一月刷题总结

原创

Uzero. 于 2022-01-21 22:14:15 发布 2214 收藏
文章标签： 安全 web安全

攻防世界--mail

布尔盲注，session伪造，format格式化字符串漏洞

攻防世界--weiphp

weiphp5.0框架漏洞：.git泄漏、SQL注入、文件上传漏洞(利用.phtml)

高校战疫网络安全分享赛: webtmp

pickle反序列化漏洞学习

BUUCTF--[CISCN2019 华北赛区 Day1 Web2]ikun

cookie伪造，pickle反序列化

攻防世界--Confusion1

SSTI

攻防世界--Confusion2

md5爆破，cookie伪造，php反序列化，pickle反序列化

BUUCTF--[CISCN2019 华北赛区 Day1 Web1]Dropbox

phar反序列化

长安战“疫”--Flag配送中心

HTTPoxy漏洞（CVE-2016-5385）

长安战“疫”--Baby_Upload

文件上传（利用.shtml）

长安战“疫”--flask

沙箱逃逸，ssti绕过

攻防世界--upload3

文件上传，php反序列化

攻防世界--url

php中伪协议利用

攻防世界--TimeKeeper

Flask debug pin安全问题

目录穿越

攻防世界--Web_python_flask_sql_injection

SQL注入

攻防世界--Web_python_block_chain

区块链双花攻击中的51% attack

攻防世界--upload
利用文件名SQL注入

攻防世界--Background_Management_System
gopher协议

攻防世界--smarty
SSTI，突破disable_functions

攻防世界--ics-02
SSRF，sql注入

攻防世界--filemanager
文件上传，二次注入

攻防世界--love_math
利用常用数学符号构成payload

攻防世界--blgdel
文件上传，利用.htaccess执行命令

buuctf--easyflask
session伪造+pickle反序列化

长安战“疫”-- Shiro?
log4j2利用

长安战“疫”
php无参数rce