基本信息

漏洞类型：未授权访问漏洞

漏洞等级：高危

厂商信息：此处需要手动搜索

漏洞简述

漏洞描述

整个网站服务器因为校验不严格，配置不完善导致不经过验证就能访问获取敏感数据

产生原因

1 后端代码没有对校验完整性检查，导致未授权访问  
 2 服务器配置错误，不严格的校验导致可以直接访问  
 3 对有效凭证没有定期检测与校验

漏洞危害

1 未授权直接登陆，可能导致敏感数据泄露  
 2 没有经过权限的校验，可能会导致任意用户直接接管账号权限  
 3 可能会造成数据库服务器的信息丢失

漏洞详情

网站漏洞报表

漏洞地址:https://bx.baidu.com:9200/\_cat/master

漏洞类型:Elasticsearch未授权访问漏洞

网站信息报表

百度权重 获取失败

网站主页 https://bx.baidu.com:9200

网站描述 暂无信息

网站标题 https://bx.baidu.com:9200

IP\_\_坐标 获取失败

所属\_\_IP 获取失败

网站年龄 暂无信息

备案编号 暂无信息

备案性质 暂无信息

备案名称 暂无信息

备案时间 暂无信息

百度收录 暂无信息

协议类型 获取失败

页面类型 获取失败

服务类型 获取失败

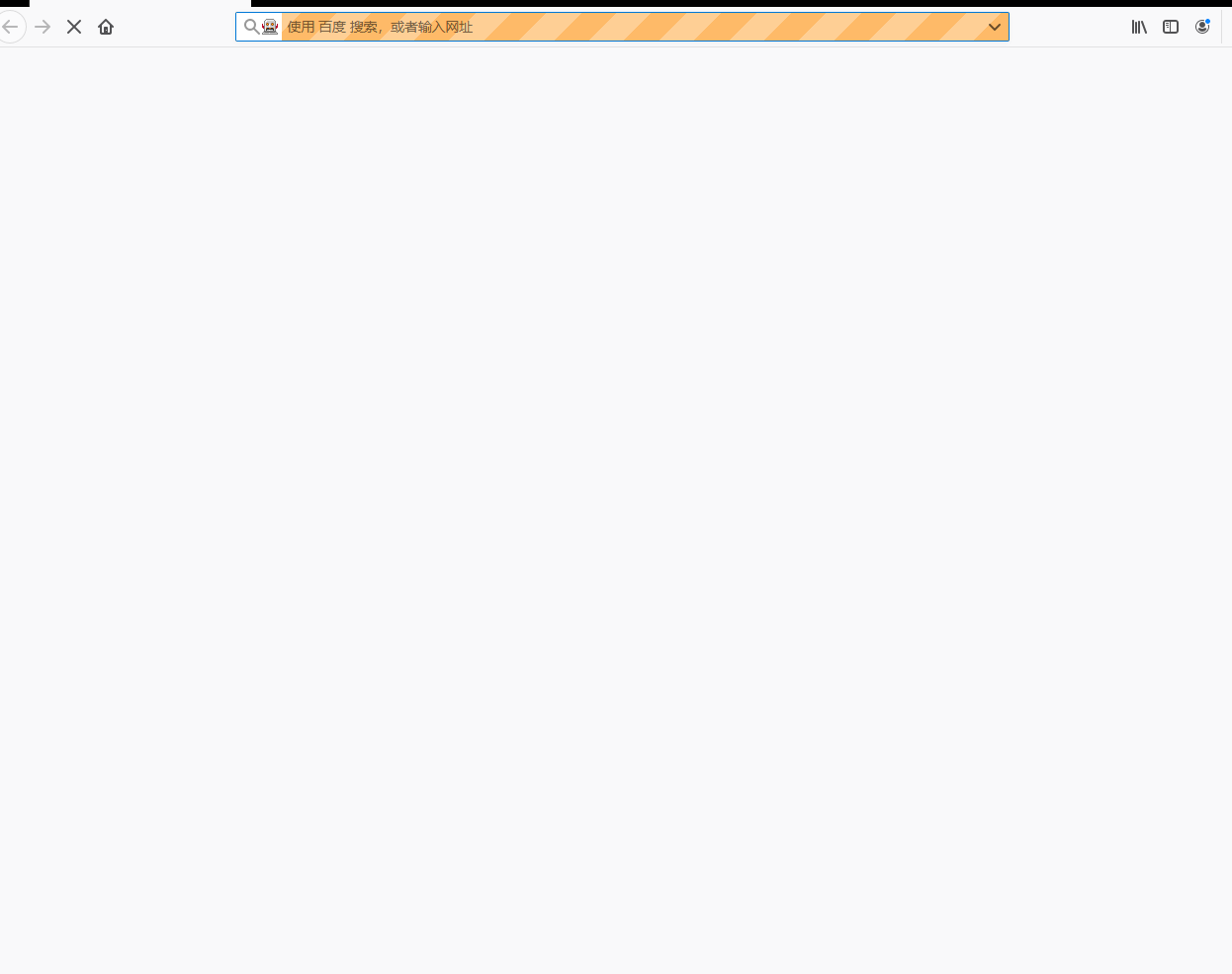
程序语言 获取失败

网站漏洞复现(使用Firefox浏览器)

访问网站

https://bx.baidu.com:9200/\_cat/master

返回结果



复现完成，验证存在未授权访问

修复建议

根源上进行修复

1 对后端校验代码加固检测  
 2 检测服务器配置文件信息  
 3 特定的文件设置合理的权限。  
 4 删除一些不需要的敏感文件。