Bug Bounty Reference

转载

Bug Bounty Reference

根据Bug归类的Bug赏金记录列表，灵感来自https://github.com/djadmin/awesome-bug-bounty

介绍

我几个月来一直在阅读Bug Bounty的文章，我发现当我发现某种类型的漏洞而我不知道如何利用它时阅读相关的文章是非常有用的。假设你在一个网站上找到了一个RPO（Relativce Path Overwrite），但是你不知道如何利用它，那么完美的去处就在这里。或者您发现您的客户正在使用oauth机制，但您不知道我们应该如何测试它，另一个理想的去处就是这里

我的目的是制作一份完整且完整的常见漏洞列表，这些漏洞是公开披露的bug赏金，并让Bug Bounty Hunter使用此页面作为参考，当他们想在Bug悬赏期间了解某种特定漏洞并测试时，随时提交pull请求。

Cross-Site Scripting (XSS)

- Sleeping stored Google XSS Awakens a $5000 Bounty by Patrik Fehrenbach
- RPO that lead to information leakage in Google by filedescriptor

- God-like XSS, Log-in, Log-out, Log-in in Uber by Jack Whitton
- Three Stored XSS in Facebook by Nirgoldshlager
- Using a Braun Shaver to Bypass XSS Audit and WAF by Frans Rosen
- An XSS on Facebook via PNGs & Wonky Content Types by Jack Whitton
    - he is able to make stored XSS from a irrelevant domain to main facebook domain
- Stored XSS in *.ebay.com by Jack Whitton
- Complicated, Best Report of Google XSS by Ramzes
- Tricky Html Injection and Possible XSS in sms-be-vip.twitter.com by secgeek
- Command Injection in Google Console by Venkat S
- Facebook's Moves - OAuth XSS by PAULOS YIBELO
- Stored XSS in Google Docs (Bug Bounty) by Harry M Gertos
- Stored XSS on developer.uber.com via admin account compromise in Uber by James Kettle (albinowax)
- Yahoo Mail stored XSS by Klikki Oy
- Abusing XSS Filter: One ^ leads to XSS(CVE-2016-3212) by Masato Kinugawa
- Youtube XSS by fransrosen
- Best Google XSS again - by Krzysztof Kotowicz
- IE & Edge URL parsin Problem - by detectify
- Google XSS subdomain Clickjacking
- Microsoft XSS and Twitter XSS
- Google Japan Book XSS
- Flash XSS mega nz - by frans
- Flash XSS in multiple libraries - by Olivier Beg
- xss in google IE, Host Header Reflection
- Years ago Google xss
- xss in google by IE weird behavior
- xss in Yahoo Fantasy Sport
- xss in Yahoo Mail Again, worth $10000 by Klikki Oy
- Sleeping XSS in Google by securityguard
- Decoding a .htpasswd to earn a payload of money by securityguard
- Google Account Takeover
- AirBnb Bug Bounty: Turning Self-XSS into Good-XSS #2 by geekboy
- Uber Self XSS to Global XSS
- How I found a $5,000 Google Maps XSS (by fiddling with Protobuf) by Marin MoulinierFollow
- Airbnb – When Bypassing JSON Encoding, XSS Filter, WAF, CSP, and Auditor turns into Eight Vulnerabilities by Brett
- XSSI, Client Side Brute Force
- postMessage XSS Bypass
- XSS in Uber via Cookie by zhchbin
- Stealing contact form data on www.hackerone.com using Marketo Forms XSS with postMessage frame-jumping and jQuery-JSONP by frans
- XSS due to improper regex in third party js Uber 7k XSS
- XSS in TinyMCE 2.4.0 by Jelmer de Hen
- Pass uncoded URL in IE11 to cause XSS
- Twitter XSS by stopping redirection and javascript scheme by Sergey Bobrov
- Auth DOM Uber XSS
- Managed Apps and Music: two Google reflected XSSes
- App Maker and Colaboratory: two Google stored XSSes
- XSS in www.yahoo.com
- Stored XSS, and SSRF in Google using the Dataset Publishing Language

- Stored XSS on Snapchat

Brute Force

- Web Authentication Endpoint Credentials Brute-Force Vulnerability by Arne Swinnen
- InstaBrute: Two Ways to Brute-force Instagram Account Credentials by Arne Swinnen
- How I Could Compromise 4% (Locked) Instagram Accounts by Arne Swinnen
- Possibility to brute force invite codes in riders.uber.com by r0t
- Brute-Forcing invite codes in partners.uber.com by Efkan Gökbaş (mefkan)
- How I could have hacked all Facebook accounts by Anand Prakash
- Facebook Account Take Over by using SMS verification code, not accessible by now, may get update from author later by Arun Sureshkumar

SQL Injection

- SQL injection in Wordpress Plugin Huge IT Video Gallery in Uber by glc
- SQL Injection on sctrack.email.uber.com.cn by Orange Tsai
- Yahoo – Root Access SQL Injection – tw.yahoo.com by Brett Buerhaus
- Multiple vulnerabilities in a WordPress plugin at drive.uber.com by Abood Nour (syndr0me)
- GitHub Enterprise SQL Injection by Orange
- Yahoo SQL Injection to Remote Code Exection to Root Privilege by Ebrahim Hegazy

Stealing Access Token

- Facebook Access Token Stolen by Jack Whitton -

  Obtaining Login Tokens for an Outlook, Office or Azure Account by Jack Whitton
- Bypassing Digits web authentication's host validation with HPP by filedescriptor
- Bypass of redirect_uri validation with /../ in GitHub by Egor Homakov
- Bypassing callback_url validation on Digits by filedescriptor
- Stealing livechat token and using it to chat as the user - user information disclosure by Mahmoud G. (zombiehelp54)
- Change any Uber user's password through /rt/users/passwordless-signup - Account Takeover (critical) by mongo (mongo)
- Internet Explorer has a URL problem, on GitHub by filedescriptor.
- How I made LastPass give me all your passwords by labsdetectify
- Steal Google Oauth in Microsoft
- Steal FB Access Token
- Paypal Access Token Leaked
- Steal FB Access Token
- Appengine Cool Bug
- Slack post message real life experience
- Bypass redirect_uri by nbsriharsha
- Stealing Facebook Messenger nonce worth 15k

  Steal Oculus Nonce and Oauth Flow Bypass

Google oauth bypass

- Bypassing Google Authentication on Periscope's Administration Panel By Jack Whitton

CSRF

- Messenger.com CSRF that show you the steps when you check for CSRF by Jack Whitton
- Paypal bug bounty: Updating the Paypal.me profile picture without consent (CSRF attack) by Florian Courtial
- Hacking PayPal Accounts with one click (Patched) by Yasser Ali

- Add tweet to collection CSRF by vijay kumar
- Facebookmarketingdevelopers.com: Proxies, CSRF Quandry and API Fun by phwd
- How i Hacked your Beats account ? Apple Bug Bounty by @aaditya_purani
- FORM POST JSON: JSON CSRF on POST Heartbeats API by Dr.Jones
- Hacking Facebook accounts using CSRF in Oculus-Facebook integration

Remote Code Execution

- JDWP Remote Code Execution in PayPal by Milan A Solanki
- XXE in OpenID: one bug to rule them all, or how I found a Remote Code Execution flaw affecting Facebook's servers by Reginaldo Silva
- How I Hacked Facebook, and Found Someone's Backdoor Script by Orange Tsai
- How I Chained 4 vulnerabilities on GitHub Enterprise, From SSRF Execution Chain to RCE! by Orange Tsai
- uber.com may RCE by Flask Jinja2 Template Injection by Orange Tsai
- Yahoo Bug Bounty - *.login.yahoo.com Remote Code Execution by Orange Tsai (Sorry its in Chinese Only)
- How we broke PHP, hacked Pornhub and earned $20,000 by Ruslan Habalov
    - *Alert*, God-like Write-up, make sure you know what is ROP before clicking, which I don't =(
- RCE deal to tricky file upload by secgeek
- WordPress SOME bug in plupload.flash.swf leading to RCE in Automatic by Cure53 (cure53)
- Read-Only user can execute arbitraty shell commands on AirOS by 93c08539 (93c08539)
- Remote Code Execution by impage upload! by Raz0r (ru_raz0r)
- Popping a shell on the Oculus developer portal by Bitquark
- Crazy! PornHub RCE AGAIN!!! How I hacked Pornhub for fun and profit - 10,000$ by 5haked
- PayPal Node.js code injection (RCE) by Michael Stepankin
- eBay PHP Parameter Injection lead to RCE
- Yahoo Acqusition RCE
- Command Injection Vulnerability in Hostinger by @alberto__segura
- RCE in Airbnb by Ruby Injection by buerRCE
- RCE in Imgur by Command Line
- RCE in git.imgur.com by abusing out dated software by Orange Tsai
- RCE in Disclosure
- Remote Code Execution by struct2 Yahoo Server
- Command Injection in Yahoo Acquisition
- Paypal RCE
- $50k RCE in JetBrains IDE
- $20k RCE in Jenkin Instance by @nahamsec
- Yahoo! RCE via Spring Engine SSTI
- Telekom.de Remote Command Execution! by Ebrahim Hegazy
- Magento Remote Code Execution Vulnerability! by Ebrahim Hegazy
- Yahoo! Remote Command Execution Vulnerability by Ebrahim Hegazy

Deserialization

- Java Deserialization in manager.paypal.com by Michael Stepankin
- Instagram's Million Dollar Bug by Wesley Wineberg
- (Ruby Cookie Deserialization RCE on facebooksearch.algolia.com by Michiel Prins (michiel)
- Java deserialization by meals

Image Tragick

- Exploiting ImageMagick to get RCE on Polyvore (Yahoo Acquisition) by NaHamSec
- Exploting ImageMagick to get RCE on HackerOne by c666a323be94d57
- Trello bug bounty: Access server's files using ImageTragick by Florian Courtial
- 40k fb rce
- Yahoo Bleed 1
- Yahoo Bleed 2

Direct Object Reference (IDOR)

- Trello bug bounty: The websocket receives data when a public company creates a team visible board by Florian Courtial
- Trello bug bounty: Payments informations are sent to the webhook when a team changes its visibility by Florian Courtial
- Change any user's password in Uber by mongo
- Vulnerability in Youtube allowed moving comments from any video to another by secgeek
    - It's *Google* Vulnerability, so it's worth reading, as generally it is more difficult to find Google vulnerability
- Twitter Vulnerability Could
  Credit Cards from Any Twitter Account by secgeek
- One Vulnerability allowed deleting comments of any user in all Yahoo sites by secgeek
- Microsoft-careers.com Remote Password Reset by Yaaser Ali
- How I could change your eBay password by Yaaser Ali
- Duo Security Researchers Uncover Bypass of PayPal's Two-Factor Authentication by Duo Labs
- Hacking Facebook.com/thanks Posting on behalf of your friends! by Anand Prakash
- How I got access to millions of [redacted] accounts
- All Vimeo Private videos disclosure via Authorization Bypass with Excellent Technical Description by Enguerran Gillier (opnsec)
- Urgent: attacker can access every data source on Bime by Jobert Abma (jobert)
- Downloading password protected / restricted videos on Vimeo by Gazza (gazza)
- Get organization info base on uuid in Uber by Severus (severus)
- How I Exposed your Primary Facebook Email Address (Bug worth $4500) by Roy Castillo
- DOB disclosed using "Facebook Graph API Reverse Engineering" by Raja Sekar Durairaj
- Change the description of a video without publish_actions permission in Facebook by phwd
- Response To Request Injection (RTRI) by ?, be honest, thanks to this article, I have found quite a few bugs because of using his method, respect to the author!
- Leak of all project names and all user names , even across applications on Harvest by Edgar Boda-Majer (eboda)
- Changing paymentProfileUuid when booking a trip allows free rides at Uber by Matthew Temmy (temmyscript)
- View private tweet
- Uber Enum UUID
- Hacking Facebook's Legacy API, Part 1: Making Calls on Behalf of Any User by Stephen Sclafani
- Hacking Facebook's Legacy API, Part 2: Stealing User Sessions by Stephen Sclafani
- Delete FB Video
- Delete FB Video
- Facebook Page Takeover by Manipulating the Parameter by arunsureshkumar
- Viewing private Airbnb Messages
- IDOR tweet as any user by kedrisec
- Classic IDOR endpoints in Twitter
- Mass Assignment, Response to Request Injection, Admin Escalation by sean
- Getting any Facebook user's friend list and partial payment card details
- Manipulation of ETH balance

XXE

- How we got read access on Google's production servers by detectify
- Blind OOB XXE At UBER 26+ Domains Hacked by Raghav Bisht
- XXE through SAML
- XXE in Uber to read local files
- XXE by SVG in community.lithium.com

Unrestricted File Upload

- File Upload XSS in image uploading of App in mopub by vijay kumar
- RCE deal to tricky file upload by secgeek
- File Upload XSS in image uploading of App in mopub in Twitter by vijay kumar (vijay_kumar1110)

Server Side Request Forgery (SSRF)

- ESEA Server-Side Request Forgery and Querying AWS Meta Data by Brett Buerhaus
- SSRF to pivot internal network
- SSRF to LFI
- SSRF to query google internal server
- SSRF by using third party Open redirect by Brett BUERHAUS
- SSRF tips from BugBountyHQ of Images
- SSRF to RCE
- XXE at Twitter
- Blog post: Cracking the Lens: Targeting HTTP's Hidden Attack-Surface
- Plotly AWS Metadata SSRF (and a stored XSS)

Race Condition

- Race conditions on Facebook, DigitalOcean and others (fixed) by Josip Franjković
- Race Conditions in Popular reports feature in HackerOne by Fábio Pires (shmoo)
- Hacking Starbuck for unlimited money by Egor Homakov

Business Logic Flaw

- How I Could Steal Money from Instagram, Google and Microsoft by Arne Swinnen
- How I could have removed all your Facebook notes
- Facebook - bypass ads account's roles vulnerability 2015 by POUYA DARABI
- Uber Ride for Free by anand praka
- Uber Eat for Free by

Authentication Bypass

- OneLogin authentication bypass on WordPress sites via XMLRPC in Uber by Jouko Pynnönen (jouko)
- 2FA PayPal Bypass by henryhoggard
- SAML Bug in Github worth 15000
- Authentication bypass on Airbnb via OAuth tokens theft
- Uber Login CSRF + Open Redirect -> Account Takeover at Uber
- Administrative Panel Access by c0rni3sm
- Uber Bug Bounty: Gaining Access To An Internal Chat System by mishre
- Flickr Oauth Misconfiguration by mishre
- Slack SAML authentication bypass by Antonio Sanso
- Shopify admin authentication bypass using partners.shopify.com by uzsunny

HTTP Header Injection

- Twitter Overflow Trilogy in Twitter by filedescriptor
- Twitter CRLF by filedescriptor
- Adblock Plus and (a little) more in Google
- $10k host header by Ezequiel Pereira

Subdomain Takeover

- Hijacking tons of Instapage expired users Domains & Subdomains by geekboy
- Reading Emails in Uber Subdomains
- Slack Bug Journey - by David Vieira-Kurz
- Subdomain takeover and chain it to perform authentication bypass by Arne Swinnen
- Hacker.One Subdomain Takeover - by geekboy

Author Write Up

- Payment Flaw in Yahoo
- Bypassing Google Email Domain Check to Deliver Spam Email on Google's Behalf
- When Server Side Request Forgery combine with Cross Site Scripting

XSSI

- Plain Text Reading by XSSI
- JSON hijacking
- OWASP XSSI
- Japan Identifier based XSSI attacks
- JSON Hijack Slide

Email Related

- This domain is my domain - G Suite A record vulnerability
- I got emails - G Suite Vulnerability
- How I snooped into your private Slack messages [Slack Bug bounty worth $2,500]
- Reading Uber's Internal Emails [Uber Bug Bounty report worth $10,000]
- Slack Yammer Takeover by using TicketTrick by Inti De Ceukelaire
- How I could have mass uploaded from every Flickr account!

Money Stealing

- Round error issue -> produce money for free in Bitcoin Site by 4lemon

2017 Local File Inclusion

- Disclosure Local File Inclusion by Symlink
- Facebook Symlink Local File Inclusion
- Gitlab Symlink Local File Inclusion
- Gitlab Symlink Local File Inclusion Part II
- Multiple Company LFI
- LFI by video conversion, excited about this trick!

Miscellaneous

- SAML Pen Test Good Paper
- A list of FB writeup collected by phwd by phwd
- NoSQL Injection by websecurify

- CORS in action
- CORS in Fb messenger
- Web App Methodologies
- XXE Cheatsheet
- The road to hell is paved with SAML Assertions, Microsoft Vulnerability
- Study this if you like to learn Mongo SQL Injection by cirw
- Mongo DB Injection again by websecrify
- w3af speech about modern vulnerability by w3af
- Web cache attack that lead to account takeover
- A talk to teach you how to use SAML Raider
- XSS Checklist when you have no idea how to exploit the bug
- CTF write up, Great for Bug Bounty
- It turns out every site uses jquery mobile with Open Redirect is vulnerable to XSS by sirdarckcat
- Bypass CSP by using google-analytics
- Payment Issue with Paypal
- Browser Exploitation in Chinese
- XSS bypass filter
- Markup Impropose Sanitization
- Breaking XSS mitigations via Script Gadget
- X41 Browser Security White Paper
- Bug Bounty Cheatsheets By EdOverflow
- Messing with the Google Buganizer System for $15,600 in Bounties
- Electron Security White Paper
- Twitter's Vine Source code dump - $10080
- SAML Bible
- Bypassing Google’s authentication to access their Internal Admin panels—Vishnu Prasad P G
- Smart Contract Vulnerabilities

转载于:https://www.cnblogs.com/17bdw/p/10254053.html