

WEB全套资料 干货满满

转载

锋刃科技



于 2018-12-20 15:12:10 发布



1997



收藏 6

sql注入

MySql

[MySQL False注入及技巧总结](#)

[MySQL 注入攻击与防御](#)

[sql注入学习总结](#)

[SQL注入防御与绕过的几种姿势](#)

[MySQL偏门技巧](#)

[mysql注入可报错时爆表名、字段名、库名](#)

[高级SQL注入:混淆和绕过](#)

MSSQL

[MSSQL DBA权限获取WEBSHELL的过程](#)

[MSSQL 注入攻击与防御](#)

[CLR在SQL Server中的利用技术分析](#)

PostgreSQL

[postgresql数据库利用方式](#)

[PostgreSQL渗透测试指南](#)

MongoDB

[MongoDB安全 – PHP注入检测](#)

技巧

[我的WafBypass之道（SQL注入篇）](#)

[Bypass 360主机卫士SQL注入防御](#)

[SQL注入之骚姿势小记](#)

[CTF比赛中SQL注入的一些经验总结](#)

[如何绕过WAF/NGWAF的libinjection实现SQL注入](#)

[HackMe-SQL-Injection-Challenges](#)

绕过WAF注入

[bypassGET和POST的注入防御思路分享](#)

[SQL注入的常规思路及奇葩技巧](#)

[Beyond SQLi: Obfuscate and Bypass](#)

工具

[使用burp macros和sqlmap绕过csrf防护进行sql注入](#)

[sqlmap 使用总结](#)

[SQLmap tamper脚本注释](#)

[通过Burp以及自定义的Sqlmap Tamper进行二次SQL注入](#)

前端安全I

XSS

[漫谈同源策略攻防](#)

[再谈同源策略](#)

[跨域方法总结](#)

[浅谈跨站脚本攻击与防御](#)

[跨站的艺术-XSS入门与介绍](#)

[Content Security Policy 入门教程](#)

[LoRexxar-CSP](#)

[XSS小记](#)

[DOMXSS Wiki](#)

[XSS Bypass Cookbook](#)

[从瑞士军刀到变形金刚—XSS攻击面拓展](#)

[我们要在任何可能的地方测试XSS漏洞](#)

[Alternative to Javascript Pseudo-Protocol](#)

[Bypassing CSP using polyglot JPEGs](#)

[Bypass unsafe-inline mode CSP](#)

[Chrome XSS Auditor – SVG Bypass](#)

[Cross site scripting payload for fuzzing](#)

[CRLF Injection and Bypass Tencent WAF](#)

[XSS Without Dots](#)

[不常见的xss利用探索](#)

[XSS攻击另类玩法](#)

[XSS易容术—bypass之编码混淆篇+辅助脚本编写](#)

[Xssing Web With Unicodes](#)

[Chrome 是怎么过滤反射型 XSS 的呢?](#)

[XSS Tricks - 从 Self-XSS 到登录你的账户](#)

[Electron hack —— 跨平台 XSS](#)

[XSS without HTML: Client-Side Template Injection with AngularJS](#)

[一个URL跳转引发的一系列“惨案”](#)

[利用反射型XSS二次注入绕过CSP form-action限制](#)

[看我如何挖到GoogleMaps XSS漏洞并获得5000刀赏金](#)

[利用XSS和CSRF漏洞远程实现PayPal合作方网站未授权账户访问](#)

[Modern Alchemy: Turning XSS into RCE](#)

[先知XSS挑战赛 - L3m0n Writeup](#)

CSRF

[用代码来细说Csrf漏洞危害以及防御](#)

[Cookie-Form型CSRF防御机制的不足与反思](#)

[关于JSON CSRF的一些思考](#)

[Exploiting JSON Cross Site Request Forgery \(CSRF\) using Flash](#)

[浅谈Session机制及CSRF攻防](#)

其他

[safari本地文件读取漏洞之扩展攻击面](#)

[利用脚本注入漏洞攻击ReactJS应用程序](#)

[当代 Web 的 JSON 劫持技巧](#)

SSRF

[Build Your SSRF Exploit Framework SSRF](#)

[SSRF攻击案例解析](#)

SSRF攻击实例解析

SSRF漏洞分析与利用

SSRF漏洞的挖掘经验

SSRF漏洞的利用与学习

SSRF漏洞中绕过IP限制的几种方法总结

利用ssrf漏洞获取google内部的dns信息

What is Server Side Request Forgery (SSRF)?

Use DNS Rebinding to Bypass SSRF in Java

DNS Rebinding技术绕过SSRF/代理IP限制

Discuz ssrf漏洞利用的几个python脚本

Discuz X系列门户文章功能SSRF漏洞挖掘与分析

SSRF to GET SHELL

SSRF Tips

XXE

浅谈XXE漏洞攻击与防御

XXE漏洞分析

XML实体注入漏洞攻与防

XML实体注入漏洞的利用与学习

XXE注入:攻击与防御 - XXE Injection: Attack and Prevent

XXE (XML External Entity Injection) 漏洞实践

黑夜的猎杀-盲打XXE

Hunting in the Dark - Blind XXE

XML External Entity漏洞培训模块

如何挖掘Uber网站的XXE注入漏洞

XXE被提起时我们会想到什么

XXE漏洞的简单理解和测试

XXE漏洞攻防之我见

XXE漏洞利用的一些技巧

神奇的Content-Type——在JSON中玩转XXE攻击

XXE-DTD Cheat Sheet

XML? Be cautious!

JSONP注入

JSONP注入解析

JSONP 安全攻防技术

一次关于JSONP的小实验与总结

利用JSONP跨域获取信息

关于跨域和jsonp的一些理解(新手向)

SSTI

Jinja2 template injection filter bypasses

乱弹Flask注入

服务端模板注入攻击 (SSTI) 之浅析

Exploring SSTI in Flask/Jinja2

Flask Jinja2开发中遇到的服务端注入问题研究

Flask Jinja2 开发中遇到的服务端注入问题研究 II

Exploring SSTI in Flask/Jinja2, Part II

Injecting Flask

Server-Side Template Injection: RCE for the modern webapp

Exploiting Python Code Injection in Web Applications

Exploiting Python Code Injection in Web Applications

利用 Python 特性在 Jinja2 模板中执行任意代码

Python 模板字符串与模板注入

代码执行

Command Injection/Shell Injection

PHP Code Injection Analysis

利用环境变量LD_PRELOAD来绕过php disable_function执行系统命令

Hack PHP mail additional_parameters

详细解析PHP mail()函数漏洞利用技巧

在PHP应用程序开发中不正当使用mail()函数引发的血案

BigTree CMS - Bypass CSRF filter and execute code with PHPMailer

基于时间反馈的RCE

正则表达式使用不当引发的系统命令执行漏洞

文件包含

Turning LFI into RFI

PHP文件包含漏洞总结

常见文件包含发生场景与防御

基于云端的本地文件包含漏洞

zip或phar协议包含文件

文件包含漏洞 一

文件包含漏洞 二

文件上传 / 解析漏洞

我的WafBypass之道（upload篇）

文件上传漏洞（绕过姿势）

服务器解析漏洞

文件上传总结

文件上传绕过姿势总结

尽最大可能分析上传源码及漏洞利用方式

从XSSer的角度测试上传文件功能

代码审计之逻辑上传漏洞挖掘

渗透测试方法论之文件上传

逻辑漏洞

代码审计之逻辑上传漏洞挖掘

逻辑至上——内含各种酷炫姿势

Web安全测试中常见逻辑漏洞解析（实战篇）

逻辑漏洞之密码重置

逻辑漏洞之支付漏洞

逻辑漏洞之越权访问

密码找回逻辑漏洞总结

一些常见的重置密码漏洞分析整理

密码逻辑漏洞小总结

漏洞挖掘之逻辑漏洞挖掘

tom0li: 逻辑漏洞小结

其他漏洞

Web之困笔记

常见Web源码泄露总结

Github信息泄露升级版案例
Hacking iSCSI

RPO(relative path overwrite)

初探 Relative Path Overwrite

Detecting and exploiting path-relative stylesheet import (PRSSI) vulnerabilities

RPO

A few RPO exploitation techniques

Web Cache

浅析 Web Cache 欺骗攻击

redis

利用redis写webshell

Redis 未授权访问配合 SSH key 文件利用分析

redis未授权访问漏洞利用总结

PHP相关I

弱类型

从弱类型利用以及对象注入到SQL注入

PHP中运算符的安全问题

PHP弱类型安全问题总结

浅谈PHP弱类型安全

php比较操作符的安全问题

随机数问题

Cracking PHP rand()

php里的随机数

php_mt_seed - PHP mt_rand() seed cracker

The GLIBC random number generator

一道伪随机数的CTF题

伪协议

谈一谈php://filter的妙用

php 伪协议

利用 Gopher 协议拓展攻击面

PHP伪协议之 Phar 协议（绕过包含）

PHP伪协议分析与应用

LFI、RFI、PHP封装协议安全问题学习

java-WebI

序列化

PHP反序列化漏洞

浅谈php反序列化漏洞

PHP反序列化漏洞成因及漏洞挖掘技巧与案例

php mail header injection

What is Email Header Injection?

PHP Email Injection Example

其他

[从WordPress SQLi谈PHP格式化字符串问题](#)

[php & apache2 & 操作系统之间的一些黑魔法](#)

[php内存破坏漏洞exp编写和禁用函数绕过](#)

[挖掘PHP禁用函数绕过利用姿势](#)

[.user.ini文件构成的PHP后门](#)

php代码审计

[论PHP常见的漏洞](#)

[浅谈代码审计入门实战：某博客系统最新版审计之旅](#)

[ctf中的php代码审计技巧](#)

[PHP代码审计tips](#)

[代码审计之文件越权和文件上传搜索技巧](#)

[PHP代码审计入门集合](#)

[PHP代码审计学习](#)

[PHP漏洞挖掘思路+实例](#)

[PHP漏洞挖掘思路+实例 第二章](#)

[浅谈代码审计入门实战：某博客系统最新版审计之旅](#)

反序列

[Java-Deserialization-Cheat-Sheet](#)

[如何攻击Java反序列化过程](#)

[深入理解JAVA反序列化漏洞](#)

[Attacking Java Deserialization](#)

[jackson反序列化详细分析](#)

Struct2

[Struts2 命令执行系列回顾](#)

java-Web代码审计

[Java代码审计连载之一—SQL注入](#)

[Java代码审计连载之一任意文件下载](#)

[Java代码审计连载之一—XSS](#)

[Java代码审计连载之一—添油加醋](#)

其他

[层层放大java审计的攻击面](#)

[以Java的视角来聊聊SQL注入](#)

[站在Java的视角，深度分析防不胜防的小偷——“XSS”](#)

[你的 Java web 配置安全吗？](#)

[Java代码审计PPT](#)

[spring任意文件读取](#)

python-Web

[Exploiting Python Deserialization Vulnerabilities](#)

[Python 格式化字符串漏洞（Django为例）](#)

[format注入](#)

[Be Careful with Python's New-Style String Format](#)

Be Careful with Python's New-Style String Format

Python urllib HTTP头注入漏洞

Hack Redis via Python urllib HTTP Header Injection

Python Waf黑名单过滤下的一些Bypass思路

Python Sandbox Bypass

pyt: 针对 Python 应用程序的源码静态分析工具

Node.js

Pentesting Node.js Application : Nodejs Application Security(需翻墙)

从零开始学习渗透Node.js应用程序

WAF相关

牛逼牛逼的payload和bypass总结

WAF绕过参考资料

浅谈WAF绕过技巧

addslashes防注入的绕过案例

浅谈json参数解析对waf绕过的影响

WAF攻防研究之四个层次Bypass WAF

使用HTTP头去绕过WAF

会找漏洞的时光机: Pinpointing Vulnerabilities

渗透测试I

Course

Web Service 渗透测试从入门到精通

渗透标准

Penetration Testing Tools Cheat Sheet

信息收集

看我如何收集全网IP的whois信息

浅谈Web渗透测试中的信息收集

渗透测试教程：如何侦查目标以及收集信息？

本屌的web漏洞扫描器思路 技巧总结（域名信息收集篇）

子域名的艺术

实例演示如何科学的进行子域名收集

【渗透神器系列】搜索引擎

域渗透基础简单信息收集（基础篇）

内网渗透定位技术总结

后渗透攻防的信息收集

安全攻城师系列文章—敏感信息收集

子域名枚举的艺术

论二级域名收集的各种姿势

我眼中的渗透测试信息搜集

大型目标渗透—01入侵信息搜集

乙方渗透测试之信息收集

渗透

【玩转Linux系统】Linux内网渗透

渗透测试指南之域用户组的范围

内网主机发现技巧补充

[Linux 端口转发特征总结](#)

[内网渗透（持续更新）](#)

[实战 SSH 端口转发](#)

[多重转发渗透隐藏内网](#)

[内网转发姿势](#)

[内网转发的工具](#)

[Linux 下多种反弹 shell 方法](#)

[php 反弹shell](#)

[利用ew轻松穿透多级目标内网](#)

[windows内网渗透杂谈](#)

[Windows域横向渗透](#)

[内网渗透中转发工具总结](#)

[内网渗透思路整理与工具使用](#)

[Cobalt strike在内网渗透中的使用](#)

[反向socks5代理\(windows版\)](#)

[Windows渗透基础](#)

[通过双重跳板漫游隔离内网](#)

[A Red Teamer's guide to pivoting](#)

[穿越边界的姿势](#)

[内网端口转发及穿透](#)

[秘密渗透内网——利用 DNS 建立 VPN 传输隧道](#)

[Reverse Shell Cheat Sheet](#)

渗透实战

[挖洞经验 | 看我如何综合利用4个漏洞实现GitHub Enterprise远程代码执行](#)

[Splash SSRF到获取内网服务器ROOT权限](#)

[Pivoting from blind SSRF to RCE with HashiCorp Consul](#)

[我是如何通过命令执行到最终获取内网Root权限的](#)

[信息收集之SVN源代码社工获取及渗透实战](#)

[SQL注入+XXE+文件遍历漏洞组合拳渗透Deutsche Telekom](#)

[渗透 Hacking Team](#)

[由视频系统SQL注入到服务器权限](#)

[From Serialized to Shell :: Exploiting Google Web Toolkit with EL Injection](#)

[浅谈渗透测试实战](#)

[渗透测试学习笔记之案例一](#)

[渗透测试学习笔记之案例二](#)

[渗透测试学习笔记之案例四](#)

[记一次内网渗透](#)

提权

[提权技巧](#)

[linux-kernel-exploits Linux平台提权漏洞集合](#)

[windows-kernel-exploits Windows平台提权漏洞集合](#)

[Linux MySQL Udf 提权](#)

[windows提权系列上篇](#)

[Windows提权系列中篇](#)

渗透技巧

[乙方渗透测试之Fuzz爆破](#)

[域渗透神器Empire安装和简单使用](#)

[如何将简单的Shell转换为完全交互式的TTY](#)

[60字节 - 无文件渗透测试实验](#)

[内网渗透思路探索之新思路的探索与验证](#)

[Web端口复用正向后门研究实现与防御](#)

[谈谈端口探测的经验与原理](#)

[端口渗透总结](#)

[端口扫描那些事](#)

[渗透技巧——通过cmd上传文件的N种方法](#)

[域渗透TIPS: 获取LAPS管理员密码](#)

[域渗透——Security Support Provider](#)

[内网渗透随想](#)

[域渗透之流量劫持](#)

[渗透技巧——快捷方式文件的参数隐藏技巧](#)

[后门整理](#)

[Linux后门整理合集（脉搏推荐）](#)

运维

[黑客入侵应急分析手工排查](#)

[企业常见服务漏洞检测&修复整理](#)

[Linux基线加固](#)

CTFI

技巧总结

[ctf-wiki](#)

[CTF中那些脑洞大开的编码和加密](#)

[CTF加密与解密](#)

[CTF中图片隐藏文件分离方法总结](#)

[Md5扩展攻击的原理和应用](#)

[CTF比赛中关于zip的总结](#)

[十五个Web狗的CTF出题套路](#)

[CTF备忘录](#)

[rcoil:CTF线下攻防赛总结](#)

杂

[谈谈HTML5本地存储——WebStorage](#)

[Linux下容易被忽视的那些命令用法](#)

[各种脚本语言不同版本一句话开启 HTTP 服务器的总结](#)

[WebAssembly入门：将字节码带入Web世界](#)

[phpwind 利用哈希长度扩展攻击进行getshell](#)

[深入理解hash长度扩展攻击（sha1为例）](#)

[Joomla 框架的程序执行流程及目录结构分析](#)

[如何通过恶意插件在Atom中植入后门](#)

本文标题:Web-Security-Learning

文章作者:chybeta

发布时间:2017年08月19日 - 10:08

最后更新:2017年09月13日 - 08:09

原始链接:<http://chybeta.github.io/2017/08/19/Web-Security-Learning/>

许可协议: 署名-非商业性使用-禁止演绎 4.0 国际 转载请保留原文链接及作者。

文章转载自T00LS论坛<https://www.t00ls.net/articles-41759.html>（转载已获得作者算命縉子许可）