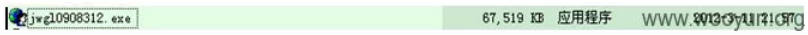
正方教务管理系统数据库任意操作漏洞

编号	10358
Url	http://www.wooyun.org/bug.php?action=view&id=10358 (http://www.wooyun.org/bug.php?action=view&id=10358)
漏洞状态	已交由第三方合作机构(cncert国家互联网应急中心)处理
漏洞标题	正方教务管理系统数据库任意操作漏洞
漏洞类型	默认配置不当 (/bug/index?BugSearch%5Bbug_type%5D=%E9%BB%98%E8%AE%A4%E9%85%8D%E7%BD%AE%E4%B8%8D%E5%BD%93)
厂商	杭州正方 (/bug/index?BugSearch%5Bvendor%5D=%E6%9D%AD%E5%B7%9E%E6%AD%A3%E6%96%B9)
白帽子	峙酿君edwardz (/bug/index?BugSearch%5Bauthor%5D=%E5%B3%99%E9%85%BF%E5%90%9Bedwardz)
提交日期	2012-07-30 12:02:00
公开日期	2012-08-04 12:03:00
修复时间	*(not set)*
确认时间	0000-00-00 00:00:00
Confirm Spend	-1
漏洞标签	无
关注数	0
收藏数	0
白帽评级	高
白帽自评rank	20
厂商评级	无
厂商评rank	0
漏洞简介	存在数据库任意操作漏洞，只需知道服务器IP，可执行任意数据库操作。因为全国1000多所高校都在使用该系统，该漏洞可以直接实现成绩修改，学生信息导出。故影响一

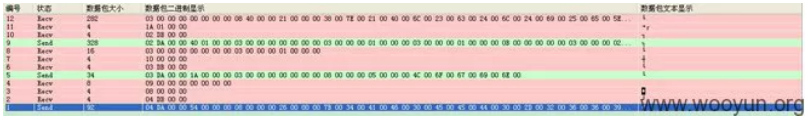
漏洞细节

杭州正方教务管理系统是国内用的比较多一个教务管理系统，据杭州正方官网http://www.zfsoft.com/type_14.html 说正方数字化校园信息平台软件用户名单（共3区1000多所高校），因此这个漏洞危害和影响还是相当大的。
正方软件股份有限公司开发的教务管理系统除了.net 开发的B/S供学生查看成绩，选课，老师录入成绩以外，还采用Delphi开发了一个C/S客户端，用于教务员和等软件截图如下。

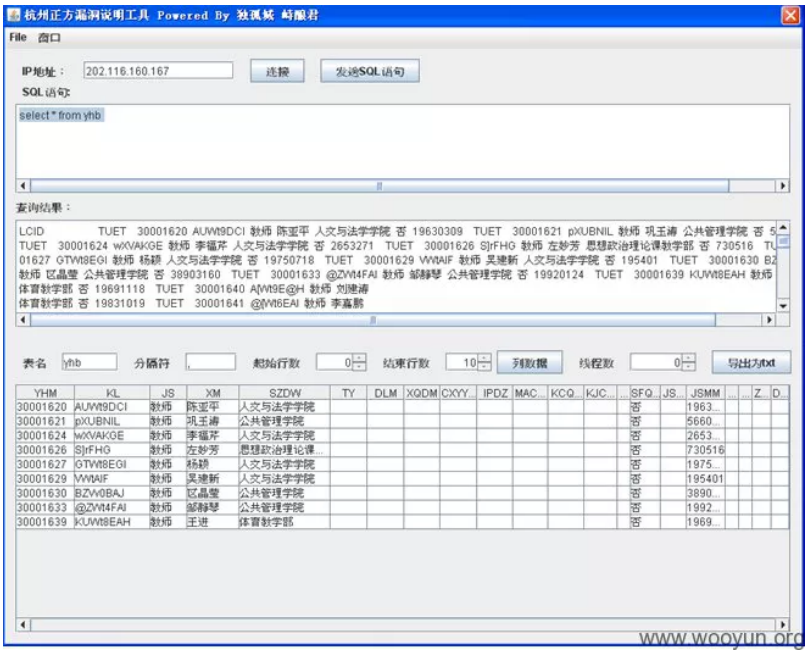


(https://images-bugs.shuimugan.com//upload/201207/3011552114f5615c7a7d6a00b1c9d9a0907eeb30.png.webp)

然而通过分析发现该软件存在许多重大漏洞，用户只要知道了服务端IP，就可以管理整个后台Oracle数据库，导致学生老师的个人隐私信息泄露，以及被篡改成绩。过我们的测试发现许多C/S服务端和B/S服务端在同一个服务器上面，比如218.75.208.58(湖南工业大学)，202.116.160.167(华南农业大学)，如果两个服务端不在面，也比较好找，因为C/S服务端使用的端口是211，因此很容易通过端口扫描软件扫描整个C段或临近的网段找到服务器IP。
? 漏洞原理解析
我们通过对客户端软件和服务端通信抓包过程发现，每次打开客户端软件时，客户端软件就跟服务器进行了三次TCP会话就完成了验证过程。经过我们的多次分析那台服务器，这三次TCP会话都是固定的，截图如下：


(https://images-bugs.shuimugan.com//upload/201207/301155458dd1648817927e8998769dd778a4bdcf.png.webp)

三次TCP会话后，客户端就可以向服务端发送任意SQL语句了，然后服务端就会返回查询结果。
SQL语句是这样构造的
02DA0000+接下来数据的总字节数+0300000000000000003000000022D31010300000001000000B000000FFFF0300000002000000030000000000000008000
Unicode编码后的字节数+SQL的Unicode编码+0800000006000000440053005005F0071003100
发送给服务器后，然后通过分析服务器就会返回数据包就可以得到返回的 S Q L 结果。

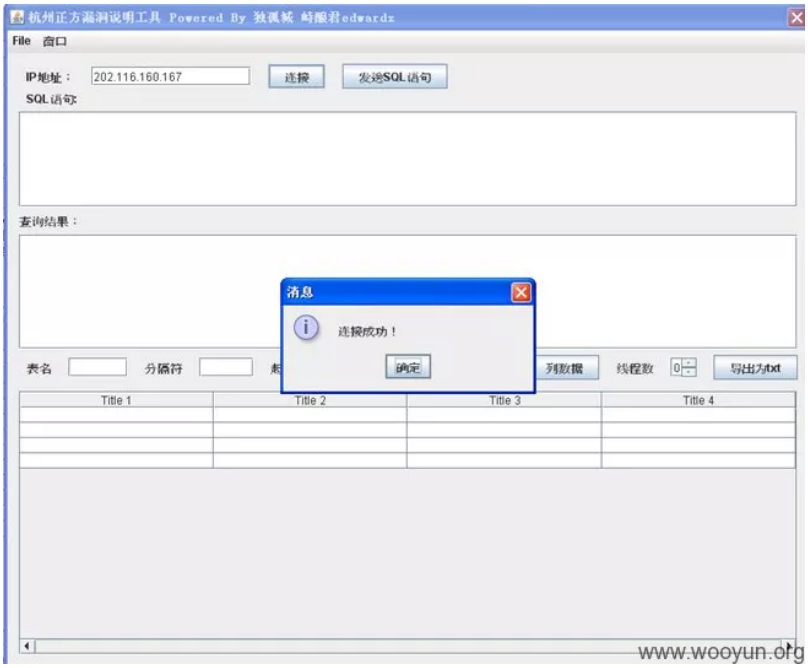


(https://images-bugs.shuimugan.com//upload/201207/3011585225c2e6f3f1ef7b27e7bc26e26be0b5ff.png.webp)

?

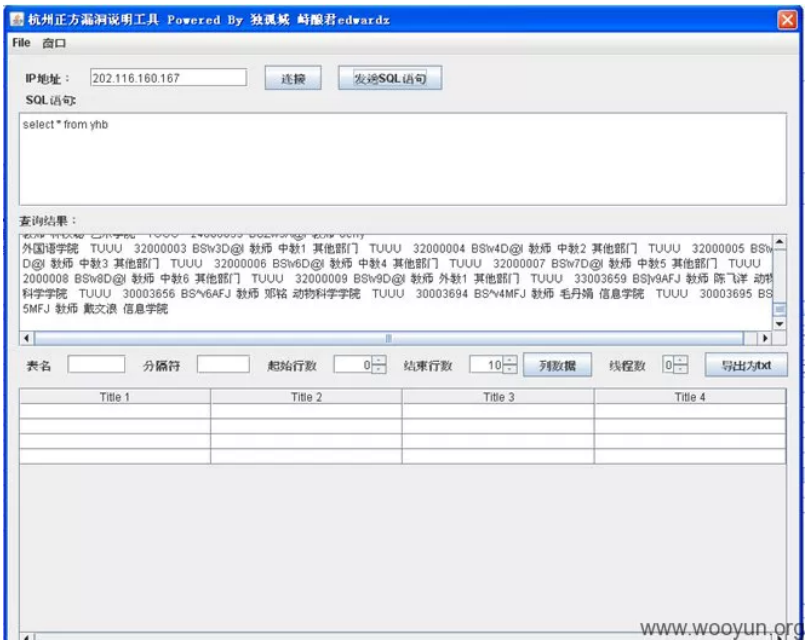
POC

为了更好的说明漏洞的危害，我们采用Java开发了漏洞说明软件，并以华南农业大学(202.116.160.167)为例说明漏洞危害。



(https://images-bugs.shuimugan.com//upload/201207/30115634cdf4968af5cfe6d286f76469a5c90faf.png.webp)

将华南农业大学服务器ＩＰ输入IP地址栏后，点击连接，软件提示连接成功。



(https://images-bugs.shuimugan.com//upload/201207/30115709f590ce6ef3c3f466479924754c42125b.png.webp)

管理系统后台数据库里面有个表yhb,里面放着教师和管理的账户信息，包括加密后的密码，不过前段时间乌云报告了加密方式时可逆的，很容易就能解密出来。
点击发送SQL语句。将返回查询结果，SQL语句可以是增删改查的其他任何符合Oracle的语句。

在表明里面输入yhb,分隔符输入逗号，然后点击列数据，就可以看到查询数据了，并且可以导出为TXT。
通过上述说明，此漏洞确实很危险，感觉就像在裸奔一样，全国1000多所学校都在使用杭州正方教务管理系统，因此波及范围很广。
最后，欢迎关注微博:
http://weibo.com/evilniang
http://weibo.com/bingobest

修复方案	通讯加密
状态信息	2012-07-30： 细节已通知厂商并且等待厂商处理中 2012-08-04： 厂商已经主动忽略漏洞，细节向公众公开
厂商回复	None漏洞Rank：20 (WooYun评价)
回应信息	危害等级：无影响厂商忽略忽略时间：2012-08-04 12:03

Showing **1-85** of **85** items.

评论内容 (/bug/view?bug_no=10358&sort=comment_text)	评论人 (/bug/view?bug_no=10358&sort=author_name)	点赞数 (/bug/view?bug_no=10358&sort=love_hits)	评论时间 (/bug/view?bug_no=10358&sort=comment_time)
这个略屌	Comver	0	2014-08-21 14:47:00
@峙酿君edwardz 求漏洞检测工具下载地址	j2ck3r	0	2013-08-12 11:27:00
我想说的是，我们的客户端直接放在图书馆，有外接键盘。 我直接把它打包发到邮箱， 然后回去反汇编一下， 发现oracle地址 账号 口令 全在里面。 这个是软件架构的问题， 很难改的。	叶问	0	2013-06-10 16:23:00
求工具。。。。	ayys	0	2013-05-26 18:57:00
如何得知通信协议的？ 根据3次 交互猜出的？	neal	0	2012-12-20 23:16:00
@Docee 嗯 写出来了	西瓜	0	2012-11-30 20:17:00
@西瓜 网上有算法啊。就是异或而已，很简单的。	Docee	0	2012-11-30 17:04:00
@pangshenjie 不是每个学校都是这个名字吧，这个是浙江大学的缩写吧	西瓜	0	2012-11-29 19:01:00
@西瓜 zjdx.dll	pangshenjie	0	2012-11-29 09:53:00
@Docee 逆向密码何解？	西瓜	0	2012-11-28 21:27:00
@Docee %>_<%好吧。、。、	低调的瘦子	0	2012-11-17 17:14:00
@低调的瘦子 下照片并没有写成软件，只是代码调试中运行而已。。。对你用处不大的。。。就几行代码。	Docee	0	2012-11-17 14:49:00
@Docee 那下照片的程序也不能共享？	低调的瘦子	0	2012-11-17 13:47:00
@低调的瘦子 这个会坐牢的，不敢乱传。貌似漏洞到现在都还没修复..改成绩，逆向算教务处密码，完全木有问题。	Docee	0	2012-11-16 23:20:00
@Docee 厉害~~你滴利用程序还真写完了~~可共享否？	低调的瘦子	0	2012-11-14 11:52:00
@Docee 确实如你所述啊,haha!	独孤城	0	2012-10-08 14:50:00
@独孤城 洞主上面有些地方写错了，【SQL语句的Unicode编码后的字节数】这个应该是编码后的字节数的一半，而且后面发送SQL语句还要...你懂的！	Docee	0	2012-10-05 11:39:00
洞主厉害！亲测成功！正在写利用程序！！！	Docee	0	2012-10-03 17:23:00
求客户端来分析	Wdot	0	2012-09-17 13:07:00
貌似广东的高校都用的这个啊！！	Passer_by	0	2012-09-05 09:06:00
@独孤城 写下原理吧，或者能不能分享下工具的源码	Power	0	2012-09-04 00:21:00
以前听说一个同学写了一个软件直接查分我还不信，今天我信了	Power	0	2012-09-03 18:40:00
他思想不单纯坏掉了！呼呼	黄色沙漠	0	2012-08-08 17:34:00

评论内容 (/bug/view?bug_no=10358&sort=comment_text)	评论人 (/bug/view?bug_no=10358&sort=author_name)	点赞数 (/bug/view?bug_no=10358&sort=love_hits)	评论时间 (/bug/view?bug_no=10358&sort=comment_time)
@低调的瘦子 这个被发现了真的可以坐牢，劝你别做。有学长在牢里呆着呢。至于不会被发现的侥幸心理，详见 http://zone.wooyun.org/content/633	CCOz	0	2012-08-07 20:05:00
@独孤城 @CCOz 你看你看 孤独城说了~~~。，，虽然我确实是有邪恶的想法~~哈哈哈~~是否可以打包一份发我邮箱呢？870659132@qq.com	低调的瘦子	0	2012-08-07 14:55:00
@低调的瘦子 回编程序也写不出exp,因为三次会话的截图不完整。	独孤城	0	2012-08-07 12:12:00
还是得先建立通讯撒，不是学生的路过，不是大学生，没进过大学门	Vty	0	2012-08-07 11:30:00
@独孤城 - -其实我想说我不会写程序。。鄙视我把~~	低调的瘦子	0	2012-08-07 11:08:00
@CCOz 俺从发现漏洞到搞出EXP用了四天。	独孤城	0	2012-08-06 21:53:00
@CCOz 你知道的太多了~~~	低调的瘦子	0	2012-08-06 21:37:00
@低调的瘦子 人家原理都说了，三次会话都截图了，足够自己写个exp出来了，难不成你想干坏事？	CCOz	0	2012-08-06 18:35:00
楼主，，求工具~~870659132@qq.com~~在此谢过~~	低调的瘦子	0	2012-08-06 18:13:00
擦，改分改分，我高数挂了	猪头子	0	2012-08-04 20:25:00
@qiaoy 是的	峙酿君edwardz	0	2012-08-04 17:19:00
@峙酿君edwardz 简单搜了一下，确实分布很广，而且搞了一台服务器瞅了瞅这软件，貌似对学生十分重要啊，学籍、学分什么的都在上面，丫厂商太不负责人了！	qiaoy	0	2012-08-04 16:43:00
@qiaoy 早期基本都这样~~	se55i0n	0	2012-08-04 14:19:00
@峙酿君edwardz 目前国内的负责任的企业你觉得很多么？	se55i0n	0	2012-08-04 14:18:00
@qiaoy 这个漏洞服务和客户端都要修改。而且分布比较广，修复需要的时间不少。 这样忽略太不负责	峙酿君edwardz	0	2012-08-04 14:13:00
@se55i0n 官方说是忽略，估计偷偷补了。	qiaoy	0	2012-08-04 14:09:00
尼玛，这也能忽略~~	se55i0n	0	2012-08-04 13:54:00
@峙酿君edwardz 周一我和cert沟通下	xsser	0	2012-08-04 12:57:00
@xxser 我去，这个是神马情况，正方啊，真心沧心。这漏洞都能忽略？	峙酿君edwardz	0	2012-08-04 12:55:00
X乃，这尼玛就公开了	风萧萧	0	2012-08-04 12:16:00
还是教务系统有爱。。考虑挖教务系统？	生生不息	0	2012-08-02 17:44:00
@CCOz 不是学生的飘过，哇哦哦	黄色沙漠	0	2012-08-02 08:41:00
@CCOz 正解。。。哈哈。。。。	pangshenjie	0	2012-08-01 19:37:00

评论内容 (/bug/view?bug_no=10358&sort=comment_text)	评论人 (/bug/view?bug_no=10358&sort=author_name)	点赞数 (/bug/view?bug_no=10358&sort=love_hits)	评论时间 (/bug/view?bug_no=10358&sort=comment_time)
@xsser 目测都是大学生，一个漏洞把乌云的学生党全揪出来了，不是学生的很难接触到这个东西了……	CCOz	0	2012-08-01 18:52:00
我是老师，楼上的学生萌小心点	f1eecy	0	2012-08-01 18:37:00
那青涩的，懵懂的，撸撸无为的学生时代……	刺刺	0	2012-08-01 17:24:00
楼上都是学生么？	xsser	0	2012-08-01 17:07:00
围观	wefgod	0	2012-08-01 17:04:00
@峙酿君edwardz 膜拜lz，我发的那个只不过一个查成绩！	黄色沙漠	0	2012-07-31 23:00:00
@her0ma 不一样的，亲	峙酿君edwardz	0	2012-07-31 22:00:00
WooYun: 正方教务系统漏洞导致妹子成绩随便查照片随意看 和这个莫非一样？	her0ma	0	2012-07-31 20:32:00
@xsser 求目测继续求目测	黄色沙漠	0	2012-07-31 20:06:00
@xsser 求目测	PiaCa	0	2012-07-31 11:36:00
@xiaokinghk (*^__^*) 嘻嘻……	峙酿君edwardz	0	2012-07-30 23:24:00
@xsser 表示我的漏洞怎么还有一片在审核。。。审核不过能否告知天天想着能审核过。。。。	xiaokinghk	0	2012-07-30 22:34:00
看来好多学校又危险了！！！	se55i0n	0	2012-07-30 22:33:00
@峙酿君edwardz 呼呼 好东西。。。。。关注	xiaokinghk	0	2012-07-30 22:32:00
@pangshenjie 我把我们学校的上网服务器和正方搞混了。。。是.NET没错。。。	CCOz	0	2012-07-30 20:59:00
@CCOz 我们的是.net的啊~你看wooyun上那几个洞都是.net的	pangshenjie	0	2012-07-30 19:17:00
@pangshenjie 正方教务系统不是lamp架构么，反正我们学校都用的linux	CCOz	0	2012-07-30 19:05:00
@刺刺 正方那个有个bug，iis好像是system运行的~	pangshenjie	0	2012-07-30 18:45:00
@CCOz 耐心的等待吧 =。=	xsser	0	2012-07-30 16:25:00
@刺刺 目测不是，看他说有IP就行。。。	CCOz	0	2012-07-30 16:23:00
不会是webservice或是越权操作吧	刺刺	0	2012-07-30 14:32:00
真的假的，难以置信啊	笨猪	0	2012-07-30 14:12:00
不会是爆用户名密码了吧	波波虎	0	2012-07-30 13:53:00
~~ 淡定	exploits	0	2012-07-30 13:51:00
围观下	WooYuner	0	2012-07-30 13:33:00
@cnrstar 数据库连接的ip也是有限制的啊`	pangshenjie	0	2012-07-30 13:29:00
挂科重修过很多次的路过T_T	猥琐	0	2012-07-30 13:26:00

评论内容 (/bug/view?bug_no=10358&sort=comment_text)	评论人 (/bug/view?bug_no=10358&sort=author_name)	点赞数 (/bug/view?bug_no=10358&sort=love_hits)	评论时间 (/bug/view?bug_no=10358&sort=comment_time)
@峙酿君edwardz @坏虾	Valo洛洛	0	2012-07-30 13:24:00
@Valo洛洛 请好好学习，天天上相	峙酿君edwardz	0	2012-07-30 13:20:00
@Valo洛洛 请老老实实的看书，补考，重考或者重修。不要做违法的事情，得不偿失。	坏虾	0	2012-07-30 13:11:00
@峙酿君edwardz 只要知道IP就可以？？？！！不是吧，连数据库还得要密码啊~	cnrstar	0	2012-07-30 13:08:00
应该可以说是程序逻辑设计缺陷。	独孤城	0	2012-07-30 13:06:00
@峙酿君edwardz 求交流，我还挂着N科 - -	Valo洛洛	0	2012-07-30 13:04:00
@xsser 又要等上半个月 :(	Valo洛洛	0	2012-07-30 13:04:00
@m4trix1 严格的说也不是默认配置不当，不过wooyun的漏洞选项里面我也不知道选什么了	峙酿君edwardz	0	2012-07-30 12:58:00
漏洞类型： 默认配置不当	m4trix1	0	2012-07-30 12:47:00
@Valo洛洛 目测不是	xsser	0	2012-07-30 12:39:00
难道是有默认账号？	Valo洛洛	0	2012-07-30 12:26:00
.....	Valo洛洛	0	2012-07-30 12:24:00

网络安全交流群: 869661360