网站安全评估报告

|  |  |
| --- | --- |
| 安全级别 | |
| 紧急 |  |
| 高危 |  |
| 中危 |  |
| 低危 |  |
| 提示 |  |
| 安全 | ● |

目标站点：http://www.jnszyy.com/

扫描时间：2022/06/27

扫描耗时：01:00:13

扫描模式：全部漏洞扫描

目录

[1 主机概况](#_bookmark1)

[1.1 任务信息](#_bookmark2)

[2 脆弱账号](#_bookmark3)

[2.1 脆弱账号列表](#_bookmark4)

[3 漏洞信息](#_bookmark5)

[3.1 全部漏洞概况](#_bookmark6)

[3.2 紧急漏洞概况](#_bookmark6)

[3.3 高危漏洞概况](#_bookmark6)

[3.4 中危漏洞概况](#_bookmark6)

[3.5 低危漏洞概况](#_bookmark6)

[4 业务风险信息](#_bookmark5)

[4.1 业务风险概况](#_bookmark6)

5 其他信息

5.1 操作系统类型

5.2 端口信息

5.3 安装软件信息

1 主机概况

1.1 任务信息

|  |  |
| --- | --- |
| 目标站点 | http://www.jnszyy.com/ |
| IP地址 | 139.129.116.10 |
| 扫描开始时间 | 2022/06/27 16:47:25 GMT+08:00 |
| 扫描结束时间 | 2022/06/27 17:47:38 GMT+08:00 |
| 漏洞扫描检查模板 | 全部漏洞扫描 |

2 脆弱账号

2.1 脆弱账号列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主机IP | 用户名 | 密码 | 应用类型 | 端口 |
| 未找到数据 | | | | |

3 漏洞信息

3.1 扫描总揽

|  |  |  |
| --- | --- | --- |
| 检测类型 | 检测项目 | 检测结果 |
| 预扫描 | 信息泄露 | ●安全 |
| HTTP安全头检查 | ●安全 |
| 传输层保护不足 | ●安全 |
| SSL安全配置检查 | ●安全 |
| 网站安全漏洞 | 跨站请求伪造 | ●安全 |
| 信息泄露 | ●安全 |
| 注入攻击 | ●安全 |
| 路径遍历 | ●安全 |
| 授权问题 | ●安全 |
| 弱密码 | ●安全 |
| 跨站脚本攻击 | ●安全 |

3.2 紧急漏洞概况

|  |  |  |  |
| --- | --- | --- | --- |
| 端口 | 协议 | 服务 | 漏洞 |
| 未发现 | | | |

3.3 高危漏洞概况

|  |  |  |  |
| --- | --- | --- | --- |
| 端口 | 协议 | 服务 | 漏洞 |
| 未发现 | | | |

3.4 中危漏洞概况

|  |  |  |  |
| --- | --- | --- | --- |
| 端口 | 协议 | 服务 | 漏洞 |
| 未发现 | | | |

3.5 低危漏洞概况

|  |  |  |  |
| --- | --- | --- | --- |
| 端口 | 协议 | 服务 | 漏洞 |
| 未发现 | | | |

4 业务风险信息

4.1 业务风险概况

|  |  |  |  |
| --- | --- | --- | --- |
| 风险类型 | 风险数量 | 风险内容 | 影响URL |
| 未发现 | | | |

5 其他信息

5.1 操作系统类型

|  |  |
| --- | --- |
| 操作系统 | 版本号 |
| Windows | Server 2019 Datacenter |

5.2 端口信息

|  |  |  |  |
| --- | --- | --- | --- |
| 端口 | 协议 | 状态 | 服务 |
| 80 | TCP | open | Hypertext Transfer Protocol (HTTP) | QUIC (from Chromium) for HTTP |
| 443 | TCP | open | Hypertext Transfer Protocol over TLS/SSL (HTTPS) | QUIC (from Chromium) for HTTPS |

5.3 安装软件信息

|  |  |
| --- | --- |
| 软件名称 | 版本号 |
| Apache | 未知 |