|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 项目名称 | 业务系统运维服务项目-安全等保常态化服务项目 | | | | |
| 项目编号 |  | | 项目经理 |  | |
| 密　　级 | □公开使用 ■内部受控 | | | | |
| 总 页 数 |  | 正　　文 |  | 附　　件 |  |
| 编制/日期 | 2024年11月11日 | | 审核/日期 | 2024年11月11日 | |
| 批准/日期 |  | | | | |

**北京市生态环境局**

**重点排污单位自动监控与基础数据库系统**

**渗透测试报告**

**北京华夏航通信息技术有限公司**

**2024年11月11日**

**文件修订记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **版本号** | **变化状态** | **简要说明** | **变更人** | **变更日期** | **备注** |
| V1.0 | C | 创建编制 | 渗透技术 | 20241111 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

变化状态：C-创建，A-增加，M-修改，D-删除

|  |  |  |  |
| --- | --- | --- | --- |
| **测试对象** | 重点排污单位自动监控与基础数据库系统 | | |
| **测试类别** | 黑盒测试 | **委托日期** | 2024年11月11日 |
| **检测时间** | 2024年11月11日~ 2024年11月11日 | | |
| **测试结果** | 本次为第1次渗透测试。  通过本次渗透测试工作，在渗透测试范围内共发现2个可能潜在的安全问题。安全问题按照风险等级从高到低可分为高、中、低三个等级，其中高风险级别的问题有1个，中风险级别的问题1个，低风险为0个。  详情请看“安全漏洞详细分析”。  2024年11月11日 | | |

# 项目概述

## 前言

Web应用是网络应用和业务的集成，为所有用户提供方便的信息共享和应用共享。Web业务平台已经在电子商务、企业信息化中得到广泛的应用，企业都纷纷将应用架设在Web平台上，为客户提供更为方便、快捷的服务支持。伴随着这种趋势，入侵者也将注意力从以往对传统网络服务器的攻击逐步转移到了对 Web 业务的攻击上。根据 Gartner 的调查，信息安全攻击有 75% 都是发生在 Web 应用层而非网络层面上。同时，数据也显示，三分之二的 Web 站点都相当脆弱和易受攻击。

为了保障Web应用的稳定、安全、持续运行，就要对网上业务系统的信息安全风险做到早发现、早预防。渗透测试将结合国际国内信息安全最佳安全实践，通过对外网业务系统进行渗透测试，并根据测试结果提出相应的整改加固建议，协助用户完成整改加固实施，最终提高用户网上业务系统的安全水平。

## 渗透测试目的

分析客户WEB应用系统的安全现状，检测WEB应用系统的漏洞和安全问题，并验证其他已知的脆弱点。对系统的任何弱点、技术缺陷或漏洞的主动分析，并且以有利于攻击为目的而对漏洞加以利用。从而全面了解和掌握WEB应用系统的信息安全威胁和风险，为WEB应用系统开展安全调优及加固建设提供依据，并指导客户实施调优及加固工作，具体的目标包括：

帮助客户理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路；

通过改进建议，保证WEB应用系统和相关基础设施满足标准的安全性基线；

降低WEB应用系统信息安全事件发生的可能性；

保障WEB应用系统的安全、可靠、稳定运行。

## 渗透测试组织

为了保证渗透测试工作的顺利实施，确保项目质量达到预期目标，加强管理和协调合作，使工作和责任更加清晰明确，特建立分工明确，职责清楚，层次分明同时又能协调配合的项目管理组织结构。

渗透测试实施按照工作内容划分为以下职能小组：

* 领导协调小组：
  + 沟通协调参与各方的相关事宜；
  + 监督、控制项目进度及质量，及时发现项目实施过程中存在的问题，并及时组织改进；
  + 对重大问题进行决策；
* 项目经理：
  + 负责项目各阶段和总体工作的准备和实施工作；
  + 总体把握项目风险控制、时间安排和项目质量工作；
  + 向项目领导协调小组反馈问题；
  + 组织项目验收工作。
* 渗透测试小组：
  + 负责渗透测试中的信息收集、渗透测试和报告编写等各项实施工作；
  + 向项目经理反馈问题。

## 渗透测试原则

本次渗透测试工作中严格遵循以下原则：

标准性原则：渗透性测试方案的设计和实施应依据行业、国家、国际的相关标准进行；

规范性原则：服务提供商的工作过程和所有文档，应具有很好的规范性，以便于项目的跟踪和控制；

可控性原则：在保证测试质量的前提下，按计划进度执行，需要保证对渗透测试工作的可控性。安全评估的工具、方法和过程要在双方认可的范围之内合法进行；

整体性及有限性原则：渗透性测试的内容应包括用户等各个层面，渗透性测试的对象应包括和仅限于用户所指定的具体设备及系统，未经用户授权不得减小或扩大渗透性测试的范围和对象；

最小影响原则：渗透性测试工作应尽量避免影响系统和网络的正常运行，不对正常运行的系统和网络构成破坏和造成停产；

保密原则：渗透性测试的过程和结果应严格保密，不能泄露测试项目所涉及的任何打印和电子形式的有效数据和文件。

# 渗透测试方法



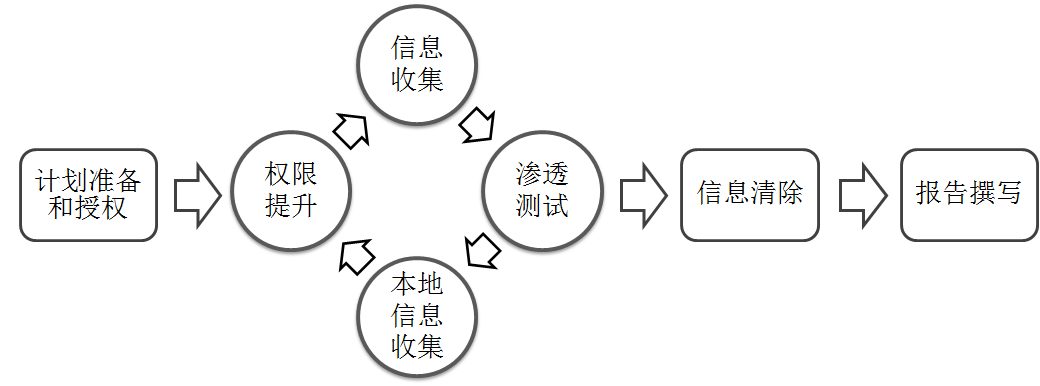
## 概述

渗透测试工作主要是对于已经采取了安全防护措施（安全产品、安全服务）或者即将采用安全防护措施的用户而言，明确网络当前的安全现状并对下一步的安全建设有重大的指导意义。渗透测试服务用于验证在当前的安全防护措施下网络、系统抵抗黑客攻击的能力。

任务组利用各种主流的攻击技术对网络、系统和应用进行远程攻击测试，目的是发现网络、系统和应用层面存在的安全漏洞和隐患，并提出相应的整改建议。

## 渗透测试方法

此次渗透测试的工作流程如下图所示：



计划和准备：在实际工作开展前需要同客户就渗透测试的目标、范围、工作方式以及实施成果进行讨论，并签订保密协议，成立渗透测试工作小组，在得到客户的渗透测试授权书后开展工作。

信息收集操作：收集渗透性测试所需信息（包括设备存活情况、网络拓扑情况以及扫描发现漏洞情况等），准备相关测试工具。

渗透测试：按照互联网渗透性测试实施计划进行测试验证。

本地信息收集：根据渗透深度情况，不断收集相关环境信息及漏洞情况，并进行综合分析。

权限提升：根据环境条件进行相关的权限提升，直到最高权限。

循环：在整个渗透过程中，就是不断地进行信息收集操作、渗透测试、本地信息收集和权限提升这一系列操作过程。

信息清除：根据渗透过程中使用的一些工具情况进行必要的清除过程。

报告撰写：根据渗透过程输出报告。

## 风险控制和管理

在渗透测试中，测试过程的安全可控是非常重要的。按照相关规定，任务组特别注意了测试过程本身的安全性问题，制定了安全控制措施和安全控制策略，采取了适当的风险规避、风险降低等方法，尽量避免影响业务的正常运行。在某些测试中，若无法确定测试过程是否安全，任务组将放弃相关测试以确保测试对象的安全。

另外，对于安全防护措施严密的网络、系统，在有限的时间内进行渗透测试可能不会获得成功结果。这从另一角度证明了网络、系统能够在一定程度上抵抗黑客的攻击。

## 风险等级说明

风险等级划分标准如下：

|  |  |
| --- | --- |
| **风险等级** | **等级划分依据** |
| 高风险 | 获得管理员权限，完全控制机器和应用系统；利用该漏洞能够实现文件上传建立目录，从中获取大量的数据库表结构信息或利用该漏洞发起的攻击直接引起应用系统服务器故障、响应异常或资金损失。 |
| 中风险 | 获取部分访问权限，尚未完全控制机器和应用系统；利用该漏洞能够实现提取应用系统上相关信息，下载文件，但暂时无法实现文件上传或者建立目录。利用该漏洞攻击间接影响应用系统运行或引起客户敏感信息外泄。 |
| 低风险 | 无法验证的可能存在风险以及需要依赖客户风险意识薄弱方可触发的风险。 |

# 渗透测试情况

## 渗透测试范围

根据前期的调研和了解，本次渗透测试工作范围如下：

| **序号** | **网站名称** | **地址** |
| --- | --- | --- |
| 1 | 重点排污单位自动监控与基础数据库系统 | https://zdjk.sthjj.beijing.gov.cn/amOnline/zdjk-company-base/login |

## 渗透测试记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **测试时间** | **漏洞情况** | **项目人** | **测试号** | **备注** |
| 1 | 20241111 | 高危：1 中危：1 低危：0 | 渗透技术 | P1.0 |  |

## 风险等级概况

通过本次渗透测试工作，在渗透测试范围内共发现2个可能潜在的安全问题。安全问题按照风险等级从高到低可分为高、中、低三个等级，其中高风险级别的问题有1个，中风险级别的问题有1个，低风险为0个。

按照风险等级分类如下图所示：

# 安全漏洞详细分析

## **重点排污单位自动监控与基础数据库**系统

### 跨站脚本漏洞（高危）

#### 漏洞情况

POST /amOnline/app/baseroute/requestRoute!list.page?method=/communicationSign/qy/order&\_t=1731295667817 HTTP/1.1

Host: zdjk.sthjj.beijing.gov.cn

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0

Accept: application/json, text/plain, \*/\*

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/json

Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJqb2ludHNreSIsImlhdCI6MTczMTI5NTA2NDI4MiwiZXhwIjoxNzMxMzA1ODY0MjgyLCJ1c2VyIjoiMTUwNjU4OTk5MDAifQ==.F490D3A23AE2F07DEFE8C9FFDA467885C05DFCC819AE19F19A914054E4B97E44

Content-Length: 1613

Origin: https://zdjk.sthjj.beijing.gov.cn

Connection: close

Referer: https://zdjk.sthjj.beijing.gov.cn/amOnline/zdjk-company/?v\_\_=1731294945810

Cookie: JSESSIONID=B13CF3A25AB34F6D9502E11A12823615; jointframe.cluster.sessionid=HZ7D69D376D7EF439CAAFBB5C7A2A49262; \_va\_id=830385d52861918e.1709972939.16.1725470969.1725470969.; \_va\_ref=%5B%22%22%2C%22%22%2C1725470969%2C%22https%3A%2F%2Fbjjp.bjysgl.cn%2F%22%5D; sensorsdata2015jssdkcross=%7B%22distinct\_id%22%3A%2218e5b602587a-01b0f0eb687cc4-e565623-1327104-18e5b602588822%22%7D

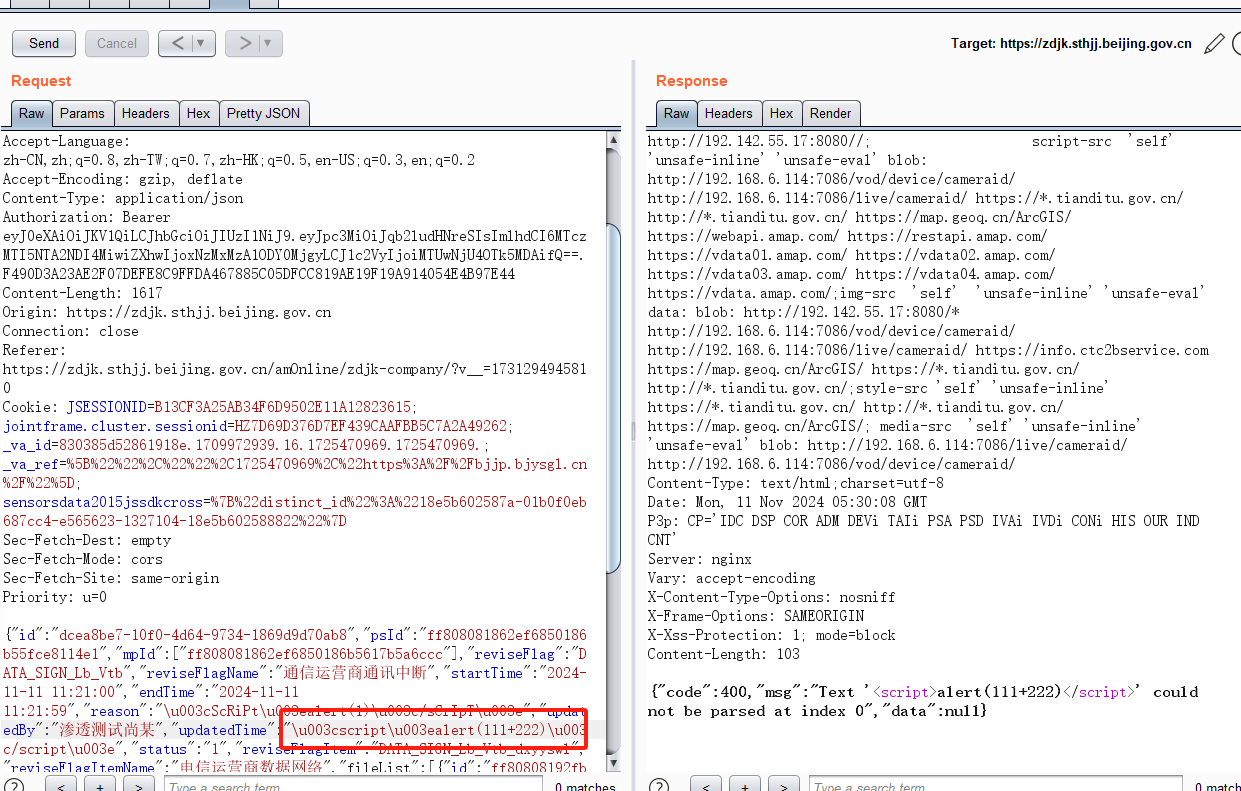
Sec-Fetch-Dest: empty

Sec-Fetch-Mode: cors

Sec-Fetch-Site: same-origin

Priority: u=0

{"id":"dcea8be7-10f0-4d64-9734-1869d9d70ab8","psId":"ff808081862ef6850186b55fce8114e1","mpId":["ff808081862ef6850186b5617b5a6ccc"],"reviseFlag":"DATA\_SIGN\_Lb\_Vtb","reviseFlagName":"通信运营商通讯中断","startTime":"2024-11-11 11:21:00","endTime":"2024-11-11 11:21:59","reason":"\u003cScRiPt\u003ealert(1)\u003c/sCrIpT\u003e","updatedBy":"渗透测试尚某","updatedTime":"\u003cscript\u003ealert(1+1)\u003c/script\u003e","status":"1","reviseFlagItem":"DATA\_SIGN\_Lb\_Vtb\_dxyyswl","reviseFlagItemName":"电信运营商数据网络","fileList":[{"id":"ff80808192fb2b070193193e7d3a15a8","ownerId":"7d6638b3-cb78-43c9-a018-7d3f3b913caf","regionCode":110000000,"module":"外部通讯中断附件","name":"111.docx","ext":"docx","filePath":"20241111/461004f912c14bb08ea6b2dea93d2132.docx","preview":null,"comment":null,"createdBy":"渗透测试尚某","createdTime":[2024,11,11,11,22,25,914000000],"dataStatus":1,"updatedBy":"渗透测试尚某","updatedTime":[2024,11,11,11,22,25,914000000],"newName":"461004f912c14bb08ea6b2dea93d2132.docx","uid":1731295657114,"status":"success"}],"duration":"0.01","psName":"非考核企业测试数据使用001、测试功能","mpName":"测试数据","isFileOpen":"1","isFileUpload":"1","signageType":null,"signageTime":null,"createdBy":"extractvalue(1,concat(char(126),md5(1951133048)))","createdTime":"2024-11-11 11:17:04","moduleCode":null,"shId":null,"shName":null,"monitorCode":null,"monitorName":null,"idMpId":[{"id":"dcea8be7-10f0-4d64-9734-1869d9d70ab8","mpId":"ff808081862ef6850186b5617b5a6ccc"}],"groupId":"c8dff316-439d-4a42-82e2-29592e844319","commitmentDesc":""}



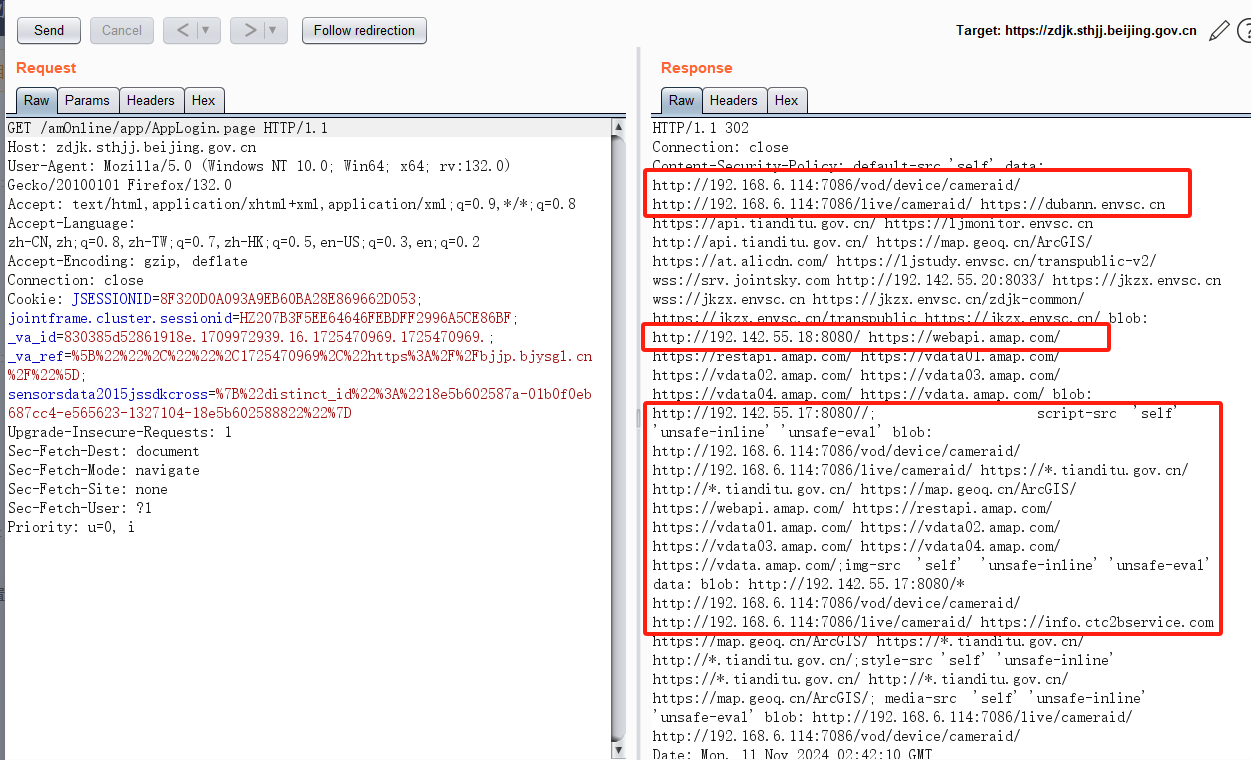


#### 漏洞危害

跨站脚本漏洞可以再分成两类：Stored attack 和 Reflected attack。这两种攻击的主要区别在于有效负荷到达服务器的方式。Stored attack 仅以某种形式存储在目标服务器上（例如在数据库中），或通过提交至公告板或访问者日志来进行存储。如果请求了所存储的信息，受害者将在自己的浏览器中检索和执行攻击代码。而 Reflected attack 则来自其他地方。当通过动态生成的网页中的服务器端，直接将 Web 客户端的用户输入包含在内时，就会出现 Reflected attack。通过某些社会工程手段，例如通过恶意链接或“伪装”表单，攻击者可以哄骗受害者提交信息，然后对信息进行修改以包含攻击代码，并将其发送至合法服务器。注入的代码随后将反射回用户的浏览器，由于此代码来自受信任的服务器，用户的浏览器将会执行此代码。两种攻击的影响都是相同的。

### 内网IP地址泄露（中危）

#### 漏洞情况

https://zdjk.sthjj.beijing.gov.cn/amOnline/app/AppLogin.page

#### 漏洞危害

攻击者发现泄露内网ip地址，该漏洞可能为攻击者提供内网主机信息收集便利。

# 整改建议

整改方案建议是建立在对用户远程渗透测试结果的基础之上提出的整改建议。

## 针对跨站脚本漏洞整改建议

xss漏洞本质上是一种html注入，也就是将html代码注入到网页中。那么其防御的根本就是在将用户提交的代码显示到页面上时做好一系列的过滤与转义

1.假定所有输入都是可疑的，必须对所有输入中的script、iframe等字样进行严格的检查。这里的输入不仅仅是用户可以直接交互的输入接口，也包括HTTP请求中的Cookie中的变量，HTTP请求头部中的变量等。

2.不仅要验证数据的类型，还要验证其格式、长度、范围和内容。

3.不要仅仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。

4.对输出的数据也要检查，数据库里的值有可能会在一个大网站的多处都有输出，即使在输入做了编码等操作，在各处的输出点时也要进行安全检查。

## 针对内网IP地址泄露漏洞整改建议

1、避免在互联网系统中泄露内网系统地址；

2、建议在不影响业务的情况下，删除泄露内网地址