الأمنية؟ أعلى قابلية للاستغلال عندما يحتاج الهجومفقط إلى متصفح ويب وأقل مستوى هو البرمجة والأدوات المتقدمة.

360

- **قابليةالكشف -**
  - مامدى سهولة اكتشاف التهديد؟ أعلها هي المعلومات المعروضة على URL أو النموذجأو رسالة الخطأ وأقلها هي رمز المصدر.
- **التأثيرأو الضرر -**
  - مامقدار الضرر الذي سيحدث إذا تم الكشف عن الثغرة الأمنية أو مهاجمتها؟ الأعلى هوتعطل النظام الكامل والأدنى لا شيء على الإطلاق.

# 1) SQL Injection




361

361

# 1) SQL Injection-cont.

**Description**

- Injection is a security vulnerability that allows an attacker to alter backend SQL statements by manipulating the user supplied data.
- Injection occurs when the user input is sent to an interpreter as part of command or query and trick the interpreter into executing unintended commands and gives access to unauthorized data.
- The SQL command which when executed by web application can also expose the back-end database.

**وصف**

- الحقنهو ثغرة أمنية تسمح للمهاجم بتغيير عبارات SQL الخلفية من خلالمعالجة البيانات المقدمة من المستخدم.
- يحدثالحقن عندما يتم إرسال مدخلات المستخدم إلى مترجم كجزء من الأمرأو الاستعلام وخداع المترجم الفوري لتنفيذ أوامر غير مقصودة وإتاحة الوصولإلى البيانات غير المصرح بها.
- أمرSQL الذي عند تنفيذه بواسطة تطبيق ويب يمكنه أيضاً عرض قاعدة البياناتالخلفية.



362

# 1) SQL Injection-cont.

**Implication**

- An attacker can inject malicious content into the vulnerable fields.
- Sensitive data like User Names, Passwords, etc. can be read from the database.
- Database data can be modified (Insert/Update/ Delete).
- Administration Operations can be executed on the database

**Vulnerable Objects**

- Input Fields
- URLs interacting with the database.

**يتضمن**

- يمكنللمهاجم حقن محتوى ضار في الحقول المعرضة للخطر.
- يمكنقراءة البيانات الحساسة مثل أسماء المستخدمين وكلمات المرور وما إلى ذلك من قاعدة البيانات.
- يمكنتعديل بيانات قاعدة البيانات (إدراج / تحديث / حذف).
- يمكنتنفيذ عمليات الإدارة على قاعدة البيانات

**الكائناتالمعرضة للخطر**

- حقولالإدخال
- تتفاعلعناوين URL مع قاعدة البيانات.



363

# 1) SQL Injection-cont.

**Examples:**

- SQL injection on the Login Page

  Logging into an application without having valid credentials.

  Valid userName is available, and password is not available.

  Test URL: http://demo.testfire.net/default.aspx

  User Name: sjones

  Password: 1=1' or pass123

  SQL query created and sent to Interpreter as below

  SELECT * FROM Users WHERE User_Name = sjones AND Password = 1=1' or pass123;

364

**أمثلة:**

- حقنSQL في صفحة تسجيل الدخول

تسجيلالدخول إلى تطبيق دون الحصول على بيانات اعتماد صالحة.

اسمالمستخدم الصالح متاح ، وكلمة المرور غير متاحة. اختبار

URL: http://demo.testfire.net/default.aspx

اسمالمستخدم: sjones

كلمةالمرور: 1 = 1 'أو pass123

تمإنشاء استعلام SQL وإرساله إلى المترجم الفوري على النحو التالي

حدد* من المستخدمين حيث User_Name = sjones وكلمة المرور = 1 = 1 'أو pass123 ؛

364

# 1) SQL Injection-cont.

- **Recommendations**
  1. White listing the input fields
  2. Avoid displaying detailed error messages that are useful to an attacker.

- **التوصيات**

1.قائمة بيضاء بحقول الإدخال

2.تجنب عرض رسائل خطأ مفصلة تفيد المهاجم.

365

365

# 2) Cross Site Scripting

- **Description**
  - Cross Site Scripting is also shortly known as XSS.
  - XSS vulnerabilities target scripts embedded in a page that are executed on the client side i.e. user browser rather then at the server side. These flaws can occur when the application takes untrusted data and send it to the web browser without proper validation.
  - Attackers can use XSS to execute malicious scripts on the users in this case victim browsers. Since the browser cannot know if the script is trusty or not, the script will be executed, and the attacker can hijack session cookies, deface websites, or redirect the user to an unwanted and malicious websites.
  - XSS is an attack which allows the attacker to execute the scripts on the victim's browser.

366

- **وصف**
  - تعُرف البرمجة النصية عبر الموقع أيضاً باختصار باسم XSS.
  - تستهدف ثغرات XSS البرامج النصية المضمنة في الصفحة التي يتم تنفيذها على جانب العميل ، أي متصفح المستخدم بدلاً من جانب الخادم. يمكن أن تحدث هذه العيوب عندما يأخذ التطبيق بيانات غير موثوق بها ويرسلها إلى متصفح الويب دون التحقق المناسب من الصحة.
  - يمكن للمهاجمين استخدام XSS لتنفيذ نصوص ضارة على المستخدمين في هذه الحالة المتصفحات الضحية. نظراً لأن المتصفح لا يمكنه معرفة ما إذا كان البرنامج النصي موثوقاً أم لا ، فسيتم تنفيذ البرنامج النصي ، ويمكن للمهاجم اختطاف ملفات تعريف الارتباط للجلسة أو تشويه مواقع الويب أو إعادة توجيه المستخدم إلى مواقع ويب غير مرغوب فيها وضارة.
  - هوهجوم يسمح للمهاجم بتنفيذ البرامج النصية على متصفح الضحية XSS.

366

# 2) Cross Site Scripting-cont.

- **Implication:**
  - Making the use of this security vulnerability, an attacker can inject scripts into the application, can steal session cookies, deface websites, and can run malware on the victim's machines.
- **Vulnerable Objects**
  - Input Fields
  - URLs

- **يتضمن:**
  - باستخدام هذه الثغرة الأمنية ، يمكن للمهاجم حقن البرامج النصية في التطبيق ، ويمكنه سرقة ملفات تعريف الارتباط للجلسة ، وتشويه مواقع الويب ، ويمكنه تشغيل برامج ضارة على أجهزة الضحية.
  - **الكائنات المعرضة للخطر**
    - حقول الإدخال
    - عناوين URL

367

# 2) Cross Site Scripting-cont.

- **Examples**
  - 1. http://www.vulnerablesite.com/home?"<script>alert("xss")</script>
  - The above script when run on a browser, a message box will be displayed if the site is vulnerable to XSS.
  - The more serious attack can be done if the attacker wants to display or store session cookie.
  - 2. http://demo.testfire.net/search.aspx?txtSearch <iframe> <src = http://google.com width = 500 height 500></iframe>
  - The above script when run, the browser will load an invisible frame pointing to http://google.com.
  - The attack can be made serious by running a malicious script on the browser.

368

- **أمثلة**
  - 1. http://www.vulnerablesite.com/home؟ ">script< تنبيه )" xss "( >/script<
  - عندتشغيل البرنامج النصي أعلاه على متصفح ، سيتم عرض مربع رسالة إذا كان الموقععرضة لـ XSS.
  - يمكنتنفيذ الهجوم الأكثر خطورة إذا أراد المهاجم عرض ملف تعريف ارتباط الجلسة أو تخزينه.
  - >src = http://google.com width = 500 height 500< >/iframe<
    2. http://demo.testfire.net/search.aspx؟txtSearch >iframe<
  - عندتشغيل البرنامج النصي أعلاه ، سيقوم المتصفح بتحميل إطار غير مرئي يشير إلى http://google.com.
  - يمكنجعل الهجوم خطيراً عن طريق تشغيل برنامج نصي ضار على المتصفح.

368

# 2) Cross Site Scripting-cont.

- **Recommendations**
  1. White Listing input fields
  2. Input Output encoding

- **التوصيات**

1.حقول إدخال القائمة البيضاء

2.إدخال ترميز الإخراج

369

369

# 3) Broken Authentication and Session Management

- **Description**
  - The websites usually create a session cookie and session ID for each valid session, and these cookies contain sensitive data like username, password, etc. When the session is ended either by logout or browser closed abruptly, these cookies should be invalidated i.e. for each session there should be a new cookie.
  - If the cookies are not invalidated, the sensitive data will exist in the system. For example, a user using a public computer (Cyber Cafe), the cookies of the vulnerable site sits on the system and exposed to an attacker. An attacker uses the same public computer after some time, the sensitive data is compromised.

370

- **وصف**
  - عادةً ما تنشئ مواقع الويب ملف تعريف ارتباط جلسة ومعرف جلسة لكل جلسة صالحة ، وتحتوي ملفات تعريف الارتباط هذه على بيانات حساسة مثل اسم المستخدم وكلمة المرور وما إلى ذلك. عندما تنتهي الجلسة إما عن طريق تسجيل الخروج أو إغلاق المتصفح فجأة ، يجب إلغاء ملفات تعريف الارتباط هذه ، أي لكل جلسة يجب أن يكون هناك ملف تعريف ارتباط جديد.
  - إذا لم يتم إبطال ملفات تعريف الارتباط ، فستتواجد البيانات الحساسة في النظام. على سبيل المثال ، مستخدم يستخدم جهاز كمبيوتر عام (مقهى الإنترنت) ، فإن ملفات تعريف الارتباط الخاصة بالموقع الضعيف تجلس على النظام وتتعرض للمهاجم. يستخدم المهاجم نفس الكمبيوتر العام بعد مرور بعض الوقت ، يتم اختراق البيانات الحساسة.

370

# 3) Broken Authentication and Session Management- cont.

- **Description**
  - In the same manner, a user using a public computer, instead of logging off, he closes the browser abruptly. An attacker uses the same system, when browses the same vulnerable site, the previous session of the victim will be opened. The attacker can do whatever he wants to do from stealing profile information, credit card information, etc.
  - A check should be done to find the strength of the authentication and session management. Keys, session tokens, cookies should be implemented properly without compromising passwords.

371

- **وصف**
  - بنفس الطريقة ، مستخدم يستخدم جهاز كمبيوتر عام ، بدلاً من تسجيل الخروج ، يقوم بإغلاق المتصفح فجأة. يستخدم المهاجم نفس النظام ، عند تصفح نفس الموقع المعرض للخطر ، سيتم فتح الجلسة السابقة للضحية. يمكن للمهاجم أن يفعل ما يشاء من سرقة معلومات الملف الشخصي ، ومعلومات بطاقة الائتمان ، وما إلى ذلك.
  - يجب إجراء فحص للعثور على قوة المصادقة وإدارة الجلسة. يجب تنفيذ المفاتيح ورموز الجلسة وملفات تعريف الارتباط بشكل صحيح دون المساس بكلمات المرور.

371

# 3) Broken Authentication and Session Management- cont.

- **Vulnerable Objects**
  - Session IDs exposed on URL can lead to session fixation attack.
  - Session IDs same before and after logout and login.
  - Session Timeouts are not implemented correctly.
  - Application is assigning same session ID for each new session.
  - Authenticated parts of the application are protected using SSL and passwords are stored in hashed or encrypted format.
  - The session can be reused by a low privileged user.

- **الكائناتالمعرضة للخطر**
  - يمكنأن تؤدي معرفات الجلسات المعروضة على عنوان URL إلى هجوم تثبيت الجلسة.
  - معرفاتالجلسات هي نفسها قبل وبعد تسجيل الخروج وتسجيل الدخول.
  - لميتم تنفيذ مهلات الجلسة بشكل صحيح.
  - يقومالتطبيق بتعيين نفس معرف الجلسة لكل جلسة جديدة.
  - تتمحماية الأجزاء المصادق عليها من التطبيق باستخدام SSL ويتم تخزين كلمات المروربتنسيق مجزأ أو مشفر.
  - يمكنإعادة استخدام الجلسة بواسطة مستخدم ذي امتيازات منخفضة.

372

372

# 3) Broken Authentication and Session Management- cont.

- **Implication**
  - Making use of this vulnerability, an attacker can hijack a session, gain unauthorized access to the system which allows disclosure and modification of unauthorized information.
  - The sessions can be high jacked using stolen cookies or sessions using XSS.

- **يتضمن**
  - باستخدامهذه الثغرة الأمنية ، يمكن للمهاجم خطف جلسة ، والحصول على وصول غيرمصرح به إلى النظام الذي يسمح بالكشف عن المعلومات غير المصرح بها وتعديلها.
  - يمكنرفع الجلسات باستخدام ملفات تعريف الارتباط المسروقة أو الجلسات باستخدام XSS.

373

373

# 3) Broken Authentication and Session Management- cont.

- **Examples**
  1. Airline reservation application supports URL rewriting, putting session IDs in the URL:
  2. http://Examples.com/sale/saleitems;jsessionid=2P0OC2oJM0DPXSNQPLME34SER TBG/dest=Maldives (Sale of tickets to Maldives)
  3. An authenticated user of the site wants to let his friends know about the sale and sends an email across. The friends receive the session ID and can be used to do unauthorized modifications or misuse the saved credit card details.
  4. An application is vulnerable to XSS, by which an attacker can access the session ID and can be used to hijack the session.
  5. Applications timeouts are not set properly. The user uses a public computer and closes the browser instead of logging off and walks away. The attacker uses the same browser some time later, and the session is authenticated.

374

- **أمثلة**

1.يدعم تطبيق حجز الخطوط الجوية إعادة كتابة عناوين URL ، ووضع معرفات الجلسة في عنوان URL:

2. http://Examples.com/sale/saleitems؛jsessionid=2P0OC2oJM0DPXSNQPLME34SER TBG / dest = Maldives( بيع تذاكر جزر المالديف)

3.يريد المستخدم المعتمد للموقع السماح لأصدقائه بمعرفة البيع وإرسال بريد إلكتروني عبره. يتلقى الأصدقاء معرف الجلسة ويمكن استخدامه لإجراء تعديلات غير مصرح بها أو إساءة استخدام تفاصيل بطاقة الائتمان المحفوظة.

4.يكون التطبيق عرضة لـ XSS ، حيث يمكن للمهاجم الوصول إلى معرف الجلسة ويمكن استخدامه لاختطاف الجلسة.

5.لم يتم تعيين مهلات التطبيقات بشكل صحيح. يستخدم المستخدم جهاز كمبيوتر عام ويغلق المتصفح بدلاً من تسجيل الخروج ويبتعد. يستخدم المهاجم نفس المتصفح في وقت لاحق ، ويتم مصادقة الجلسة.

374

# 3) Broken Authentication and Session Management- cont.

- **Recommendations**
  1. All the authentication and session management requirements should be defined as per OWASP Application Security Verification Standard.
  2. Never expose any credentials in URLs or Logs.
  3. Strong efforts should be also made to avoid XSS flaws which can be used to steal session IDs.

375

- **التوصيات**

1.يجب تحديد جميع متطلبات المصادقة وإدارة الجلسة وفقاً لمعيار OWASP للتحقق من أمان التطبيقات.

2.لا تكشف أبداً أي بيانات اعتماد في عناوين URL أو السجلات.

3.يجب أيضاً بذل جهود قوية لتجنب عيوب XSS التي يمكن استخدامها لسرقة معرفات الجلسة.

375

# 4) Insecure Direct Object References

- **Description**
  - It occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key as in URL or as a FORM parameter. The attacker can use this information to access other objects and can create a future attack to access the unauthorized data.
- **Implication**
  - Using this vulnerability, an attacker can gain access to unauthorized internal objects, can modify data or compromise the application.
- **Vulnerable Objects**
  - In the URL.

376

- **وصف**
  - يحدثذلك عندما يعرض المطور مرجعاً إلى كائن تنفيذ داخلي ، مثل ملف أو دليل أو مفتاحقاعدة بيانات كما هو الحال في URL أو كمعامل FORM. يمكن للمهاجم استخدام هذهالمعلومات للوصول إلى كائنات أخرى ويمكنه إنشاء هجوم مستقبلي للوصول إلى البياناتغير المصرح بها.
- **يتضمن**
  - باستخدامهذه الثغرة الأمنية ، يمكن للمهاجم الوصول إلى كائنات داخلية غير مصرح بها ،ويمكنه تعديل البيانات أو اختراق التطبيق.
- **الكائناتالمعرضة للخطر**
  - فيURL.

376

# 4) Insecure Direct Object References-cont.

- **Examples:**
  - Changing "userid" in the following URL can make an attacker to view other user's information.
  - http://www.vulnerablesite.com/userid=123 Modified to http://www.vulnerablesite.com/userid=124
  - An attacker can view others information by changing user id value.

- **أمثلة:**
  - يمكنأن يؤدي تغيير "معرف المستخدم" في عنوان URL التالي إلى جعل المهاجم يعرض معلومات المستخدمالآخر.
  - http://www.vulnerablesite.com/userid=124 تم التعديل على http://www.vulnerablesite.com/userid=123
  - يمكنللمهاجم عرض معلومات الآخرين عن طريق تغيير قيمة معرف المستخدم.

377

377

# 4) Insecure Direct Object References-cont.

- **Recommendations:**
  1. Implement access control checks.
  2. Avoid exposing object references in URLs.
  3. Verify authorization to all reference objects.

- **التوصيات:**

1.تنفيذ فحوصات التحكم في الوصول.
2.تجنب فضح مراجع الكائنات في عناوين المواقع.
3.تحقق من الإذن لجميع الكائنات المرجعية.





# 5) Cross Site Request Forgery

- **Description**
  - Cross Site Request Forgery is a forged request came from the cross site.
  - CSRF attack is an attack that occurs when a malicious website, email, or program causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated.
  - A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application.
  - A link will be sent by the attacker to the victim when the user clicks on the URL when logged into the original website, the data will be stolen from the website.

- **وصف**



- التزويرعبر الموقع هو طلب مزور جاء من الموقع المتقاطع.
- هجومCSRF هو هجوم يحدث عندما يتسبب موقع ويب أو بريد إلكتروني أو برنامج ضار في قيام مستعرض المستخدم بإجراء غير مرغوب فيه على موقع موثوق به تمت مصادقةالمستخدم من أجله حالياً.
- يفرضهجوم CSRF على متصفح الضحية الذي قام بتسجيل الدخول إرسال طلب HTTP مزيف ، بما في ذلك ملف تعريف ارتباط جلسة الضحية وأي معلومات مصادقةأخرى مضمنة تلقائياً ، إلى تطبيق ويب ضعيف.
- سيتمإرسال رابط من قبل المهاجم إلى الضحية عندما ينقر المستخدم على عنوان URL عند تسجيل الدخول إلى موقع الويب الأصلي ، وستُسرق البيانات من موقع الويب.

# 5) Cross Site Request Forgery-cont.

- **Implication**
  - Using this vulnerability as an attacker can change user profile information, change status, create a new user on admin behalf, etc.
- **Vulnerable Objects**
  - User Profile page
  - User account forms
  - Business transaction page

- **يتضمن**
  - يمكنأن يؤدي استخدام هذه الثغرة الأمنية كمهاجم إلى تغيير معلومات ملف تعريف المستخدم وتغييرالحالة وإنشاء مستخدم جديد نيابة عن المسؤول وما إلى ذلك.
- **الكائناتالمعرضة للخطر**
  - صفحةملف تعريف المستخدم
  - نماذجحساب المستخدم
  - صفحةالمعاملات التجارية



380

# 5) Cross Site Request Forgery-cont.

- **Examples**
  - The victim is logged into a bank website using valid credentials. He receives mail from an attacker saying "Please click here to donate $1 to cause."
  - When the victim clicks on it, a valid request will be created to donate $1 to a particular account.
  - http://www.vulnerablebank.com/transfer.do?account=cause&amount=1
  - The attacker captures this request and creates below request and embeds in a button saying "I Support Cause."
  - http://www.vulnerablebank.com/transfer.do?account=Attacker&amount=1000
  - Since the session is authenticated and the request is coming through the bank website, the server would transfer $1000 dollars to the attacker.

- **أمثلة**
  - يتمتسجيل دخول الضحية إلى موقع ويب مصرفي باستخدام بيانات اعتماد صالحة. يتلقى بريداً منأحد المهاجمين يقول "الرجاء النقر هنا للتبرع بدولار واحد للتسبب".
  - عندماينقر الضحية عليه ، سيتم إنشاء طلب صالح للتبرع بدولار واحد لحساب معين.
  - http://www.vulnerablebank.com/transfer.do?account=cause&amount=1
  - يلتقطالمهاجم هذا الطلب وينشئ الطلب أدناه ويقوم بتضمينه في زر يقول "أنا أؤيد السبب".
  - http://www.vulnerablebank.com/transfer.do?account=Attacker&amount=1000
  - نظراًللمصادقة على الجلسة وصدور الطلب من خلال موقع البنك على الويب ، فسيقوم الخادمبتحويل 1000 دولار إلى المهاجم.



381

# 5) Cross Site Request Forgery-cont.

- **Recommendation**
  1. Mandate user's presence while performing sensitive actions.
  2. Implement mechanisms like CAPTCHA, Re-Authentication, and Unique Request Tokens.

- **توصية**

1.فرض حضور المستخدم أثناء تنفيذ الإجراءات الحساسة.
2.تنفيذ آليات مثل CAPTCHA وإعادة المصادقة ورموز الطلب الفريدة.

382



# 6) Security Misconfiguration

- **Description**
  - Security Configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform. If these are properly configured, an attacker can have unauthorized access to sensitive data or functionality.
  - Sometimes such flaws result in complete system compromise. Keeping the software up to date is also good security.

- **وصف**
  - يجبتحديد تكوين الأمان ونشره للتطبيق ، وأطر العمل ، وخادم التطبيق ، وخادم الويب ،وخادم قاعدة البيانات ، والنظام الأساسي. إذا تم تكوينها بشكل صحيح ، يمكن للمهاجمالحصول على وصول غير مصرح به إلى البيانات أو الوظائف الحساسة.
  - فيبعض الأحيان تؤدي هذه العيوب إلى تسوية كاملة للنظام. يعد الحفاظ على تحديثالبرنامج أيضاً أماناً جيداً.

383

# 6) Security Misconfiguration-cont.

- **Implication**
  - Making use of this vulnerability, the attacker can enumerate the underlying technology and application server version information, database information and gain information about the application to mount few more attacks.
- **Vulnerable objects**
  - URL
  - Form Fields
  - Input fields

- **يتضمن**
  - باستخدامهذه الثغرة الأمنية ، يمكن للمهاجم تعداد التكنولوجيا الأساسية ومعلومات إصدارخادم التطبيق ومعلومات قاعدة البيانات والحصول على معلومات حول التطبيقلشن المزيد من الهجمات القليلة.
- **الأشياءالمعرضة للخطر**
  - URL
  - حقولالنموذج
  - حقولالإدخال

384



# 6) Security Misconfiguration-cont.

- **Examples**
  1. The application server admin console is automatically installed and not removed. Default accounts are not changed. The attacker can log in with default passwords and can gain unauthorized access.
  2. Directory Listing is not disabled on your server. Attacker discovers and can simply list directories to find any file.

- **أمثلة**

1.يتم تثبيت وحدة تحكم مشرف خادم التطبيق تلقائياً ولا تتم إزالتها. لم يتم تغيير الحساباتالافتراضية. يمكن للمهاجم تسجيل الدخول بكلمات مرور افتراضية ويمكنهالحصول على وصول غير مصرح به.

2.لم يتم تعطيل قائمة الدليل على الخادم الخاص بك. يكتشف المهاجم ويمكنه ببساطة سردالدلائل للعثور على أي ملف.

385

# 6) Security Misconfiguration-cont.

- **Recommendations**
  1. A strong application architecture that provides good separation and security between the components.
  2. Change default usernames and passwords.
  3. Disable directory listings and implement access control checks.

- **التوصيات**

1.بنية تطبيق قوية توفر فصلاً جيداً وأماناً بين المكونات.

2.تغيير أسماء المستخدمين وكلمات المرور الافتراضية.

3.تعطيل قوائم الدليل وتنفيذ عمليات فحص التحكم في الوصول.

386



# 7) Insecure Cryptographic Storage

- **Description**
  - Insecure Cryptographic storage is a common vulnerability which exists when the sensitive data is not stored securely.
  - The user credentials, profile information, health details, credit card information, etc. come under sensitive data information on a website.
  - This data will be stored on the application database. When this data are stored improperly by not using encryption or hashing*, it will be vulnerable to the attackers.

(*Hashing is transformation of the string characters into shorter strings of fixed length or a key. To decrypt the string, the algorithm used to form the key should be available)

- **وصف**
  - التخزينالمشفر غير الآمن هو ثغرة أمنية شائعة توجد عندما لا يتم تخزين البيانات الحساسةبشكل آمن.
  - تأتيبيانات اعتماد المستخدم ومعلومات الملف الشخصي والتفاصيل الصحية ومعلومات بطاقة الائتمان وماإلى ذلك ضمن معلومات البيانات الحساسة على موقع الويب.
  - سيتمتخزين هذه البيانات في قاعدة بيانات التطبيق. عندما يتم تخزين هذه البيانات بشكل غيرصحيح من خلال عدم استخدام التشفير أو التجزئة * ، فإنها ستكون عرضة للمهاجمين.

(* التجزئة هي تحويل أحرف السلسلة إلى سلاسل أقصر بطول ثابت أو مفتاح. لفك تشفير السلسلة ، يجب أنتكون الخوارزمية المستخدمة لتكوين المفتاح متاحة)

387

# 7) Insecure Cryptographic Storage-cont.

- **Implication**
  - By using this vulnerability, an attacker can steal, modify such weakly protected data to conduct identity theft, credit card fraud or other crimes.
- **Vulnerable objects**
  - Application database.

- **يتضمن**
  - باستخدامهذه الثغرة الأمنية ، يمكن للمهاجم سرقة أو تعديل هذه البيانات المحمية بشكل ضعيفلإجراء سرقة الهوية أو الاحتيال على بطاقة الائتمان أو جرائم أخرى.
- **الأشياءالمعرضة للخطر**
  - قاعدةبيانات التطبيق.

388

388

# 7) Insecure Cryptographic Storage-cont.

- **Examples**
  - In one of the banking application, password database uses unsalted hashes * to store everyone's passwords. An SQL injection flaw allows the attacker to retrieve the password file. All the unsalted hashes can be brute forced in no time whereas, the salted passwords would take thousands of years.
  - (*Unsalted Hashes – Salt is a random data appended to the original data. Salt is appended to the password before hashing)

- **امثله**
  - في أحد التطبيقات المصرفية ، تستخدم قاعدة بيانات كلمات المرور تجزئات غير مملحة * لتخزينكلمات مرور الجميع. يسمح خطأ حقن SQL للمهاجم باسترداد ملف كلمة المرور. يمكنإجبار جميع التجزئة غير المملحة في أي وقت من الأوقات ، بينما تستغرق كلمات المرورالمملحة آلاف السنين.
  - (*تجزئة غير مملحة - الملح عبارة عن بيانات عشوائية يتم إلحاقها بالبيانات الأصلية. يتم إلحاق الملح بكلمةالمرور قبل التجزئة)

389

389

# 7) Insecure Cryptographic Storage-cont.

- **Recommendations**
  - Ensure appropriate strong standard algorithms. Do not create own cryptographic algorithms. Use only approved public algorithms such as AES, RSA public key cryptography, and SHA-256, etc.
  - Ensure offsite backups are encrypted, but the keys are managed and backed up separately.

- **التوصيات**
  - ضمان الخوارزميات القياسية القوية المناسبة. لا تقم بإنشاء خوارزميات التشفير الخاصة. استخدم فقط الخوارزميات العامة المعتمدة مثل AES وتشفير المفتاح العام RSA و SHA-256 وما إلى ذلك.
  - تأكد من تشفير النسخ الاحتياطية خارج الموقع ، ولكن المفاتيح تدار ونسخها احتياطياً بشكل منفصل.

390



# 8) Failure to restrict URL Access

- **Description**
  - Web applications check URL access rights before rendering protected links and buttons. Applications need to perform similar access control checks each time these pages are accessed.
  - In most of the applications, the privileged pages, locations and resources are not presented to the privileged users.
  - By an intelligent guess, an attacker can access privilege pages. An attacker can access sensitive pages, invoke functions and view confidential information.

- **وصف**
  - تتحقق تطبيقات الويب من حقوق الوصول إلى عنوان URL قبل تقديم الروابط والأزرار المحمية. تحتاج التطبيقات إلى إجراء عمليات تحقق مماثلة للتحكم في الوصول في كل مرة يتم فيها الوصول إلى هذه الصفحات.
  - في معظم التطبيقات ، لا يتم تقديم الصفحات والمواقع والموارد المميزة إلى المستخدمين المتميزين.
  - من خلال تخمين ذكي ، يمكن للمهاجم الوصول إلى صفحات الامتياز. يمكن للمهاجم الوصول إلى الصفحات الحساسة واستدعاء الوظائف وعرض المعلومات السرية.

391

# 8) Failure to restrict URL Access-cont.

- **Implication**
  - Making use of this vulnerability attacker can gain access to the unauthorized URLs, without logging into the application and exploit the vulnerability. An attacker can access sensitive pages, invoke functions and view confidential information.
- **Vulnerable objects:**
  - URLs

- **يتضمن**
  - يمكنأن يؤدي استخدام مهاجم الثغرة الأمنية هذا إلى الوصول إلى عناوين URL غير المصرحبها ، دون تسجيل الدخول إلى التطبيق واستغلال الثغرة الأمنية. يمكن للمهاجمالوصول إلى الصفحات الحساسة واستدعاء الوظائف وعرض المعلومات السرية.
- **الأشياءالمعرضة للخطر:**
  - عناوينURL

392



# 8) Failure to restrict URL Access-cont.

- **Examples**
  1. Attacker notices the URL indicates the role as "/user/getaccounts." He modifies as "/admin/getaccounts".
  2. An attacker can append role to the URL.

- http://www.vulnerablsite.com can be modified as http://www.vulnerablesite.com/admin

- **أمثلة**
  1.يلاحظ المهاجم أن عنوان URL يشير إلى الدور كـ "/ user / getaccounts." يعدل كـ "/ admin / getaccounts".
  2.يمكن للمهاجم إلحاق الدور بعنوان URL.

393



- يمكن http://www.vulnerablesite.com/admin تعديلهكـ http://www.vulnerablsite.com

# 8) Failure to restrict URL Access-cont.

- **Recommendations**
  1. Implement strong access control checks.
  2. Authentication and authorization policies should be role-based.
  3. Restrict access to unwanted URLs.

- **التوصيات**

1.تنفيذ عمليات فحص قوية للتحكم في الوصول.
2.يجب أن تكون سياسات المصادقة والترخيص قائمة على الأدوار.
3.تقييد الوصول إلى عناوين المواقع غير المرغوب فيها.

394



# 9) Insufficient Transport Layer Protection

- **Description**
  - Deals with information exchange between the user (client) and the server (application). Applications frequently transmit sensitive information like authentication details, credit card information, and session tokens over a network.
  - By using weak algorithms or using expired or invalid certificates or not using SSL can allow the communication to be exposed to untrusted users, which may compromise a web application and or steal sensitive information.

- **وصف**
  - يتعاملمع تبادل المعلومات بين المستخدم (العميل) والخادم (التطبيق). تنقل التطبيقاتبشكل متكرر معلومات حساسة مثل تفاصيل المصادقة ومعلومات بطاقةالائتمان ورموز الجلسة عبر الشبكة.
  - باستخدامخوارزميات ضعيفة أو استخدام شهادات منتهية الصلاحية أو غير صالحة أو عدم استخدامطبقة المقابس الآمنة (SSL) ، يمكن أن يسمح باتصال المستخدمين غير الموثوق بهم ، مماقد يعرض تطبيق ويب للخطر أو يسرق معلومات حساسة.

395

# 9) Insufficient Transport Layer Protection-cont.

- **Implication**
  - Making use of this web security vulnerability, an attacker can sniff legitimate user's credentials and gaining access to the application.
  - Can steal credit card information.
- **Vulnerable objects**
  - Data sent over the network.

- **يتضمن**
  - باستخدامهذه الثغرة الأمنية على الويب ، يمكن للمهاجم شم بيانات اعتماد المستخدمالشرعية والوصول إلى التطبيق.
  - يمكنهسرقة معلومات بطاقة الائتمان.
- **الأشياءالمعرضة للخطر**
  - البياناتالمرسلة عبر الشبكة.

396



# 9) Insufficient Transport Layer Protection-cont.

- **Recommendations**
  - Enable secure HTTP and enforce credential transfer over HTTPS only.
  - Ensure your certificate is valid and not expired.
- **Examples**:
  - An application not using SSL, an attacker will simply monitor network traffic and observes an authenticated victim session cookie. An attacker can steal that cookie and perform Man-in-the-Middle attack.

- **التوصيات**
  - قمبتمكين HTTP الآمن وفرض نقل بيانات الاعتماد عبر HTTPS فقط.
  - تأكدمن أن شهادتك صالحة وليست منتهية الصلاحية.
- **أمثلة:**
  - تطبيقلا يستخدم SSL ، سيقوم المهاجم ببساطة بمراقبة حركة مرور الشبكة ومراقبة ملف تعريفارتباط جلسة الضحية المصادق عليه. يمكن للمهاجم سرقة ملف تعريف الارتباط هذا وتنفيذهجوم Man-in-the-Middle.

397

# 10) Unvalidated Redirects and Forwards

- **Description**
  - The web application uses few methods to redirect and forward users to other pages for an intended purpose.
  - If there is no proper validation while redirecting to other pages, attackers can make use of this and can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

- **وصف**
  - يستخدمتطبيق الويب طرقاً قليلة لإعادة توجيه المستخدمين وإعادة توجيههم إلى صفحاتأخرى لغرض مقصود.
  - إذالم يكن هناك تحقق مناسب أثناء إعادة التوجيه إلى صفحات أخرى ، فيمكن للمهاجمين الاستفادةمن ذلك ويمكنهم إعادة توجيه الضحايا إلى مواقع التصيد أو البرامج الضارة ، أو استخدام إعادةالتوجيه للوصول إلى صفحات غير مصرح بها.

398



# 10) Unvalidated Redirects and Forwards-cont.

- **Implication**
  - An attacker can send a URL to the user that contains a genuine URL appended with encoded malicious URL. A user by just seeing the genuine part of the attacker sent URL can browse it and may become a victim.
- **Examples**
  - http://www.vulnerablesite.com/login.aspx?redirectURL=ownsite.com
  - Modified to
  - http://www.vulnerablesite.com/login.aspx?redirectURL=evilsite.com

- **يتضمن**
  - يمكنللمهاجم إرسال عنوان URL إلى المستخدم يحتوي على عنوان URL أصلي ملحق بعنوانURL ضار مشفر. يمكن للمستخدم من خلال رؤية الجزء الأصلي من عنوان URL الذيأرسله المهاجم أن يتصفحه وقد يصبح ضحية.

399

- **أمثلة**
  - http://www.vulnerablesite.com/login.aspx?redirectURL=ownsite.com
  - تمالتعديل إلى
  - http://www.vulnerablesite.com/login.aspx?redirectURL=evilsite.com

# 10) Unvalidated Redirects and Forwards-cont.

- **Recommendations**
  1. Simply avoid using redirects and forwards in the application. If used, do not involve using user parameters in calculating the destination.
  2. If the destination parameters can't be avoided, ensure that the supplied value is valid, and authorized for the user.

- **التوصيات**

1.ببساطة تجنب استخدام عمليات إعادة التوجيه وإعادة التوجيه في التطبيق. إذا تم استخدامها ،فلا تدخل في استخدام معلمات المستخدم في حساب الوجهة.

2.إذا تعذر تجنب معلمات الوجهة ، فتأكد من أن القيمة المقدمة صالحة ومرخصة للمستخدم.

400

400