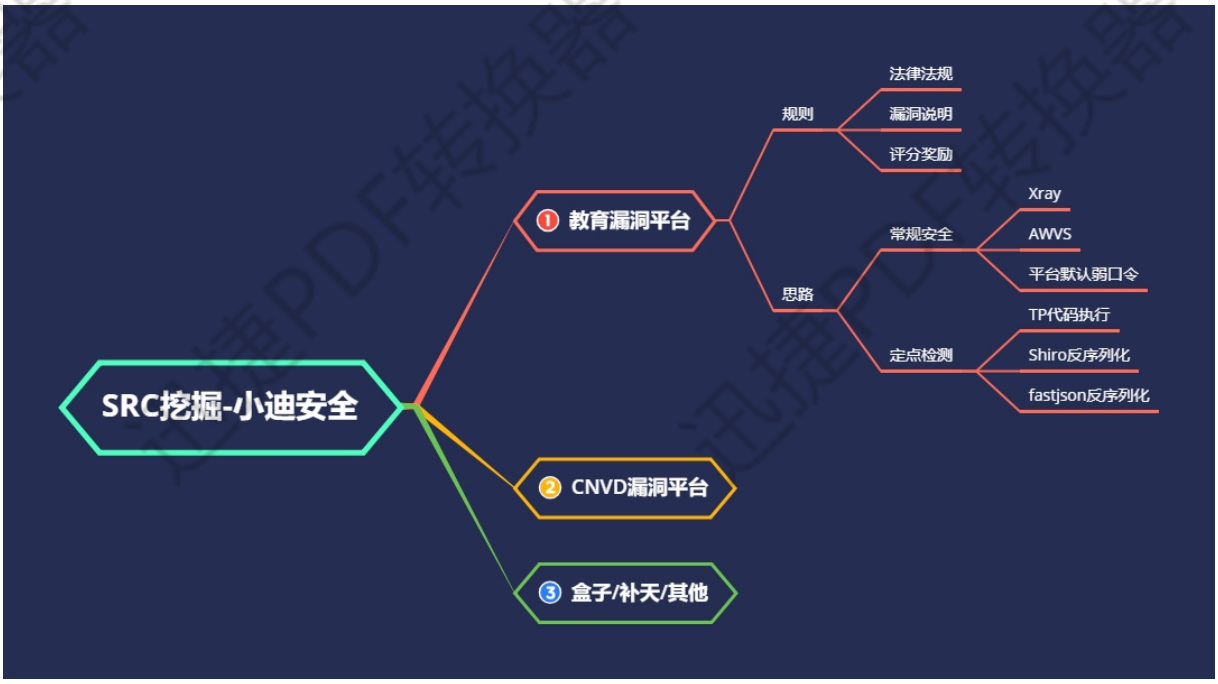
SRC 挖掘-教育行业平台&规则&批量自动化



参考：https://src.sjtu.edu.cn/introduction/

1.法律法规：

第八条 按照对信息系统机密性、可用性、完整性等三方面要素的影响评估，漏洞风险发现与技术验证应遵循无害化原则：

（一）信息系统机密性无害化验证指导场景：

可实现非授权访问或用户权限越权，在完成非授权逻辑、越权逻辑验证时，不应再获取和留存用户信息和信息系统文件信息；

可执行数据库查询条件，在获得数据库实例、库表名称等信息证明时，不应再查询涉及个人信息、业务信息的详细数据；

可获得系统主机、设备高权限，在获得当前用户系统环境信息证明时，不应再获取其他用户数据和业务数据信息；
禁止利用当前主机或设备作为跳板，对目标网络内部区域进行扫描测试。
（二） 信息系统可用性无害化验证指导场景：
应充分估计目标网络、系统的安全冗余，不进行有可能导致目标网络、主机、设备瘫痪的大流量、大规模扫描；
禁止执行可导致本地、远程拒绝服务危害的技术验证用例； 禁止执行有可能导致整体业务逻辑扰动、有可能产生用户经济财产损失的技术验证用例。
（三） 信息系统完整性无害化验证指导场景：
可获得信息系统后台功能操作权限，在获得当前用户角色属性证明时，不应再利用系统功能实施编辑、增删、篡改等操作；
可获得系统主机、设备、数据库高权限，在获得当前系统环境信息证明时，不应再执行文件、程序、数据的编辑、增删、篡改等操作；
可在信息系统上传可解析、可执行文件，在获得解析和执行权限逻辑证明时，不应驻留带有控制性目的程序、代码。

2.评分（Rank）
严重 9~10 高 7~9 中 4~7 低 0~4

3.如下漏洞将被忽略：
非（不确定）教育相关行业单位
不在奖励范围内的高校
虚假漏洞
本平台上已有其他白帽子提交过的漏洞
互联网上已经被公开的漏洞
提交到本平台后又提交到其他平台的漏洞
没有链接、截图、利用方法等漏洞详情不详细的漏洞
需要登录管理员后台才能触发的漏洞
需要中间人攻击的漏洞
Self-XSS
无敏感操作的 CSRF 漏洞
钓鱼漏洞
无敏感信息的 JSON Hijacking
扫描器取得结果，但白帽子无法提供利用方法的漏洞
无意义的源码泄露、内网 IP、域名泄露
拒绝服务漏洞

演示案例：

- Python-Fofa-Xray 联动常规批量自动化
- Python-Fofa-Exploit 联动定点批量自动化

- Python-Fofa-平台默认口令安全批量自动化

涉及资源：

https://www.seebug.org/

https://github.com/Miagz/XrayFofa

https://quake.360.cn/quake/welcome

https://github.com/TimelineSec/2020-Vulnerabilities

https://github.com/ihebski/DefaultCreds-cheat-sheet
