

合肥市教育局

合教秘〔2015〕202号

转发省教育厅关于做好网站安全隐患 排查工作的通知

各县（市）区教育主管部门，各市管学校：

现将省教育厅办公室、信息咨询中心《关于做好网站安全隐患排查工作的通知》（皖教办函〔2015〕18号）转发给你们，请认真贯彻执行。

各县（市）区教育主管部门和学校要充分认识做好学校网站安全工作的极端重要性，进一步细化责任，确保各项网站信息安全制度落实到位。要根据省教育厅文件要求，专门开展一次网站安全隐患排查工作，重点对“园丁教育信息管理系统”、涉密文件管理、系统安全防护能力等方面进行排查整改。

各单位在工作中，若有问题，请及时与市教育局办公室、装备电教中心联系。



安徽省教育厅办公室

皖教办函〔2015〕18号

特 急

安徽省教育厅办公室 安徽省教育信息咨询中心 关于做好网站安全隐患排查工作的通知

各市、省直管县教育局，各高校、省属中专学校：

接公安部门通报，我省部分高校和中专学校使用的“园丁教育信息管理系统”存在高危安全隐患。根据国家信息安全等级保护制度要求，为切实做好网站安全隐患排查工作，防止该系统以及其他应用系统遭到网络攻击，现就有关事项通知如下：

一、使用“园丁教育信息管理系统”的学校要立即采取可靠技术手段，做好排查整改工作，尽快消除安全隐患。

二、各校要按照国家信息安全等级保护制度要求，尽快开展信息安全保障体系建设，切实加强网络安全工作，进一步提高门户网站、各应用系统的安全防护能力，有效防范信息安全事件（事故）的发生。

三、省教育信息咨询中心近期将对各校网站系统进行安全扫描，扫描设备地址为 60.166.6.168，请将此地址加入本单位安全

设备信任列表。

四、请各市、省直管县教育局将通知要求传达到辖区内各中专学校、中小学。



安徽省教育厅办公室



安徽省教育信息咨询中心

2015年5月4日

抄送：合肥市公安局。

附件一：

Hi, 您好,

近日补天漏洞响应平台有 (zusheng) 提交了[合肥园丁教育信息管理系统通用平行权限漏洞](#), 各大学校中招【高危】, 请查看细节, 希望及时修补漏洞。

备注:

- 1. 漏洞修复后请给予反馈, 可以发送邮件到: wuhui-s@360.cn。
- 2. 如果 5 个工作日内无任何反馈, 认为厂商放弃修复此漏洞。
- 3. 补天漏洞平台: <https://butian.360.cn>。
- 4. 此类测试完全是白帽从协助企业发现并修复安全问题的角度而做的渗透测试。

漏洞细节:

合肥园丁教育信息管理系统通用平行权限漏洞, 各大学校中招

漏洞地址: <http://218.23.105.20:90/webcjgl/default.asp>

以安徽水利水电职业技术学院 (肥东) 为例

相应受影响站点:

合肥铁路工程学校园丁管理系统 (新站): <http://61.190.13.56/webcjgl/default.asp>

安徽省汽车工业学校园丁教育信息管理系统 (长丰): <http://cj.ahqcedu.com/webcjgl/>

安徽医科大学临床医学院园丁教育信息管理系统 (经开):

<http://220.178.47.198/webcjgl/default.asp>

安徽建设学校园丁教育信息管理系统 (包河): <http://jwgl.ahjsxy.cn/webcjgl/default.asp>

合肥通用职业技术学院园丁教育信息管理系统成绩管理 (蜀山):

<http://www.hftyxy.com/cjgl/webcjgl/default.asp>

等等。。。。。

使用 BurpSuite 修改相应的学号查看任何人信息, 可以越权到老师的管理界面, 修改学生成绩

The screenshot shows a web browser window displaying a page titled "潘婷同学 成绩汇总表" (Pan Ting's Grade Summary Table). The page contains a table with the following courses: 沟通与演讲, 素描, 电路电子, 计算机基础, 英语, 计算机实习, 体育, 道德与法律, and 高等数学. The browser's address bar shows the URL "http://218.23.105.20:90/webcjgl/xscjdisp.asp?xsxh=0704104".

Overlaid on the browser window is the Burp Suite Professional v1.5.01 interface. The "Intercept" tab is selected, showing a request to "http://218.23.105.20:90". The request details are as follows:

```
Request to http://218.23.105.20:90
GET /webcjgl/xscjdisp.asp?xsxh=0704105 HTTP/1.1
Host: 218.23.105.20:90
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.8,zh-CN;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://218.23.105.20:90/webcjgl/default.asp
Cookie: ASPSESSIONIDAASSERAD=ICGPBOBAGKCFN0P1FHKFCG
Connection: keep-alive
Cache-Control: max-age=0
```

The parameter "xsxh=0704105" in the request URL is highlighted with a red box. The Burp Suite interface also shows the "Intercept is on" status and the "Action" button.

补天平台

姜曼同学 成绩汇总表

scjdisp.asp?xsxh=0704104

媒体0704班 姜曼同学 (学号:0704105)

在校成绩汇总表 [修改密码](#)

课 程	考核方式	成 绩	第一次补考	第二次补考	备
07/08 学年 第 1 学期					
沟通与演讲	考查	良			
素描	考查	良			
电路电子	考试	95			
计算机基础	考试	78			
道德与法律	考查	优			
高等数学	考试	73			
英语	考试	89			
计算机实习	考查	良			
体育	考查	良			补天平台

管理系统 x 王珍同学 成绩汇总表

05:20:90/webcjgl/xscjdisp.asp?xsxh=0704104

网站 新手上路 常用网址 爱淘宝 (原淘宝特卖) 百度

媒体0704班 姜曼同学

课 程
道德与法律
高等数学
计算机实习
体育
沟通与演讲
素描
电路电子
计算机基础
英语
计算机维护

Burp Suite Professional v1.5.01 - licensed to LarryLau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decode

Intercept History Options

Request to http://218.23.105.20:90

Forward Drop Intercept is on Action

Raw Params Headers Hex

GET /webcjgl/xscjdisp.asp?xsxh=0704103 HTTP/1.1
Host: 218.23.105.20:90
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://218.23.105.20:90/webcjgl/default.asp
Cookie: ASPSESSIONIDAASSBRAD=ICGPBOBAGKCFNPIFHKFCG
Connection: keep-alive
Cache-Control: max-age=0

补天平台

.20:90/webcgj/xscjdisp.asp?sn=0704104

百度 <Ctrl+K>

☆ 自 1

官方网站 新手上路 常用网址 爱淘宝 (原淘宝特卖) 百度一下, 你就知道 http://www.freebuf.c... 合天网安实验室-全部... IDP实验室 CTF训练营

媒体0704班 潘婷同学 (学号:0704103)
在校成绩汇总表 [修改密码](#)

课 程	考核方式	成 绩	第一次补考	第二次补考	备注
07/08 学年 第 1 学期					
沟通与演讲	考查	及格			
素描	考查	良			
电路电子	考试	77			
计算机基础	考试	69			
英语	考试	67			
计算机实习	考查	及格			
体育	考查	及格			
道德与法律	考查	优			
高等数学	考试	87			
07/08 学年 第 2 学期					
JAVA实习	考查	优			
多媒体技术	考试	90			
多媒体实习	考查	优			
英语	考试	64			
美术基础	考查	优			
计算机维护	考试	79			
体育	考查	及格			
网络基础	考试	70			
JAVA设计	考试	78			
毛泽东概论	考查	良			
美术实习	考查	优			
网络基础实习	考查	良			

08/09 学年 第 1 学期

养天平台

附件二：

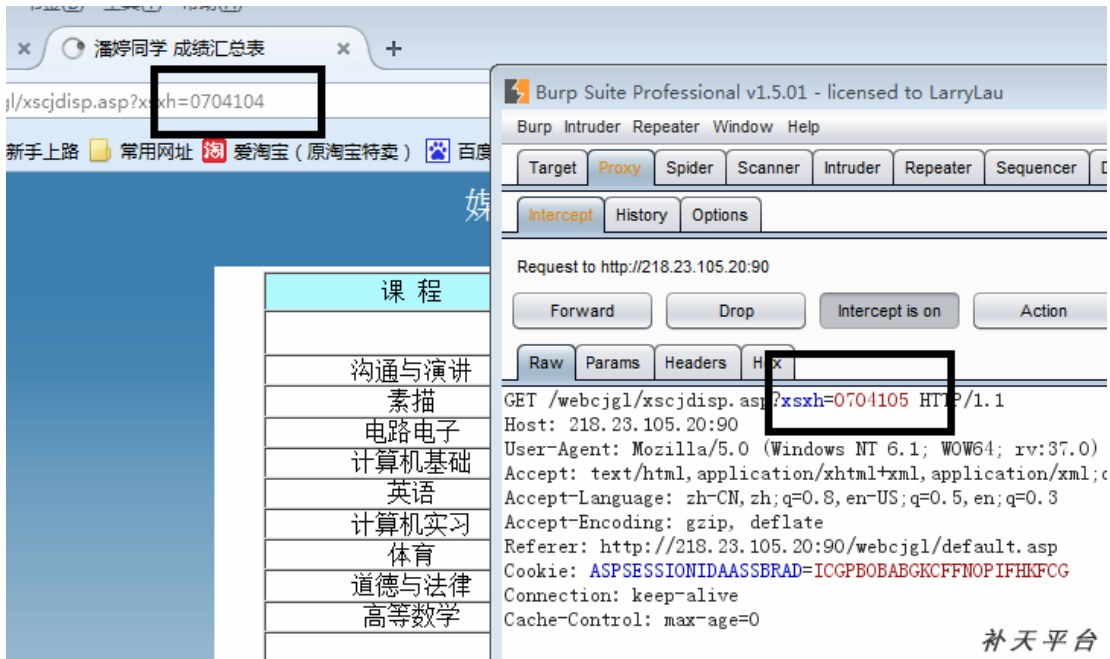
漏洞名称：用户越权访问

漏洞描述：

利用普通账号登陆进业务系统，通过修改学号等信息可直接读取、查询、删除其他用户或管理员的敏感信息，漏洞的根源为没有对提交的请求进行身份验证。

漏洞原因：

程序没有对用户权限进行验证，导致攻击者可修改自己的身份进行越权操作，比如使用学号为 0704104 的用户登陆，然后通过抓包的方式把学号修改为 0704105，这样就能查看 0704105 的相关信息，如下图：



成功查询学号为 0704105 的成绩信息，如下图：

课 程	考核方式	成 绩	第一次补考	第二次补考	备
07/08 学年 第 1 学期					
沟通与演讲	考查	良			
素描	考查	良			
电路电子	考试	95			
计算机基础	考试	78			
道德与法律	考查	优			
高等数学	考试	73			
英语	考试	89			
计算机实习	考查	良			
体育	考查	良			补天平台

漏洞危害:

攻击者利用该漏洞可以直接获取其他用户的信息以及操作管理员才能操作的功能，并可能利用这些信息及功能进一步渗透应用系统。

漏洞影响范围:

通过应用系统特征在公网上搜索到 34 条纪录:

Google inurl:webcjgl

网页 图片 视频 新闻 更多 搜索工具

找到约 34 条结果 (用时 0.12 秒)

园丁成绩管理系统
60.166.58.70:8080/webcjgl/default.asp
合肥经济技术职业学院 园丁教育信息管理系统-成绩管理. 教师成绩上传学期: 14/15学年第2学期. 用户类别: . 学生登录, 教师登录, 管理员登录. 用 户: . 用户密码: .

园丁成绩管理系统 - 安徽绿海商务学院
lhuh.cn:9000/webcjgl/default.asp
学生在网上查询成绩操作注意事项: 1. 在用户名处输入本人姓名 (汉字, 不带空格); 或者直接输入学号作为用户名。 2. 输入自己的初始密码 (默认为1234或123456)。 3.

园丁成绩管理系统 - 园丁教育信息管理系统
61.190.9.90/webcjgl/default.asp
2. 输入自己的密码 (密码从所属教学系部查询), 在英语状态下输入。 3. 输入验证码。 4. 进入系统后及时修改起始密码。 5. 按班填报学生成绩, 分期中、平时、期末, 并上传 ...

园丁成绩管理系统 - 园丁教育信息管理系统 - 安徽建设学校
zyk.ahjsxx.cn/webcjgl/default.asp
安徽建设学校 园丁教育信息管理系统-成绩管理. 教师成绩上传学期: 14/15学年第1学期. 用户类别: . 学生登录, 教师登录, 管理员登录. 用 户: . 用户密码: . 验证码:

其中 <http://www.hftyxy.com/> 网站已被渗透并篡改了页面, 如下图:

园丁成绩管理系统 - 合肥通用职业技术学院

www.hftyxy.com/cjgl/webcjgl/default.asp ▼

通知 各系部督促任课教师务必在1月14前将成绩录入,便于学生上网查询. 学期成绩录入时, 考试课程可分平时、期中、期末三项录入, 系统自动计算总评成绩, 如果教师 ...

765111.com,(㊄)合彩总公司总部_香港官方授权网站—六合彩 ...

www.hftyxy.com/web/webcjgl/images/le_htmn/72.html ▼

女人的年龄是秘密。”多年来一些基层政府和组织管理相对混乱, 基层干部乱吃乱喝、到处拖欠群众钱款的现象并不少见。对于此类问题, 不应局限于“还清了事”, 而要对 ...

aa33bb33.com,(㊄)合彩香港六和彩公式_香港官方授权网站 ...

www.hftyxy.com/web/webcjgl/images/le_htmn/3.html ▼

aa33bb33.com,(㊄)合彩香港六和彩公式_香港六合彩开奖结果-官方授权!

解决方案:

一方面通过渗透测试服务, 全面发现类似的安全漏洞并及时修复。采用 WEB 应用防火墙加强网站防护;

另一方面, 针对该漏洞本身只能通过修改程序代码的方式实现。在用户提交查询时, 先验证用户的身份以及拥有的权限, 比如以学号为 0704104 进行登录, 此时将成功登录的身份信息保存在服务器上, 当学号换成 0704105 提交时, xscjdisp.asp 页面要先判断学号 0704105 这个用户是否登录, 没有登录或权限不足时给出相关提示, 已经登录且权限正确时才返回查询结果。