

Kingdom of Saudi Arabia  
Technical and Vocational  
Training Corporation  
Madinah College of Technology  
Department of Computer  
Technology



المملكة العربية السعودية  
المؤسسة العامة للتدريب التقني  
والمهني  
الكلية التقنية بالمدينة المنورة  
قسم تقنية الحاسب الآلي

مشروع التشفير

اشراف المهندس/ فيصل احمد الحربي

اعداد المتدرب

442125915

عبدالله محمد الجريسي

---

الفصل التدريبي الثالث من العام 1444

بسم الله الرحمن الرحيم

## الشكر والتقدير

لا يشكر الله من لا يشكر الناس، نتوجه بالشكر

للمهندس / فيصل احمد الحربي

الذي رافقنا في مسيرتنا لإنجاز هذا المشروع، وكان له الفضل بعد الله في مساعدتنا على اتمام

المشروع.

ثم اتقدم بالشكر انا كاتب التقرير الى جميع من ساعدني في إتمام هذا المشروع واتمامه .

## فهرس المحتويات

1	المقدمة
3	الجدول الزمني
4	اهداف المشروع
4	UML الفصل الأول: نماذج
4	ماهي UML
4	ماهو Use Case Diagram
5	شرح الحالة كمستخدم رئيسي في Use Case Diagram
6	شرح الحالة كمستخدم USER في Use Case Diagram
8	Flowchart Diagram ماهو
10	Activity Diagram ماهو
11	الفصل الثاني: البحث والتصميم
11	HTML
12	CSS
13	JavaScript
14	PHP
14	Hypertext Preprocessor
14	SQL
14	My SQL

14	نظام إدارة قواعد البيانات
15	استخدام اللغات السابقة مع بعضها البعض
16	محرك النصوص (Visual Studio Code (VS Code
16	تشفير التبديل
17	شفرة قيصر
17	AES (Advanced Encryption Standard)
17	المكتبات
18	مكتبة CryptoJS
18	التحقق الثنائي
18	"One-Time Password" OTP
19	PHPMailer
19	mysqli_real_escape_string
19	HTTPS
20	الفصل الثالث: التنفيذ
20	الصفحة الرئيسية
21	انشاء صفحة للتسجيل وتسجيل الدخول
27	اجبار المستخدم على انشاء كلمة مرور معقدة
28	انشاء التحقق الثنائي من خلال البريد الالكتروني
33	منع استخدام رمز OTP لشخص اخر
34	انشاء صفحة إعادة تعيين كلمة المرور

36	انشاء صفحة المستخدم الرئيسي
38	انشاء صفحة لمراقبة سلوك المستخدم من خلال المستخدم الرئيسي
42	انشاء صفحة تسجيل مستخدم رئيسي جديد
43	انشاء صفحة (Home)
44	خوارزمية تشفير التبديل الخاصة بنا
45	شفرة قيصر
47	تشفير الملفات
51	منع التنقل من خلال URL
53	التأكد من ان المستخدم نشط
53	تعقيم المدخلات باستخدام <code>mysqli_real_escape_string</code>
54	الاتصال مع المستضيف
55	الخطط المستقبلية
56	الخاتمة
56	المراجع

## المقدمة

في هذا المشروع سنتحدث عن أحد اجزاء الامن السيبراني وهو التشفير نبدأ في سؤال

ماهو الأمن السيبراني؟ هو حماية الأنظمة او الشبكات او البرامج من أي هجوم عليها. ويعتبر

علم الامن السيبراني من اهم العلوم في العصر الحالي بسبب زيادة استخدام الاجهزة وزيادة عدد

الاشخاص، حيث وصل عدد مستخدمي الانترنت بحسب اخر الإحصائيات 5.16 مليار

شخص مما يشكل 64.4% وجميعهم يشكلون تهديد محتمل للأمن السيبراني لكن لن يقوم الكل

بذلك إذا افترضنا 1% من سكان العالم يحاولون عمل تهديد للأمن السيبراني فهذا يعني 51 مليون

شخص محتمل! يعتبر العدد كبير جدا.

يركز المشروع الخاص بنا على التشفير وهو عملية تحويل البيانات او المعلومات من شكل مقروء الى

شكل غير مفهوم او يصعب قراءته بواسطة خوارزميات التشفير وهي المختصة بتحويل البيانات الى

صيغة غير مفهومة للمستخدم بهدف حماية البيانات والمعلومات من الوصول غير المصرح به.

يعود تاريخ التشفير الى الألف السنين حيث كان الانسان القديم يستخدمه لضمان عدم انتهاك

سرية معلوماته، وكانت الأساليب المستخدمة بسيطة جدا مثل تشفير التبديل حيث يبدل الحرف

بحرف اخر، واستخدمت هذه الأساليب بشكل رئيسي في المراسلات العسكرية.

اما اليوم يعتبر التشفير أحد اهم عناصر الامن السيبراني حيث بعد ان تطور بشكل سريع وكبير

جدا وتواجدت اليوم خوارزميات للتشفير يصعب فكها حيث تضمن سرية البيانات.

سنركز في المشروع الخاص بنا في انشاء موقع باستخدام لغات البرمجة يمكن للمستخدم تشفير

النصوص الخاصة به بحيث يصعب قراءتها بهدف حمايتها وضمان سريتها، باستخدام أحد

خوارزميات التشفير ويمكن أيضا للمستخدم فك التشفير وهي عملية تحويل النص من نص غير

مقروء الى نص واضح يمكن قراءته.

ونسأل الله التوفيق والسداد في انجاز هذا المشروع.



## الجدول الزمني

المهام	الأسبوع	
مراجعة لما تم التدريب عليه	1444 / 8 / 20	الأول
اختيار أعضاء المجموعة وتحديد عنوان المشروع	1444 / 8 / 27	الثاني
اعداد خطة المشروع	1444 / 9 / 4	الثالث
البدء في البحث وتعلم مفاهيم التشفير والبرمجة	1444 / 9 / 11	الرابع
البدء في بناء الاكواد للموقع	1444 / 9 / 18	الخامس
البدء في تصميم صفحات الموقع	1444 / 10 / 6	السادس
التأكد من عمل الموقع بشكل سليم	1444 / 10 / 10	السابع
مناقشة المشروع مع أعضاء المشروع لتعديل واقتراح الأفكار	1444 / 10 / 17	الثامن
اعتماد المشروع من خلال أعضاء الفريق	1444 / 10 / 24	التاسع
تسليم مسودة التقرير النهائي قبل التعديل	1444 / 11 / 1	العاشر
تسليم التقرير النهائي	1444 / 11 / 10	الحادي عشر
مناقشة المشروع	1444 / 11 / 15	الثاني عشر
	1444 / 11 / 22	الثالث عشر

## اهداف المشروع

نهدف في هذا المشروع الى زيادة الوعي من طرف المستخدمين للتشفير، بحيث يتم استخدامه في

حياتهم اليومية وتسهيل استخدام التشفير للمستخدمين، وازافة بعض وسائل الأمان الى الموقع

مثل التحقق الثنائي ومنع التنقل من خلال URL وصفحة مستخدم رئيسي يمكن من خلالها

مراقبة سلوك المستخدمين.

## الفصل الأول: نماذج UML

### ماهي UML

UML هي اختصار لـ "Unified Modeling Language" وهي لغة تصميم نماذج

موحدة وموثقة تستخدم في تصميم البرمجيات والنظم المعلوماتية وغيرها من المنتجات المرتبطة بتكنولوجيا المعلومات.

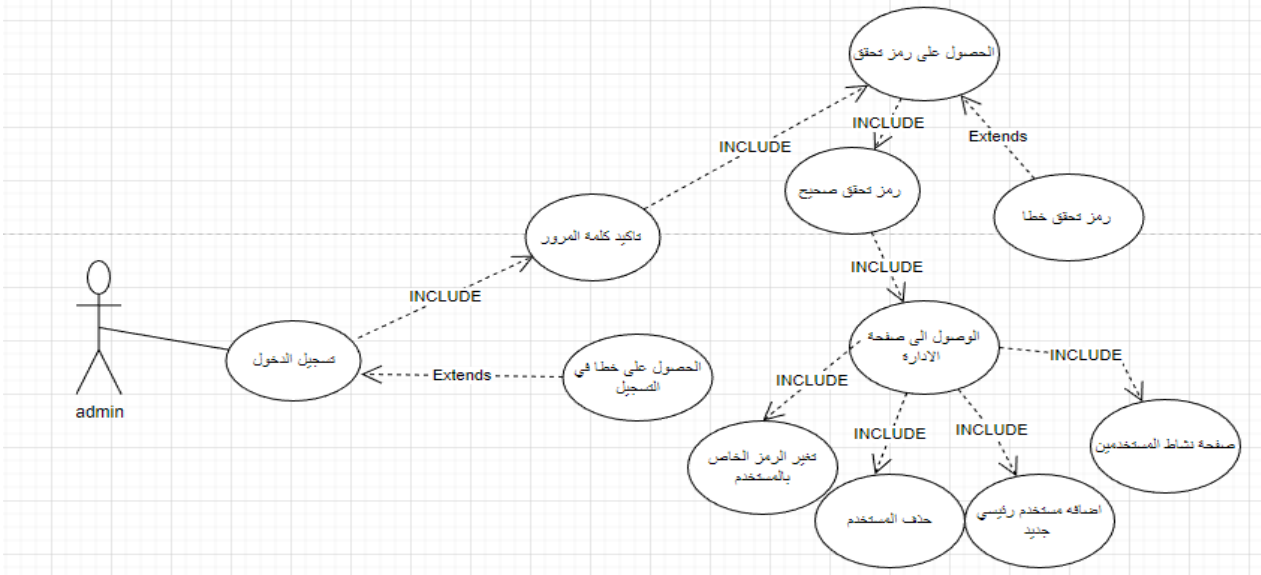
### ماهو Use Case Diagram

مخطط الحالات الاستخدام (Use Case Diagram) هو أحد أنواع مخططات التحليل

الشهيرة في هندسة البرمجيات، ويستخدم لوصف وتوضيح سلوك نظام معين من خلال تمثيل

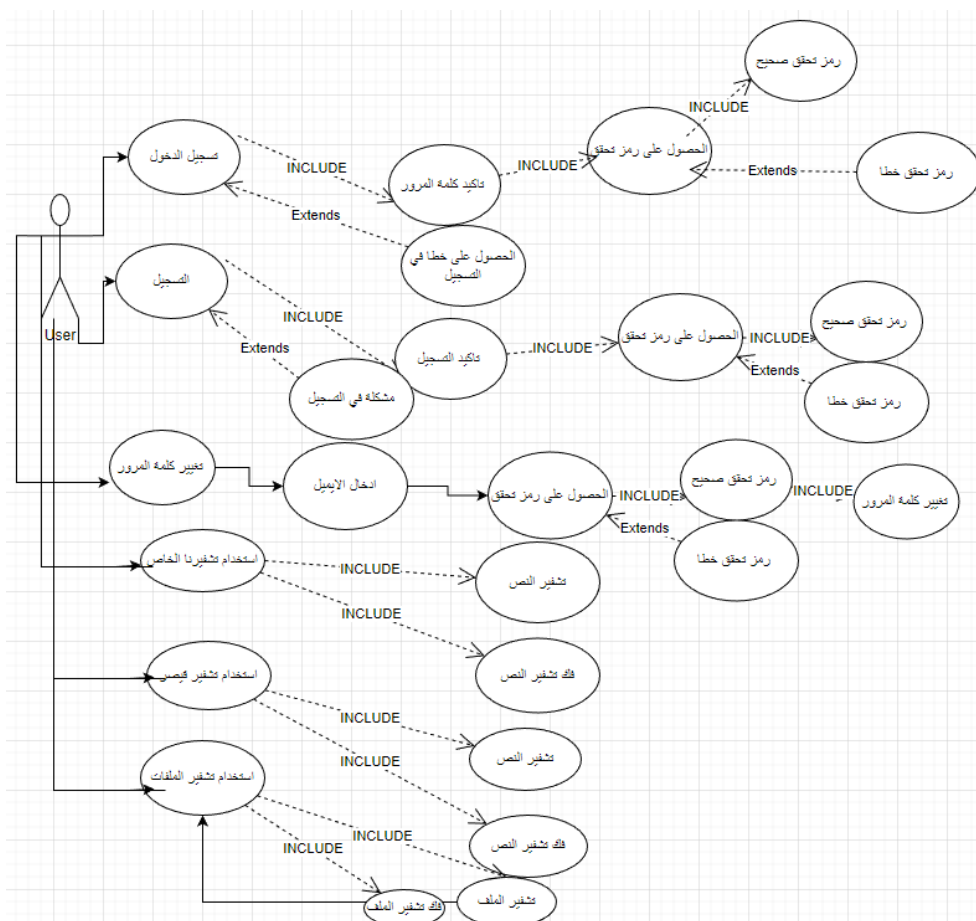
العلاقات بين الممثلين الخارجيين (المستخدمين أو الأطراف الفاعلة) والتفاعلات التي يقومون بها مع النظام.

## شرح الحالة كمستخدم رئيسي في Use Case Diagram



يمكن للمستخدم الرئيسي تسجيل الدخول فيكون له خيارين، اما ان تكون كلمة المرور خاطئة فيتم الرجوع الى صفحة تسجيل الدخول، او صحيحه فيمكنه الاستمرار والحصول على رمز التحقق على البريد الالكتروني الذي تم تسجيل دخول المستخدم به، واذا ادخل الرمز بشكل خطأ تظهر له رساله على انه تم ادخال كلمة مرور خطأ، واذا تم ادخال الرمز بشكل صحيح يدخل الى صفحة المستخدم الرئيسي، يمكن له من خلال صفحة المستخدم الرئيسي الوصول الى المستخدمين المتواجدين حاليا في قاعدة البيانات ويمكن التحكم بهم كتغيير كلمة المرور الخاصة بالمستخدم او حذف المستخدم من قاعدة البيانات، ويمكنه أيضا الوصول الى صفحة سلوك المستخدم ويمكن للمستخدم الرئيسي مراقبة أي من سلوكيات المستخدم مثل انه تم تسجيل الدخول في الساعة كذا وتم تسجيل الخروج في الساعة كذا وتم تغيير كلمة مرور المستخدم في الساعة كذا وعلى هذا يمكن للمستخدم الرئيسي أيضا اضافته مستخدم رئيسي جديد من خلال الصفحة الخاصة بإضافة مستخدم رئيس جديد.

## شرح الحالة كمستخدم USER في Use Case Diagram



يمكن للمستخدم تسجيل الدخول إذا كانت كلمة المرور خطأ يرجع الى صفحة تسجيل الدخول،

إذا كانت كلمة المرور صحيحة، ينتقل الى صفحة تأكيد الرمز حيث يتلقى رمز تحقق على البريد

الالكتروني الخاص به ثم يدخل الرمز إذا كان الرمز خطأ يتم اظهار الرمز خطأ، وإذا كان الرمز

صحيح يمكنه الانتقال الى الموقع.

يمكن للمستخدم التسجيل إذا كانت التسجيل خطأ، يرجع الى صفحة التسجيل إذا كان التسجيل

صحيح ينتقل الى صفحة تأكيد الرمز حيث يتلقى رمز تحقق على البريد الالكتروني الخاص به ثم

يدخل الرمز، إذا كان الرمز خطأ يتم اظهار الرمز خطأ، وإذا كان الرمز صحيح يمكنه الانتقال الى تسجيل الدخول.

يمكن للمستخدم تغيير كلمة المرور ينتقل الى صفحة ادخال البريد الالكتروني المرجو تغيير كلمة المرور الخاصة به ثم ينتقل الى صفحة تأكيد الرمز حيث يتلقى رمز تحقق على البريد الالكتروني الخاص به ثم يدخل الرمز،

إذا كان الرمز خطأ يتم اظهار الرمز خطأ وإذا كان الرمز صحيح يمكنه الانتقال الى صفحة تغيير كلمة المرور ويمكنه تغيير كلمة المرور من خلالها.

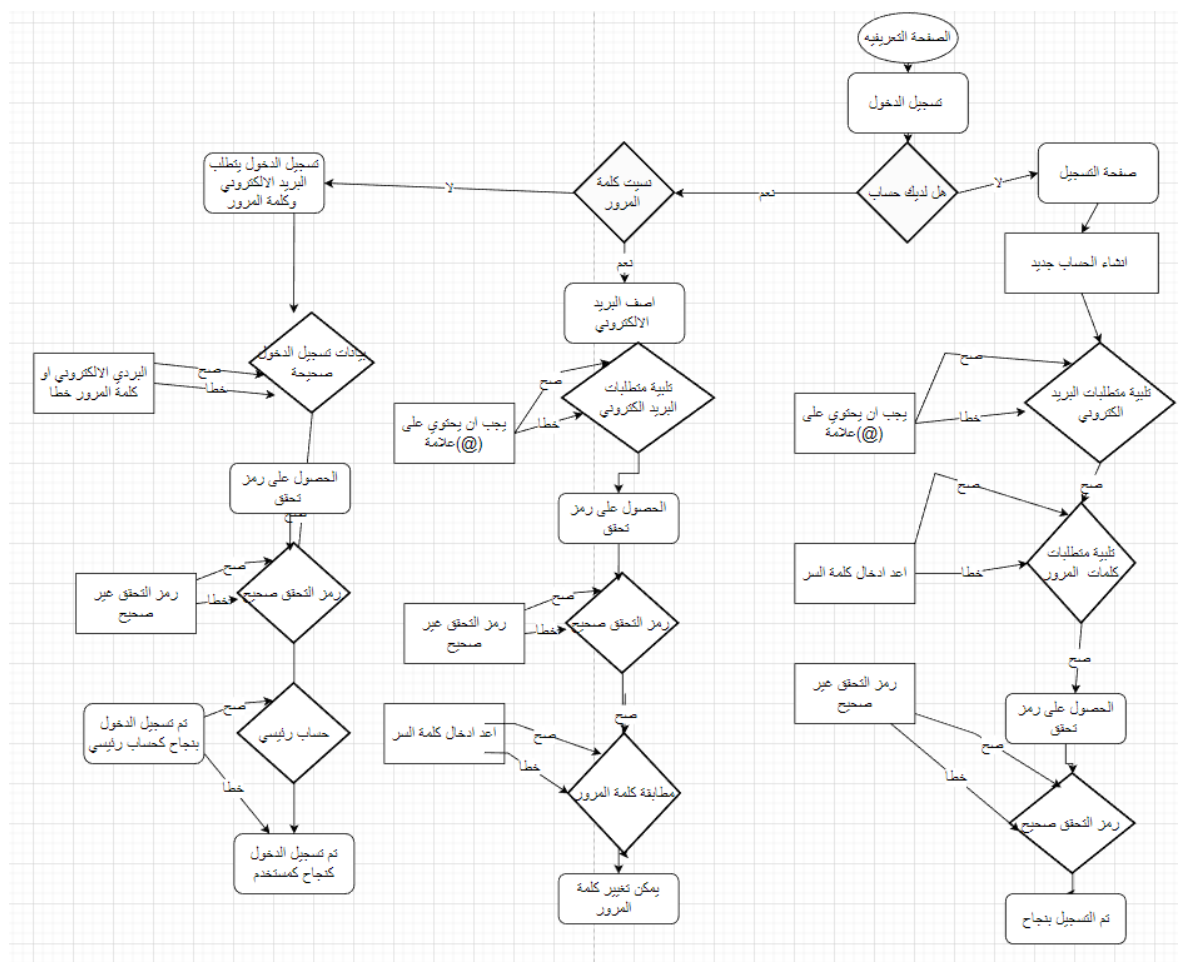
يمكن للمستخدم استخدام التشفير الخاص بنا ويمكنه التشفير او فك التشفير للنص.

يمكن للمستخدم استخدام شفرة قيصر ويمكنه التشفير او فك التشفير للنص.

يمكن للمستخدم استخدام تشفير الملفات ويمكنه التشفير او فك التشفير للملف النصي.

## Flowchart Diagram ماهو

هو نوع من رسومات التدفق الذي يستخدم لتمثيل التسلسل الزمني للخطوات والعمليات المختلفة في نظام أو عملية.



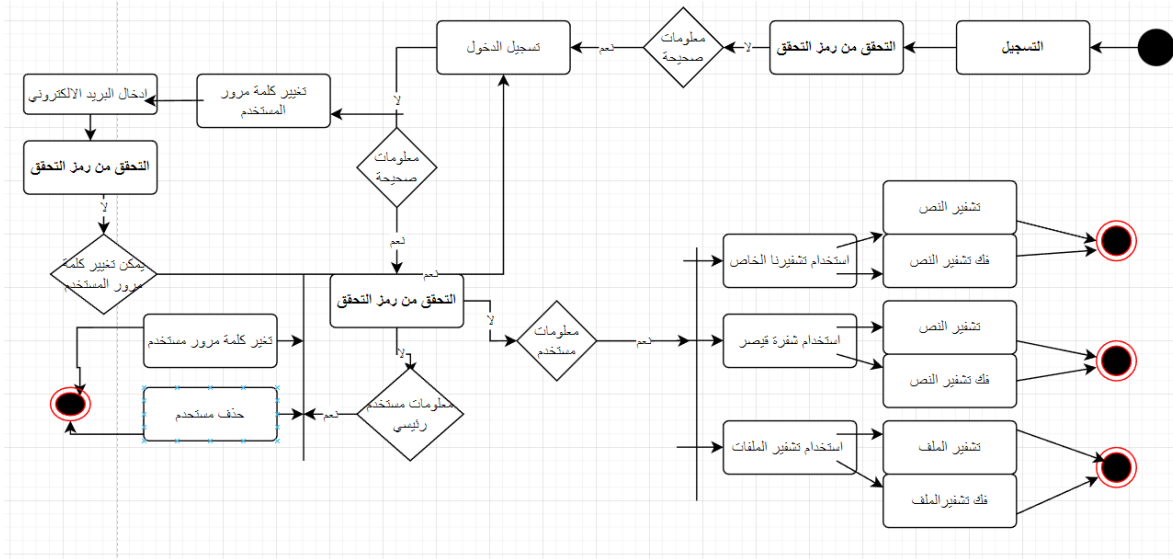
إذا دخل المستخدم الصفحة التعريفية لديه خيارين إذا كان ليس لديه حساب يمكنه انشاء حساب بعد تلبية طلبات البريد الإلكتروني وبعد تلبية متطلبات كلمة المرور وبعد الحصول على رمز التحقق وإدخال رمز التحقق بشكل صحيح يتم التسجيل بنجاح.

وإذا كان لديه حساب لكن نسي كلمة المرور يضيف البريد الإلكتروني الخاص به ويلبي طلبات البريد الإلكتروني ومن ثم يحصل على رمز تحقق ويدخل رمز التحقق الصحيح يمكنه الدخول الوصول الى صفحة تغيير كلمة المرور ويمكنه تغيير كلمة المرور بعد تلبية طلبات كلمة المرور.

وإذا كان لديه حساب ولديه كلمة المرور يمكنه تسجيل الدخول بعد تلبية طلبات البريد الإلكتروني وبعد تلبية متطلبات كلمة المرور وبعد الحصول على رمز التحقق وإدخال رمز التحقق بشكل صحيح يتحقق النظام مما إذا كان مستخدم رئيسي او لا إذا كان مستخدم رئيسي يتم التسجيل كمستخدم رئيسي وإذا كان مستخدم عادي يتم التسجيل كمستخدم.

## Activity Diagram ماهو

هو نوع من رسومات التدفق الذي يستخدم لتوضيح سلسلة الأنشطة التي يتم تنفيذها في نظام أو عملية معينة.



إذا دخل المستخدم يمكنه التسجيل ثم التحقق من رمز التحقق إذا كان صحيح يمكنه التوجه الى صفحة تسجيل الدخول يمكن من صفحة تسجيل الدخول إذا كانت معلومات الدخول صحيحة يتم التحقق من رمز التحقق المرسل إذا كان الرمز المرسل صحيح يتحقق النظام من حالة الحساب إذا كان حساب رئيسي يمكنه تغيير كلمة مرور المستخدم او حذف المستخدم.

لكن إذا كان حساب مستخدم يمكنه استخدام تشفيرنا الخاص والتشفير وفك التشفير به او استخدام شفرة قيصر والتشفير وفك التشفير بها او استخدام تشفير الملفات وتشفير وفك التشفير الملفات بها وينتهي البرنامج هنا.

إذا تم اختيار نسيت كلمة المرور يتم ادخال البريد الالكتروني المراد تغيير كلمة المرور الخاصة به ثم التحقق من الرمز المرسل على البريد الالكتروني ومن ثم يمكنه تغيير كلمة المرور.



## الفصل الثاني: البحث والتصميم

من خلال البحث الخاص بنا تم الاتفاق على انشاء موقع باستخدام لغات البرمجة وسيتم ذكرها

وذكر التقنيات المستخدمة في المشروع مع شرح بسيط لها.



# HTML

هي اختصار "Hyper Text Markup Language" وتعتبر هي لغة *1 شعار HTML5*

ترميز النصوص والعناصر في صفحات الويب، وتعتبر هي اللغة الافتراضية لتصميم صفحات الويب

اليوم، وتعتبر سهلة ومرنة في الاستخدام حيث يسهل التعامل معها من قبل المبتدئين لتطوير المواقع.

تم انشاها في عام 1989 وتم تطوير أحدث اصدار لها وهو "HTML5" في عام 2007

حيث حصلت على العديد من التطويرات وتمت إضافة عدد من العناصر، وهو الإصدار المستخدم

في وقتنا الحالي.

### World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an [executive summary](#) of the project, [Mailing lists](#), [Policy](#), [November's W3 news](#), [Frequently Asked Questions](#).

[What's out there?](#)  
Pointers to the world's online information, [subjects](#), [W3 servers](#), etc.

[Help](#)  
on the browser you are using

[Software Products](#)  
A list of W3 project components and their current state. (e.g. [Line Mode](#), [X11 Viola](#), [NeXTStep](#), [Servers](#), [Tools](#), [Mail robot](#), [Library](#).)

[Technical](#)  
Details of protocols, formats, program internals etc

[Bibliography](#)  
Paper documentation on W3 and references.

[People](#)  
A list of some people involved in the project.

[History](#)  
A summary of the history of the project.

[How can I help?](#)  
If you would like to support the web..

[Getting code](#)

وسيتم استخدامها في موقعنا لتصميم الصفحات .

*2 مثال على صفحة انترنت باستخدام HTML*



## CSS

هي اختصار "Cascading Style Sheets" وتستخدم مع "HTML"

للإضافة الاشكال والتصاميم وتنسيق الألوان والخطوط والخلفيات والتأثيرات واحجام النصوص.

تعتبر مكملة "HTML" حيث تضيف الى الاكواد الخاصة بها "روح" بحيث يجعلها مرتبة

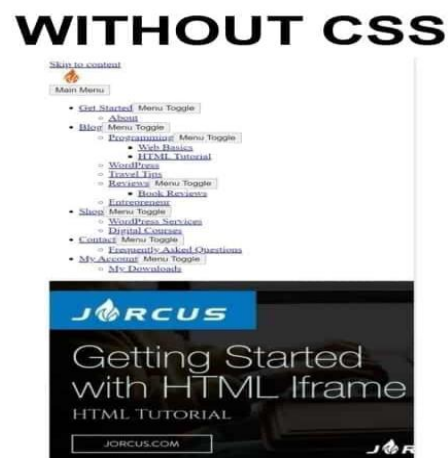
ذات منظر مريح للعين ويمكن من خلالها تحسين تجربة المستخدم.

سيتم استخداماه في مشروعنا لتحسين التصميم لكود "HTML".

تم انشاء "CSS" في عام 1996.



ومثال على صفحة HTML مع CSS



3 مثال على صفحة HTML بدون CSS



## JavaScript

هي لغة برمجية تستخدم في تطوير تطبيقات الويب وغيرها من التطبيقات البرمجية، وتوفر لصفحة

الويب المميزات التفاعلية والديناميكية، ويمكن تشغيلها مباشرة من صفحات الويب بدون الحاجة

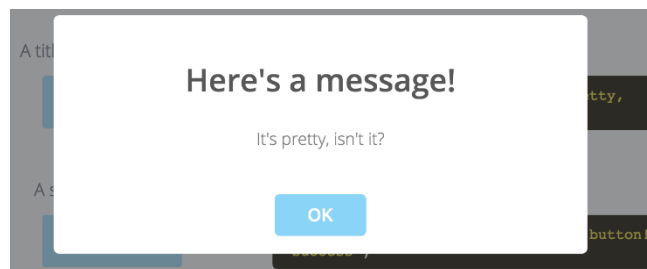
إلى برامج خارجية.

أحد استخداماتها (إضافة تفاعلية للأزرار) بحيث إذا تم الضغط على هذا الزر يحدث شيء، أو

يمكن استخدامها في (عرض تنبيه للمستخدم) من خلال الدالة "alert".

تم انشائها في عام 1995.

سيتم استخدامها في موقعنا للعمليات البرمجية وتشفير النصوص وفك تشفيرها.



4 مثال على عرض تنبيه للمستخدم من خلال JavaScript



## PHP

Hypertext Preprocessor المعالج الأولي للنص التشعبي، لغة برمجة مفتوحة.

المصدر، وتستخدم في نطاق واسع في مجال تطوير تطبيقات الويب، وسيتم استخدامها بشكل خاص في مشروعنا للتعامل مع قواعد البيانات، تم تطوير اللغة في عام 1994.



## SQL

"Structured Query Language" هي لغة برمجة خاصة بقواعد

البيانات، وهي اللغة الأساسية المستخدمة في العديد من الأنظمة، تم تطويرها في عام 1979، وهي اللغة الخاصة بالتعامل مع قواعد البيانات التي سنستخدمها في مشروعنا.



## My SQL

نظام إدارة قواعد البيانات مفتوح المصدر، يتم من خلاله إدارة قاعدة البيانات الخاصة

بمشروعنا، تتميز بسهولة استخدامها وتوافقها مع مختلف أنظمة التشغيل، تم تطوير النظام في عام 1995.



## استخدام اللغات السابقة مع بعضها البعض

يمكن استخدام اللغات السابقة مع بعضها البعض، حيث ستوفر لنا العناصر من خلال

"HTML"، والتنسيقات والألوان من خلال "CSS"، ولإضافة بعض التفاعلية للموقع سيتم

استخدام "JavaScript" وبذلك ستخرج لنا صفحة ويب متكاملة.

في مشروعنا هذا سنستخدمهم جميعا بحيث توفر لنا صفحة متكاملة.

تشفيرنا

الخط النص:

الخط:

النتيجة:



5 محرر النصوص VC Code

## محرر النصوص (VS Code) Visual Studio Code

هو محرر نصوص مصمم من قبل مايكروسوفت، ومعنى محرر النصوص هو برنامج

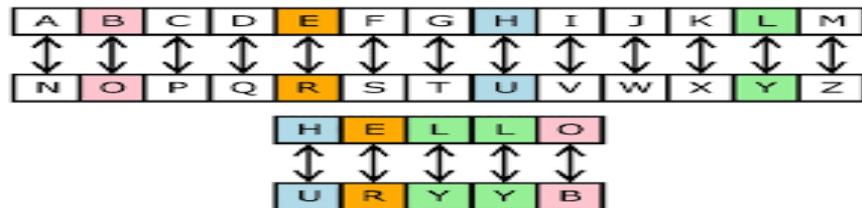
يستخدم لكتابة النصوص البرمجية، وسبب اختياره بسبب انه يدعم جميع اللغات السابقة ويوفر

سهولة وميزات إضافية. تم اصدار اول نسخة في عام 2015

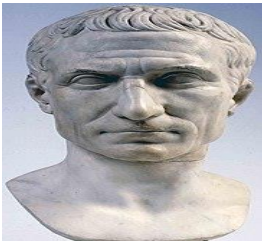
### تشفير التبديل

وهو أحد اقسام أنواع التشفير حيث يبدل الحرف بحرف اخر بحسب خوارزمية تم تحديدها مسبقا،

أحد عيوبها هي إمكانية فكها بسهولة من خلال التحليل واستخدام المنطق.



6 أحد الامثلة على تشفير التبديل



7 يوليوس قيصر

## شفرة قيصر

يوليوس قيصر كان زعيما وجنرالا روماني، تمت تسمية الخوارزمية باسمه حيث يعتقد انه من طورها.

وهي تقنية تشفير بسيطة وتعتمد على نظام الازاحة، حيث تعمل من خلال مقدار إزاحة محدد

مسبقا ويتم التشفير من خلاله.

مثلا تم اختيار الحرف "B"، ومقدار الازاحة 3، إذا ناتج التشفير هو "E".

## AES (Advanced Encryption Standard)

هي تقنية تشفير تستخدم لحماية البيانات والمعلومات المتداولة عبر الإنترنت. تم تطوير هذه التقنية

كبديل لتقنية DES (Data Encryption Standard) السابقة التي كانت تعتبر أقل

أماناً بعد أن تم اكتشاف العديد من الثغرات فيها.

وسوف يتم استخدامها في المشروع الخاص بنا لتشفير الملفات.

## المكتبات

مجموعة من الدوال أو الأوامر المعدة مسبقا والتي يمكن استخدامها مع لغات البرمجة، ويتم اعدادها

من قبل مبرمجين، وسوف يتم استخدام بعض المكتاتب في المشروع الخاص بنا.



## مكتبة CryptoJS

هي مكتبة تشفير مفتوحة المصدر لجافا سكريبت توفر مجموعة كبيرة من الأدوات لتأمين البيانات، بما في ذلك تشفير النصوص، وتشفير الملفات، وتشفير قيم الهاش، وغيرها من الخدمات الأمنية، وسوف يتم استخدامها في موقعنا لكود تشفير الملفات.

### التحقق الثنائي

هي عملية توثيق تطلب من المستخدم ادخال معلومتين مختلفتين للوصول الى حسابة، مما يوفر زيادة في الأمان والتأكد من ان المستخدم هو المالك الحقيقي للحساب. وفي المشروع الخاص بنا سيتم استخدام التحقق من خلال ارسال رسالة الى ايميل المستخدم تحتوي على OTP.

### "One-Time Password" OTP

وهي عبارة عن تقنية لإنشاء كلمات سر مؤقتة تستخدم لتوفير طبقة إضافية من الحماية في الأنظمة المعرضة للخطر. تعمل التقنية عن طريق إرسال كود أو رمز سري قصير الأجل إلى جهاز المستخدم (مثل الهاتف المحمول) عبر رسالة نصية SMS أو تطبيق خاص للحصول على الرمز، ويستخدم هذا الرمز لتأكيد الهوية الحقيقية للمستخدم.



## PHPMailer

هي مكتبة PHP مفتوحة المصدر تستخدم لإرسال رسائل البريد الإلكتروني من خلال بروتوكولات SMTP، ومن خلال استخدامها يمكن إرسال رسائل إلى أي بريد إلكتروني، وفي المشروع الخاص بنا سيتم استخدامها لإرسال رمز OTP إلى المستخدم على البريد الإلكتروني الخاص به.

## mysqli\_real\_escape\_string

هي وظيفة متوفرة في مكتبة MySQL (المعروفة أيضًا بـ MySQL improved extension) في لغة PHP. تُستخدم هذه الدالة لحماية البيانات المدخلة إلى قاعدة بيانات MySQL من الهجمات المحتملة عبر تهريب البيانات.



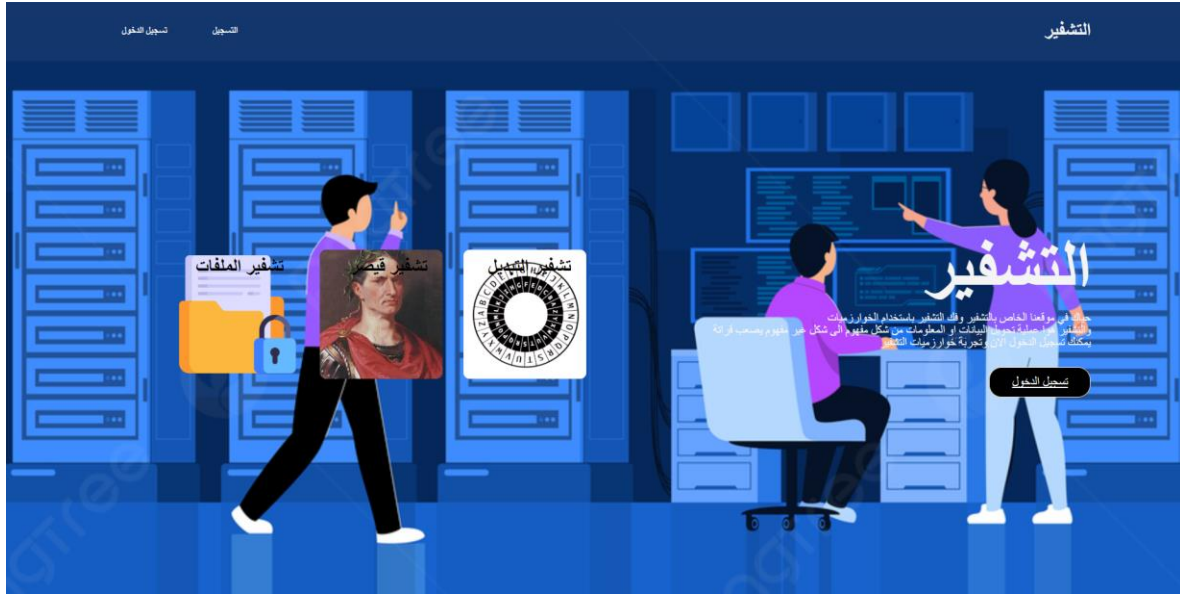
## HTTPS

هو اختصار لـ "البروتوكول الآمن لنقل النص الفائق" (Hypertext Transfer Protocol Secure). يعد HTTPS توسعًا لبروتوكول HTTP القياسي الذي يستخدم لنقل المعلومات عبر شبكة الإنترنت. يتم استخدام HTTPS لتأمين اتصالات الويب وحماية البيانات المرسلة والمستلمة بين المتصفح (العميل) والموقع الإلكتروني (الخادم).

## الفصل الثالث: التنفيذ

### الصفحة الرئيسية

بعد إتمام عملية البحث ننتقل الان الى عملية التنفيذ، في البداية سوف يتم انشاء صفحة رئيسية يمكن للمستخدم معرفة تفاصيل الموقع وماذا يقدم وستكون هي اول صفحة يتم عرضها للمستخدم ويتوجه من خلالها الى الصفحات الاخرى.



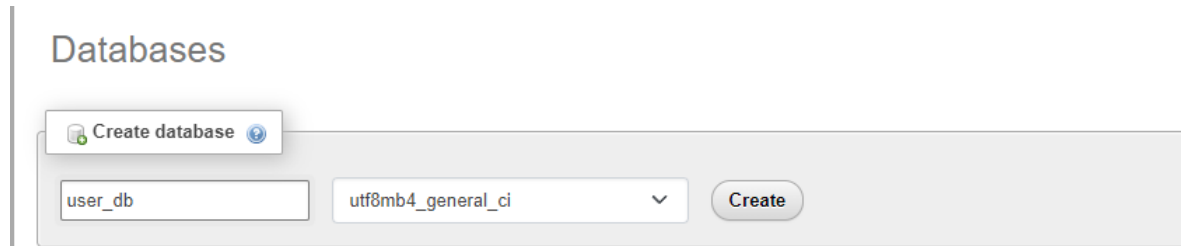
يمكن من خلال الصفحة التعرف على معنى التشفير والتعرف على الخوارزميات المتوفرة داخل موقعنا، يمكن للمستخدم الوصول الى صفحة التسجيل او تسجيل الدخول من خلال الأزرار التي توجد في يسار اعلى الصفحة، او يمكن له الوصول الى صفحة تسجيل الدخول من خلال الزر في يمين الصفحة الخاص بتسجيل الدخول.

## انشاء صفحة للتسجيل وتسجيل الدخول

بعد إتمام انشاء الصفحة الرئيسية، الخطوة التالية هي انشاء صفحة للتسجيل وصفحة لتسجيل الدخول المستخدمين لتحديد الوصول داخل الموقع، سيتم استخدام المصادقة للتحقق من هوية المستخدم.

تم استخدام نظام قاعدة البيانات "My SQL" للتمكن من إدارة قاعدة البيانات، وتم استخدام لغة البرمجة المختصة بقواعد البيانات "SQL".

في البداية تم انشاء قاعدة بيانات تحمل اسم "user\_db"

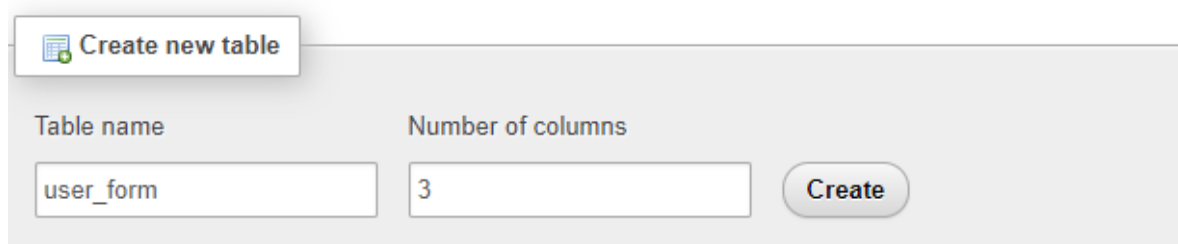


Databases

Create database

user\_db utf8mb4\_general\_ci Create

بعد ذلك تم انشاء جدول يحمل اسم "user form" يتطلب 3 مدخلات



Create new table

Table name Number of columns

user\_form 3 Create

المدخلات المطلوبة هي "id" وهو الخانة المميزة للمستخدم ويتم توليده بشكل تلقائي، المدخل الثاني "email" يطلب الايميل من المستخدم، والمدخل الأخير "password" يتطلب كلمة مرور من المستخدم.

The screenshot shows the MySQL Workbench Table Designer interface. It displays three columns: 'id' (INT, 255, None, PRIMARY), 'email' (VARCHAR, 255, None, --), and 'password' (VARCHAR, 255, None, --). The 'id' column is marked as the primary key. Below the columns, there are fields for 'Table comments:', 'Collation:', and 'Storage Engine: InnoDB'.

في الخطوة التالي تم انشاء اتصال بين قاعدة البيانات والكود الخاص بنا من خلال الامر التالي

```
<?php
$conn = mysqli_connect('localhost','root','','user_db');
?>
```

بعد ذلك تم البدء في برمجة صفحة التسجيل وصفحة تسجيل الدخول من خلال "HTML"، وتم تصميم الصفحة من خلال "CSS" وخرجنا بالمخرج التالي.

صفحة للتسجيل، تتطلب الايميل الخاص بالمستخدم، وكلمة مرور جديدة، وتكرار كلمة المرور للتأكد من صحتها، وتتطلب كلمة مرور معقدة، وتم ربط الصفحة برابط بحيث إذا كان المستخدم قد سجل من قبل يمكنه الانتقال الى صفحة التسجيل.

### سجل الان

ادخل الايميل الخاص بك

ادخل كلمة مرور جديدة

اعد ادخال كلمة المرور

سجل

إليك حساب؟ سجل دخولك

صفحة تسجيل الدخول تطلب من المستخدم الايميل الذي سجل به مسبقا وكلمة المرور، ويمكنه الانتقال من خلال الرابط في الأسفل الى صفحة التسجيل إذا لم يكن له حساب من قبل.

### سجل دخولك

ادخل الايميل الخاص بك

ادخل كلمة المرور

سجل دخولك

ليس لديك حساب؟ سجل الان

تمت إضافة بعض إضافات الأمان في (نموذج) التسجيل، مثل في حالة التسجيل إذا ادخل المستخدم ايميل مسجل من قبل تظهر له رسالة ان المستخدم مسجل.

### سجل الان

تم تسجيل الايميل من قبل

ادخل الايميل الخاص بك

ادخل كلمة مرور جديدة

اعد ادخال كلمة المرور

سجل

إليك حساب؟ سجل دخولك

او إذا ادخل المستخدم كلمة مرور غير متطابقة تظهر له رسالة ان كلمة المرور غير متطابقة.

### سجل الان

كلمة المرور غير متطابقة

ادخل الايميل الخاص بك

ادخل كلمة مرور جديدة

اعد ادخال كلمة المرور

سجل

لديك حساب؟ سجل دخولك

وفي (نموذج) تسجيل الدخول إذا ادخل المستخدم ايميل خطأ او كلمة مرور خطأ يظهر له المخرج التالي ان الايميل او كلمة المرور خطأ.

### سجل دخولك

الايميل او كلمة المرور خطأ

ادخل الايميل الخاص بك


ادخل كلمة المرور

سجل دخولك

ليس لديك حساب؟ سجل الان

ولتقليل المدخلات زيادة الأمان في (النموذج) تمت إضافة محدد بحيث يجب ان يكون المدخل ايميل فقط او يحتوي على علامة @ ويظهر له هذا التنبيه.

aa










 Please include an '@' in the email address. 'aa' is missing an '@'.

login now

تمت إضافة طريقة (الهاش) الى كلمة المرور بحيث لا يمكن لمالك قاعدة البيانات عرض كلمات المرور الخاصة بالمستخدمين.

والهاش هو تقنية تشفير من نوع (طريق واحد) تساعد في زيادة امان كلمات المرور، بحيث تشفر كلمات المرور الخاصة بالمستخدمين، وتعمل هذه التنقية من خلال توليد قيمة (هاش) محددة لكل قيمة بيانات مخزنة، ويتم حسابها باستخدام خوارزمية الهاش.

بالصورة التالية يمكنك الاطلاع على المستخدمين في قاعدة البيانات، لكن لا يمكنك عرض كلمات المرور كنص واضح، ستراها على انها نص مشفر.

		id	email	password
<input type="checkbox"/>	 Edit  Copy  Delete	1	aboody16100@gmail.com	202cb962ac59075b964b07152d234b70
<input type="checkbox"/>	 Edit  Copy  Delete	2	abdulalah19j@gmail.com	202cb962ac59075b964b07152d234b70
<input type="checkbox"/>	 Edit  Copy  Delete	3	a@gmail.com	202cb962ac59075b964b07152d234b70

تم تشفيرها من هاش من نوع (MD5) " Message-Digest Algorithm 5 "

وهو نوع من أنواع تشفير الهاش الذي يقوم بتحويل البيانات الى هاش بطريقة غير قابلة للعكس.



## اجبار المستخدم على انشاء كلمة مرور معقدة

لزيادة الأمان تمت اضافته شروط لكلمات المرور، حيث يجب ان يضيف المستخدم كلمة مرور معقدة، قد تصعب كلمة المرور المعقدة الطريق للمهاجم حيث يصعب تخمينها او فك تشفيرها. تم استخدام الدالة التالية لتلبية الشروط، حيث يجب ان تحتوي على حرف كبير وحرف صغير على الاقل، واحد الاحرف الخاصة الموجودة في الدالة وان لا تقل عن 8 أحرف.

```
function isPasswordComplex($password) {  
    $pattern = '/^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[@$!%*?&])[A-Za-z\d@$!%*?&]{8,}$/' ;  
    return preg_match($pattern, $password);  
}
```

يتم عرض هذه الرسالة إذا لم تتطابق الشروط الخاصة بداله التحقق من تعقيد كلمة المرور.

### سجل الان

كلمة المرور يجب أن تحتوي على حروف كبيرة وصغيرة وأرقام وأحرف خاصة، وتكون طولها على الأقل 8 أحرف.

ادخل الايميل الخاص بك

ادخل كلمة مرور جديدة

اعد ادخال كلمة المرور

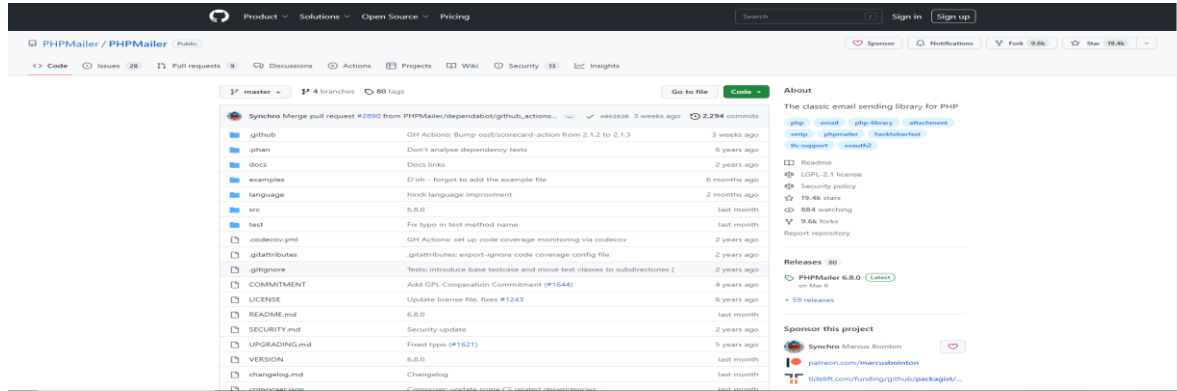
سجل

لديك حساب؟ سجل دخولك

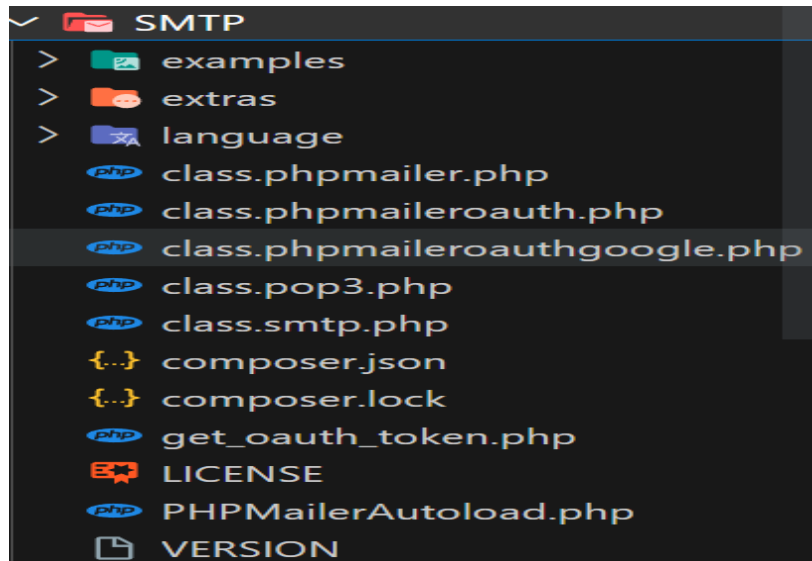
## انشاء التحقق الثنائي من خلال البريد الالكتروني

لزيادة الأمان في موقعنا وللتأكد الإضافي من هوية المستخدم، سيتم إضافة تحقق إضافي من خلال رمز OTP يتم إرساله الى البريد الالكتروني الخاص بالمستخدم عند التسجيل او تسجيل الدخول، مما يؤكد ان البريد الالكتروني الخاص بالمستخدم صحيح والتأكد من ملكيته له.

سنستخدم هنا PHPMailer وهي المكتبة التي تمكنا من ارسال رسائل الى البريد الالكتروني في البداية نحتاج تثبيت المكتبة.



بعد تثبيت المكتبة تم اضافتها الى ملفات الكود الخاص بنا.



بعد اضافتها الى الكود الخاص بنا سيتم انشاء اتصال بين الكود والمكتبة، مع إضافة البريد الالكتروني الخاص بنا وكلمة المرور، وتوليد رمز OTP يتم إرساله الى المستخدم مكون من 5 ارقام، ومن ثم إضافته بعد صفحات التسجيل وتسجيل الدخول.

```
$otp = rand(10000, 99999);

include_once("SMTP/class.phpmailer.php");
include_once("SMTP/class.smtp.php");
$message = '<div>
    <p><b>اهلا</b></p>
    <p>كود التحقق الخاص بك</p>
    <br>
    <p><b>'. $otp .'</b></p>
</div>';

$mail = new PHPMailer;
$mail->IsSMTP();
$mail->SMTPAuth = true;
$mail->Host = 'smtp.gmail.com';
$mail->Username = 'fxrpq5@gmail.com';
$mail->Password = ' ';
$mail->SMTPSecure = 'ssl';
$mail->Port = 465;
$mail->FromName = "Encryption and decryption site";
$mail->AddAddress($email);
$mail->Subject = "OTP";
$mail->isHTML( TRUE );
$mail->Body = $message;































if($mail->send()){
    $insert_query = mysqli_query($conn,"insert into tbl_otp_check set otp='$otp', is_expired='0'");
    $_SESSION['email'] = $email;
    header('location: Verification_Register.php');
    exit();
}else{
    $error[] = "لم يتم ارسال الايميل";
}
```

الصورة السابقة لحالة التسجيل، بحيث إذا تمت عملية التسجيل وبعد إضافته الى قاعدة البيانات، يتم ارسال رمز OTP، للمستخدم ويتم توجيه المستخدم لصفحة التحقق من الرمز الخاصة بالتسجيل.

بعد ارسال الرمز OTP للمستخدم يتم حفظه في جدول في قواعد البيانات خاص به لنتمكن من الرجوع له والتحقق إذا كان الرمز المدخل صحيح او لا،

وتم وضع حد للرمز وهو دقيقتين بعد ذلك الوقت لا يمكنك استخدام الرمز.

إذا كان الرمز صالح يتم قبوله من المستخدم وتوجيهه للصفحة التالية، لكن إذا كان الرمز غير صالح يتم اظهار رسالة تشير على ان الرمز غير صالح.

				id	otp	is_expired	create_at
<input type="checkbox"/>	 Edit	 Copy	 Delete	1	44253	0	2023-04-23 01:12:03
<input type="checkbox"/>	 Edit	 Copy	 Delete	2	37915	0	2023-04-23 01:13:43
<input type="checkbox"/>	 Edit	 Copy	 Delete	3	24592	0	2023-04-23 01:15:11
<input type="checkbox"/>	 Edit	 Copy	 Delete	4	33518	0	2023-04-23 01:17:55
<input type="checkbox"/>	 Edit	 Copy	 Delete	5	72478	0	2023-04-23 01:18:40
<input type="checkbox"/>	 Edit	 Copy	 Delete	6	45728	0	2023-04-23 01:19:14
<input type="checkbox"/>	 Edit	 Copy	 Delete	7	18762	0	2023-04-23 01:22:03
<input type="checkbox"/>	 Edit	 Copy	 Delete	8	13493	0	2023-04-23 01:27:50
<input type="checkbox"/>	 Edit	 Copy	 Delete	9	25612	0	2023-04-23 01:33:55
<input type="checkbox"/>	 Edit	 Copy	 Delete	10	81167	1	2023-04-23 01:41:23

في الصورة السابقة تظهر الجدول الذي يتحقق من حالة رمز OTP إذا تم استخدامه يتم تحويله الى 1، وإذا لم يتم استخدامه يكون صفر، ويتطلب أيضا الوقت الذي تم فيه ارسال الرمز للتأكد من عدم انتهاء المدة.

الصورة التالية هي مثال على الرسالة التي يتم ارسالها الى البريد الالكتروني الخاص بالمستخدم.

<fxrpq5@gmail.com> Encryption and decryption site

أنا ▾

اهلا

كود التحقق الخاص بك

77702

```
<html>
<head>
  <title>OTP Verify</title>
  <link rel="stylesheet" href="css/style_login_register_Verification.css">
</head>
<?php
session_start();

include_once('config.php');
if(isset($_REQUEST['otp_verify']))
{
    $otp = $_REQUEST['otp'];
    $select_query = mysqli_query($conn,"select * from tbl_otp_check where otp='$otp' and is_expired!=1 and NOW()<=DATE_ADD(create_at,interval 5 minute)");
    $count = mysqli_num_rows($select_query);
    if($count>0)
    {
        $select_query = mysqli_query($conn, "update tbl_otp_check set is_expired=1 where otp='$otp'");
        header('location:login_form.php');
    }
    else
    {
        $msg = "كلمة مرور المؤقتة خطأ";
    }
}
?>
<body>
<div class="form-container">

    <form action="" method="post">
    <h3 class="title">ادخل كلمة المرور المؤقتة</h3>

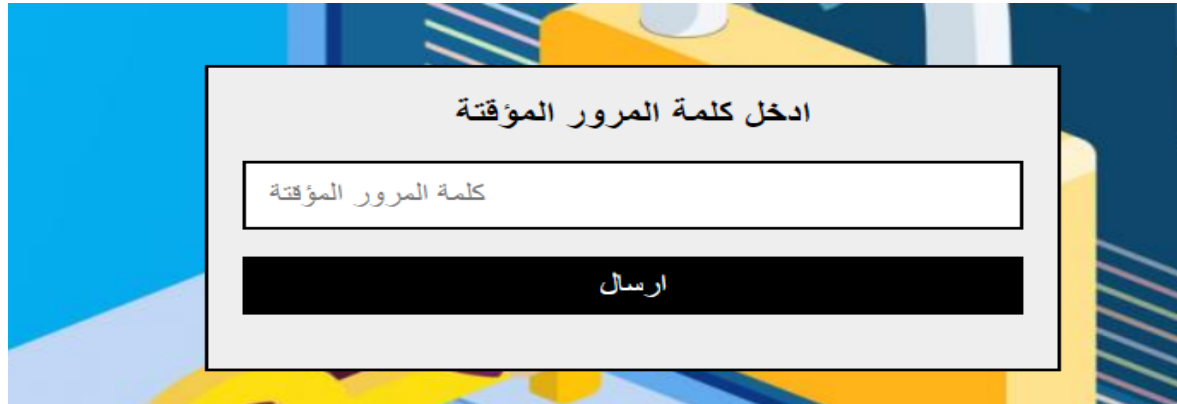
    <input type="text" name="otp" id="otp" placeholder="كلمة المرور المؤقتة" required
        data-parsley-type="otp" data-parsley-trigger="keyup" class="box"/>

    <input type="submit" id="submit" name="otp_verify" value="ارسال" class="form-btn" />
    <p class="error"><?php if(!empty($msg)){ echo $msg; } ?></p>
    </form>

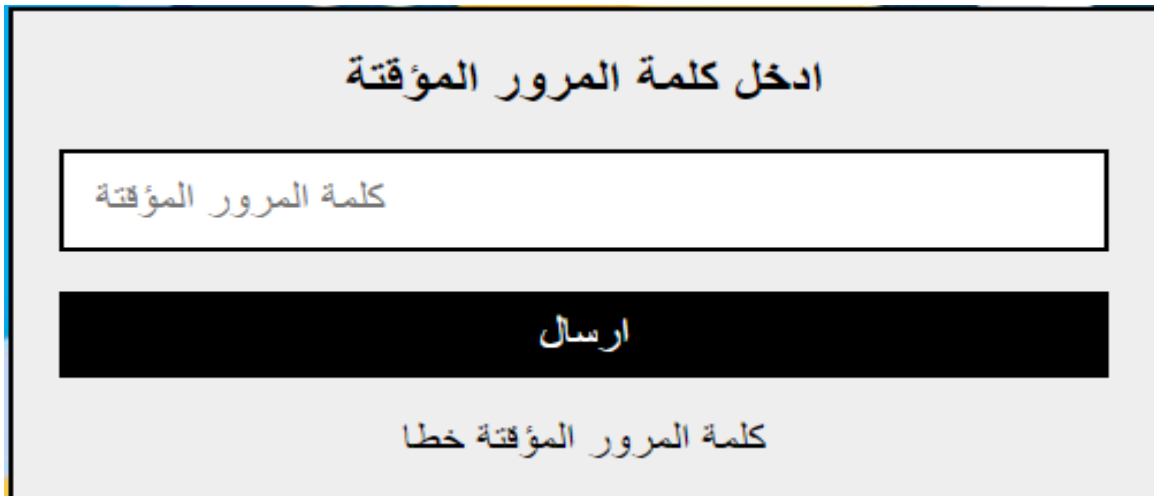
</div>
</body>
</html>
```

الصورة السابقة هي للكود الخاص بصفحة التأكد من حالة الرمز، إذا كان الرمز خطأ تظهر رسالة خطأ، وإذا كان صحيح يتم توجيه للصفحة المطلوبة.

الصورة التالية هي لصفحة التحقق من الرمز.



إذا ادخل رمز خطأ يتم عرض رسالة كلمة المرور المؤقتة خطأ.



وإذا كانت كلمة المرور صحيح في حالة التسجيل يتم نقله لصفحة تسجيل الدخول، وإذا كانت صحيحة في حالة تسجيل الدخول يتم نقله لصفحة Home.

## منع استخدام رمز OTP لشخص آخر

اثناء انشاء هذا المشروع وجدت مشكلة في كود التحقق من رمز OTP إذا لم تكن مصيبة أساسا في الكود، حيث كمثال لدينا على انني مهاجم ادخل الى صفحة إعادة تعيين كلمة المرور وادخل البريد الالكتروني الخاص بالضحية ثم يتم ارسال رمز تحقق الى الضحية ادخل انا كمهاجم من جلسة أخرى وادخل الايميل الخاص بي واحصل على رمز التحقق إذا حصلت على رمز التحقق ارجع الى جلسة الضحية ثم ادخل رمز التحقق الخاص بي فأتمكن من الدخول الى صفحة تغيير كلمة المرور ويمكنني تغيير كلمة مرور الضحية بدون علمه نعتقد ان المشكلة تحدد امان الموقع.

لذلك تم حلها من خلال وضع شرط إضافي ووضع خانة إضافة في الجدول tbl\_otp\_check حيث إذا تم ارسال رمز التحقق يرتبط بالبريد الالكتروني الخاص بالمرسل فقط.

	id	otp	is_expired	create_at	email
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	405	74299		1 2023-05-18 03:06:49	aboody16100@gmail.com

ولا يمكن للمستخدم ان يستخدمه الا إذا كانت الجلسة تحمل البريد الالكتروني المسجل.

لم نكتف بذلك أيضا، بل تمت إضافة شروط إضافية من خلال المتغيرات على انه لا يمكنك الحصول على رمز تسجيل الدخول مستخدم عادي فتتمكن من الدخول الى صفحة المستخدم الرئيسي فمن خلال المتغيرات إذا كانت true يتم قبول المستخدم في هذه الصفحة فقط. هذا مثال لتسجيل دخول مستخدم بعد ان اتم ادخال رمز التحقق بشكل صحيح يحصل على

```
$_SESSION['otp_verified_home'] = true;
```

حيث لا يمكنه الحصول على true الا عندما يتم ارسال OTP بشكل صحيح ثم ينتقل الى صفحة home.php اول شرط تحتوي عليه الصفحة هو ان يكون المتغير السابق true.

لكن في صفحة المستخدم الرئيسي يختلف اسم المتغير فلا يمكن للمستخدم العادي الدخول صفحة المستخدم الرئيسي.

### انشاء صفحة إعادة تعيين كلمة المرور

حاليا إذا نسي المستخدم كلمة المرور لا يمكنه ارجاعها لذلك سيتم انشاء زر استرجاع كلمة المرور يمكن للمستخدم من خلاله تعيين كلمة مرور جديدة.

### سجل دخولك

سجل دخولك

ليس لديك حساب؟ [سجل الان](#)

نسيت كلمة المرور؟ [اعد تعيينها](#)

يمكن للمستخدم الوصول الى الزر من صفحة تسجيل الدخول.

من خلال الزر ينتقل المستخدم الى صفحة نسيت كلمة المرور حيث يضع البريد الالكتروني،



وإذا تذكر البريد الإلكتروني يمكنه الضغط على زر سجل دخولك للرجوع الى صفحة تسجيل الدخول.

استرجاع كلمة المرور

ادخل الايميل الخاص بك

استرجاع كلمة المرور

تذكرت كلمة المرور؟ سجل دخولك

إذا ادخل المستخدم بريد الإلكتروني غير موجود تظهر له رسالة تفيد بأن البريد الإلكتروني غير موجود.

استرجاع كلمة المرور

الايمل غير موجود

ادخل الايميل الخاص بك

استرجاع كلمة المرور

تذكرت كلمة المرور؟ سجل دخولك

إذا ادخل المستخدم بريد الإلكتروني موجود ينتقل الى صفحة التحقق من الرمز OTP يتم ارساله إلى بريد إلكتروني المستخدم بنفس تفاصيل الكود السابق الذي يتم ارساله للمستخدم عند التسجيل او تسجيل الدخول.

ادخل كلمة المرور المؤقتة

كلمة المرور المؤقتة

ارسال

إذا ادخل الرمز بشكل سليم ينتقل الى صفحة إعادة تعيين كلمة المرور ويمكنه تغيير كلمة المرور مع التأكد من مطابقة شروط كلمة المرور التي تم ذكرها سابقا وبعدها ينتقل إلى صفحة تسجيل الدخول حيث يتم تحديث كلمة المرور في قاعدة البيانات ويمكنه الدخول باستخدام كلمة المرور الجديدة.

### استرجاع كلمة المرور

ادخل كلمة المرور الجديدة

اعد ادخل كلمة المرور الجديدة

استرجاع كلمة المرور

تذكرت كلمة المرور؟ [سجل دخولك](#)

## انشاء صفحة المستخدم الرئيسي

الآن سيتم انشاء مستخدم رئيسي حيث ستكون للمستخدم الرئيسي صلاحيات اعلى مثل حذف أي مستخدم او تعديل كلمة المرور لمستخدم معين او مشاهدة نشاطات المستخدمين او إضافة مستخدم رئيس جديد.

تم انشاء قاعدة بيانات خاصة للمستخدم الرئيسي بالإسم والتفاصيل التالية.

user_db	id	email	password
New	1	admin@gmail.com	202cb962ac59075b964b07152d234b70
admin_form			

تم إضافة شرط في الكود في كود تسجيل الدخول إذا كان المستخدم من جدول admin\_form وكلمة المرور صحيحة يحصل على رمز تحقق وإذا ادخل رمز التحقق بشكل سليم يمكن له الوصول الى صفحة المستخدم الرئيسي.

```
if(mysqli_num_rows($admin_result) > 0){  
    $_SESSION['usermail'] = $email;  
    header('location: admin_page.php');  
    exit();  
}
```

يمكنه للإداري عرض المستخدمين المسجلين في الموقع او حذفهم او إعادة تعيين كلمات المرور الخاصة بهم ويمكنه تسجيل الخروج.

صفحة الإدارة	
<a href="#">تسجيل</a> <a href="#">الخروج</a>	
المستخدمون	التحكم
aboody16100@gmail.com	<input type="text" value="الرمز الجديد"/> <input type="button" value="تعديل كلمة المرور"/> <input type="button" value="حذف"/>
abdulelah19j@gmail.com	<input type="text" value="الرمز الجديد"/> <input type="button" value="تعديل كلمة المرور"/> <input type="button" value="حذف"/>

تم انشاء كود إعادة التعيين مشابه للكود الخاص بإعادة التعيين للمستخدمين.

```
if(isset($_POST['change_password'])){  
    $email = mysqli_real_escape_string($conn,$_POST['email']);  
    $new_password = mysqli_real_escape_string($conn,$_POST['new_password']);  
    $hashed_password = md5($new_password);  
    $update_query = mysqli_query($conn,"UPDATE user_form SET password='$hashed_password' WHERE email='$email'");  
    if($update_query){  
        echo "تم تحديث كلمة المرور بنجاح";  
    } else {  
        echo "حدث خطأ أثناء تحديث كلمة المرور";  
    }  
}
```

وتم انشاء كود خاص جديد يمكنه حذف المستخدم من قاعدة البيانات.

```

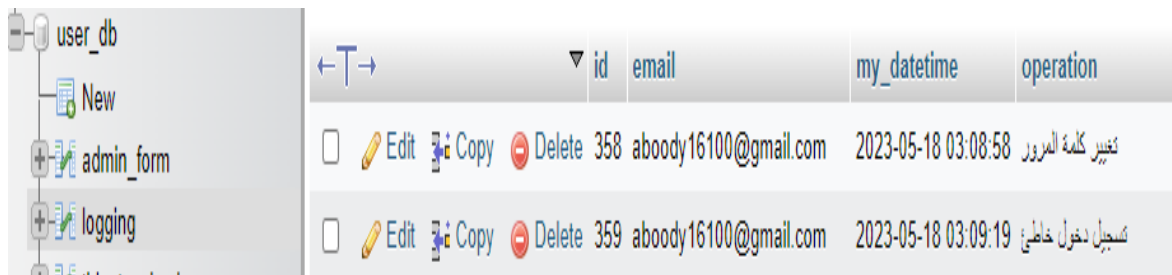
if(isset($_POST['delete'])){
    $email = mysqli_real_escape_string($conn,$_POST['email']);
    $delete_query = mysqli_query($conn,"DELETE FROM user_form WHERE email='$email'");
    if($delete_query){
        echo "تم حذف المستخدم بنجاح";
    } else {
        echo "حدث خطأ أثناء حذف المستخدم";
    }
}

```

## انشاء صفحة لمراقبة سلوك المستخدم من خلال المستخدم الرئيسي

تم انشاء صفحة يمكن للمستخدم الإداري من خلالها مراقبة سلوك المستخدم مثل متى سجل المستخدم المعين دخوله ومتى سجل خروج وهكذا.

في البداية تم انشاء جدول logging في قاعدة البيانات لتجميع جميع البيانات، وبمجرد ان يتم المستخدم عملية يتم تسجيل في هذا الجدول على انه تمت العملية، حيث يتم اخذ 4 تفاصيل أولا رقم العملية id، ثانيا البريد الالكتروني المنفذ للعملية email، ثالثا الوقت والتاريخ التي تمت به العملية my\_datetime، رابعا تحديد العملية التي قام بها المستخدم operation.



	id	email	my_datetime	operation
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	358	aboody16100@gmail.com	2023-05-18 03:08:58	تغيير كلمة المرور
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	359	aboody16100@gmail.com	2023-05-18 03:09:19	تسجيل دخول خاطئ

يتم تسجيل القيم بعد كل عملية وسيتم ذكر العمليات التي يتم تسجيلها

- تسجيل دخول مستخدم رئيسي
- تسجيل مستخدم رئيسي جديد
- حذف المستخدم من قبل مستخدم رئيسي
- تغيير كلمة المرور من قبل مستخدم رئيسي
- تسجيل دخول
- تسجيل جديد
- تسجيل الخروج
- تسجيل دخول خاطئ
- تغيير كلمة المرور

أي من هذه الحالات إذا تمت يتم تسجيل في الجدول انها تمت في الساعة التي تمت بها والتاريخ ومنفذ العملية والعملية.

هذا مثالا للكود الذي يتم إذا تم تسجيل الدخول بشكل صحيح وكيف يتم تسجيله.

```
if(mysqli_num_rows($user_result) > 0){//اكمل الخطوات التالية
    $_SESSION['usermail'] = $email;
    $insert_logging = "INSERT INTO logging(email,my_datetime,operation) VALUES('$email',now()),('تسجيل دخول')";
    mysqli_query($conn, $insert_logging);
```

بعد ان اتمنا عمليات التسجيل في قاعدة البيانات نحتاج الان الى صفحة يتم من خلالها عرض سلوكيات المستخدم التي تم انشاؤها في قاعدة البيانات، لذلك تم انشاء الصفحة الخاصة بسلوك المستخدم يمكن للمستخدم الرئيسي الوصول لها من خلال البار اعلى الشاشة.



ومن خلال الصفحة تم استخدام اوامر SQL من خلالها سيتم عرض جميع سلوكيات المستخدم التي تم تسجيلها في الموقع، وتمت اضافته زر لتسجيل الخروج المستخدم ويتم عرض البيانات داخل جدول.



توجد مشكله الان وهي ان سلوكيات المستخدم قد تزيد ولا يمكن مراقبتها بشكل جيد ويصعب على المستخدم الرئيسي البحث عن عملية لمستخدم لذلك تم إضافة عامل تصفية من خلاله يتم عرض العمليات بحسب النوع مثلا إذا اردت فقط عرض العمليات الخاصة بتسجيل الخروج فقط.

يمكنك الاختيار من القائمة المنسدلة والضغط على تصفية وسيتم عرض فقط عمليات تسجيل الخروج.

صفحة سلوك المستخدم		
<div>تسجيل الخروج</div>		
تصفية النتائج حسب: تسجيل الخروج تصفية		
العملية	التاريخ والوقت	البريد الإلكتروني
تسجيل الخروج	03:38:48 2023-05-18	aboody16100@gmail.com

وهذه هي عوامل التصفية المتواجدة في القائمة المنسدلة.

تسجيل الخروج
الكل
تسجيل دخول مستخدم رئيسي
تسجيل مستخدم رئيسي جديد
حذف المستخدم من قبل مستخدم رئيسي
تغيير كلمة المرور من قبل مستخدم رئيسي
تسجيل دخول
تسجيل جديد
تسجيل الخروج
تسجيل دخول خاطئ
تغيير كلمة المرور

## انشاء صفحة تسجيل مستخدم رئيسي جديد

إذا أراد المستخدم الرئيسي اضافته مساعد له لا يمكنه، لكن الان سيتم انشاء صفحة تسجيل مستخدم رئيسي جديد، تم استخدام كود مشابه لصفحة تسجيل مستخدم عادي لكن تمت اضافته بعض التغييرات على النصوص والشروط وان يتم تسجيل المستخدم في الجدول `admin_form`.

يمكن الوصول للصفحة من خلال البار اعلى الصفحة الخاصة بالمستخدم الرئيسي.



إذا تم الضغط على اضافته مستخدم رئيسي جديد، يتم عرض الصفحة التالية، وإذا تم ادخال بريد الإلكتروني غير موجود في الجدول `admin_form`، وتمت تلبية جميع الشروط، وهي ان تكون كلمة المرور معقدة، وان تتطابق كلمة المرور المدخلة مع إعادة الادخال، وسيتم في هذه الحالة تسجيل المستخدم في قاعدة البيانات على انه مستخدم رئيسي.

### سجل مستخدم رئيسي

لديك حساب؟ [سجل دخولك](#)



## انشاء صفحة (Home)

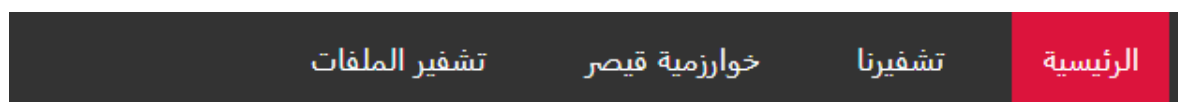
إذا سجل المستخدم حساب جديد يتم نقله بشكل تلقائي الى صفحة التسجيل بحيث يمكنه التسجيل والدخول الى الصفحة الرئيسية للموقع.

تم انشاء الصفحة التالي ترحب بالمستخدم، ومن خلال اتصالها بقاعدة البيانات يمكنها عرض المستخدم الحالي من خلال عرضها الايميل الخاص بالمستخدم الحالي، وفي الاسفل يوجد زر لتسجيل الخروج حيث يغلق الاتصال ويخرج المستخدم وينقله الى صفحة تسجيل الدخول.



تم بناء الصفحة من خلال "HTML"، وتم تصميمها من خلال "CSS"، وتم ربطها مع قاعدة البيانات بحيث تعرض الايميل الخاص بالمستخدم.

من خلال "HTML" تمت إضافة شريط للتنقل يمكن المستخدم بعد الدخول الى الموقع التنقل في صفحات الموقع بسهولة مثل انتقاله من الصفحة الرئيسة الى صفحة شفرة قيصر بمجرد الضغط على زر شفرة قيصر يمكن الانتقال اليها ومن خلال "CSS" تمت تعديل التصميم الخاص بشريط التنقل ليوفر تجربة فريدة للمستخدم.



## خوارزمية تشفير التبديل الخاصة بنا

في البداية قررنا تنفيذ خوارزمية تشفير من نوع (تشفير التبديل)، وتم صنع خوارزمية خاصة بنا.

### Our Encryption

Enter text:

Output:

بعد انشاء الخوارزمية و اضافتها في الصفحة، قررنا إضافة بعض التحسينات على الصفحة لتحسين

تجربة المستخدم من خلال "CSS"

تشفيرنا

الرجاء التكرم:

تشفير

فك التشفير

النتيجة:

تم استخدام الخوارزمية التالية حيث كمثال تستبدل الحرف "a" الى "q"

```
const substitutionKey = {  
  'a': 'q', 'b': 'w', 'c': 'e', 'd': 'r', 'e': 't',  
  'f': 'y', 'g': 'u', 'h': 'i', 'i': 'o', 'j': 'p',  
  'k': 'a', 'l': 's', 'm': 'd', 'n': 'f', 'o': 'g',  
  'p': 'h', 'q': 'j', 'r': 'k', 's': 'l', 't': 'z',  
  'u': 'x', 'v': 'c', 'w': 'v', 'x': 'b', 'y': 'n',  
  'z': 'm', '1': '0', '2': '1', '3': '2', '4': '3', '5': '4',  
  '6': '5', '7': '6', '8': '7', '9': '8', '0': '9', 'A': 'Q',  
  'B': 'W', 'C': 'E', 'D': 'R', 'E': 'T', 'F': 'Y',  
  'G': 'U', 'H': 'I', 'I': 'O', 'J': 'P', 'K': 'A',  
  'L': 'S', 'M': 'D', 'N': 'F', 'O': 'G', 'P': 'H',  
  'Q': 'J', 'R': 'K', 'S': 'L', 'T': 'Z', 'U': 'X',  
  'V': 'C', 'W': 'V', 'X': 'B', 'Y': 'N', 'Z': 'M',  
};
```

## شفرة قيصر

بعد إتمامنا انشاء صفحة خاصة (بتشفير التبدل)، اتخذنا القرار بأنشاء صفحة يمكن من خلالها

تشفير وفك التشفير باستخدام شفرة قيصر ويمكن للمستخدم إضافة رقم كمقدار للإزاحة.

### Caesar Cipher


Enter text:

KEY:

Encrypt Decrypt

Output:

بعد ذلك تمت إضافة التصميم والألوان باستخدام "CSS" وجعله مشابه للتصميم السابق.



يستعرض الكود التالي دالتين خاصة بتشفير قيصر، ووظيفتهما هيا التشفير، وفك التشفير باستخدام شفرة قيصر.

```
<script>
function encrypt() {
    var message = document.getElementById("message").value;
    var shift = parseInt(document.getElementById("shift").value);
    var result = "";
    for (var i = 0; i < message.length; i++) {
        var charCode = message.charCodeAt(i);
        if (charCode >= 65 && charCode <= 90) {
            result += String.fromCharCode((charCode - 65 + shift) % 26 + 65);
        } else if (charCode >= 97 && charCode <= 122) {
            result += String.fromCharCode((charCode - 97 + shift) % 26 + 97);
        } else {
            result += message.charAt(i);
        }
    }
    document.getElementById("output").value = result;
}

function decrypt() {
    var message = document.getElementById("message").value;
    var shift = parseInt(document.getElementById("shift").value);
    var result = "";
    for (var i = 0; i < message.length; i++) {
        var charCode = message.charCodeAt(i);
        if (charCode >= 65 && charCode <= 90) {
            result += String.fromCharCode((charCode - 65 - shift + 26) % 26 + 65);
        } else if (charCode >= 97 && charCode <= 122) {
            result += String.fromCharCode((charCode - 97 - shift + 26) % 26 + 97);
        } else {
            result += message.charAt(i);
        }
    }
    document.getElementById("output").value = result;
}
</script>
```

8 الدالتين الخاصة بتشفير وفك التشفير باستخدام خوارزمية قيصر

## تشفير الملفات

تشفير الملفات هو عملية تحويل الملفات إلى شكل غير مفهوم للمستخدمين الآخرين.

سيتم في موقعنا انشاء صفحة لتشفير الملفات النصية.

تم انشاء الكود باستخدام مكتبة cryptoJs، من خلال تشفير AES.

يطلب منك الملف المراد تشفيره او فك تشفيره، ويمكنك الاختيار من بين الازرار إذا اردت التشفير او فك التشفير، بعد وضع الملف إذا تم اختيار تشفير يتم تشفير الملف، وإذا تم اختيار فك التشفير يتم فك تشفير الملف.

## تشفير الملفات

تشفير الملف فك تشفير الملف No file chosen Choose file

بعد ذلك تمت إضافة التصميم الى الصفحة وظهرت بالشكل التالي



يتم التشفير في صفحة تشفير الملفات من خلال الدالة التالية.

```
function encryptFile() { //الدالة الخاصة بتشفير الملفات
  const fileInput = document.getElementById('fileInput');
  const file = fileInput.files[0]; // الحصول على الملف

  if (!file || file.type !== 'text/plain') {
    alert('يجب استخدام على ادخال ملفات من نوع txt فقط');// فقط TXT يرجى اختيار ملف نصي بصيغة
    return;
  }

  const reader = new FileReader();
  reader.onload = function (e) {
    const fileContent = e.target.result; // قراءة الملف
    const encryptedContent = CryptoJS.AES.encrypt(
      fileContent,
      'password_here'
    ).toString();
    // تشفير المحتوى باستخدام مكتبة CryptoJS
    const encryptedFile = new Blob([encryptedContent], {
      type: 'text/plain',
    });
    const downloadLink = document.createElement('a');
    downloadLink.href = URL.createObjectURL(encryptedFile); // إنشاء رابط لتنزيل الملف بعد التشفير
    downloadLink.download = 'encrypted_file.txt'; // اختيار اسم الملف
    downloadLink.click(); // تثبيت الملف
  };
  reader.readAsText(file);
}
```

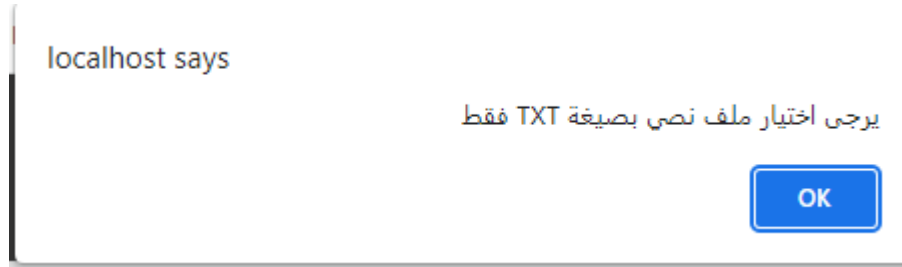
ويتم فك التشفير في صفحة تشفير الملفات من خلال الدالة التالية.

```
function decryptFile() { //الدالة الخاصة بفك تشفير الملفات
  const fileInput = document.getElementById('fileInput');
  const file = fileInput.files[0]; // الحصول على الملف

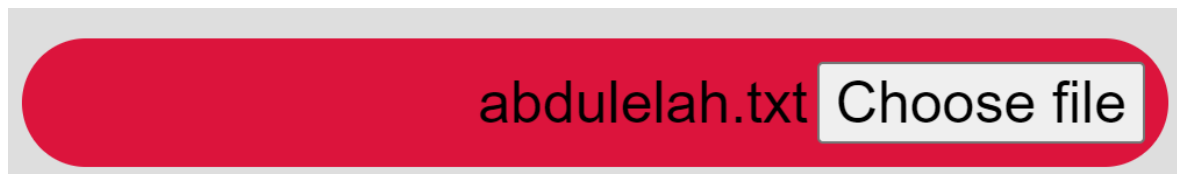
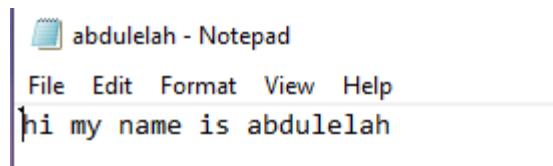
  if (!file || file.type !== 'text/plain') {
    alert('يجب استخدام على ادخال ملفات من نوع txt فقط');// فقط TXT يرجى اختيار ملف نصي بصيغة
    return;
  }

  const reader = new FileReader();
  reader.onload = function (e) {
    const fileContent = e.target.result; // قراءة الملف
    const decryptedContent = CryptoJS.AES.decrypt(
      fileContent,
      'password_here'
    ).toString(CryptoJS.enc.Utf8);
    // فك تشفير المحتوى باستخدام مكتبة CryptoJS
    const decryptedFile = new Blob([decryptedContent], {
      type: 'text/plain',
    });
    const downloadLink = document.createElement('a');
    downloadLink.href = URL.createObjectURL(decryptedFile); // إنشاء رابط لتنزيل الملف بعد فك التشفير
    downloadLink.download = 'decrypted_file.txt'; // اختيار اسم الملف
    downloadLink.click(); // تثبيت الملف
  };
  reader.readAsText(file);
}
```

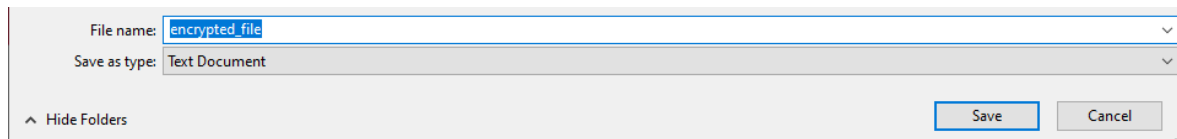
تمت إضافة شرط لمنع المدخلات الخاطئة من المستخدم، حيث يمنع المستخدم إذا ادخل ملف غير ملف txt، بسبب ان الكود الخاص بنا لا يشفر الا ملفات txt، ويتم عرض رسالة للمستخدم بذلك.



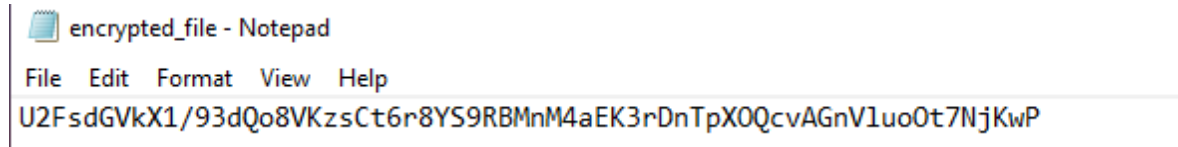
وكمثال سيتم تشفير الملف النصي التالي



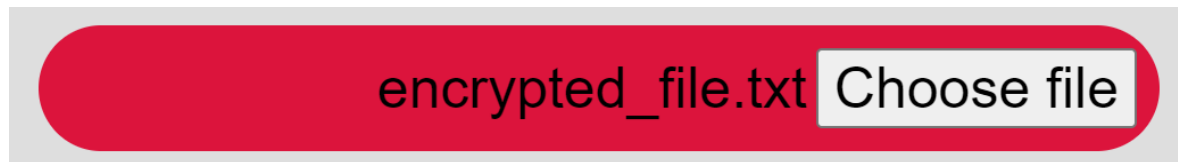
بعد اختيار الملف يتم الضغط على الزر تشفير وبمجرد ان يتم الضغط يتم تنزيل ملف نصي جديد بالاسم التالي encrypted\_file يحوي تشفير النص الذي بداخله.



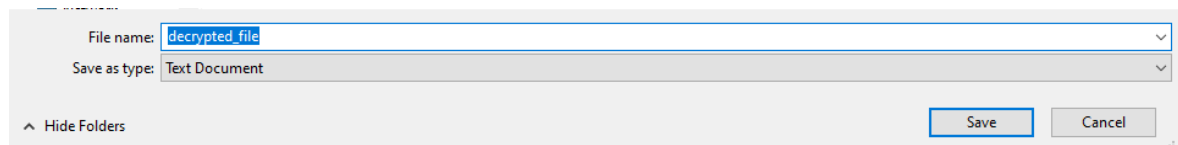
بعد فتح الملف الجديد encrypted\_file يمكنك الحصول على النص المشفر.



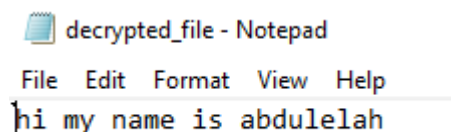
يمكن بعد ذلك فك التشفير من خلال وضع الملف encrypted\_file واختيار زر فك التشفير.



بمجرد الضغط على زر فك التشفير يتم تنزيل ملف نصي بالاسم decrypted\_file يحتوي على النص بعد فك التشفير.



إذا تم فتح الملف النصي decrypted\_file يمكنك مشاهدة النص بعد فك التشفير ونلاحظ على أنه تم فك التشفير بنجاح.





## منع التنقل من خلال URL

وجدت لدينا مشكله في الموقع حيث يمكن للمستخدم التنقل من خلال الحصول على اسم الصفحة الدخول الى أي صفحة من خلال كتيبها في الرابط، فمثلا يمكن للمستخدم كتابه home.php في رابط الموقع فيتمكن من الدخول بدون تسجيل دخول.

لذلك توجب علينا منع المستخدم من التنقل الى الصفحات بدون تسجيل الدخول وبدون ان يكون رمز OTP المرسل صحيح، لذلك تم وضع الشرط التالي للصفحات التي تتطلب تسجيل دخول، يتطلب ان تحمل الجلسة ايميل وان تحمل معها المتغير otp\_verified\_home وان تكون حاله المتغير true ولا يمكن للمتغير ان يكون true الا عند ارسال رمز OTP في الصفحة التي قبلها بشكل صحيح، إذا توافرت الشروط السابقة يمكن للمستخدم الدخول الى الصفحات التي تتطلب تسجيل دخول، إذا لا يتم ارجاعه الى صفحة login\_form.php.

```
// الصفحة الحاليه تحتوي على الكود الخاص بالتحقق من الايميل و حاله OTP من خلال الجلسه والتحقق من نشاط المستخدم
if (!isset($_SESSION['email']) || !isset($_SESSION['otp_verified_home']) || $_SESSION['otp_verified_home'] !== true) {
    header('Location: login_form.php');
    $_SESSION['otp_verified_home'] = false;
    exit();
}
```

أيضا تمت اضافته نفس الشروط السابقة لكن لصفحة تغيير كلمة المرور حيث لا يمكن الدخول لها  
الا اذا تم اكمال الشروط السابقة مع ان يساوي `otp_verified_reset = true`.

```
session_start();
if (!isset($_SESSION['email']) || !isset($_SESSION['otp_verified_reset']) || $_SESSION['otp_verified_reset'] !== true) {
    header('Location: forgot.php');
    exit();
}
```

أيضا تم منع التنقل في الصفحات المهمة مثل الصفحات التي يتطلب ان يستخدمها حساب  
رئيسي تم وضع شرط إضافي لها، ان تكون الجلسة تحمل بريد الالكتروني وان يكون البريد  
الالكتروني صحيح وموجود في الجدول `admin_form` وان تحمل المتغير  
`otp_verified_admin` وتكون قيمه المتغير `true` وب نفس الحالة السابقة لا يكون المتغير  
`true` الا عندما يكون تم استلام رمز OTP بشكل صحيح من الصفحة السابقة، وإذا لم تتوفر  
الشروط يتم ارجاع المستخدم الى صفحة `login_form.php`.

```
if(!isset($_SESSION['usermail']) || !isset($_SESSION['otp_verified_admin']) || $_SESSION['otp_verified_admin'] !== true){
    header('location:login_form.php');
    $_SESSION['otp_verified_admin'] = false;
    exit();
}
```

## التأكد من ان المستخدم نشط

تمت اضافته شرط على جميع الصفحات التي تتطلب تسجيل الدخول إذا مرت أكثر من عشر دقائق بدون أي نشاط من المستخدم يتم تسجيل الخروج مما قد توفر امان للمستخدم إذا نسي الجلسة بدون تسجيل خروج.

```
$sessionExpired = false;
if (isset($_SESSION['LAST_ACTIVITY']) && time() - $_SESSION['LAST_ACTIVITY'] > 600) {
    $sessionExpired = true;
    session_unset();
    session_destroy();
    header('Location: login_form.php');
    exit();
}

$_SESSION['LAST_ACTIVITY'] = time();
```

## تعقيم المدخلات باستخدام mysqli\_real\_escape\_string

يتم استخدام الوظيفة بالكود الخاص بنا قبل ادخال أي مدخل الى قاعدة البيانات من المستخدم حيث تصعب على المهاجم إضافة بيانات او أوامر SQL بهدف مهاجمة النظام وهذا مثال قبل تسجيل مستخدم جديد يتم تعقيم المدخلات.

```
$email = mysqli_real_escape_string($conn, $_POST['usermail']);
$pass = mysqli_real_escape_string($conn, $_POST['password']);
$cpass = mysqli_real_escape_string($conn, $_POST['cpassword']);
```

## الاتصال مع المستضيف

في نهاية المشروع تم التسجيل مع مزود استضافة للموقع، والمستضيف هو مزود خدمة يملك او يشغل العديد من السيرفرات، حيث إذا رفعت له جميع ملفات المشروع يمكن للمستخدمين في أي مكان الاتصال مع مزود الخدمة من خلال رابط الموقع والوصول الى موقعنا ويوفر لنا مزود الخدمة أيضا الشهادات التي توفر لنا HTTPS.

يمكن الوصول الى الموقع من خلال الرابط التالي

[/https://graduationproject984.000webhostapp.com](https://graduationproject984.000webhostapp.com)

تم الاتصال مع مزود خدمة بشكل مجاني لمدة محددة واسم مزود الخدمة 000webhost



## الخطط المستقبلية

- إضافة تشفير للرمز OTP قبل إرساله للمستخدم.
- إضافة مستخدم مساعد للمستخدم الرئيسي.
- اختبار الموقع من قبل مختبر اختراق.
- تطويرات إضافية في التصميم وإغلاق بعض نقاط الضعف داخل الموقع.
- إضافة أنواع تشفير أخرى داخل الموقع.

## الختام

الحمد لله جل جلاله فهو وحده سبحانه من وفقنا لما تمكنا من تقديمه إليكم، وها هي آخر محطاتنا في البحث الذي قد أخذ الكثير من الوقت والجهد لكي يخرج بتلك النتائج، ولكنه جهد ثمين غير ضائع، حيث توصلنا من خلاله إلى الفهم التام والإدراك الكافي لجميع جوانب موضوعنا والإجابة حول جميع ما قد يرد حوله من تساؤلات، نتمنى أن يكون بحثنا نال إفادتكم وأتى على النحو الذي كنتم ترجونه منه.

## المراجع

<a href="https://arab-box.com/introduction-to-research-on-computers">https://arab-box.com/introduction-to-research-on-computers</a>	مقدمه عن الحاسب
<a href="https://cutt.us/9nMCO">https://cutt.us/9nMCO</a>	ماهي HTML
<a href="https://harmash.com/tutorials/css/overview">https://harmash.com/tutorials/css/overview</a>	لغة CSS
<a href="https://n9.cl/g4m0c">https://n9.cl/g4m0c</a>	شفرة قيصر
<a href="https://aws.amazon.com/ar/what-is/javascript">https://aws.amazon.com/ar/what-is/javascript</a>	JavaScript
<a href="https://code.visualstudio.com">https://code.visualstudio.com</a>	visualstudio
<a href="https://cutt.us/CeEy2">https://cutt.us/CeEy2</a>	عدد مستخدمي الإنترنت في العالم 2023
<a href="https://privacycanada.net/substitution-ciphers">https://privacycanada.net/substitution-ciphers</a>	شفرة الاستبدال
<a href="https://cutt.us/F6Ypl">https://cutt.us/F6Ypl</a>	ويكيبيديا شفرة قصير
<a href="https://cutt.us/105AT">https://cutt.us/105AT</a>	ويكيبيديا مكتبة البرمجية
<a href="https://en.wikipedia.org/wiki/Advanced_Encryption_Standard">https://en.wikipedia.org/wiki/Advanced_Encryption_Standard</a>	معيار التشفير المتقدم
<a href="https://cryptojs.gitbook.io/docs">https://cryptojs.gitbook.io/docs</a>	CryptoJS
<a href="https://www.microsoft.com/ar-ww/security/business/security-101/what-is-two-factor-authentication-2fa">https://www.microsoft.com/ar-ww/security/business/security-101/what-is-two-factor-authentication-2fa</a>	التحقق الثنائي
<a href="https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp">https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp</a>	One Time Password

	(OTP)
<a href="https://github.com/PHPMailer/PHPMailer">https://github.com/PHPMailer/PHPMailer</a>	PHPMailer
<a href="https://www.w3schools.com/php/php_intro.asp">https://www.w3schools.com/php/php_intro.asp</a>	php
<a href="https://www.php.net/manual/en/mysqli.real-escape-string.php">https://www.php.net/manual/en/mysqli.real-escape-string.php</a>	mysqli_real_escape_string
<a href="https://www.techtarget.com/searchsoftwarequality/definition/HTTPS">https://www.techtarget.com/searchsoftwarequality/definition/HTTPS</a>	HTTPS
<a href="https://www.techtarget.com/searchdatamanagement/definition/SQL">https://www.techtarget.com/searchdatamanagement/definition/SQL</a>	SQL
<a href="https://www.mysql.com">/https://www.mysql.com</a>	MySQL
<a href="https://www.uml.org">/https://www.uml.org</a>	UML