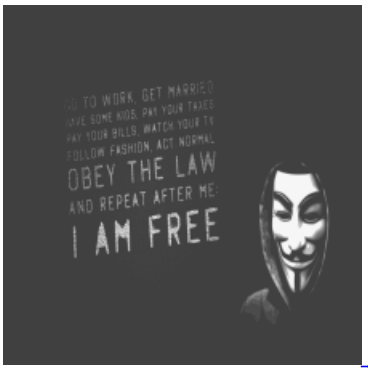
BUUCTF全题解目录（一）

原创



漏洞原理 题目知识点讲的详细：
王叹之
https://www.cnblogs.com/wangtanzhi/p/12239918.html

web

[HCTF 2018]WarmUp
※※※※
全解：https://www.jianshu.com/p/1c2998973197
PHP 代码审计
phpmyadmin 4.8.1任意文件包含

[强网杯 2019]随便注
※※※※
比赛web题全解：https://www.jianshu.com/p/db6e2576b674
fuzz一下，过滤规则得出，然后
show tables =>得表名
show columns from table_name =>

[护网杯 2018]easy_tornado
※※※※

模板注入，服务端模板注入攻击 （SSTI）,Tornado是python写web的应用框架；
http://www.creatapd.com/2018%E6%8A%A4%E7%BD%91%E6%9D%AFwriteup/
https://www.anquanke.com/post/id/161849?from=groupmessage#h2-1

[SUCTF 2019]EasySQL1

https://www.jianshu.com/p/5644f7c39c68

https://blog.csdn.net/qq_43619533/article/details/103434935

[SUCTF 2019]CheckIn1文件上传

https://xz.aliyun.com/t/6091

利用.user.ini来上传php后门

服务器脚本语言为PHP

服务器使用CGI / FastCGI模式

上传目录下要有可执行的php文件

[RoarCTF 2019]Easy Calc1

代码审计绕waf,chr(ascii)绕过

https://www.freebuf.com/articles/web/213359.html

https://blog.csdn.net/qq_41575340/article/details/102657091

[CISCN2019 华北赛区 Day2 Web1]Hack World PHP SQL注入

※※※

fuzz下 空格等被过滤

https://blog.csdn.net/weixin_44077544/article/details/102669185

脚本跑bool盲注

[De1CTF 2019]SSRF Me

极客大挑战web赛题复盘(全)

http://www.pdsdt.lovepdsdt.com/index.php/2019/11/19/2019_geek_web/

https://blog.csdn.net/qq_45372008/article/details/103018362

[极客大挑战 2019]LoveSQL

fuzz admin' or 11

用informationschema查询，%23用来注释

最后flag在passwordli,要将密码一起查出来，直接登入没用 □

[极客大挑战 2019]Secret File远程文件包含

没有过滤直接用

?filename=php://filter/read=convert.base64-encode/resource=xxx.php

出现两次302跳转，重点在抓包找到302页面所给的信息。

可以通过源代码查看，也可以bp抓包

[极客大挑战 2019]PHP(又来一只猫)

※※※

源码泄露：www.zip

反序列化:

1.private参数：url编码绕过

2.绕过__wake():当成员属性数目大于实际数目时可绕过wakeup方法(CVE-2016-7124)

https://blog.csdn.net/qq_45372008/article/details/103018362

[极客大挑战 2019]Upload

上传 .phtm后缀使服务器可以解析
bp抓包伪造图片数据

[网鼎杯 2018]Fakebook
※※※
https://www.cnblogs.com/wangtanzhi/p/11900128.html
SSRF
https://www.cnblogs.com/wangtanzhi/p/11900128.html
curl支持较多协议，常用的dict协议探测端口、利用gopher协议访问redis反弹shell。

> 禁用不需要的协议，仅仅允许http和https请求，可以防止类似于file://, gopher://, ftp:// 等引起的问题。
> 服务端需要认证交互，禁止非正常用户访问服务；
> 过滤输入信息，永远不要相信用户的输入，判断用户的输入是否是一个合理的URL地址
> 过滤返回信息，验证远程服务器对请求的响应是比较容易的方法，如果web应用是去获取某一种类型的文件。那么在把返*
> 回结果展示给用户之前先验证返回的信息是否符合标准。
> 统一错误信息，避免用户可以根据错误信息来判断远端服务器的端口状态。
> 禁止30x跳转
> 设置URL白名单或限制内网IP

方法有几种，非预期解
https://www.cnblogs.com/20175211lyz/p/11469695.html

[0CTF 2016]piapiapia PHP序列化
类题在请转到：
https://blog.csdn.net/qq_42812036/article/details/104273421
※※※※
目录扫描、网站代码审计、构造序列化、绕过过滤》
相关文章
https://www.cnblogs.com/Mrsm1th/p/6835592.html
https://p0sec.net/index.php/archives/114/
https://www.cnblogs.com/tr1ple/p/11156279.html
题解：
https://blog.csdn.net/zz_Caleb/article/details/96777110

[RoarCTF 2019]Easy Java 源码泄露
※※※※
类题在请转到：
https://blog.csdn.net/qq_42812036/article/details/104280196

[BUUCTF 2018]Online Tool
类题在请转到：
https://blog.csdn.net/qq_42812036/article/details/104290522

[SUCTF 2019]Pythonginx

类题在请转到：

https://blog.csdn.net/qq_42812036/article/details/104291695

题解：

https://www.cnblogs.com/wangtanzhi/p/12181032.html

https://bvlog.csdn.net/qq_42181428/article/details/99741920

[GXYCTF2019]Ping Ping Ping

类题在请转到：

https://blog.csdn.net/qq_42812036/article/details/104297163
