中国石油天然气股份有限公司勘探开发研究院

移动端渗透测试报告

2023年04月

# 项目概述

通过人工渗透的方式对中国石油勘探开发研究院移动端信息系统进行渗透测试，保证中国石油勘探开发研究院移动端信息系统安全稳定运行，减少攻击面。

# 测试范围

|  |  |  |
| --- | --- | --- |
| IP地址 | 外网IP | 域名 |
| 11.8.55.1/11.8.55.2 | / | pfcrawl.eip.cnpc |
| 11.8.55.3/11.8.55.4 | / | pfissue.eip.cnpc |
| 11.8.55.5/11.8.55.6 | 106.39.36.235 | mfile.eip.cnpc/wmh.cnpc.com.cn |
| 11.8.55.7/11.8.55.8  11.8.55.9/11.8.55.10  11.8.55.21/11.8.55.14  11.8.55.15/11.8.55.16 | 114.255.212.99 | m.cnpc.com.cn/ mweb.eip.cnpc |
| 11.8.55.11/11.8.55.12  11.8.55.17/11.8.55.18  11.8.55.19/11.8.55.20 | / | moutapi.eip.cnpc |

# 漏洞统计

通过对中国石油勘探开发研究院移动端的信息系统进行渗透测试，共计发现漏洞13个，其中2个高风险，10个中风险，1个低风险；存在一定的安全隐患，需引起关注。

# 漏洞详情

#### 验证码绕过

|  |  |
| --- | --- |
| **测试项** | http://11.8.55.7/eip/login/login?ver=1681455548281 |
| **风险等级** | 中风险 |
| **风险描述** | 登陆界面的验证码可被绕过，输入图形验证码进行抓包，验证码不会过期可多次使用，攻击者可利用该漏洞执行暴力破解等操作。 |
| **相应证据截图** |  |
| **整改建议** | 1、系统在开发时注意验证识别后销毁session中的验证码。  2、限制用户提交的验证码不能为空  3、判断提交的验证码与服务器上存储的是否一致  4、禁止将验证码明文信息发送至客户端。 |

#### 弱口令

|  |  |
| --- | --- |
| **测试项** | http://11.8.55.7/eip/login/login?ver=1681799812533 |
| **风险等级** | 高风险 |
| **风险描述** | 登陆界面存在弱口令，攻击者可利用互联网公开的常见弱口令（空用户名/123456）尝试登录管理后台，对网站造成一定的影响。 |
| **相应证据截图** |  |
| **整改建议** | 禁止使用弱口令，口令应满足一定的复杂度，如8位以上包含大小写字母，数字，特殊符号。 |

#### 任意文件上传

|  |  |
| --- | --- |
| **测试项** | http://11.8.55.8/eip/file/uploadFileBase64 |
| **风险等级** | 中风险 |
| **风险描述** | 上传图像功能处存在任意文件上传，攻击者可利用该漏洞上传html等文件，在html文件中注入恶意的xss语句，可造成xss攻击，甚至窃取受害者的cookie，或者制作钓鱼网页，利用公司或单位网站的信任度来欺骗他人。 |
| **相应证据截图** | 头像上传处 |
| **整改建议** | 建议使用白名单方式，结合MIME Type、后缀检查等方式（即只允许允许的文件类型进行上传）；此外对于图片的处理可以使用压缩函数或resize函数，处理图片的同时破坏其包含的HTML代码。 |

#### 跨目录上传

|  |  |
| --- | --- |
| **测试项** | http://11.8.55.8/eip/file/uploadFileBase64 |
| **风险等级** | 高风险 |
| **风险描述** | APP上传图像功能处存在跨目录上传，开发者未对上传路径或文件命名中的参数进行过滤，导致攻击者可利用“../../”等字符在任意高层目录下上传恶意文件，对网站造成影响，甚至造成系统数据的破坏。 |
| **相应证据截图** | 头像上传处    上传测试文件至web根目录 |
| **整改建议** | 净化数据，对用户传过来的文件路径或命名参数进行硬编码或统一编码，对文件类型进行白名单控制，对包含恶意字符或者空字符的参数进行拒绝。 |

#### 敏感信息泄露

|  |  |
| --- | --- |
| **测试项** | http://11.8.55.8/eip/information/getRelateNewsMobileData?ver=&docId= |
| **风险等级** | 低风险 |
| **风险描述** | 在抓包时对某些参数id置空或输入其他字符会造成错误页面返回详细错误信息。报错信息中可能会包含服务器代码信息、数据库连接信息、SQL语句或者敏感文件的路径，为攻击者收集信息提供了方便。 |
| **相应证据截图** | 咨询-推荐-任意一个新闻，删除docid值 |
| **整改建议** | 1、编码时增加异常处理模块，对错误页面做统一的自定义返回界面，隐藏服务器版本信息；  2、不对外输出程序运行时产生的异常错误信息详情。 |

#### Druid未授权访问---8处

|  |  |
| --- | --- |
| **测试项** | http://11.8.55.7/eip/druid/websession.html  http://11.8.55.8/eip/druid/websession.html  http://11.8.55.9/eip/druid/websession.html  http://11.8.55.10/eip/druid/websession.html  http://11.8.55.21/eip/druid/websession.html  http://11.8.55.14/eip/druid/websession.html  http://11.8.55.15/eip/druid/websession.html  http://11.8.55.16/eip/druid/websession.html |
| **风险等级** | 中风险 |
| **风险描述** | Druid未授权访问，攻击者可以读取URI监控获取web的接口信息、Session监控获取最近登录用户的session等。 |
| **相应证据截图** | http://11.8.55.7/eip/druid/websession.html  IMG_256  http://11.8.55.8/eip/druid/websession.html  IMG_257  http://11.8.55.9/eip/druid/websession.html  IMG_258  http://11.8.55.10/eip/druid/websession.html  IMG_259  http://11.8.55.21/eip/druid/websession.html  IMG_260  http://11.8.55.14/eip/druid/websession.html  IMG_261  http://11.8.55.15/eip/druid/websession.html  IMG_262  http://11.8.55.16/eip/druid/websession.html  IMG_263 |
| **整改建议** | 1、建议Druid监控管理功能加上身份验证功能；  2、使用强口令。 |

# 项目总结

本次渗透测试主要针对中国石油勘探开发研究院移动端信息系统进行安全检查，降低受攻击可能性，减少攻击面。通过渗透测试结果情况来看，中国石油勘探开发研究院移动端信息系统存在验证码绕过、弱口令、任意文件上传、跨目录上传、敏感信息泄漏、Druid未授权访问等安全风险，建议针对整改建议进行整改。