Binary search

This script searches hashed passwords in a text file.

Datafile: download SHA1 hashed file, ordered byhash from https://haveibeenpwned.com/Passwords

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <title>Hacked passwords</title>
</head>

<body>
   <form action="index.php" method="get">
     password: <input type="text" name="password">
     <input type="submit" value="Submit">
   </form>

<?php
function hashDiff($hash1, $hash2) {
   $array1 = str_split($hash1);
   $array2 = str_split($hash2);

   for( $i=0; $i<strlen($hash1); $i++ ) {
      if ($array1[$i] <> $array2[$i]) {
         break;
      }
   }

   return($i);
}

function searchPassword($password){
   $filename="pwned-passwords-sha1-ordered-by-hash-v4.big.txt";

   $hashedPassword = strtoupper(sha1($password));
   echo "<br>Searching for: ".$password;
```

```
echo "<br> Hash: ". $hashedPassword;

if (! $largeFileHandle = fopen($filename, "r")) {
    echo "Cannot open large file ".$filename;
    return;
}

$fileSize = filesize($filename);
$pointer = $fileSize/2;
$step = $fileSize/4;
$maxLineLen = 50;

echo "<br> file size: ".number_format($fileSize,0, "." , " " );

while (true) {
    fseek ( $largeFileHandle , $pointer-$maxLineLen , SEEK_SET );
    $line = fgets($largeFileHandle);
    $line = fgets($largeFileHandle);
    list($lineHash, $lineNumber) = explode(":", $line);

    $currPos = ftell($largeFileHandle);
    //echo "<br> file pos: ".number_format($currPos,0, "." , " " );

    if ($lineHash < $hashedPassword) {
        $pointer = $pointer+$step;
    } elseif ($lineHash > $hashedPassword)  {
        $pointer=$pointer-$step;
    } else { // hash found
        return($line);
    }

    $step = (int)($step/2);

    if ( $step < $maxLineLen ) {
        break;
    }
}

if ($lineHash > $hashedPassword) {
    fseek ( $largeFileHandle , $pointer-50 , SEEK_SET );
    $line = fgets($largeFileHandle);
```

```
        $line = fgets($largeFileHandle);
        list($lineHash, $lineNumber) = explode(":",$line);
    }

    if ($lineHash == $hashedPassword) {
        return($line);
    }

    while ($lineHash > $hashedPassword) {
        fseek($largeFileHandle, ftell($largeFileHandle)-2*$maxLineLen);
        $line = fgets($largeFileHandle);
        $line = fgets($largeFileHandle);
        echo "<br>itterating down, ". $line;
        list($lineHash, $lineNumber) = explode(":", $line);
    }

    while ($lineHash < $hashedPassword) {
        $line = fgets($largeFileHandle);
        list($lineHash, $lineNumber) = explode(":", $line);
        echo "<br>itterating up, ". $line;
        if ($lineHash == $hashedPassword) {
            return($line);
        }
    }

    if ($lineHash == $hashedPassword) {
        return($line);
    }

    return(""); //nothing found

}

if ( isset($_GET['password']) ) {
    $password=$_GET['password'];
    $result = searchPassword($password);

    echo "<br>";

    if ( strlen($result) > 0 ) {
        list($lineHash, $lineNumber) = explode(":", $result);
```

```
        echo "<br><b>".$password." FOUND ".number_format( (int)$lineNumber, 0 , "." , " " )." times</b>";
    } else {
        echo "<br><b>".$password." NOT found</b>";
    }
}

?>

</body>
</html>
```

Revision #2
Created 17 August 2019 21:34:25 by Admin
Updated 17 August 2019 21:39:51 by Admin