Study how to extract cookies and password files for a Chrome user and provide this service via a website

Ali Khader Ibrahim*

Ammar Monzer Speeh**

(Startingdate3/3/2022 . Enddate13/6/2022)

□ ABSTRACT □

With a large number of search engines spread around the world, many users suffer from forgetting the names of the sites they visited before in addition to forgetting passwords.

We will use the Python programming language to extract all the cookies of the google chrome user from the beginning of his use on your device, in addition to extracting the passwords with the date and time.

Employ all of the above on a website that offers this service "Cookies & Password.com"

Keywords: cookies ،password ،AES256 ،base64،cipher،key,initialization vector،data

• **Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria** Aliibrahim99hz@gmail.com

•• **Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria** Ammaerspeeh@gmail.com

دراسة كيفية استخراج ملفات تعريف الارتباط وملفات كلمات المرور لمستخدم chrome وتقديم هذه الخدمة عبر موقع الكتروني

الطالب. علي خضر إبراهيم*

الطالب. عمار منذر صبيح**

(تاريخ البدء 2022/3/3 . تاريخ الانتهاء2022/6/13)

□ ملخّص □

في ظل انتشار عدد كبير من محركات البحث حول العالم يعاني الكثير من المستخدمين من نسيان أسماء المواقع التي تمت زيارتها من قبل بالإضافة لنسيان كلمات المرور.

سوف نقوم باستخدام لغة البرمجة بايثون لاستخراج كافة ملفات تعريف الارتباط لمستخدم google chrome منذ بداية استخدامه على جهازك بالإضافة لاستخراج كلمات المرور مع ذكر التاريخ والوقت.

سيتم مناقشة الية التشفير المستخدمة وكيف تم فك التشفير.

توظيف كل ما سبق في موقع الكتروني يقدم هذه الخدمة "Cookies&Password.com "

الكلمات المفتاحية: cookies، password، AES256، base64، cipher،key،initialization vector،data

. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Aliibrahim99hz@gmail.com

.. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Ammarspeeh@gmail.com

مقدّمة:

تستخدم ملفات تعريف الارتباط على كافة مواقع الويب تقريبا حيث انها تعد جزء صغير من البيانات التي يتم تخزينها في ملف خاص على الجهاز في اغلب الأحيان يكون مساره موحد بين العديد من أنواع الحواسيب

المسار المعتاد:C:Users\PC\AppData\Local\Google\Chrome\UserData\Default\Network\Cookies

دراستنا سوف تتمحور حول متصفح google chrome وكيفية يتم تخزين ملفات تعريف الارتباط و ملفات كلمات المرور وما تقنيات التشفير المتبعة من قبل google

البيانات التي سيتم استخراجها هي وقت بدء الجلسة ووقت انتهاء الجلسة اسم الموقع الذي تم زيارته كلمة المرور واسم المستخدم

أهمية البحث وأهدافه:

تأتي أهمية هذا البحث من كون الكثير من المستخدمين ل google chrome يقومون بالدخول للكثير من المواقع بشكل يومي لهذا السبب قد لا يتذكر المستخدم أسماء المواقع الذي قام بزيارتها

مهمة هذا الشروع هو إيجاد هذه المواقع

بالإضافة الى ذلك هناك الكثير من المواقع تطلب تسجيل الدخول باسم مستخدم وكلمة مرور قبل الدخول وهذه المعلومات بسبب كثرة المواقع هي عرضة للنسيان

لذلك من مهام هذا المشروع أيضا هو إيجاد كلمات المرور واسم المستخدم

طرائق البحث ومواده:

تم تنفيذ هذا البحث بالكامل بلغة python تم الاعتماد على محرر الاكواد vscode لكتابة البرنامج

تم التنفيذ بجزمة python 3.10 64 bit استخدمنا مكاتب جاهزة منها(os,json,base64,datetime)

ومكاتب تم تثبتها (pycryptodome)

وتم اظهار النتائج على cmd

. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Aliibrahim99hz@gmail.com

.. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Ammarspeeh@gmail.com

1. ملفات تعريف الارتباط"cookies "

لملفات تعريف الارتباط وظائف كثيرة نذكر من أهمها:

- تذكر المستخدم عند تسجيل الدخول من جديد وعدم طلب الايميل او كلمة المرور
- تتبع سلوك المستخدمين على الانترنت
- يمكن حظر استخدامها في معظم متصفحات الويب الحالية
- جميع المعلومات المقدمة مجهولة المصدر (على سبيل المثال ما هو متصفح الويب الذي تستخدمه واسم المجال و **ISP** الخلص بك)
- مراقبة استخدام المواقع من قبل المستخدم وهذا يسمح بتحسين خدمات المواقع

ومن اجل توجيه الإعلانات للفئات المحددة

وذلك يحد من عدد الإعلانات التي تظهر لك اثناء تصفح المواقع

لا يمكنها الوصول الى ملفات الجهاز الخاصة والاضرار بالجهاز

1.1 يوجد أنواع من ملفات تعريف الارتباط تختلف عن بعضها بالوظائف:

Strictly necessary cookies- وهي ملفات تعريف الارتباط الضرورية للغاية لتصحيح سير عمل المواقع حيث تسمح للمستخدم بالوصول الى ملفات صفحات تسجيل الدخول الامنة,استخدام عربة التسوق ,المدفوعات عبر الانترنت

Analytical/performance cookies ملفات تعريف الارتباط التحليلية/الخاصة تسمح بتحديد زوار مواقع الويب وتحليل استخدامهم مما يساعد على تحسن المواقع بالإضافة الى العثور على المعلومات ذات الصلة بك في وقت سريع

Functionality cookies تستخدم ملفات تعريف الارتباط الوظيفية لتحديد هوية المستخدم عند عودته مرة أخرى مما يتيح للموقع تخصيص المحتوى الخاص بالمستخدم مثلا تذكر اللغة

Targeting cookies:تستخدم لاخبارنا بصفحات الويب التي قمت لاستعراضها و الروابط التي نقرت عليها

. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

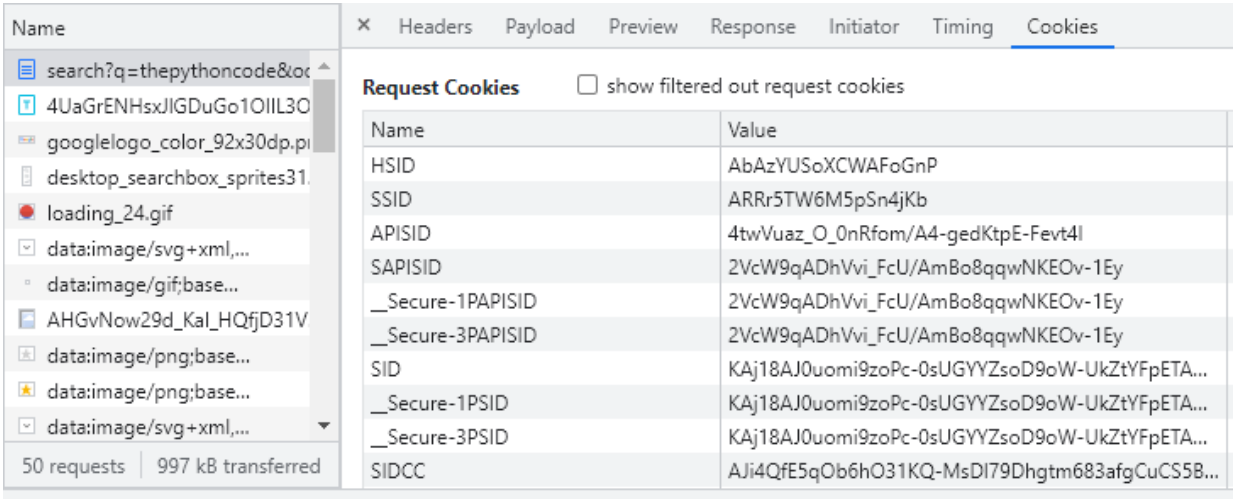
Aliibrahim99hz@gmail.com

.. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Ammarspeeh@gmail.com

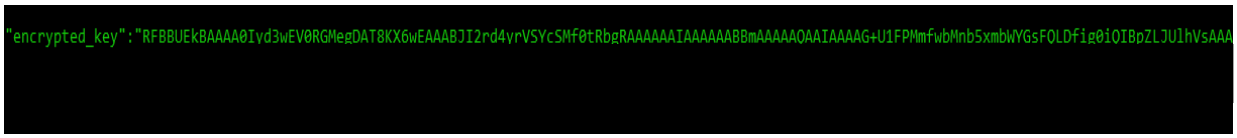
2.1 كيف يتعامل google chrome مع هذه المعلومات وأين يخزنها :

يتعامل google chrome مع عمليات بحث المستخدم حيث انه في كل عملية بحث عن صفحة ما يرسل اكثر من طلب لجلب روابط صور بيانات تسجيل دخول و الكثير من المعلومات كل طلب من هذه الطلبات له name cookies خاصة به و value cookies



في ملف cookies.db يتم تخذين اسم الموقع و تاريخ بدء الجلسة وتاريخ انتهائها و name cookies و value cookies بالإضافة ل لقيمة ال value لكن مشفرة بتشفير AES ومن خلالها نحصل على VALUE في حال عدم وجودها

ومن اجل فك تشفير value نحتاج الى إيجاد مفتاح التشفير الموجود في ملف local state



مفتاح التشفير الموجود في ملف الlocal state يكون مشفر وفق base64

1.2.1 Base64:

يتم استخدام ترميز Base64 لتحويل وحدات البايت التي تحتوي على بيانات ثنائية أو نصية إلى أحرف ASCII
يمنع التشفير البيانات من التلف عند نقلها أو معالجتها من خلال نظام نصي فقط.
سنناقش تشفير وفك تشفير Base64 واستخداماته لترميز وفك تشفير البيانات الثنائية والنصية
ترميز Base64:
إنه نوع من تحويل البايت إلى أحرف ASCII
قائمة أحرف Base64 المتاحة مذكورة أدناه:
٢٦ حرفًا كبيرًا
٢٦ حرفًا صغيرًا
١٠ أرقام
+ و / للخطوط الجديدة
يمثل كل حرف Base64 6بتات من البيانات. من المهم أيضًا ملاحظة أنه لا يُقصد به التشفير لأسباب واضحة

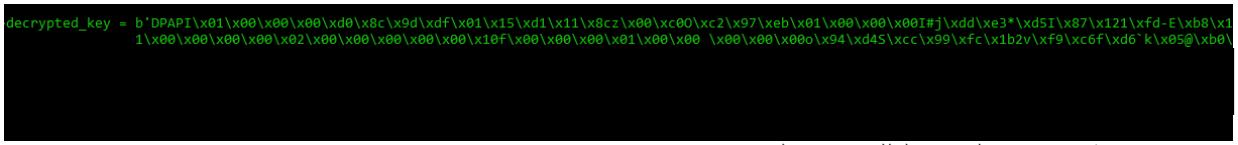
. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
Aliibrahim99hz@gmail.com
.. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
Ammarspeeh@gmail.com

2.2.1 لتحويل سلسلة إلى حرف Base64 ، يجب اتباع الخطوات التالية:

احصل على قيمة ASCII لكل حرف في السلسلة.
حساب المكافئ الثنائي ٨ بت لقيم ASCII
قم بتحويل مجموعة الأحرف المكونة من ٨ بتات إلى أجزاء من ٦ بتات عن طريق إعادة تجميع الأرقام
قم بتحويل المجموعات الثنائية ذات ٦ بتات إلى القيم العشرية الخاصة بها.
استخدم جدول ترميز Base64 لمحاذاة قيم Base64 ذات الصلة لكل قيمة عشرية.
توفر لنا الصورة أدناه جدول تشفير Base64.

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/

استخدام python لتشفير السلاسل:
في Python ، تُستخدم الوحدة النمطية base64 لتشفير البيانات وفك تشفيرها
أولاً ، يتم تحويل السلاسل إلى كائنات تشبه البايت ثم يتم تشفيرها باستخدام وحدة base64
يوضح الصورة التالية مفتاح التشفير الأصلي "بعد فك تشفيره"



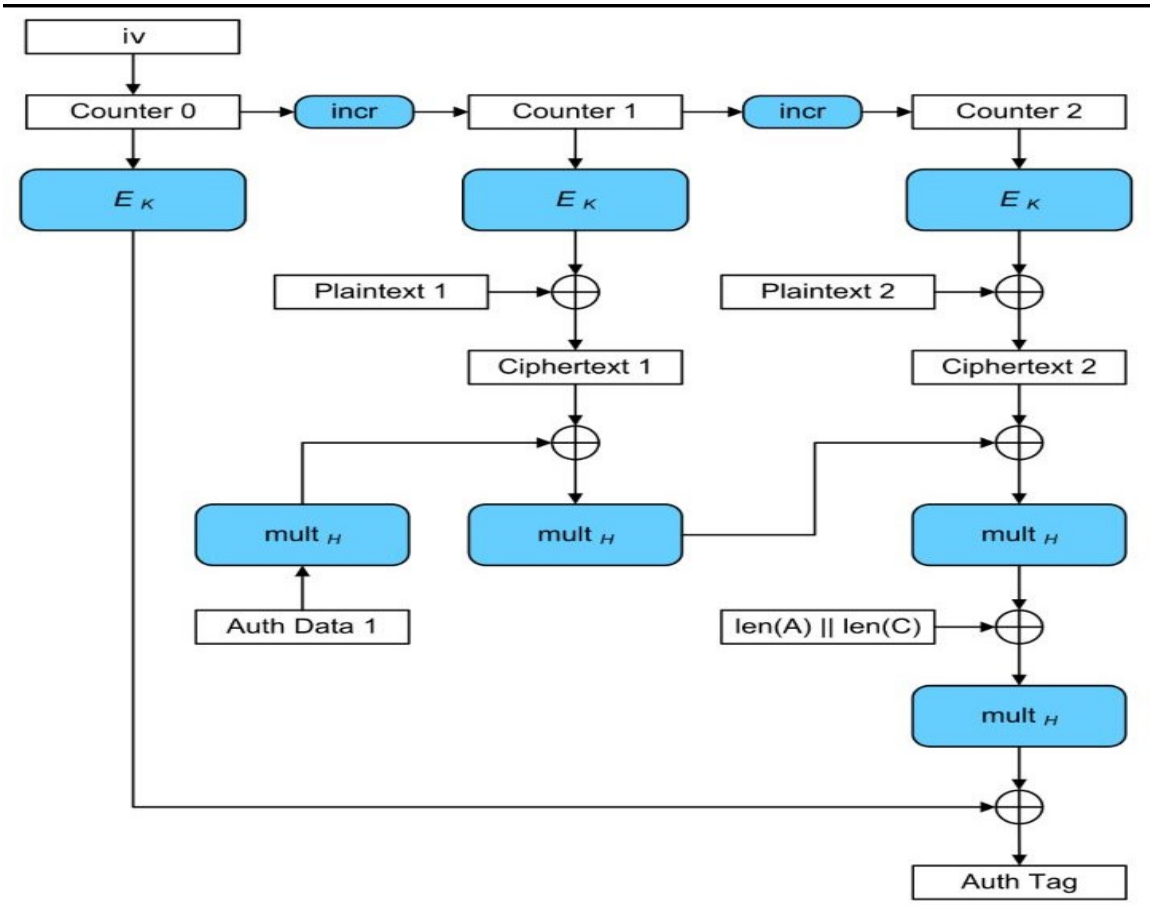
القيم DPAPI ثابتة في جميع المفاتيح لذلك يتم اهمالها

. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
Aliibrahim99hz@gmail.com
.. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
Ammarspeeh@gmail.com

3.1 ملفات ال cookies لمستخدم google chrome تستخدم تشفير AES-256 لتشفير cookies value

1.3.1 AES-256:

كما هو الحال في وضع العداد العادي يتم ترقيم الكتل بالتسلسل ثم يتم دمج رقم الكتلة مع متجه التهيئة iv ويتم تشفيره باستخدام block cipher E يتم بعد ذلك استخدام XORed لنتيجة التشفير مع النص العادي لانتاج النص المشفر



2.3.1 مثال على قيمة value مشفرة ب AES265

```
encrypted_value = b'v10\xaf\xae\x9af\x8c=\xa0b<\x93d\xecs!cV\x1a\xa2\xcb\xa9\xd3\xaba\xc6^\x1c\xa5\xb5FJ\xec{\xa7?F\xae\xbb\xccL\x8e'
```


. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Aliibrahim99hz@gmail.com

.. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Ammarspeeh@gmail.com

لفك هذا النص المشفر لدينا مفتاح التشفير الأصلي المستخرج من local state

القيم v10 ثابتة في جميع بيانات المشفرة لcookies value

initialization vector قيمه من ٣ حتى ١٥ من encrypted_value والقيم المتبقية تمثل ال data الحقيقية

نطبق AES-256 على مفتاح التشفير و initialization vector فينتج ما يسمى ب cipher وهي بمثابة مفتاح خاص

مطبقه على ال data فينتج القيمة الاصلية

```
Cookie value (decrypted): hO6g6LHRWglA
```

مثال يوضح المعلومات التي حصلنا عليها من اجل هذه القيمة

```
Host: .contextweb.com
Cookie name: V
Cookie value (decrypted): hO6g6LHRWglA
Creation datetime (UTC): 2022-03-14 05:42:28.889660
encrypted_value = b'v10\xaf\xae\x9af\x8c=\xa0b<\x93d\xecs!cV\x1a\xa2\xcb\xa9\xd3\xaba\xc6^\x1c\xa5\xb5FJ\xec{\xa7?F\xae\xbb\xccL\x8e'
Last access datetime (UTC): 2022-05-04 15:51:59.660063
Expires datetime (UTC): 4769-11-16 09:46:39.999999
================================================================
```


- طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Aliibrahim99hz@gmail.com

.. طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Ammarspeeh@gmail.com

2. ملفات password لمستخدم google chrome تستخدم تشفير AES-256 لتشفير password

1.2 مثال على ذلك

```
encryptedrow_password b'v10\xe4\xb8\xf9\x0ex\x1e\x1e\xba\xfa\x16\r\x86h\t\'B"\xe9\xc4\xf1qMj~\xe8\xbf\xd5g\x95Xw\xb6<b\xc0{'
```

لفك هذا النص المشفر لدينا مفتاح التشفير الأصلي المستخرج من local state

القيم v10 ثابتة في جميع بيانات المشفرة لcookies value

initialization vector قيمه من ٣ حتى ١٥ من encrypted_value والقيم المتبقية تمثل ال data الحقيقية

نطبق AES-256 على مفتاح التشفير و initialization vector فينتج ما يسمى ب cipher وهي بمثابة مفتاح خاص

مطبقه على ال dataفينتج القيمة الاصلية

```
Password: AAaa1122
```

مثال يوضح المعلومات التي حصلنا عليها من اجل هذه القيمة

```
Origin URL: http://23.226.22.178:29842/
Action URL:
Username: jwalla01
encrypted_password: b'v10\xe4\xb8\xf9\x0ex\x1e\x1e\xba\xfa\x16\r\x86h\t\'B"\xe9\xc4\xf1qMj~\xe8\xbf\xd5g\x95Xw\xb6<b\xc0{'
Password: AAaa1122
Creation date: 2022-03-09 17:07:42.918223
Last Used: 2022-03-09 17:07:37.729680
==========================================
```

• طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Aliibrahim99hz@gmail.com

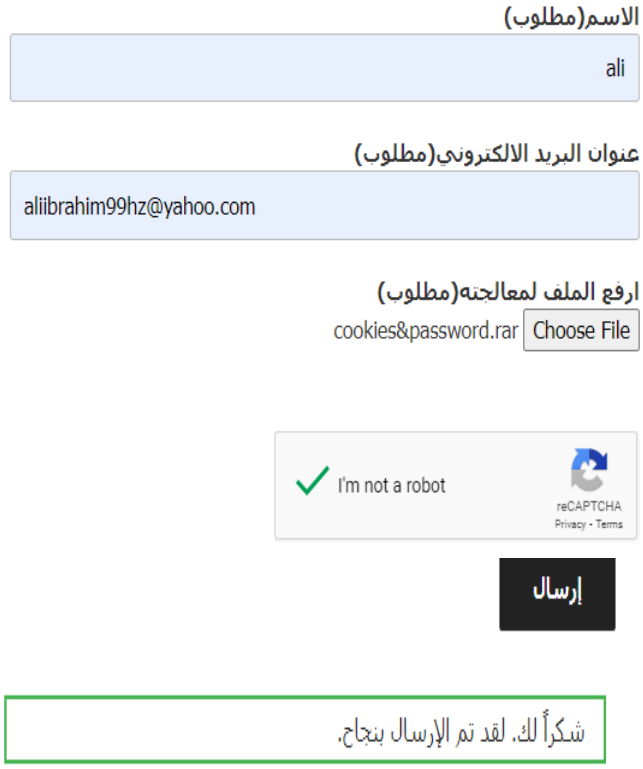
•• طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

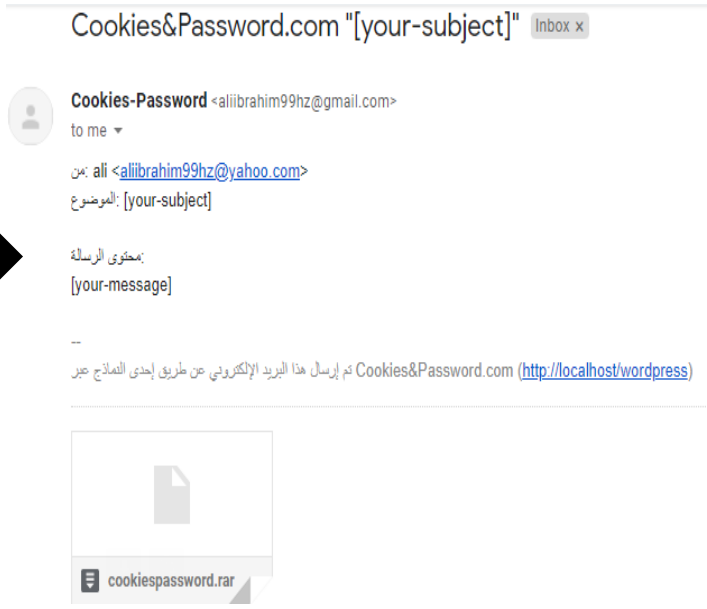
Ammarspeeh@gmail.com

3. Cookies&Password in Wordpress

اطلاقا من أهمية هذا المشروع في مساعدة مستخدمين google chrome تم امشاء موقع الكتروني مبني باستخدام الwordpress

1.3 عند الخول الى الموقع يظهر لك تعليمات عليك اتباعها ومن ثم ملئ هذا النموذج





• طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
Aliibrahim99hz@gmail.com
•• طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
Ammarspeeh@gmail.com

4. المشاكل والحلول:

عند محاولة ارسال أي رسالة عبر النموذج يظهر الخطأ التالي

الحل:

إضافة WP mail smtp وتمكين الوصول بين الإضافة و google developer consol

- **طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا**

Aliibrahim99hz@gmail.com

- **طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا**

Ammarspeeh@gmail.com

References:

[1] **Thepythoncode.com**

https://www.thepythoncode.com/article/extract-chrome-cookies-python

[2] **Thepythoncode.com**

https://www.thepythoncode.com/article/extract-chrome-passwords-python

[3] **stackoverflow.com**

https://stackoverflow.com/questions/55729726/python-how-to-use-chrome-cookies-in-requests

[4] Distinguisher and Related-Key Attack on the Full AES-256

https://link.springer.com/chapter/10.1007/978-3-642-03356-8_14

[5] **stackabuse.com**

https://stackabuse.com/encoding-and-decoding-base64-strings-in-python/

Github.com

https://github.com/Alih99z/cookies-and-password

• طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Aliibrahim99hz@gmail.com

•• طالب، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

Ammarspeeh@gmail.com