Web开发-Python应用&Flask框架&Jinja模版&绑定路由&参数传递&页面解析&SSTI注入



#知识点：  
1、安全开发-原生PHP-超级全局变量  
2、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
0、安全开发-原生PHP-数据库通讯  
1、安全开发-原生PHP-身份验证技术  
2、安全开发-Cookie&Session&Token  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-弱类型脆弱  
2、安全开发-原生PHP-函数&数据类型  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-开发组件集合  
2、安全开发-原生PHP-模版引擎渲染  
3、安全开发-原生PHP-第三方编辑器  
---------------------------------------------  
1、安全开发-框架技术-ThinkPHP  
2、安全开发-框架安全-版本&写法  
3、安全开发-ThinkPHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-文件安全操作  
2、安全开发-原生PHP-上传读取删除包含等  
3、安全开发-原生PHP-代码审计文件安全---------------------------------------------  
1、安全开发-原生PHP-RCE安全  
2、安全开发-原生PHP-代码执行&命令注入  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-PHP.INI安全  
2、安全开发-原生PHP-全局文件&单函数  
3、安全开发-原生PHP-流量检测&AI算法  
---------------------------------------------  
1、安全开发-原生JS-语法模型概念  
2、安全开发-Ajax技术-JQuery&Axios  
3、安全开发-Ajax应用-文件上传&用户登录---------------------------------------------  
1、安全开发-原生JS-DOM树&BOM对象  
2、安全开发-原生JS-DOM安全&安全案例  
---------------------------------------------  
1、安全开发-原生JS-数据加密&代码混淆  
2、安全开发-原生JS-数据解密安全案例  
---------------------------------------------  
1、安全开发-NodeJS-开发环境&功能实现  
2、安全开发-NodeJS-安全漏洞&案例分析  
3、安全开发-NodeJS-特有漏洞&代码审计  
---------------------------------------------  
1、安全开发-WebPack-构建打包器  
2、安全开发-WebPack-源码泄漏还原  
---------------------------------------------  
1、安全开发-微信小程序-搭建&开发&架构&安全  
2、安全开发-微信小程序-编译调试&反编译&泄露  
---------------------------------------------  
1、安全开发-JavaEE-Servlet技术  
2、安全开发-JavaEE-监听器&过滤器  
---------------------------------------------  
0、安全开发-JavaEE-构建工具-Maven  
1、安全开发-JavaEE-ORM框架-JDBC  
2、安全开发-JavaEE-ORM框架-Mybatis  
3、安全开发-JavaEE-ORM框架-Hibernate  
4、安全开发-JavaEE-ORM框架-SQL注入&预编译  
---------------------------------------------  
1、安全开发-JavaEE-类加载器&反射机制&链安全  
2、安全开发-JavaEE-成员变量&成员方法&构造方法  
---------------------------------------------  
1、安全开发-JavaEE-动态代理&序列化&反序列化  
2、安全开发-JavaEE-readObject&toString方法---------------------------------------------  
1、安全开发-JavaEE-原生序列化-URLDNS链分析  
2、安全开发-JavaEE-FastJson-JdbcRowSetImpl链分析  
---------------------------------------------  
1、安全开发-JavaEE-JNDI注入-LADP&RMI&DNS等  
2、安全开发-JavaEE-JNDI注入-项目工具&手工原理等  
---------------------------------------------  
1、安全开发-JavaEE-第三方依赖开发安全  
2、安全开发-JavaEE-数据转换&FastJson&XStream  
3、安全开发-JavaEE-Shiro身份验证&Log4j日志处理  
---------------------------------------------  
1、安全开发-JavaEE-开发框架-SpringBoot&路由&传参  
2、安全开发-JavaEE-模版引擎-Thymeleaf&Freemarker&Velocity  
---------------------------------------------  
1、安全开发-JavaEE-常见依赖-Actuator&Swagger  
2、安全开发-JavaEE-安全问题-配置安全&接口测试  
---------------------------------------------  
1、安全开发-JavaEE-身份验证-JWT&Security  
2、安全开发-JavaEE-安全问题-不安全写法&版本漏洞  
---------------------------------------------  
1、安全开发-JavaEE-WAR&JAR打包&反编译  
2、安全开发-JavaEE-SnakeYaml反序列化&链  
---------------------------------------------  
1、安全开发-Python-Flask&Jinja2  
2、安全开发-Python-路由传参&SSTI注入  
   
#章节点：(待补充)  
#具体点：(待补充)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **引擎** | **RCE** | **盲注** | **代码评估** | **文件读取** | **件写入** |
| Mako | ✓ | ✓ | Python | ✓ | ✓ |
| Jinja2 | ✓ | ✓ | Python | ✓ | ✓ |
| Python (code eval) | ✓ | ✓ | Python | ✓ | ✓ |
| Tornado | ✓ | ✓ | Python | ✓ | ✓ |
| Nunjucks | ✓ | ✓ | JavaScript | ✓ | ✓ |
| Pug | ✓ | ✓ | JavaScript | ✓ | ✓ |
| doT | ✓ | ✓ | JavaScript | ✓ | ✓ |
| Marko | ✓ | ✓ | JavaScript | ✓ | ✓ |
| JavaScript (code eval) | ✓ | ✓ | JavaScript | ✓ | ✓ |
| Dust (<= dustjs-helpers@1.5.0) | ✓ | ✓ | JavaScript | ✓ | ✓ |
| EJS | ✓ | ✓ | JavaScript | ✓ | ✓ |
| Ruby (code eval) | ✓ | ✓ | Ruby | ✓ | ✓ |
| Slim | ✓ | ✓ | Ruby | ✓ | ✓ |
| ERB | ✓ | ✓ | Ruby | ✓ | ✓ |
| Smarty (unsecured) | ✓ | ✓ | PHP | ✓ | ✓ |
| Smarty (secured) | ✓ | ✓ | PHP | ✓ | ✓ |
| PHP (code eval) | ✓ | ✓ | PHP | ✓ | ✓ |
| Twig (<=1.19) | ✓ | ✓ | PHP | ✓ | ✓ |
| Freemarker | ✓ | ✓ | Java | ✓ | ✓ |
| Velocity | ✓ | ✓ | Java | ✓ | ✓ |
| Twig (>1.19) | × | × | × | × | × |
| Dust (> dustjs-helpers@1.5.0) | × | × | × | × | × |

演示案例：

* WEB开发-Python-Flask框架&Jinja2模版
* WEB开发-Python-路由&传参&SSTI注入

#Flask+Jinja2  
0、Pycharm  
配置Python解析  
新建Flask项目  
   
1、路由传参  
@app.route('/')  
@app.route('/<id>')  
request.args.get  
request.form.get  
   
2、模版解析  
Template.render  
render\_template  
render\_template\_string  
   
3、SSTI安全  
<https://github.com/vladko312/SSTImap>  
   
4、实际应用  
CTF赛题：  
<https://www.cnblogs.com/gaorenyusi/p/18213835>  
代码审计：  
<https://mp.weixin.qq.com/s/e9xTNgqIE3Q3R3cNbMUH8A>

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)