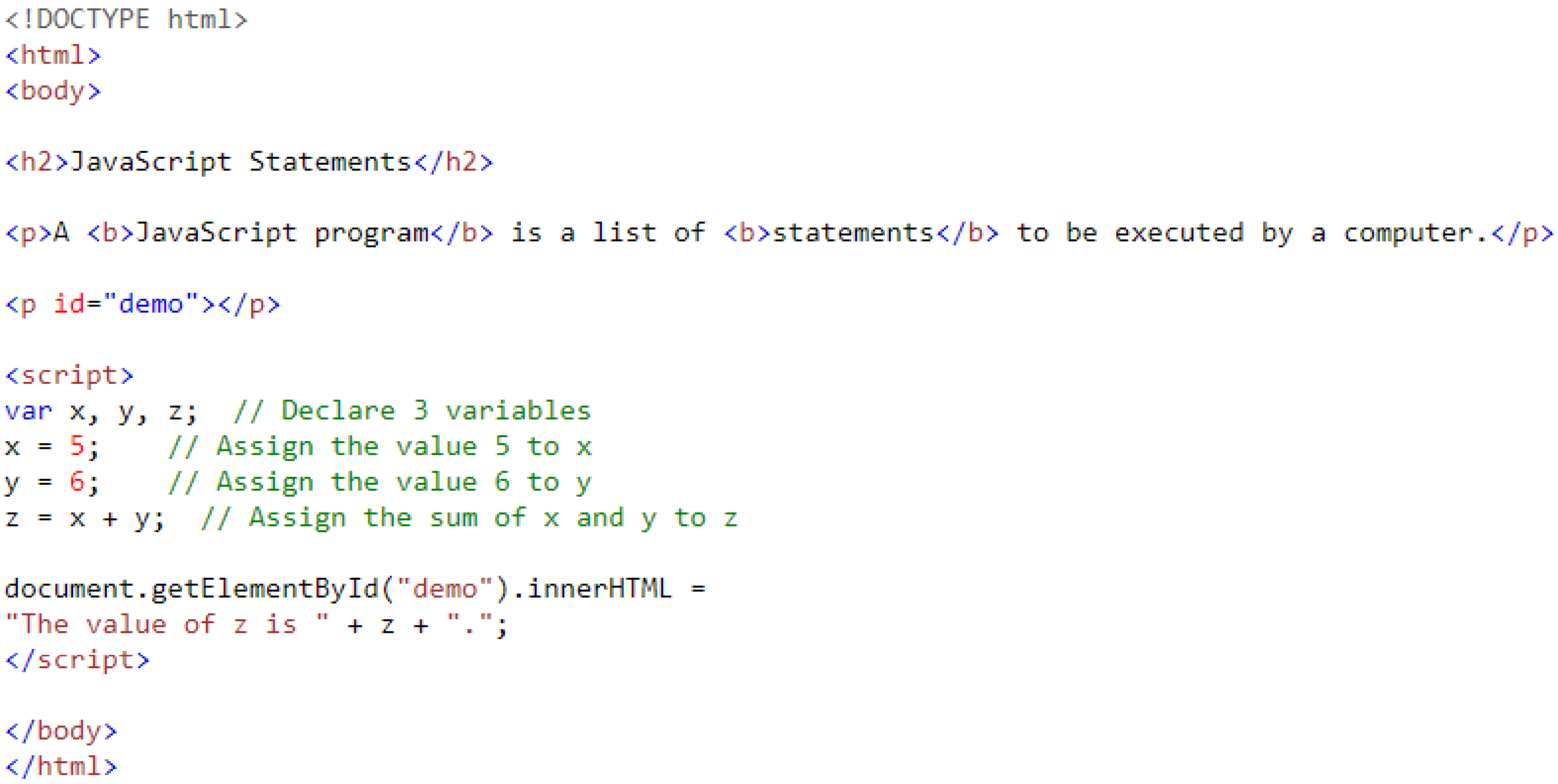
Javascript

JavaScript was initially created to *“make web pages alive”*.

Scripts are provided and executed as plain text. They don’t need special preparation or compilation to run.



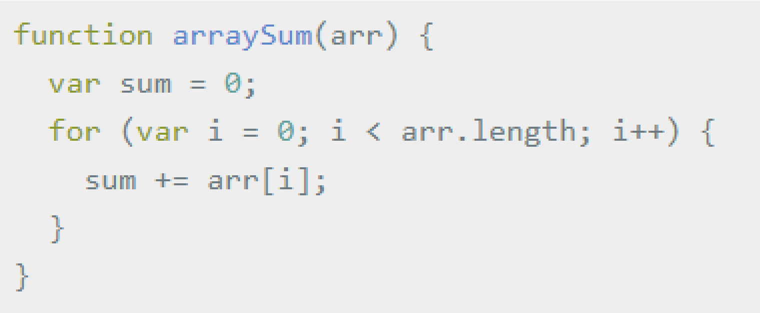
```
<!DOCTYPE html>
<html>
<body>

<h2>JavaScript Statements</h2>

<p>A <b>JavaScript program</b> is a list of <b>statements</b> to be executed by a computer.</p>

<p id="demo"></p>

<script>
var x, y, z;  // Declare 3 variables
x = 5;    // Assign the value 5 to x
y = 6;    // Assign the value 6 to y
z = x + y;  // Assign the sum of x and y to z

document.getElementById("demo").innerHTML =
"The value of z is " + z + ".";
</script>

</body>
</html>
```

https://www.w3schools.com/js/js_examples.asp

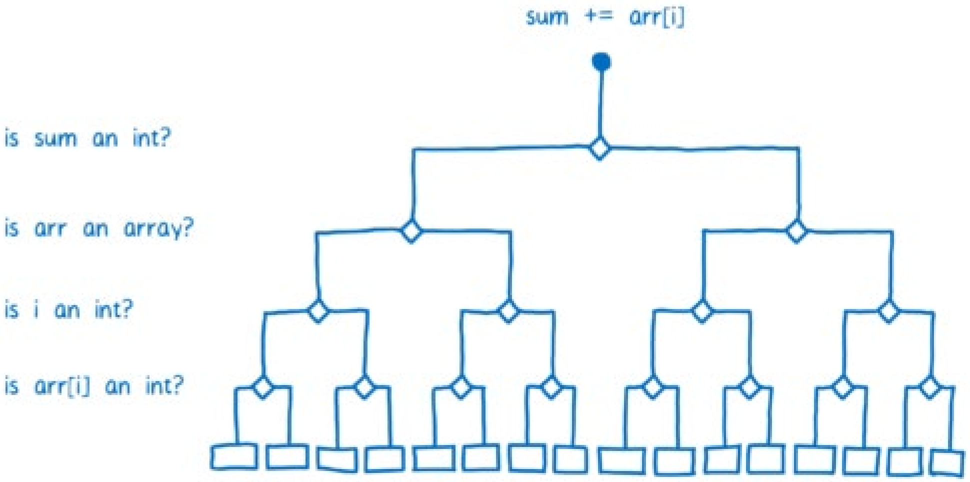
Javascript

Javascript è un linguaggio debolmente tipizzato

https://hacks.mozilla.org/2017/02/a-crash-course-in-just-in-time-jit-compilers/



```
function arraySum(arr) {
  var sum = 0;
  for (var i = 0; i < arr.length; i++) {
    sum += arr[i];
  }
}
```



Javascript

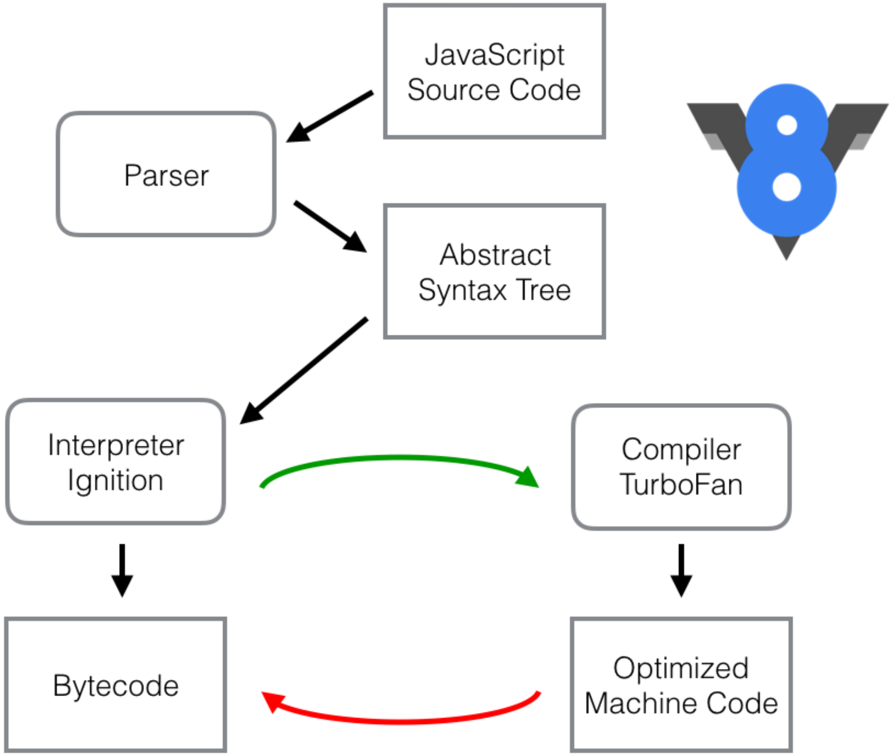
(SpiderMonkey)

(Nitro)

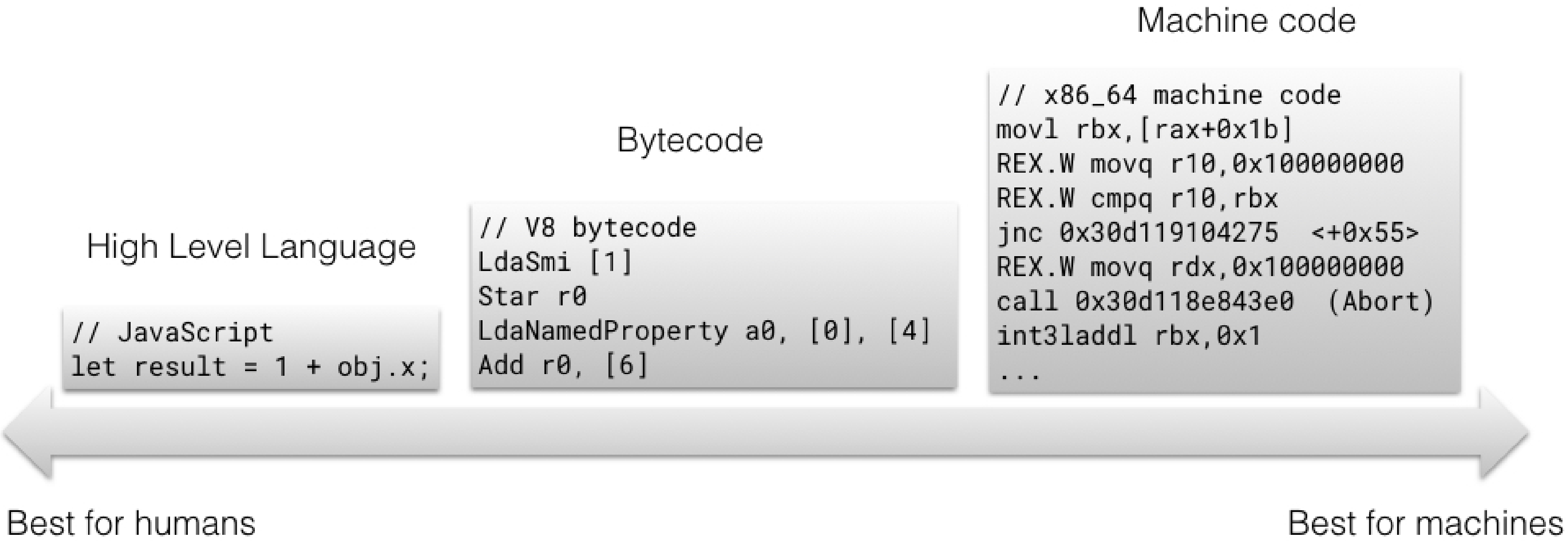
1. The engine (embedded if it’s a browser) reads (“parses”) the script.

2. Then it converts (“compiles”) the script to the machine language.

3. And then the machine code runs, pretty fast.



Javascript



High Level Language

```
// JavaScript
let result = 1 + obj.x;
```

Bytecode

```
// V8 bytecode
LdaSmi [1]
Star r0
LdaNamedProperty a0, [0], [4]
Add r0, [6]
```

Machine code

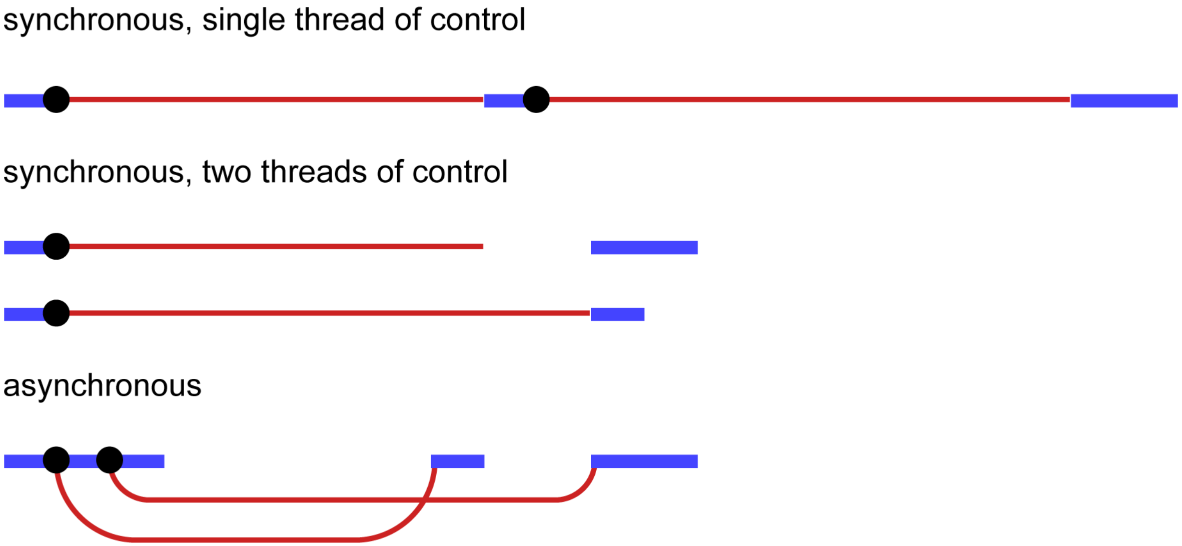
```
// x86_64 machine code
movl rbx,[rax+0x1b]
REX.W movq r10,0x100000000
REX.W cmpq r10,rbx
jnc 0x30d119104275  <+0x55>
REX.W movq rdx,0x100000000
call 0x30d118e843e0  (Abort)
int3laddl rbx,0x1
...
```

Best for humans

Best for machines

Javascript

JavaScript is always synchronous and single-threaded. If you're executing a JavaScript block of code on a page then no other JavaScript on that page will currently be executed.



synchronous, single thread of control

synchronous, two threads of control

asynchronous

Javascript – Callback and Promise

One approach to asynchronous programming is to make functions that perform a slow action take an extra argument, a *callback function*. The action is started, and when it finishes, the callback function is called with the result.

```
setTimeout(() => console.log("Tick"), 500);
```

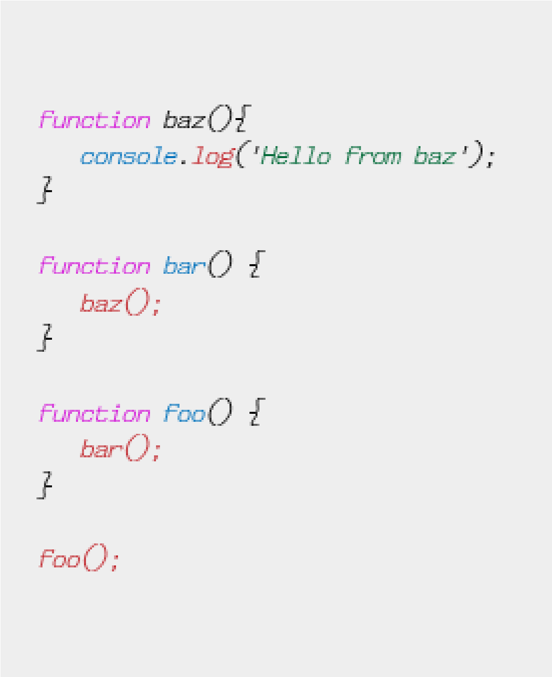
A *promise* is an asynchronous action that may complete at some point and produce a value. It is able to notify anyone who is interested when its value is available.

```
let fifteen = Promise.resolve(15);
fifteen.then(value => console.log(`Got ${value}`));
```

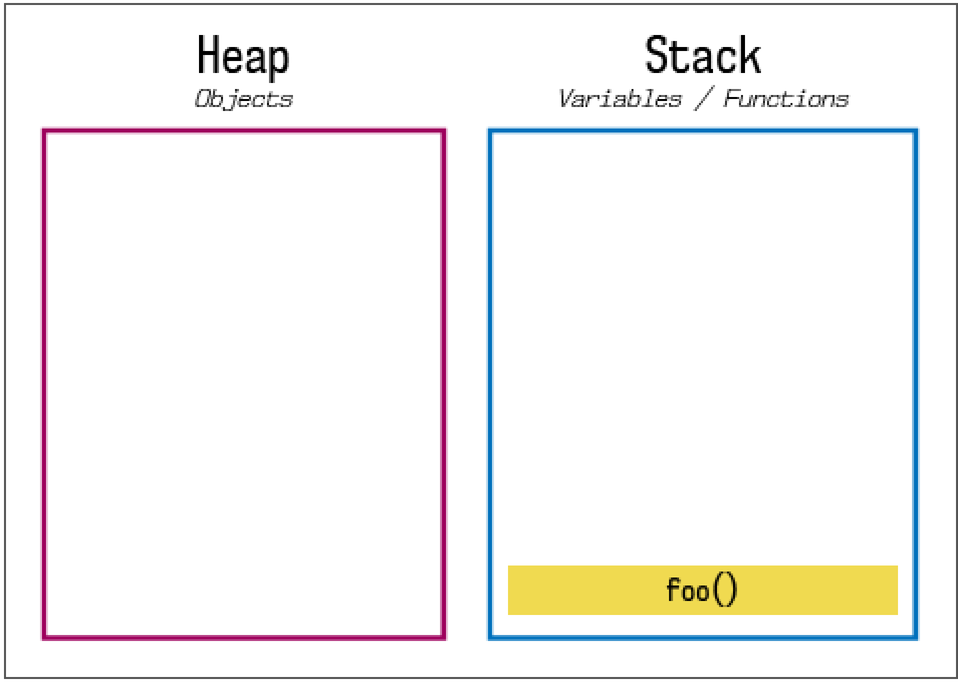
Javascript – Callback and Promise

JavsScript Program

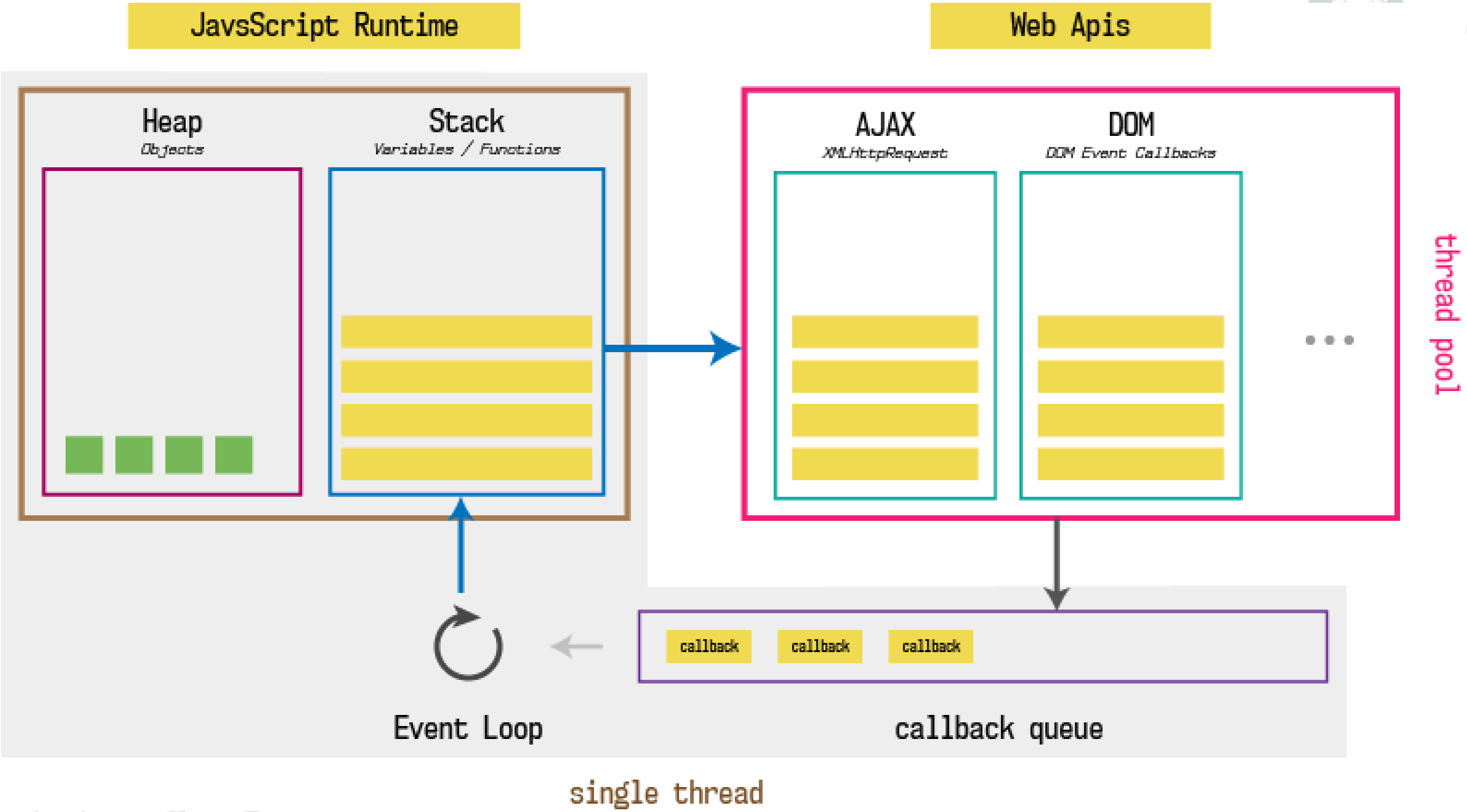
JavsScript Runtime



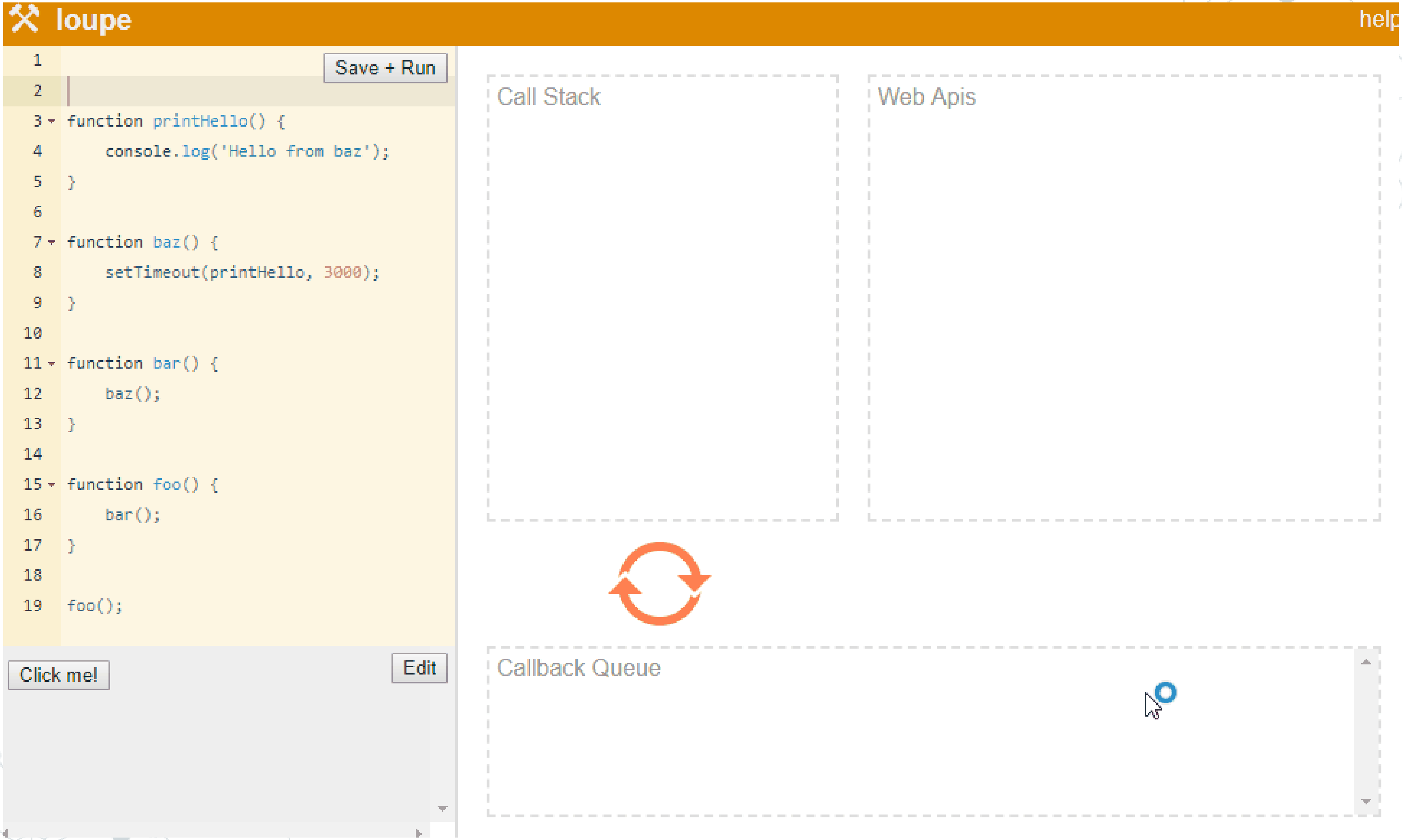
```
function baz(){
    console.log('Hello from baz');
}

function bar() {
    baz();
}

function foo() {
    bar();
}

foo();
```



Javascript – Callback and Promise



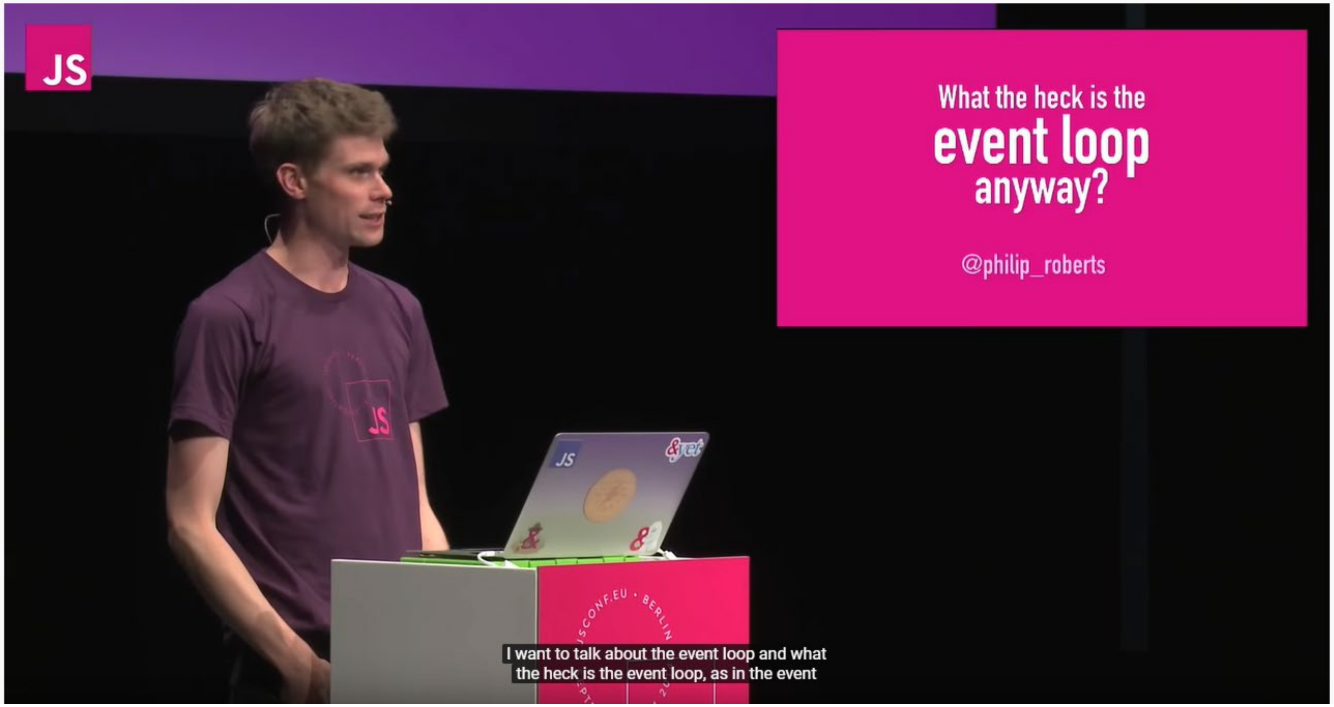
Javascript – Callback and Promise



```javascript


function printHello() {
    console.log('Hello from baz');
}

function baz() {
    setTimeout(printHello, 3000);
}

function bar() {
    baz();
}

function foo() {
    bar();
}

foo();
```

Javascript – Callback and Promise

https://www.youtube.com/watch?v=8aGhZQkoFbQ



What the heck is the
event loop
anyway?

@philip_roberts

I want to talk about the event loop and what
the heck is the event loop, as in the event

OT: Come gestire le password

Sicurezza

No matter how secure you think you might be, something malicious can always happen. Because, **"*With the right tools and Talent, a Computer is an open book.*"**

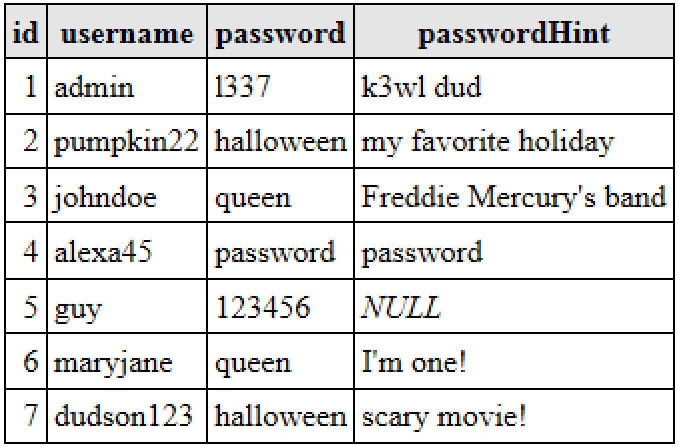
Joanna Rutkowska

Sicurezza

Sono riuscito a violare un Sistema. Cosa faccio?

1. Apertura file wp-config.php (wordpress) o configuration.php (joomla)
2. Individuazione delle informazioni in chiaro della connessiona al mysql
3. Esecuzione di uno script per il dump del DB
4. Download del dump in locale

Password in chiaro:



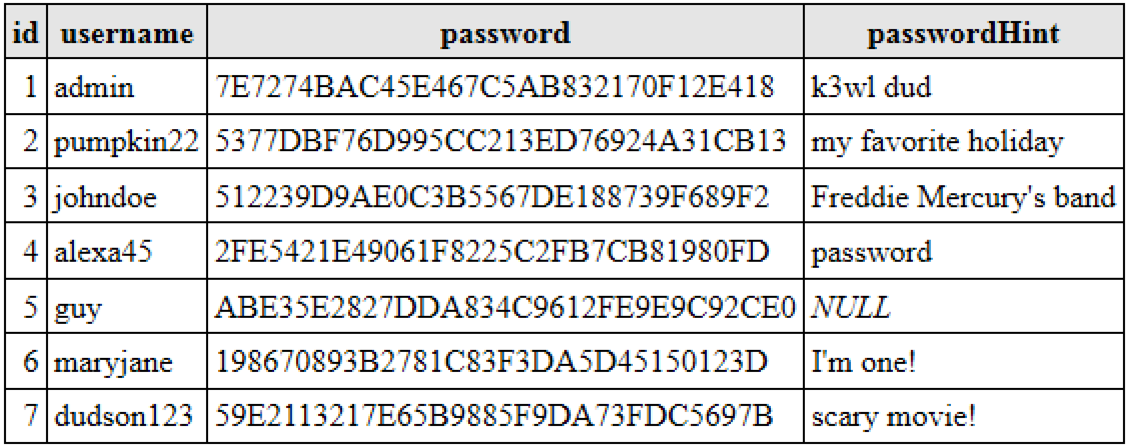
id	username	password	passwordHint
1	admin	1337	k3wl dud
2	pumpkin22	halloween	my favorite holiday
3	johndoe	queen	Freddie Mercury's band
4	alexa45	password	password
5	guy	123456	*NULL*
6	maryjane	queen	I'm one!
7	dudson123	halloween	scary movie!

Sicurezza

MD5 : funzione di hash non reversibile

Password = MD5(PasswordInseritaDallUtente);

Password crittografate:



id	username	password	passwordHint
1	admin	7E7274BAC45E467C5AB832170F12E418	k3wl dud
2	pumpkin22	5377DBF76D995CC213ED76924A31CB13	my favorite holiday
3	johndoe	512239D9AE0C3B5567DE188739F689F2	Freddie Mercury's band
4	alexa45	2FE5421E49061F8225C2FB7CB81980FD	password
5	guy	ABE35E2827DDA834C9612FE9E9C92CE0	*NULL*
6	maryjane	198670893B2781C83F3DA5D45150123D	I'm one!
7	dudson123	59E2113217E65B9885F9DA73FDC5697B	scary movie!

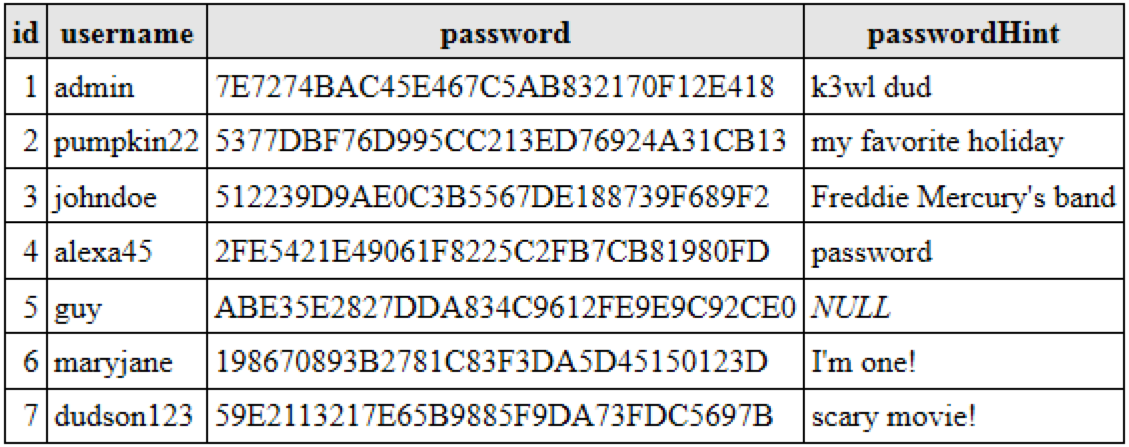
Potrei avere un db ti migliaia di hash generati da password conosciuti e scoprire le password.

Sicurezza

Secret: Bdy~])/S%@QgSHYH^MdO3&>c9q*2#i

Password = MD5(PasswordInseritaDallUtente + **Secret**);

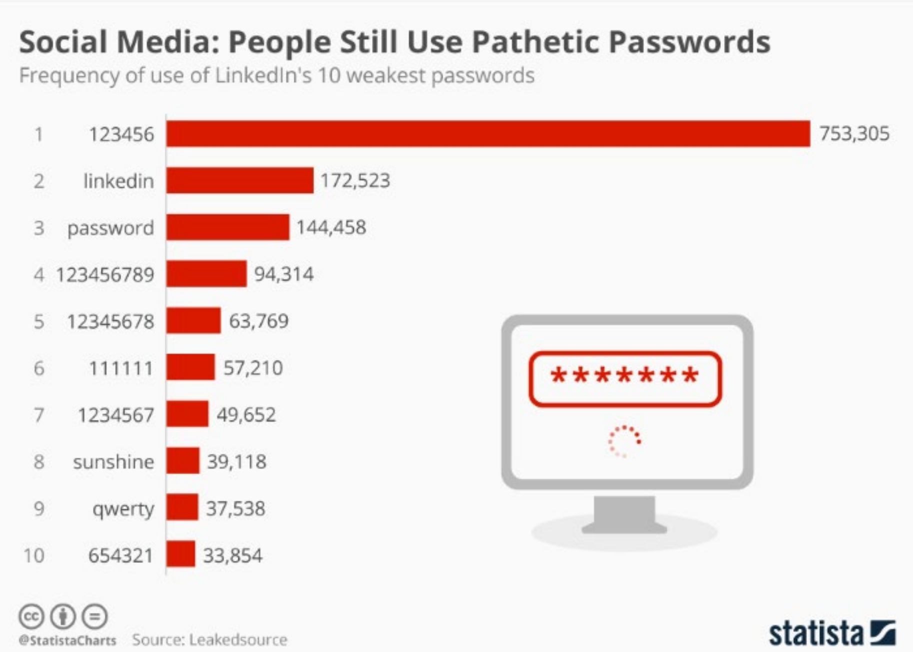
Password crittografate:



id	username	password	passwordHint
1	admin	7E7274BAC45E467C5AB832170F12E418	k3wl dud
2	pumpkin22	5377DBF76D995CC213ED76924A31CB13	my favorite holiday
3	johndoe	512239D9AE0C3B5567DE188739F689F2	Freddie Mercury's band
4	alexa45	2FE5421E49061F8225C2FB7CB81980FD	password
5	guy	ABE35E2827DDA834C9612FE9E9C92CE0	*NULL*
6	maryjane	198670893B2781C83F3DA5D45150123D	I'm one!
7	dudson123	59E2113217E65B9885F9DA73FDC5697B	scary movie!

Non posso più utilizzare tabelle di password conosciute perché la Secret è differente dalla mia. Dovrei rigenerarmi tutta la mia tabella di password conosciute con la Secret.

Sicurezza



Social Media: People Still Use Pathetic Passwords

Frequency of use of LinkedIn's 10 weakest passwords

Source: Leakedsource

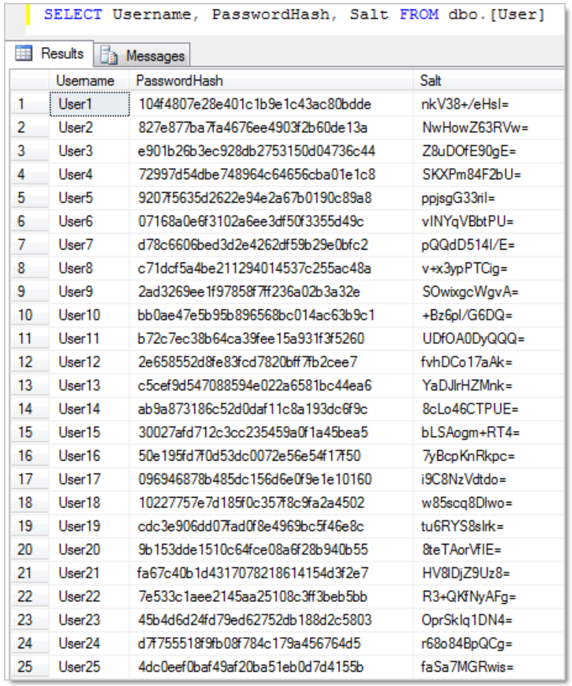
Individuo nei file php la Secret usata da wordpress/joomla.
Utilizzare un dizionario di password più utilizzate per essere più veloce e generare una lista di password da confrontare con quella del db

Sicurezza

Secret: Bdy~])/S%@QgSHYH^MdO3&>c9q*2#i

Salt: differente per ogni utente

Password = MD5(PasswordInseritaDallUtente + **Secret + Salt**);

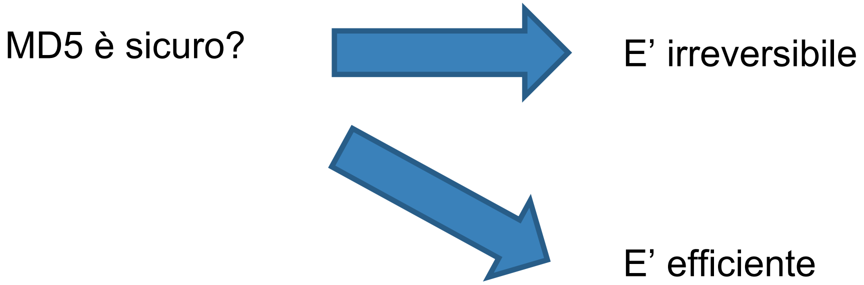


```
SELECT Username, PasswordHash, Salt FROM dbo.[User]
```

	Username	PasswordHash	Salt
1	User1	104f4807e28e401c1b9e1c43ac80bdde	nkV38+/eHsI=
2	User2	827e877ba7fa4676ee4903f2b60de13a	NwHowZ63RVw=
3	User3	e901b26b3ec928db2753150d04736c44	Z8uDOfE90gE=
4	User4	72997d54dbe748964c64656cba01e1c8	SKXPm84F2bU=
5	User5	9207f5635d2622e94e2a67b0190c89a8	ppjsgG33riI=
6	User6	07168a0e6f3102a6ee3df50f3355d49c	vINYqVBbtPU=
7	User7	d78c6606bed3d2e4262df59b29e0bfc2	pQQdD514I/E=
8	User8	c71dcf5a4be211294014537c255ac48a	v+x3ypPTCig=
9	User9	2ad3269ee1f97858f7ff236a02b3a32e	SOwixgcWgvA=
10	User10	bb0ae47e5b95b896568bc014ac63b9c1	+Bz6pI/G6DQ=
11	User11	b72c7ec38b64ca39fee15a931f3f5260	UDfOA0DyQQQ=
12	User12	2e658552d8fe83fcd7820bff7fb2cee7	fvhDCo17aAk=
13	User13	c5cef9d547088594e022a6581bc44ea6	YaDJlrHZMnk=
14	User14	ab9a873186c52d0daf11c8a193dc6f9c	8cLo46CTPUE=
15	User15	30027afd712c3cc235459a0f1a45bea5	bLSAogm+RT4=
16	User16	50e195fd7f0d53dc0072e56e54f17f50	7yBcpKnRkpc=
17	User17	096946878b485dc156d6e0f9e1e10160	i9C8NzVdtdo=
18	User18	10227757e7d185f0c357f8c9fa2a4502	w85scq8DIwo=
19	User19	cdc3e906dd07fad0f8e4969bc5f46e8c	tu6RYS8sIrk=
20	User20	9b153dde1510c64fce08a6f28b940b55	8teTAorVfIE=
21	User21	fa67c40b1d43170782186141 54d3f2e7	HV8IDjZ9Uz8=
22	User22	7e533c1aee2145aa25108c3ff3beb5bb	R3+QKfNyAFg=
23	User23	45b4d6d24fd79ed62752db188d2c5803	OprSkIq1DN4=
24	User24	d7f755518f9fb08f784c179a456764d5	r68o84BpQCg=
25	User25	4dc0eef0baf49af20ba51eb0d7d4155b	faSa7MGRwis=

Individuo il Salt per ogni utente e devo rieseguire l’hash del mio dizionario
Per ogni combinazione di salt. Poi confronto il risultato con il db

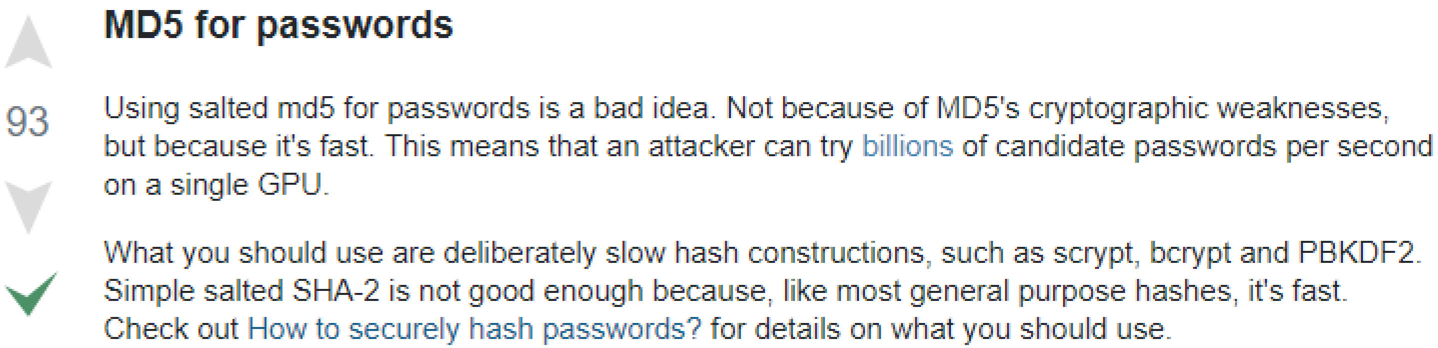
Sicurezza



MD5 è sicuro?

E’ irreversibile

E’ efficiente



MD5 for passwords

Using salted md5 for passwords is a bad idea. Not because of MD5's cryptographic weaknesses, but because it's fast. This means that an attacker can try billions of candidate passwords per second on a single GPU.

What you should use are deliberately slow hash constructions, such as scrypt, bcrypt and PBKDF2. Simple salted SHA-2 is not good enough because, like most general purpose hashes, it's fast. Check out How to securely hash passwords? for details on what you should use.

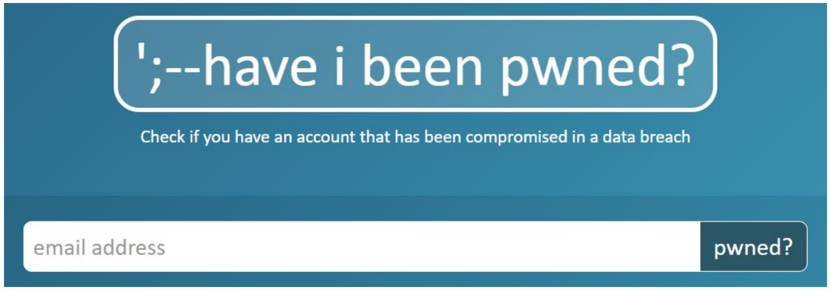
Sicurezza

Scoprite se siete stati **pwned**

A corruption of the word "Owned." This originated in an online game called **Warcraft**, where a map designer misspelled "owned." When the computer beat a player, it was supposed to say, **so-and-so** "has been owned."

Instead, it said, so-and-so "has been pwned."

https://haveibeenpwned.com/



';--have i been pwned?

Check if you have an account that has been compromised in a data breach