Tipos de ataques,

cómo actúan los piratas informáticos

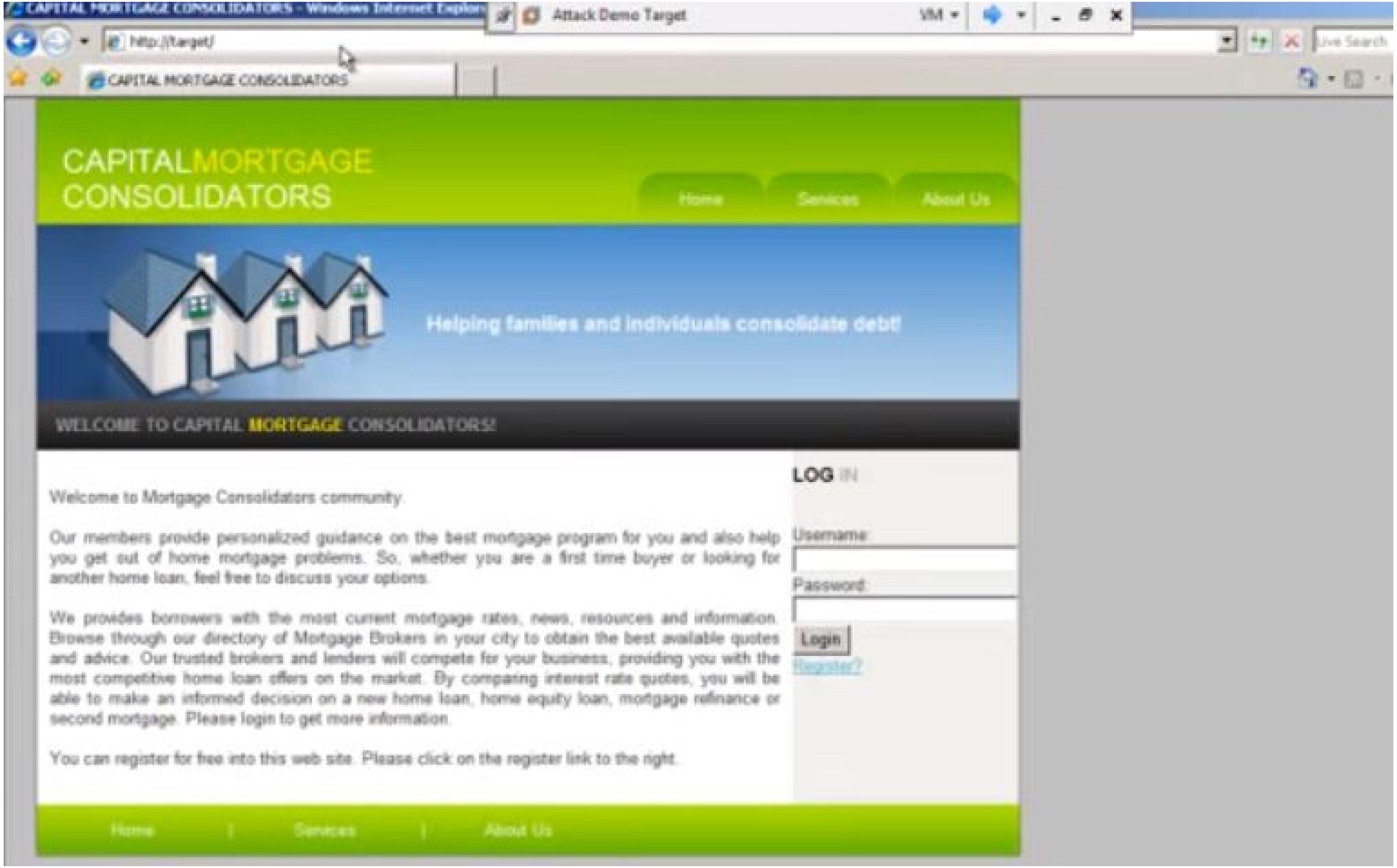
Emilio Aparicio Benítez

Ataque por Inyección

Ataque por Inyección / SQL injection

SQL Injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.


CAPITAL MORTGAGE CONSOLIDATORS - Windows Internet Explor
Attack Demo Target
VM
http://target/
CAPITAL MORTGAGE CONSOLIDATORS
Live Search
Home
Services
About Us

CAPITALMORTGAGE CONSOLIDATORS

Helping families and individuals consolidate debt!

WELCOME TO CAPITAL MORTGAGE CONSOLIDATORS!

Welcome to Mortgage Consolidators community.

Our members provide personalized guidance on the best mortgage program for you and also help you get out of home mortgage problems. So, whether you are a first time buyer or looking for another home loan, feel free to discuss your options.

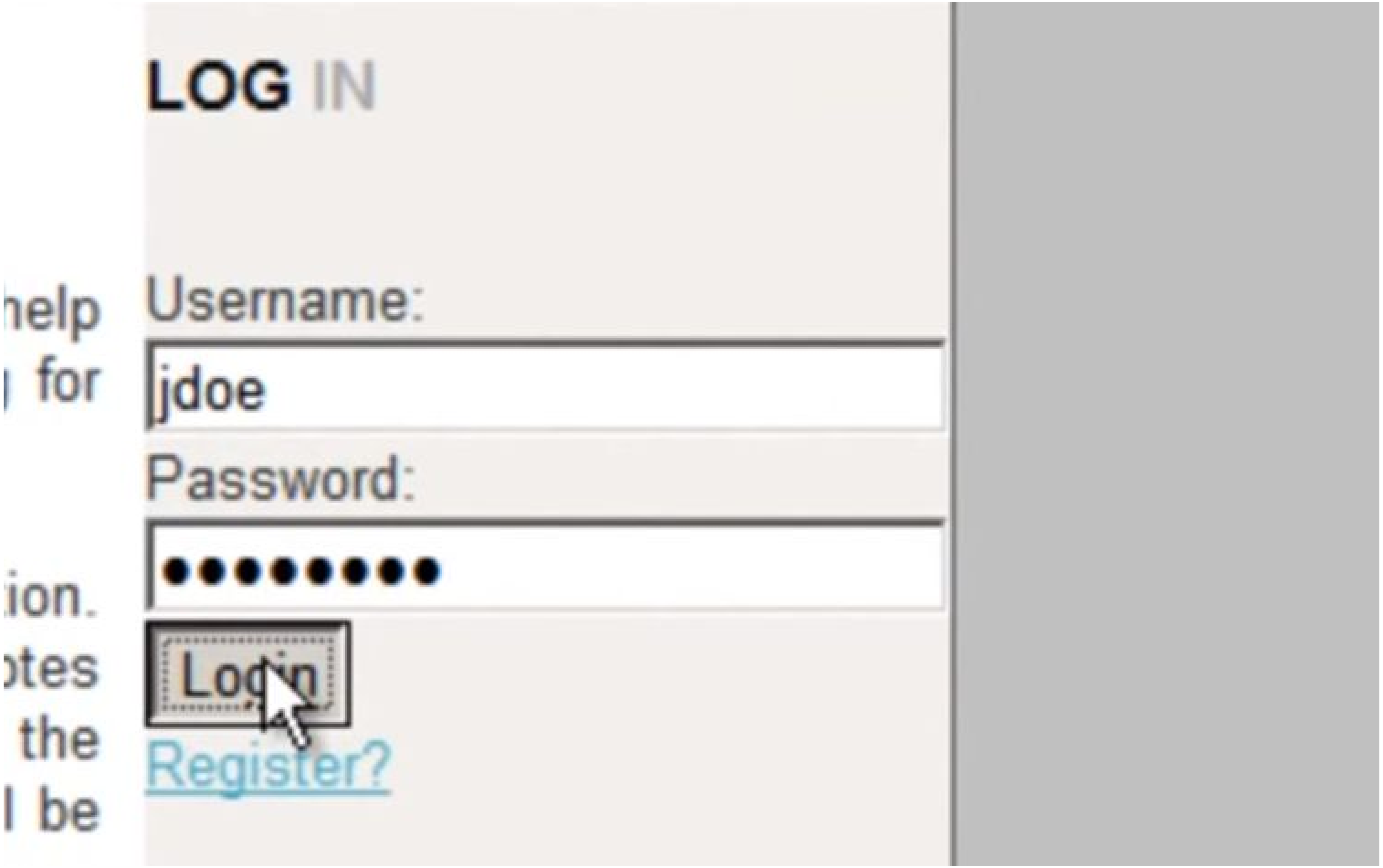
We provides borrowers with the most current mortgage rates, news, resources and information. Browse through our directory of Mortgage Brokers in your city to obtain the best available quotes and advice. Our trusted brokers and lenders will compete for your business, providing you with the most competitive home loan offers on the market. By comparing interest rate quotes, you will be able to make an informed decision on a new home loan, home equity loan, mortgage refinance or second mortgage. Please login to get more information.

You can register for free into this web site. Please click on the register link to the right.

LOG IN

Username:

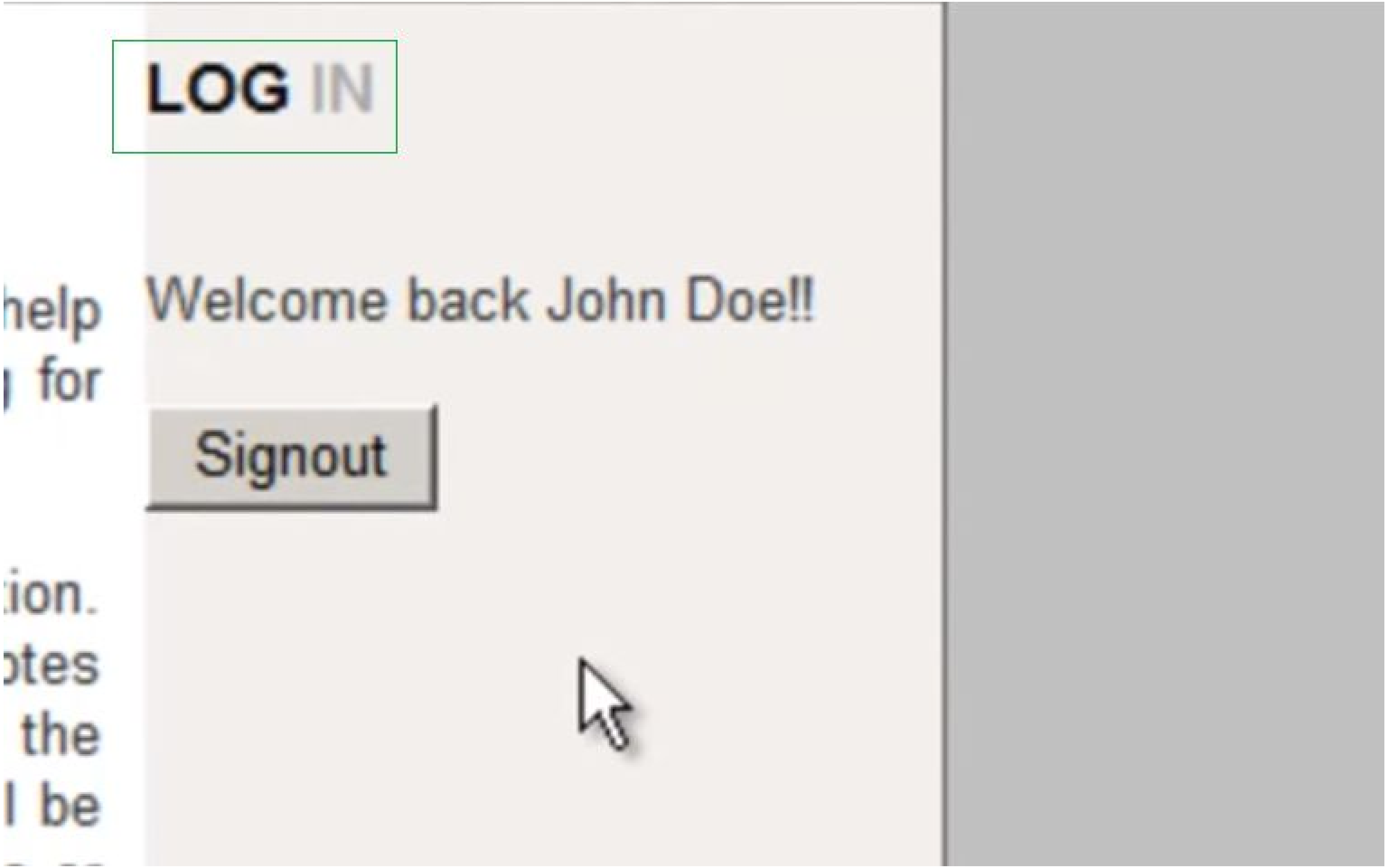
Password:



LOG IN

Username: jdoe

Password: ●●●●●●●●●



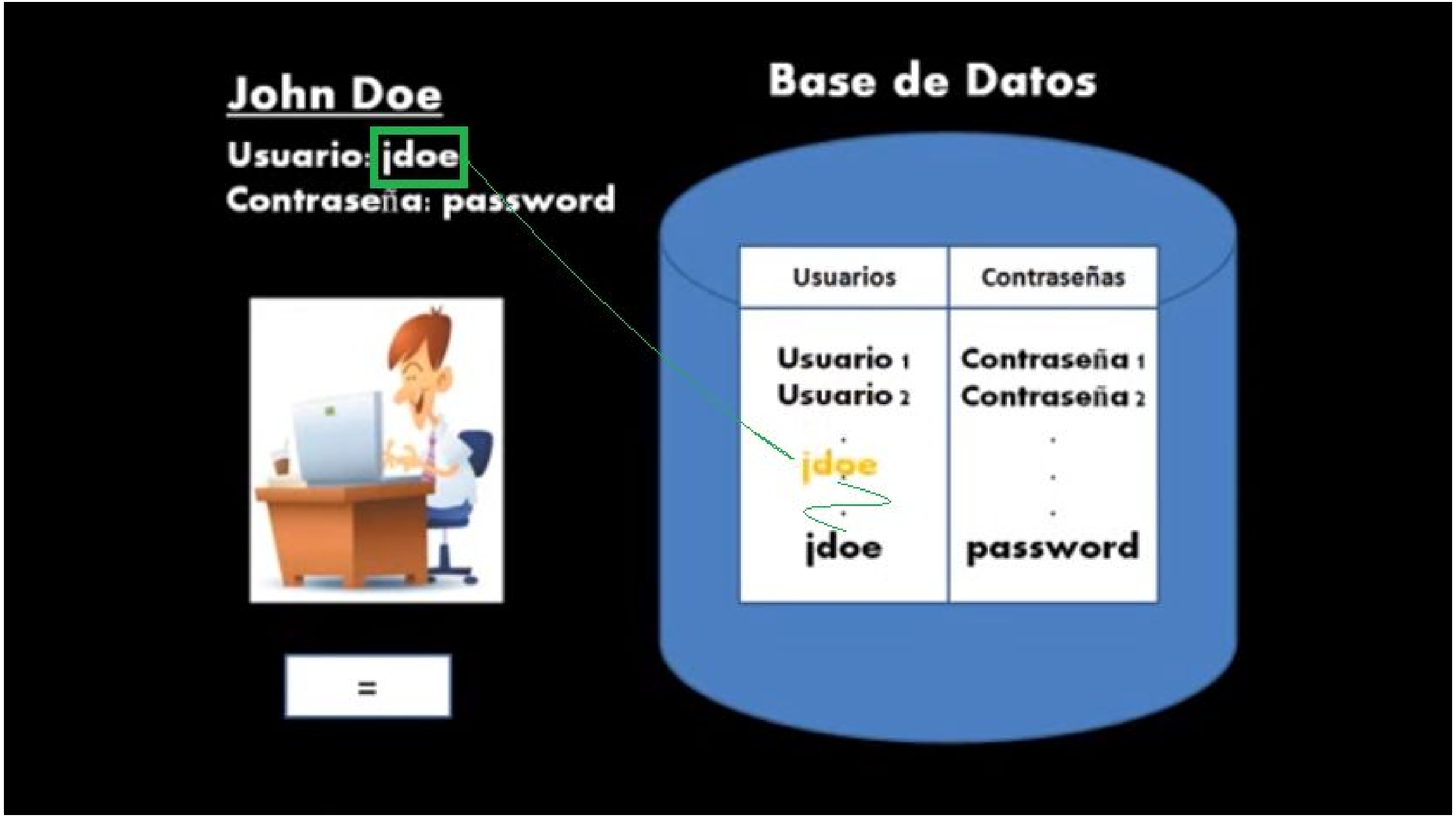
LOG IN

help
for

ion.
otes
the
l be

Welcome back John Doe!!

PASO 1 : AUTENTICACIÓN



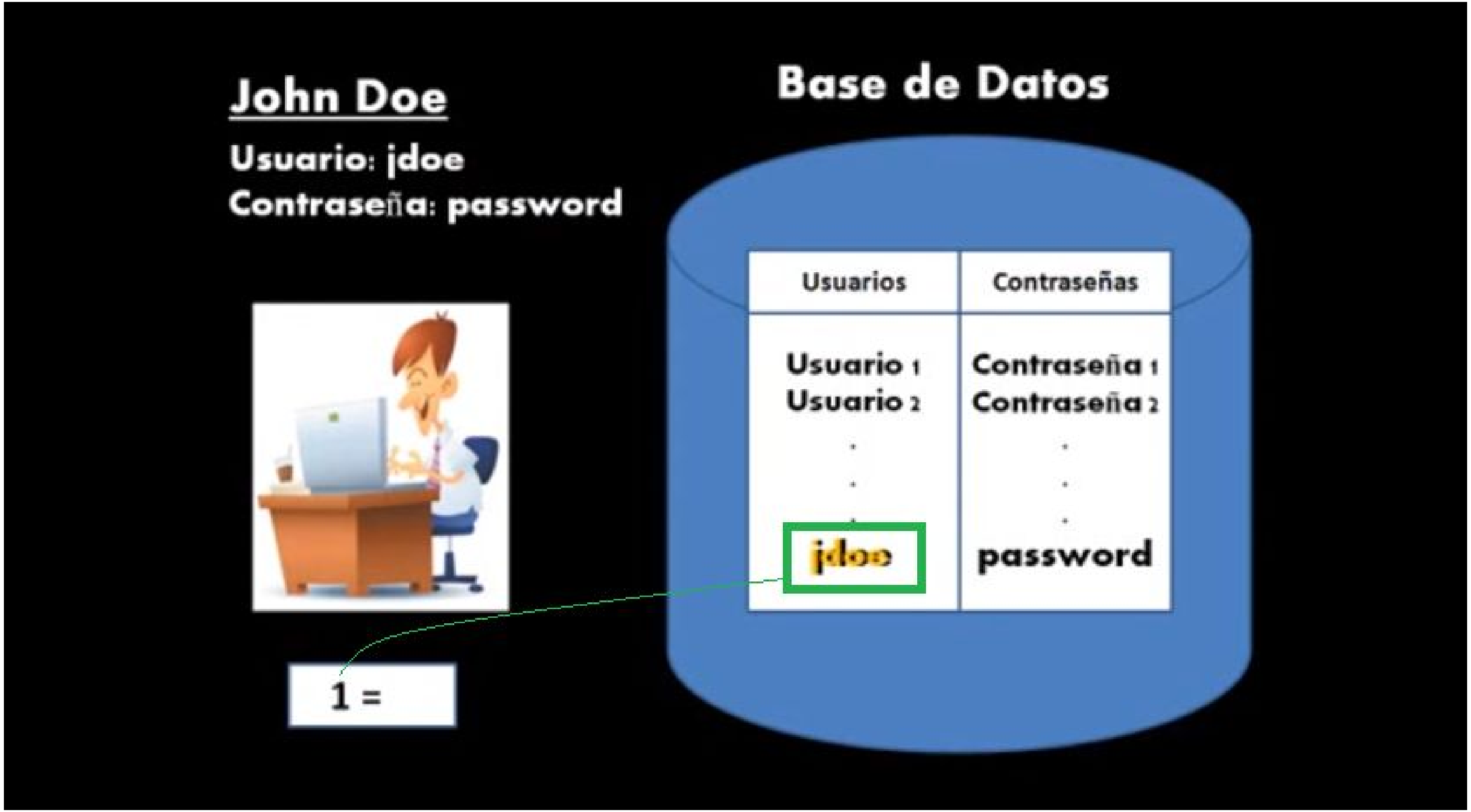
John Doe

Usuario: jdoe

Contraseña: password

Usuarios	Contraseñas
Usuario 1	Contraseña 1
Usuario 2	Contraseña 2
.	.
jdoe	.
.	.
jdoe	password

PASO 1 : AUTENTICACIÓN



John Doe

Usuario: jdoe

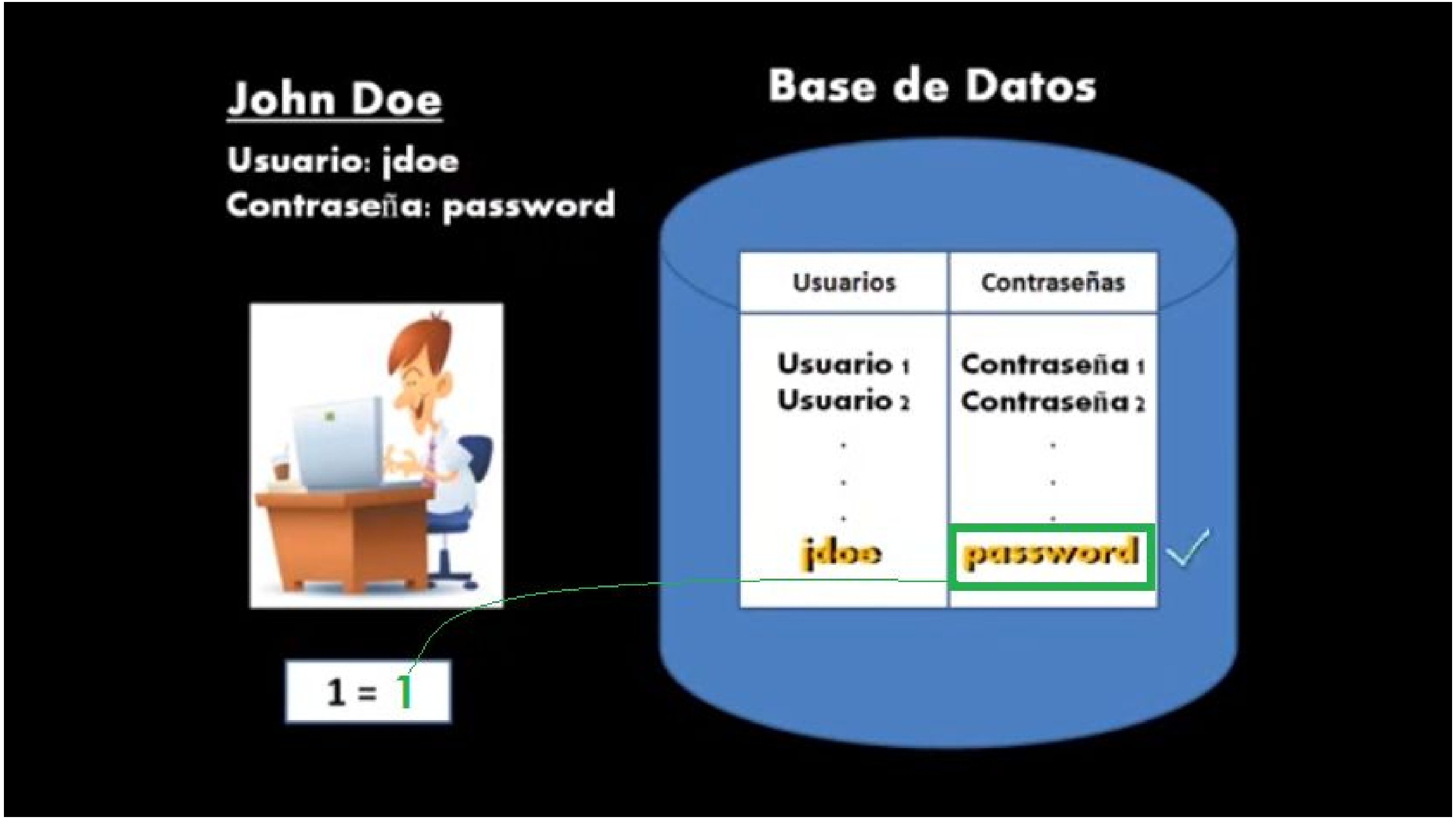
Contraseña: password

Base de Datos

Usuarios	Contraseñas
Usuario 1 Usuario 2 . . . jdoe	Contraseña 1 Contraseña 2 . . . password

1 =

PASO 1 : AUTENTICACIÓN



John Doe

Usuario: jdoe

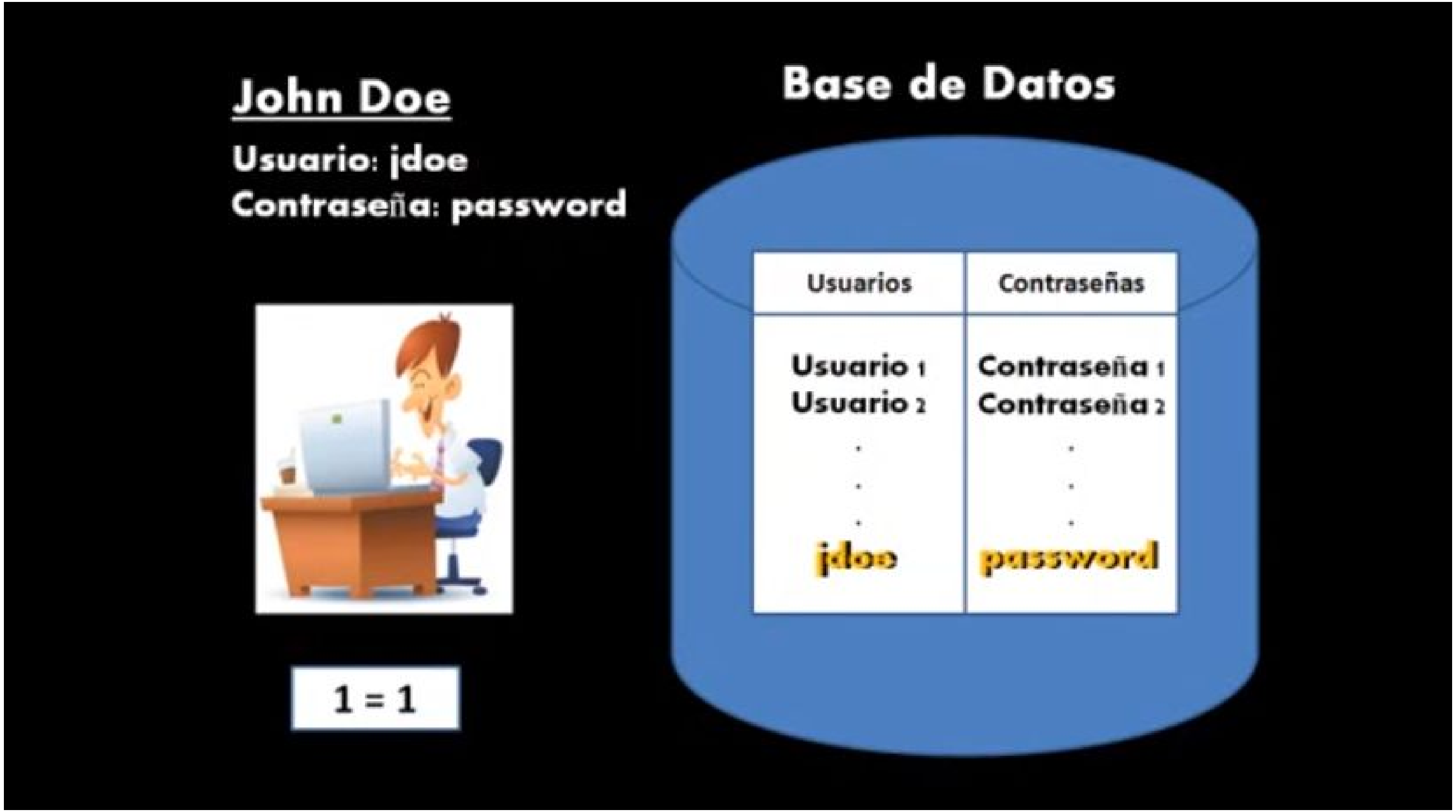
Contraseña: password

Base de Datos

Usuarios	Contraseñas
Usuario 1	Contraseña 1
Usuario 2	Contraseña 2
.	.
.	.
.	.
jdoe	password ✓

1 = 1

PASO 1 : AUTENTICACIÓN



John Doe

Usuario: jdoe

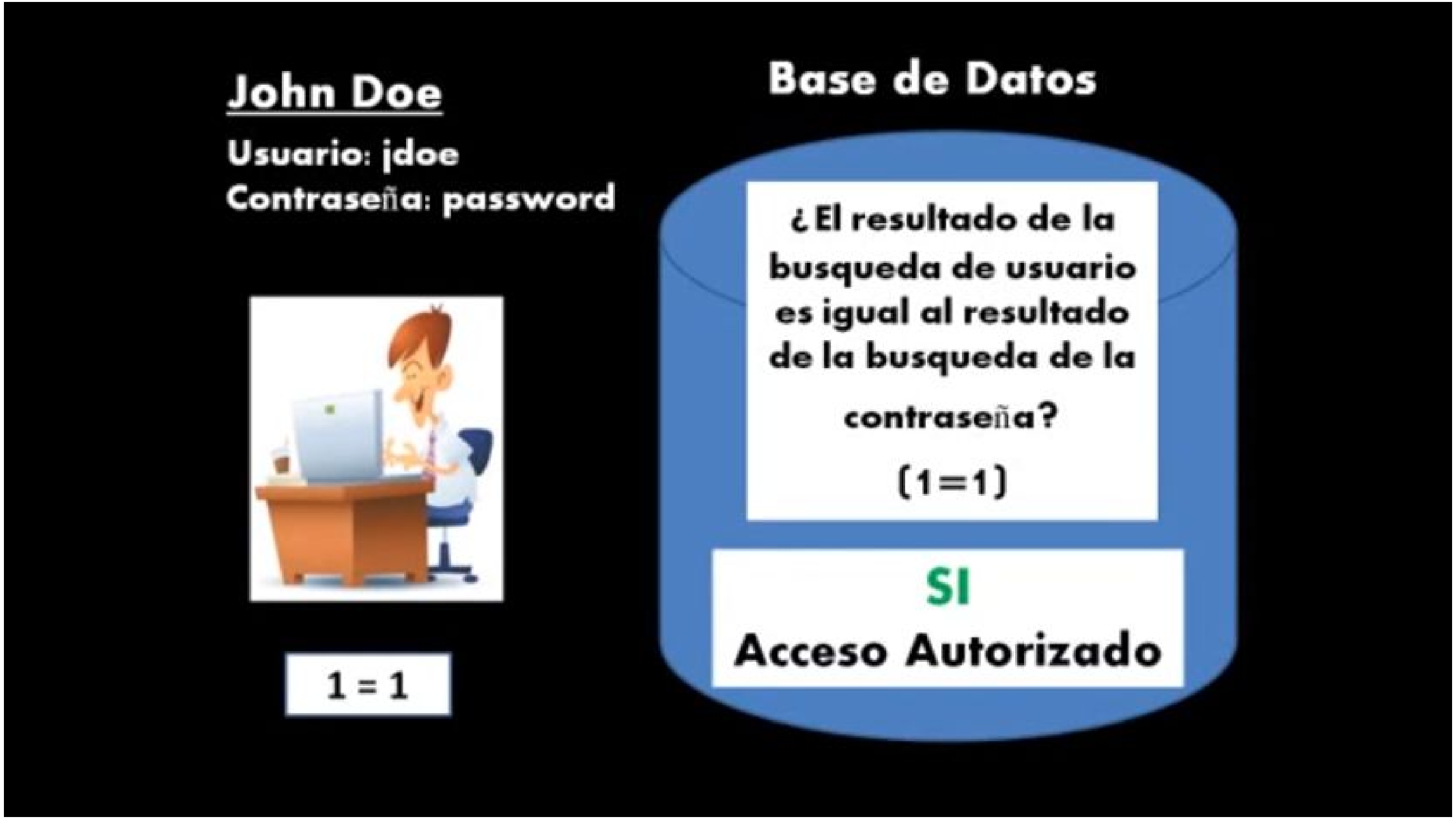
Contraseña: password

1 = 1

Base de Datos

Usuarios	Contraseñas
Usuario 1	Contraseña 1
Usuario 2	Contraseña 2
.	.
.	.
.	.
jdoe	password

PASO 2 : AUTORIZACIÓN



John Doe

Usuario: jdoe

Contraseña: password

1 = 1

Base de Datos

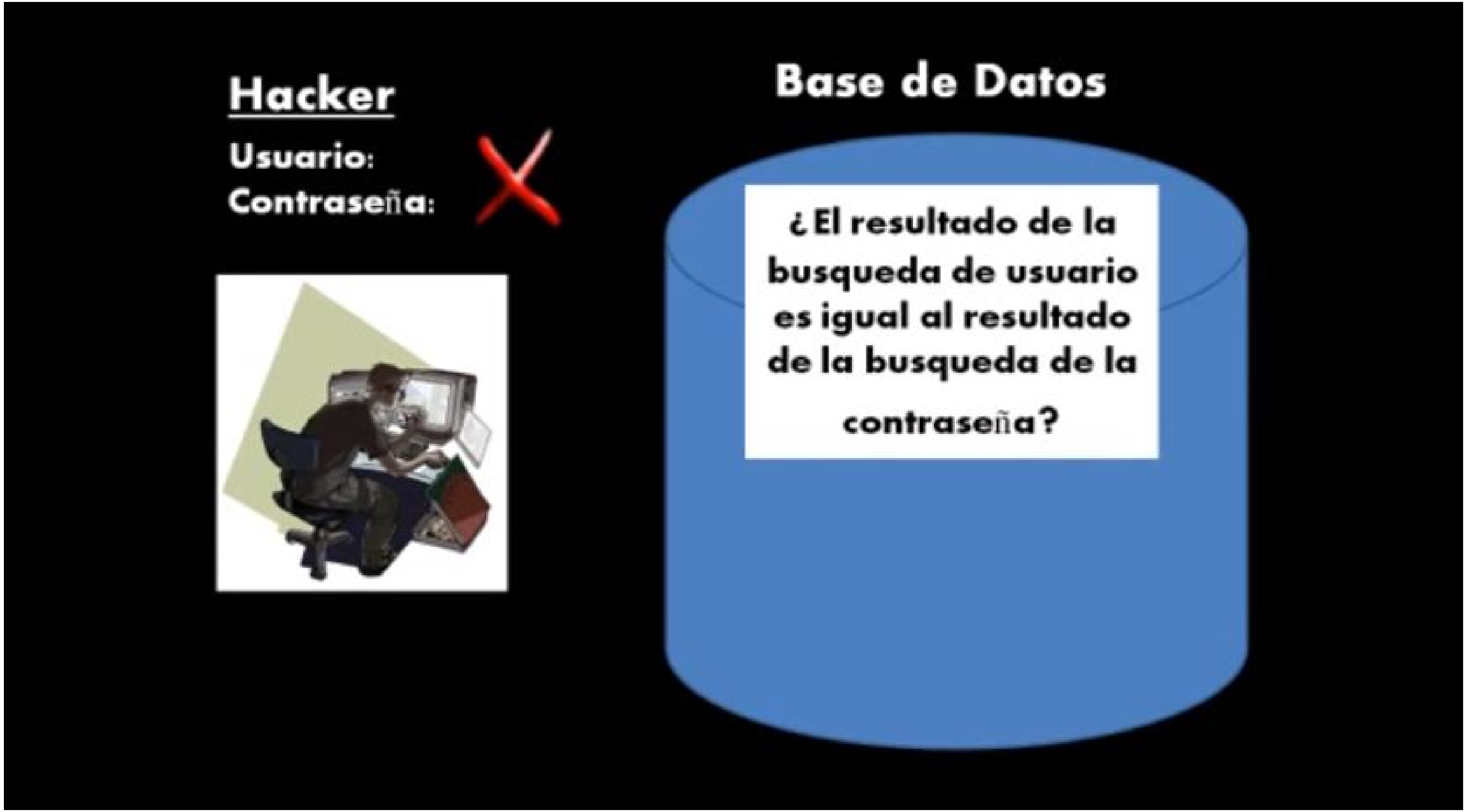
¿El resultado de la busqueda de usuario es igual al resultado de la busqueda de la contraseña?

(1=1)

SI

Acceso Autorizado

¿Qué hace un Hacker?



Hacker

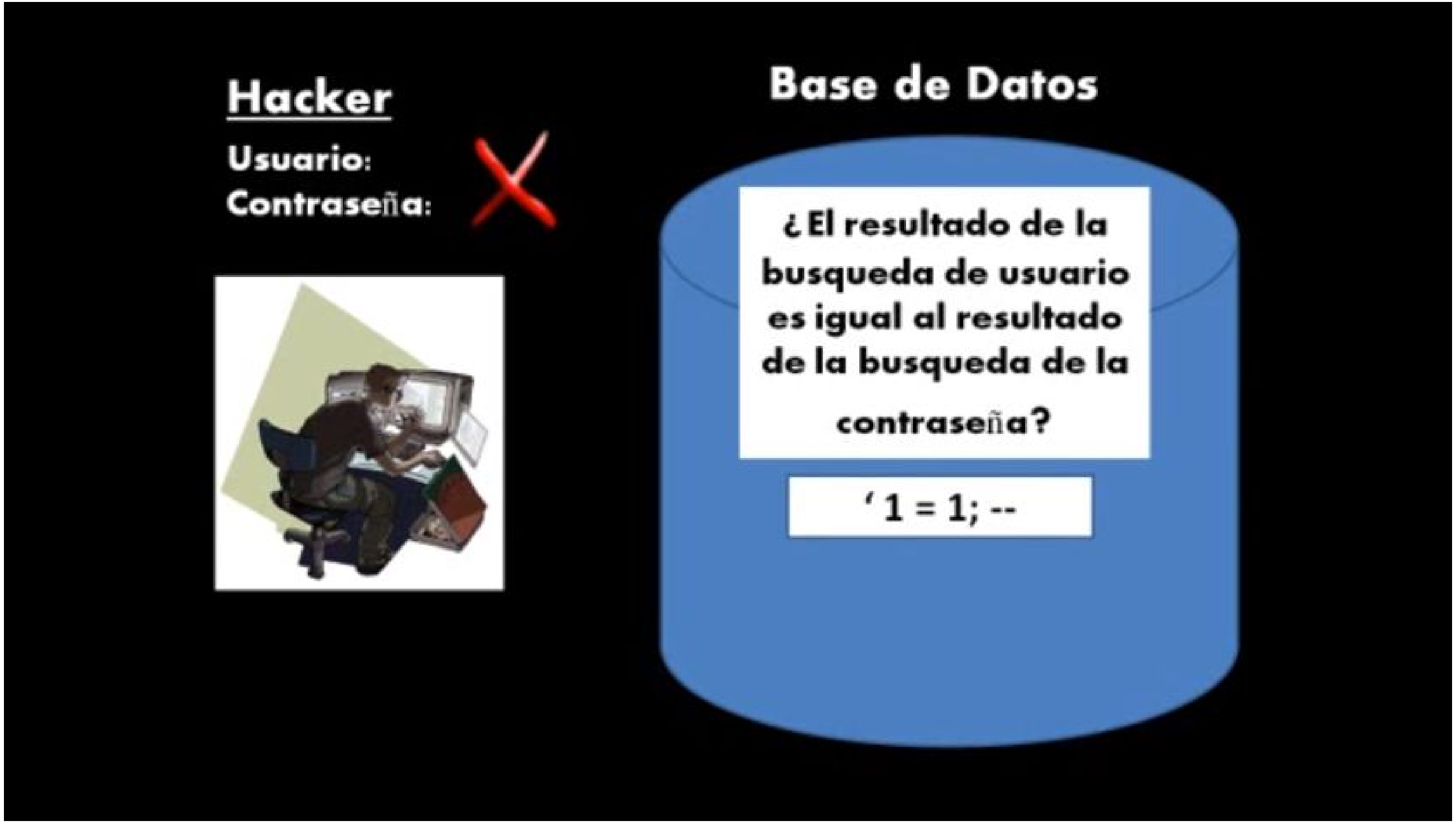
Usuario:

Contraseña:

Base de Datos

¿El resultado de la busqueda de usuario es igual al resultado de la busqueda de la contraseña?

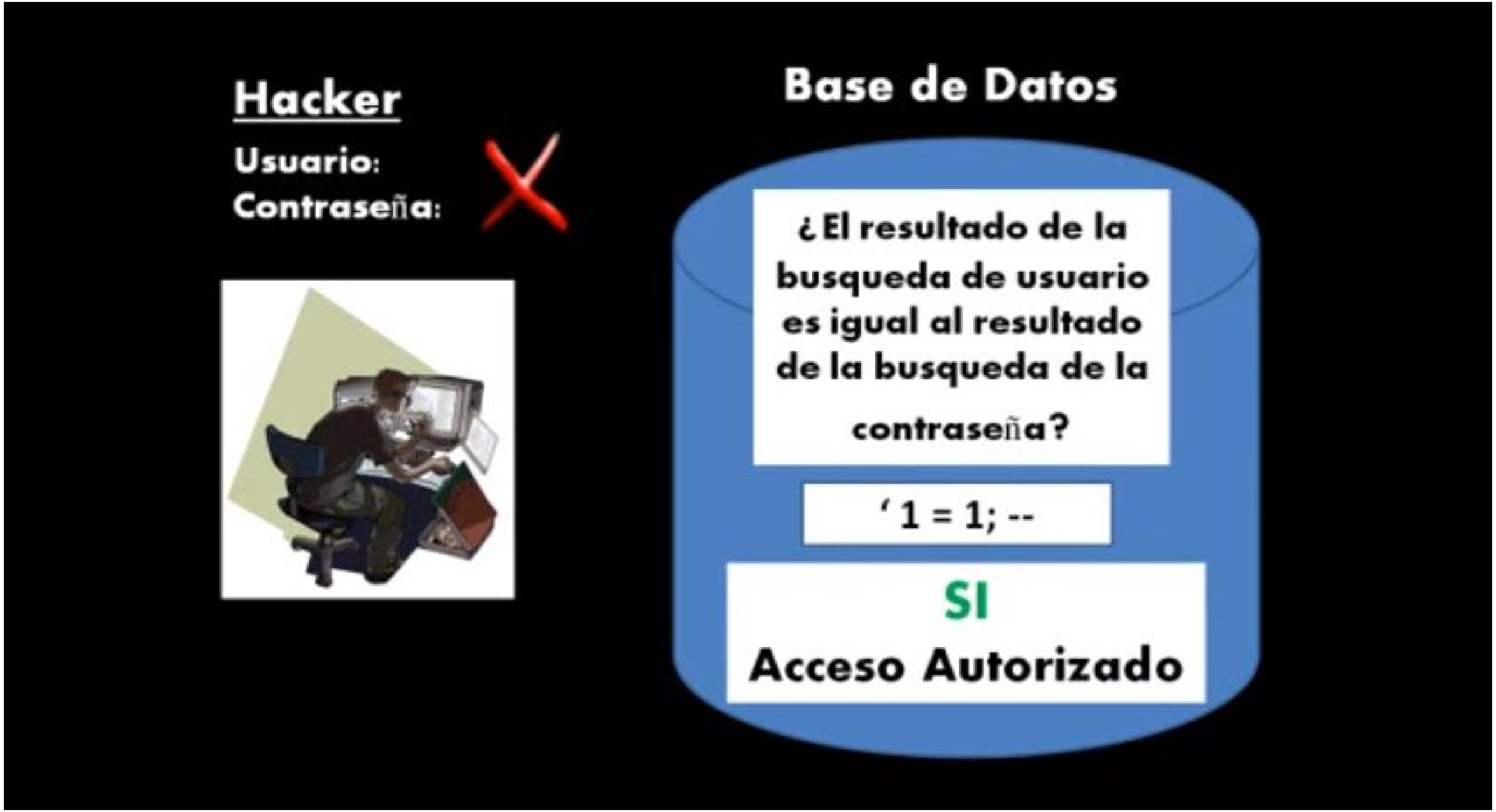
¿Qué hace un Hacker?



¿El resultado de la busqueda de usuario es igual al resultado de la busqueda de la contraseña?

```
' 1 = 1; --
```

¿Qué hace un Hacker?



Hacker

Usuario:

Contraseña:

Base de Datos

¿El resultado de la busqueda de usuario es igual al resultado de la busqueda de la contraseña?

‘1 = 1; --

SI

Acceso Autorizado

DDoS

DDoS:

In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

Hay 3 Variedades principales:

1. **Los ataques de volumen**, donde el ataque intenta desbordar el ancho de banda en un sitio específico.

2. **Los ataques de protocolo**, donde los paquetes intentan consumir servicios o recursos de la red.

3. **Ataques a aplicaciones**, donde las peticiones se hacen con la intención de “explotar” el servidor web, mediante la capa de aplicación.

10 NOV 2016

Así han atacado los ‘hackers’ las webs de Twitter, Spotify o Ebay

El incidente, que empezó en EE UU,
es el más grave de la última década

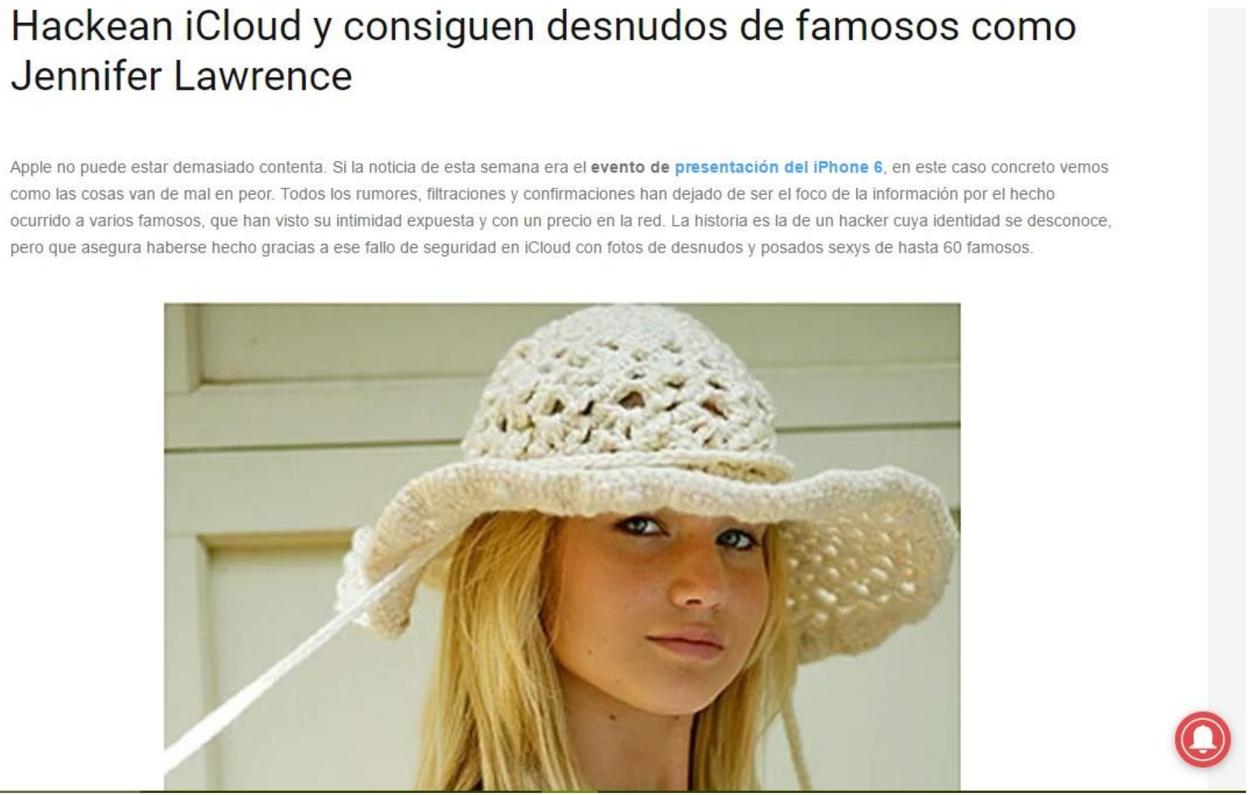
Fuerza bruta

Fuerza bruta / Brute Force Attack

In cryptography, a brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

A brute-force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier.

Ejemplo:

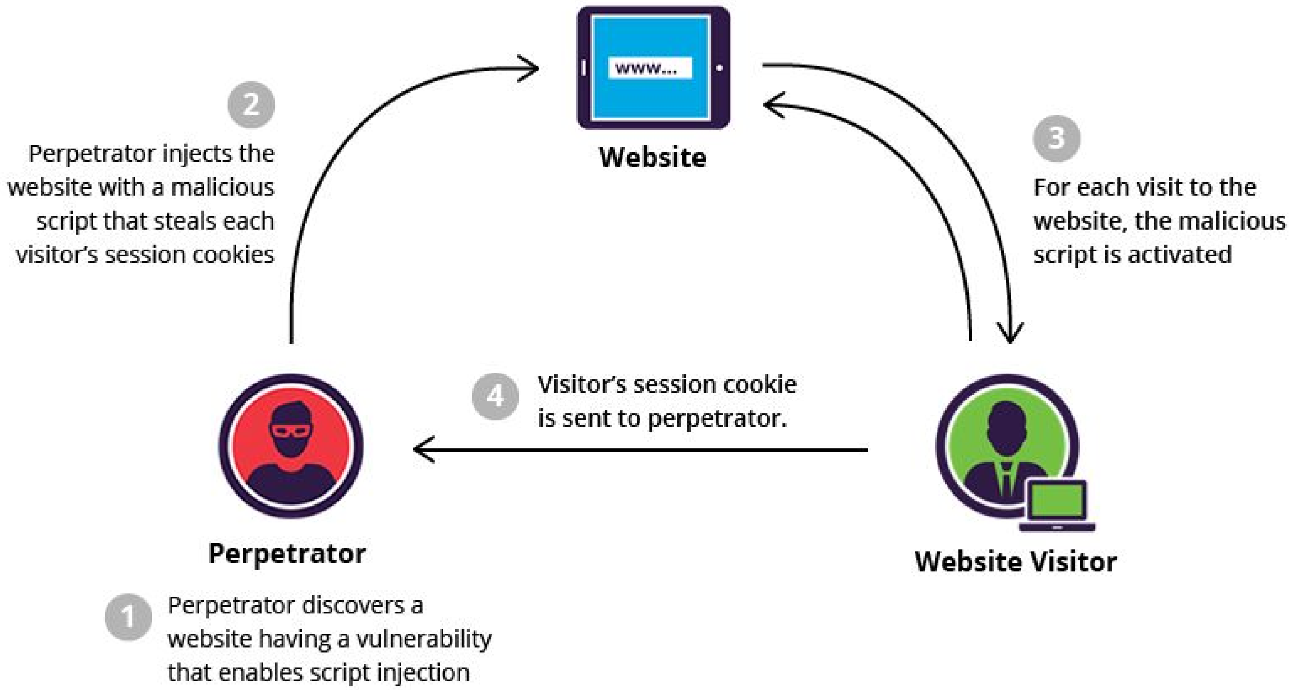


Hackean iCloud y consiguen desnudos de famosos como Jennifer Lawrence

Apple no puede estar demasiado contenta. Si la noticia de esta semana era el **evento de presentación del iPhone 6**, en este caso concreto vemos como las cosas van de mal en peor. Todos los rumores, filtraciones y confirmaciones han dejado de ser el foco de la información por el hecho ocurrido a varios famosos, que han visto su intimidad expuesta y con un precio en la red. La historia es la de un hacker cuya identidad se desconoce, pero que asegura haberse hecho gracias a ese fallo de seguridad en iCloud con fotos de desnudos y posados sexys de hasta 60 famosos.

Cross Site Scripting

Cross Site Scripting



1 Perpetrator discovers a website having a vulnerability that enables script injection

2 Perpetrator injects the website with a malicious script that steals each visitor's session cookies

3 For each visit to the website, the malicious script is activated

4 Visitor's session cookie is sent to perpetrator.

¿Por qué Hackean los sitios web?