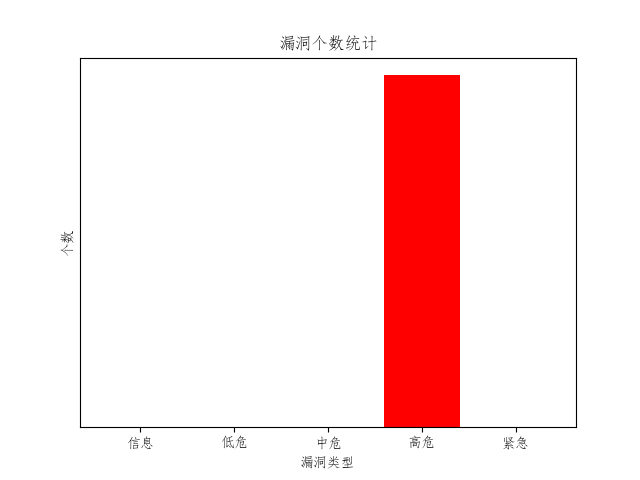
# "bWAPP - Login"网站安全报告

## **一、网站概况**

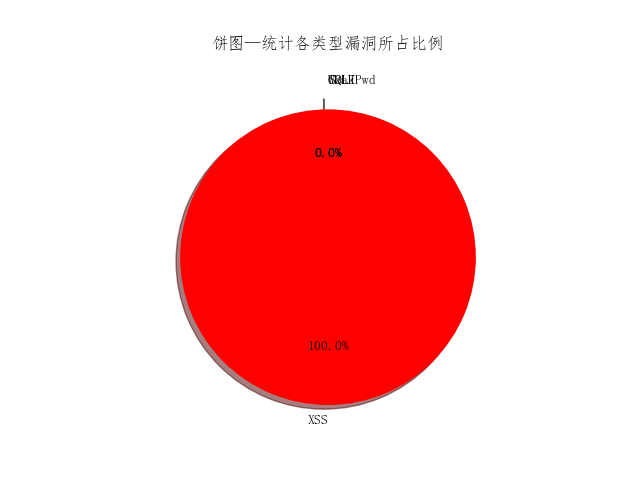
本次针对bWAPP - Login网站进行扫描，共发现1个漏洞，其中紧急漏洞0个，高危漏洞1个，中危漏洞0个，扫描共用时长为5分10秒。网站基本信息如下：

1. 域名：192.168.177.161
2. 扫描url总数：50
3. 扫描时长：5分10秒

## **二、漏洞分布情况**



等级漏洞情况



各类型漏洞分布

## **三、漏洞详情列表**

|  |  |
| --- | --- |
| 漏洞类型 | XSS |
| 漏洞等级 | 高危 |
| 漏洞URL | http://adfsdsf |
| 漏洞危害 | 1）网络钓鱼，盗取各类用户的账号 。   2）窃取用户Cookie，获取用户隐私或管理员权限，利用用户身份进一步执行操作，例如进行非法转账、强制发表日志等 。   3）强制弹出广告页面，刷流量等。   4）进行恶意操作，例如任意篡改页面信息，删除文章等，传播跨站脚本蠕虫，网页挂马等 。   5）进行基于大量的客户端攻击，如DDOS攻击。 |
| 修复建议 | 每个提交信息的客户端页面，通过服务器端脚本（JSP、ASP、ASPX、PHP等脚本）生成的客户端页面，提交的表单（FORM）或发出的连接请求中包含的所有变量，必须对变量的值进行检查。过滤其中包含的特殊字符，或对字符进行转义处理。特殊字符包括：  HTML标签的<符号、“符号、’符号、%符号等，以及这些符号的Unicode值；  客户端脚本（Javascript、VBScript）关键字：javascript、script等；  此外，对于信息搜索功能，不应在搜索结果页面中回显搜索内容。同时应设置出错页面，防止Web服务器发生内部错误时，错误信息返回给客户端。 |