    当你百无聊赖的看着扫描器W像往常一样，默默无闻的，一页一页的爬，一页一页的测试的时候，你的内心一定没有丝毫的波澜。悠然的品着三十块钱一斤的顶级新春绿茶，浏览浏览国内外最新的文娱播报，跟群里的黑阔们扯着不疼不痒的淡，尽情地享受着这美妙生活的每一刻。偶尔冒出个念头，也必定会是质疑W这个家伙是不是落伍了，怎么就是整不出来点让兄弟兴奋的东东，悲催啊，人生不如意十之八九。

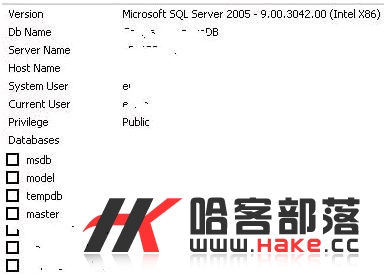
    一个小时过去了，两个小时过去了，三个小时过去了，这哥们还真是持久有耐力，木看到人家歇过啊……

哦了，终于扫完了，结果亦如平时，三三两两的躺着几个疑似注入点，机械式地重复着点击、尝试利用、获取信息，再看着屏幕上NULL、NULL，还是NULL的显示，你会觉得人生为何总是如此灰暗，灰暗到想拍案而起，找W的作者去论论理，你丫咋这么不给力呢……

    当然，有鉴于W的免费开源精神，再想想我们要为和谐社会做贡献啊，身为一名坚定的GCDY，怎么能够如此的不淡定，如此的小肚鸡肠咧。所以，每当我邪恶的小内心有强烈地犯罪冲动的时候，我都会毅然决然的选择《大悲咒》，那宁静致远的曲调，还有那穿破天际、扣人心弦的天籁之音，让我瞬间回归自然，重新走上幸福良民的康庄大道，“敢问路在何方，路在脚下……”[1]。

    挑一个有重大嫌疑的注入点换用工具P来跑跑，确保检测结果的有效性。COPY URL，COPY 关键字，选择注入类型，点确认按钮，就看P在那里嗖嗖的跑着，“妹妹，你大胆地往前跑呀” [2]。我靠，这都是真的吗？不会又误报吧，看着P把数据库类型还有期待已久的数据库利用界面弹出来的时候，我鸡冻了，太鸡冻了，难道这一切都是真的吗？

    我一边反复的数着自己身上的排骨，一边告诫自己要淡定，不排除P也有误报的时候，或者即使能跑出来，也有可能是那让人心烦意乱的乱码AAAAAAAAAAAAA……。Select All，Go！只见那数据库的信息刷刷刷的往外冒，yeah，真是久违的注入点，我太tmd鸡冻了。请看图：

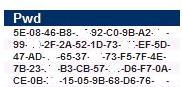


（艺术源于生活，而高于生活）

    感谢W、感谢P、感谢ZF、感谢DANG，感谢将来可能会有也可能不会有的粉丝，是你们一直支持着我，关心我，鼓励我，在我最孤立无援的时候，是你们，给了我一碗香喷喷的泡馍，让我又坚定了活着的信念。我爱你们~

         跑数据，嘿嘿，先跑五十个用户名、密码，你能想象当这些数据一列一列的出现在屏幕上的时候，作为一名职业非黑阔（俺们可都是经过授权的，敬爱的JCSS，请相信我），我的内心是多么的汹涌又澎湃，兴奋加亢奋，哇哈哈，简直可以媲美于中了双色球、大乐透的幸福心情，当然，准确的说应该等同于中了面值十块的彩票的心情。那怎是一个爽字了得。

         俗话说，天有不测风云，夏天雷阵雨比较多，所以，轻易不要洗车，轻易不要太鸡冻，不然你只能在风雨过后，顶着彩虹，一个人默默的含着如花的泪滴，擦去前风挡上那梅花鹿般的泥点。请看图：



（图中斑点为我所涂，请勿怪罪于夏天）

    傻眼了，这是什么加密方式，也许有大牛可以一眼看出其中门道，无奈我这只入门级的菜鸟，只得反复的尝试，MD5、16进制、UNICODE……，都没有结果。苍天呐，你为什么要这样对我。

    此路不通，另行他路吧，赶上堵车的时候，真是再心急也木得热豆腐吃，索性发扬我党两个务必的精神，谦虚谨慎、戒骄戒躁。不然真要刮了蹭了的，也只能自个担着，走保险还影响明年的费率咧，我看，就木有这个必要了吧。

    毛爷爷说过，只要信念不滑坡，办法总比困难多[3]。好吧，聪明的一休哥要开动脑筋了。怎么找规律呢，看看有没有重复的口令，忽然发现了两个用户的口令一样，都是7D-\*\*-85-51-22-\*\*-7D-0E-F8-\*\*-，再看他们的用户名，一个是2390116，另一个是2390116343，那口令会不会是2390116呢？是骡子是马拉出来溜溜呗，开页面，输入用户名、口令、验证码，哇哈哈，成功登陆，我不是黑阔我怕谁，太崇拜自己了。

    翻来覆去木找到啥上传点，sigh，命运总是这样的无奈。

    有个admin账户，嘿嘿，让我逮到你了，口令：1\*-\*\*-85-41-44-\*6-3A-8\*-76-\*\*-，对比一下，木有重复的，扩大搜索范围，索性把两千多个账号都整出来拉倒。

    嘻唰唰，嘻唰唰，嘻唰唰，呜呜，伤啊伤晃啊晃装啊装，多可惜哦!想啊想藏啊藏嚷啊嚷。请你拿了我的给我送回来，吃了我的给我吐出来，闪闪红星里面的记载，变成此时对白[4]！木一会记录就全出来了，果然没有相同的口令。灵机一动，不会是弱口令吧，admin、admin，HOHO，成功登录，爱自己爱自己！！！

    又傻眼了，\*\*\*\*公司，我靠，敢情普通用户也能注册这个账号？我@￥#%￥……！请看图：



（安全第一，安全第一）

    继续翻，终于找到网站自己的账号了，嘿嘿，口令：\*\*-D5-C2-\*\*-1D-E4-\*\*-E1-2E-\*\*-，这咋破解啊……，再对比有木有雷同的。我倒，竟然有35个，那必须是弱口令了，不然管理员的口令怎么可能跟普通用户的口令一样。猜吧，这是俺滴强项，谁让俺如此的冰雪咧。123456,12345678,1234,123,654321,111111,1111,111,666666,666,888888,888,admin,admin888,admin123,adminadmin,…… 这可是虾米弱口令啊，真费劲咧！

         我就不信了，舒展舒展我的小筋骨，再仔细数数我的小排骨，抖擞精神，恩，有木有可能是000000，有木有！有木有！哇哈哈哈哈，成功！！！我爱我自己！我是最牛X的非黑阔！各位看官别骂我，那一刻太鸡冻了。

         本次检测暂时告一段落，在一个木有后台，木有上传点的网站里，我们只能落寞的使用着各种免费与收费的工具，不停的寻找着一个又一个的漏洞。时间紧，任务重，造就了我们大量使用工具的现状，本次检测过程，因为是非目标网站，所以木有使用手工注入，木有再继续构造小马、大马、上传点之类的，只是想写下来一个渗透测试工作者看似枯燥与重复，其实又充满乐趣的工作过程。找不到漏洞，拿不到权限，从好的方面来想，客户确实越来越重视安全了，信息系统也越来越安全了。不管是从客户自身，抑或是国家这个高度，感觉信息安全都在打开一片新的天空。从不好的方面来想，是不是我们自身的技术不够，手段不足，创新不力？就像我们看到扫描器一次又一次的扫描无果之后，我们是该怀疑它的可靠程度，还是该无奈的承认客户的信息系统足够安全？

         在不平静中，寻找宁静。在不轻松中，寻找J点。让我们每一天都笑口常开吧，哇哈哈！O(∩\_∩)O

【参考文献】

[1] 闫肃. 敢问路在何方[X]. 北京：央视1988年版《[西游记](http://baike.baidu.com/view/2583.htm)》片尾曲，1984年1月.  
[2] 张艺谋. 妹妹你大胆地往前走[X]. 西安：《红高粱》插曲，1987年.  
[3] 毛主席. 毛主席语录. 不详：不详，不详.  
[4] 花儿乐队. 嘻唰唰[X]. 不详：《花季王朝》专辑，2005年.