常見的用戶密碼加密方式以及破解方法

發佈於2018-08-16 10:45:21 閱讀10.2K

要完全防止信息洩露是非常困難的事情，除了防止黑客外，還要防止內部人員洩密。但如果採用合適的算法去加密用戶密碼，即使信息洩露出去，黑客也無法還原出原始的密碼（或者還原的代價非常大）。也就是說我們可以將工作重點從防止洩露轉換到防止黑客還原出數據。

本文首發於InfoQ垂直號「聊聊架構」。

作為互聯網公司的信息安全從業人員經常要處理撞庫掃號事件，產生撞庫掃號的根本原因是一些企業發生了信息洩露事件，且這些洩露數據未加密或者加密方式比較弱，導致黑客可以還原出原始的用戶密碼。

目前已經曝光的信息洩露事件至少上百起，其中包括多家一線互聯網公司，洩露總數據超過10億條。本文作者就職於攜程技術中心信息安全部，文中他將分享用戶密碼的加密方式以及主要的破解方法。

用戶密碼加密

用戶密碼保存到數據庫時，常見的加密方式有哪些，我們該採用什麼方式來保護用戶的密碼呢？以下幾種方式是常見的密碼保存方式：

1. 直接明文保存，比如用戶設置的密碼是“123456”，直接將“123456”保存在數據庫中，這種是最簡單的保存方式，也是最不安全的方式。但實際上不少互聯網公司，都可能採取的是這種方式。

2. 使用對稱加密算法來保存，比如3DES、AES等算法，使用這種方式加密是可以通過解密來還原出原始密碼的，當然前提條件是需要獲取到密鑰。不過既然大量的用戶信息已經洩露了，密鑰很可能也會洩露，當然可以將一般數據和密鑰分開存儲、分開管理，但要完全保護好密鑰也是一件非常複雜的事情，所以這種方式並不是很好的方式。

1. 使用MD5、SHA1等單向HASH算法保護密碼，使用這些算法後，無法通過計算還原出原始密碼，而且實現比較簡單，因此很多互聯網公司都採用這種方式保存用戶密碼，曾經這種方式也是比較安全的方式，但隨著彩虹表技術的興起，可以建立彩虹表進行查表破解，目前這種方式已經很不安全了。

1. 特殊的單向HASH算法，由於單向HASH算法在保護密碼方面不再安全，於是有些公司在單向HASH算法基礎上進行了加鹽、多次HASH等擴展，這些方式可以在一定程度上增加破解難度，對於加了“固定鹽”的HASH算法，需要保護“鹽”不能洩露，這就會遇到“保護對稱密鑰”一樣的問題，一旦“鹽”洩露，根據“鹽”重新建立彩虹表可以進行破解，對於多次HASH，也只是增加了破解的時間，並沒有本質上的提升。

1. PBKDF2算法，該算法原理大致相當於在HASH算法基礎上增加隨機鹽，並進行多次HASH運算，隨機鹽使得彩虹表的建表難度大幅增加，而多次HASH也使得建表和破解的難度都大幅增加。使用PBKDF2算法時，HASH算法一般選用sha1或者sha256，隨機鹽的長度一般不能少於8字節，HASH次數至少也要1000次，這樣安全性才足夠高。一次密碼驗證過程進行1000次HASH運算，對服務器來說可能只需要1ms，但對於破解者來說計算成本增加了1000倍，而至少8字節隨機鹽，更是把建表難度提升了N個數量級，使得大批量的破解密碼幾乎不可行，該算法也是美國國家標準與技術研究院推薦使用的算法。

作者介紹

華章科技

北京華章圖文信息有限公司新媒體運營

關注 專欄

文章 閱讀量 獲贊 作者排名

2.2K 1.2M 5.5K 71

1. bcrypt、scrypt等算法，这两种算法也可以有效抵御彩虹表，使用这两种算法时也需要指定相应的参数，使破解难度增加。

下表对比了各个算法的特性：

算法	特点	有效破解方式	破解难度	其它
明文保存	实现简单	无需破解	简单	
对称加密	可以解密出明文	获取密钥	中	需要确保密钥不泄露
单向HASH	不可解密	碰撞、彩虹表	中	
特殊HASH	不可解密	碰撞、彩虹表	中	需要确保“盐”不泄露
Pbkdf2	不可解密	无	难	需要设定合理的参数

用户密码破解

用户密码破解需要针对具体的加密方式来实施，如果使用对称加密，并且算法足够安全（比如AES），必须获取到密钥才能解密，没有其它可行的破解方式。

如果采用HASH算法（包括特殊HASH），一般使用彩虹表的方式来破解，彩虹表的原理是什么呢？我们先来了解下如何进行HASH碰撞。单向HASH算法由于不能进行解密运算，只能通过建表、查表的方式进行碰撞，即将常用的密码及其对应的HASH值全计算出来并存储，当获取到HASH值是，直接查表获取原始密码，假设用MD5算法来保护6位数字密码，可以建如下表：

原始密码	MD5值
0	670B14728AD9902AECBA32E22FA4F6BD
1	04FC711301F3C784D66955D98D399AFB
…	…
999999	52C69E3A57331081823331C4E69D3F2E

全表共100W条记录，因为数据量不大，这种情况建表、查表都非常容易。但是当密码并不是6位纯数字密码，而是数字、大小写字母结合的10位密码时，建立一个这样的表需要（26+26+10）^ 10 ≈ 83亿亿（条记录），存储在硬盘上至少要占用2000W TB的空间，这么大的存储空间，成本太大，几乎不可行。

有什么办法可以减少存储空间？一种方法是“预计算哈希链”，“预计算哈希链”可以大幅减少HASH表的存储空间，但相应的增加了查表时的计算量，其原理大致如下：

建表过程：

先对原始数据“000000”进行一次HASH运算得到“670B1E”，再对HASH值进行一次R运算，R是一个定制的算法可以将HASH值映射到明文空间上（这里我们的明文空间是000000~999999），R运算后得到“283651”，再对“283651”进行hash运算得到“1A99CD”，然后在进行R运算得到“819287”，如此重复多次，得到一条哈希链。然后再选用其它原始数据建立多条哈希链。最终仅将链头和链尾保存下来，中间节点全都去掉。

查表过程：假设拿到了一条HASH值“670B1E”，首先进行一次R运算，得到了“283651”，查询所有链尾是否有命中，如果没有，则再进行一次HASH、一次R，得到了“819287”，再次所有链尾，可以得到看出已经命中。

这样我们就可以基本确认“670B1E”对应的明文就在这条链上，然后我们把这条链的生成过程进行重新计算，计算过程中可以发现“000000”的HASH值就是“670B1E”，这样就完成了整个查表过程。这种表就是“预计算哈希链”。这种方式存在一个问题，多条链之间可能存在大量的重复数据，如下图所示：

为了解决这个问题，我们将R算法进行扩展，一条链上的多次R运算采用不同的算法，如下图：

一条链上的每个R算法都不一样，就像彩虹的每层颜色一样，因此取名的为彩虹表。

当然彩虹表除了可以用户破解HASH算法外，理论上还可以用于破解对称加密算法，比如DES算法，由于DES算法密钥比较短，建立彩虹表破解是完全可行的；但对于AES算法，由于密钥比较长，建表几乎不可行（需要耗时N亿年）

小结

采用PBKDF2、bcrypt、scrypt等算法可以有效抵御彩虹表攻击，即使数据泄露，最关键的“用户密码”仍然可以得到有效的保护，黑客无法大批量破解用户密码，从而切断撞库扫号的根源。当然，对于已经泄露的密码，还是需要用户尽快修改密码，不要再使用已泄露的密码。

END

黑客 编程算法 安全 数据库

举报

点赞 4 分享

相关文章

常见的WiFi密码破解原理与方法

今天的目的是破解我那些不认识的小白鼠邻居的路由器密码，顺便限制对方网络访问等。

知识与交流

总结常见的10种破解密码方法

为了防止键盘记录工具，产生了使用鼠标和图片录入密码的方式，这时黑客可以通过木马程序将用户屏幕截屏下来然…

C4rpeDime

php用户名的密码加密更安全的方法

php中对用户密码的加密主要有两种方法，一种是利用md5加密，另一种是利用password_hash加密，两种方法中后一…

砸漏

js的常见的三种密码加密方式-MD5加密、Ba…

写前端的时候，很多的时候是避免不了注册这一关的，但是一般的注册是没有任何的难度的，无非就是一些简单的获…

何处锦绣不灰堆

破解密码的手段总结

黑客最常用的一个攻击方式，就是获取目标口令，有了对方密码口令，就相当于有了你家的入户门钥匙，那么接下来…

7089bAt@PowerLi

谁蹭了我的WiFi？浅谈家用无线路由器攻防

家用无线路由器作为家庭里不可或缺的网络设备，在给普通人带来极大便利的同时，也给处于互联网时代的我们带来…

FB客服

用户密码到底要怎么加密存储?

目前已经曝光的信息泄露事件至少上百起，其中包括多家一线互联网公司，泄露总数据超过10亿条。

Java技术栈

干货 | 如果信息泄露不可避免，我们该如何…

作者简介 张辉，就职于携程技术中心信息安全部，负责安全产品的设计与研发。 作为互联网公司的信息安全从业人员…

携程技术

Web登录其实没你想的那么简单

标准的HTML语法中，支持在form表单中使用<input></input>标签来创建一个HTTP提交的属性，现代的WEB登录中，常见的是下面这样的表单：

java思维导图

幸运哈希竞猜游戏系统开发加密哈希算法

哈希算法（Hash function）又称散列算法，是一种从任何数

V13z4z77z558

【Web技术】247-Web登录其实没那么简单

标准的HTML语法中，支持在form表单中使用<input></input>
标签来创建一个HTTP提交的属性，现代的WEB登录中，…

pingan8787

浅谈密码加密

我们的项目如果是使用flask框架开发的话，那么可以使用
flask中提供的安全模块，将密码进行加密。这样做的好处…

小闫同学啊

Web登录很简单？你在开玩笑吧！

本文通过 Web 登录的例子探讨安全问题，登录不仅仅是简单
地表达提交和记录写入，其安全问题才是重中之重。

业余草

Web登录很简单？开玩笑！

導讀：Web登錄不僅僅是一個form 那麼簡單，你知道它裡面存在的安全問題嗎？優質教程請關注微信公眾號“Web項目聚集地”

用戶1093975

密碼及加密方式

保護密碼的最好方法是使用加鹽哈希； 哈希算法哈希算法是一種單向函數，把任意數量的數據轉換成固定長度的“指紋”，這個過程無法逆轉。如果輸入發生一點改變，由…

春哥大魔王

為什麼說用MD5 存儲密碼非常危險，這些你…

很多軟件工程師都認為MD5 是一種加密算法，然而這種觀點
其實是大錯特錯並且十分危險的，作為一個1992 年第一次…

Bug開發工程師

為什麼說用MD5 存儲密碼非常危險，這些你…

很多軟件工程師都認為MD5 是一種加密算法，然而這種觀點
其實是大錯特錯並且十分危險的，作為一個1992 年第一次…

程序IT圈

為什麼說用MD5 存儲密碼非常危險，這些你該清楚

很多軟件工程師都認為MD5 是一種加密算法，然而這種觀點其實是大錯特錯並且十分危險的，作為一個1992 年第一次被公開的算法，到今天為止已經被發現了一些致命…

AlbertZhang

更多文章