

CTF:web

梁瀚中
Trinity

目录

- ✓ 工具使用
 - ✓ Firefox及其插件
 - ✓ burpsuite
- ✓ 前端入门
 - ✓ 三剑客简介
 - ✓ 前端trick
- ✓ 前端安全
 - ✓ XSS
- ✓ 后端安全
 - ✓ PHP
 - ✓ SQL注入

注意：

本课程及工具仅供交流学习使用，请勿用于违法犯罪目的，否则后果自负！

00

法律法规

刑法中关于计算机犯罪相关条款

- 第285条一(非法侵入计算机信息系统罪)
 - 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。
- 第286条一(破坏计算机信息系统罪)
 - (1) 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。
 - (2) 违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。
 - (3) 故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。
- 第287条一(利用计算机实施的各类犯罪)
 - 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

00

法律法规

刑法修正案-285条

- 2009年2月刑法修正案(七)，十号主席令
- 285条增加两款
 - 侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。
 - 提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚
- 拓展法律保护的范围，加强了惩罚力度

网络安全法

- 第二十六条
 - 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。
- 第二十七条
 - 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。
- 第六十三条
 - 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

00

法律法规



01

工具使用

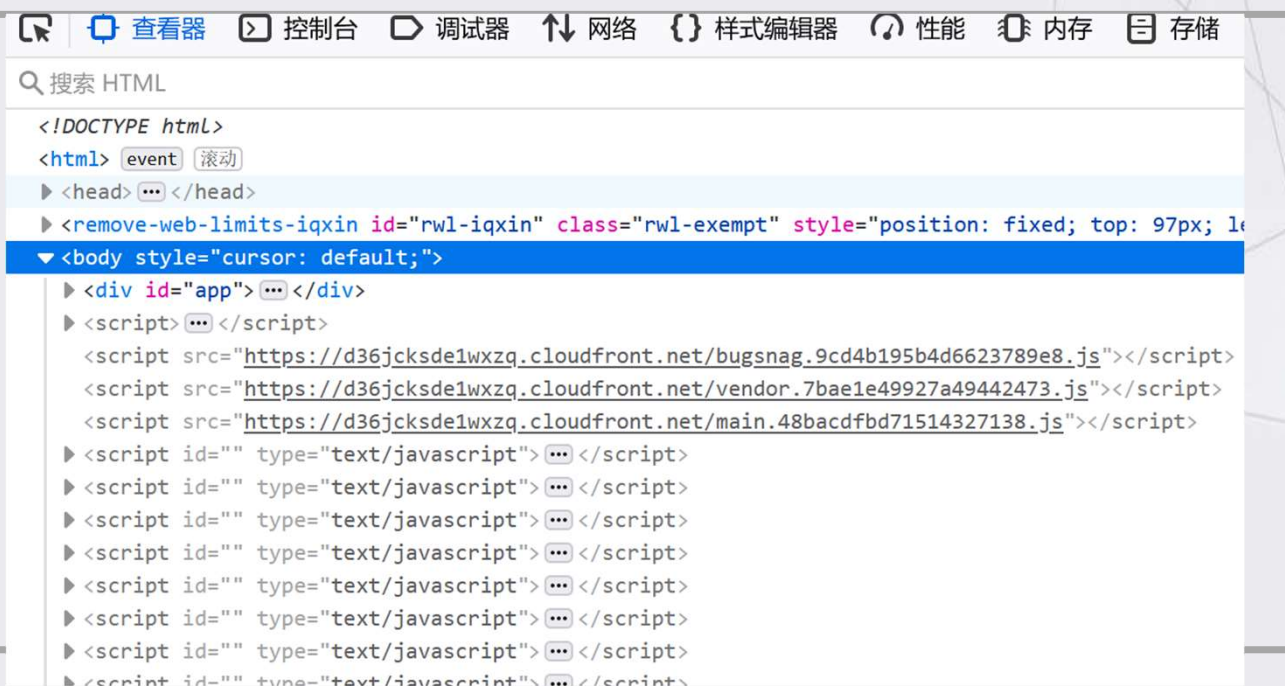
01 工具使用

Firefox

- 由Mozilla基金会发布的开源浏览器
- Gecko内核
- Firebug集成
- 丰富的插件库（hackbar）

Firefox

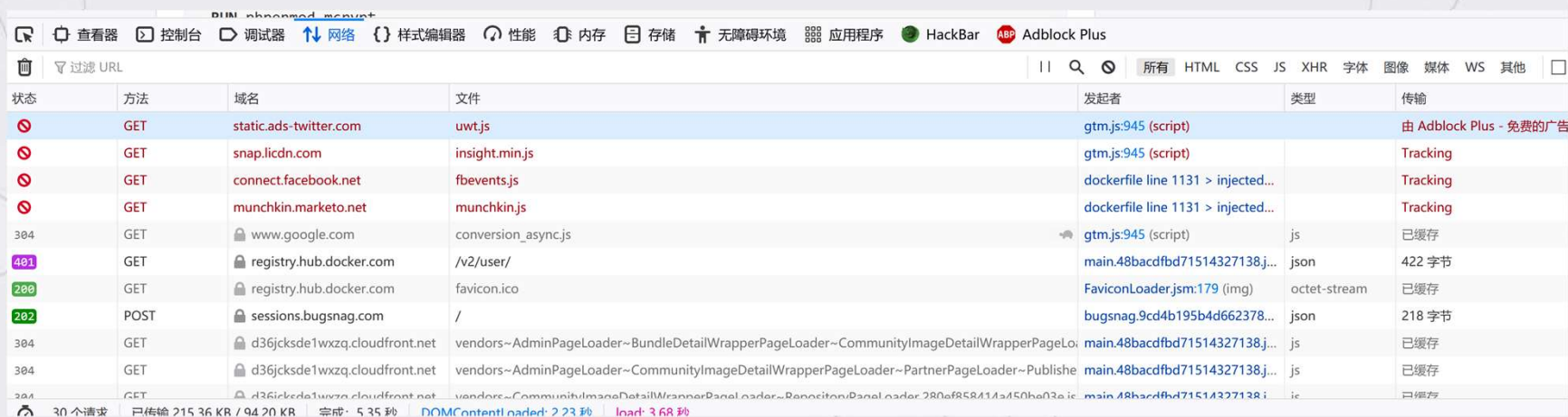
- HTML查看器



01 工具使用

Firefox

• 检测网络



状态	方法	域名	文件	发起者	类型	传输
❌	GET	static.ads-twitter.com	uwt.js	gtm.js:945 (script)		由 Adblock Plus - 免费的广告
❌	GET	snap.licdn.com	insight.min.js	gtm.js:945 (script)		Tracking
❌	GET	connect.facebook.net	fbevents.js	dockerfile line 1131 > injected...		Tracking
❌	GET	munchkin.marketo.net	munchkin.js	dockerfile line 1131 > injected...		Tracking
304	GET	www.google.com	conversion_async.js	gtm.js:945 (script)	js	已缓存
401	GET	registry.hub.docker.com	/v2/user/	main.48bacdfbd71514327138.j...	json	422 字节
200	GET	registry.hub.docker.com	favicon.ico	FaviconLoader.jsm:179 (img)	octet-stream	已缓存
202	POST	sessions.bugsnap.com	/	bugsnag.9cd4b195b4d662378...	json	218 字节
304	GET	d36jcksde1wxzq.cloudfront.net	vendors~AdminPageLoader~BundleDetailWrapperPageLoader~CommunityImageDetailWrapperPageLo	main.48bacdfbd71514327138.j...	js	已缓存
304	GET	d36jcksde1wxzq.cloudfront.net	vendors~AdminPageLoader~CommunityImageDetailWrapperPageLoader~PartnerPageLoader~Publishe	main.48bacdfbd71514327138.j...	js	已缓存
304	GET	d36jcksde1wxzq.cloudfront.net	vendors~CommunityImageDetailWrapperPageLoader~PartnerPageLoader~Publishe	main.48bacdfbd71514327138.j...	js	已缓存

30 个请求 | 已传输 215.36 KB / 94.20 KB | 完成 5.35 秒 | DOMContentLoaded: 2.23 秒 | load: 3.68 秒

01 工具使用

Firefox

- 重放

The screenshot shows the Firefox Developer Tools Network tab. The top toolbar includes icons for View, Console, Debugger, Network, Styles, Performance, Memory, Storage, Accessibility, Application, HackBar, and Adblock Plus. The Network tab is active, displaying a list of requests. The selected request is a GET request to `hm.gif?hca=37942C5052C4FDEF&cc=1&ck=1&cl=24-bit&ds=1920x1080&vl=713&ep=949*77; hm.js:23 (img)` from `hm.baidu.com`. The details panel on the right shows the request headers, including `Accept`, `Accept-Language`, `Cache-Control`, `Connection`, `Host`, `Referer`, `User-Agent`, and `Cookie`. The status bar at the bottom indicates 15 requests, 1.49 MB transferred, and 518.89 KB received.

状态	方法	域名	文件	发起者	类型	传输	大小
200	GET	duxiaofa.baidu.com	detail?searchType=statute&from=aladdin_28231&originquery=网络: browsing-context.j...		html	1.51 KB	3...
200	GET	hm.baidu.com	hm.gif?cc=1&ck=1&cl=24-bit&ds=1920x1080&vl=713&ep=949*77; hm.js:23 (img)	hm.js:23 (img)	gif	299 字节	4...
200	GET	hm.baidu.com	hm.gif?hca=37942C5052C4FDEF&cc=1&ck=1&cl=24-bit&ds=1920x1080&vl=713&ep=949*77; hm.js:23 (img)	hm.js:23 (img)	gif	299 字节	4...
200	GET	duxiaofa.baidu.com	chunk-vendors.a1149328.js	script	js	441.17 KB	1....
304	GET	duxiaofa.baidu.com	chunk-common.4fae7a08.js	script	js	已缓存	6....
304	GET	duxiaofa.baidu.com	detail.1b137456.js	script	js	已缓存	2....
200	GET	hm.baidu.com	hm.js?ac8fb11c31cd3cf585523fd58e170e95	detail:51 (script)	js	14.82 KB	4...
200	GET	hm.baidu.com	hm.gif?cc=1&ck=1&cl=24-bit&ds=1920x1080&vl=352&et=0&fl=32	hm.js:23 (img)	gif	299 字节	4...
200	GET	mpks-law.cdn.bce...	revision_logo_small.png	chunk-vendors.a11...	png	10.33 KB	9....
200	GET	mpks-law.cdn.bce...	duxiaofa_logo_small.png	chunk-vendors.a11...	png	6.75 KB	6....
200	GET	mpks-law.cdn.bce...	arcode_waibo.png	chunk-vendors.a11...	png	25.05 KB	2...

15 个请求 | 已传输 1.49 MB / 518.89 KB | 完成: 854 毫秒 | DOMContentLoaded: 492 毫秒 | load: 634 毫秒

消息头 | Cookie | 请求 | 响应 | 耗时 | 栈跟踪 | 安全性

拦截 重发

GET https://hm.baidu.com/hm.gif?hca=37942C5052C4FDEF&cc=1&ck=1&cl=24-bit&ds=1920x1080&vl=713&ep=949*77; hm.js:23 (img) 200 OK
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en;q=0.7
Cache-Control: no-cache
Connection: keep-alive
Host: hm.baidu.com
Referer: https://www.baidu.com/link?url=ukPRJt8yeHZ9U4c93Gj-nq8fNS5UjX98puxO966bD7lqOZlp5LnBAvW3vH_4UkvSHCVD4bKYCGclQ2nCo7AZCTuVQVJ7XCwNwedKnAgmqCkA5dpd9ubSx4NIEy5u8cucPNsH8JCWMZ3brj_1eTTpae98u1g5Ho3kml-PxcpZyHUpPE4c67wYKjBOzNYOxM0xEqC9qTAG3Vj_vyPjmRqVIARHZtdtDopkAGMdV7v56f9TMIHAXdt4yC4DUwWZu&wd=&eqid=811241010009d88a000000035fa55c0e&v=1.2.77&lv=1&sn=48054&r=0&ww=1538&u=https://duxiaofa.baidu.com/detail?searchType=statute&from=aladdin_28231&originquery=%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95&count=79&cid=f66f830e45c0490d589f1de2fe05e942_law


状态: 200 OK
版本: HTTP/1.1
传输: 299 字节 (大小 43 字节)


01 工具使用


Firefox

[Hackbar](#)

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

 Load URL

 Split URL

 Execute

☐ Post data ☐ Referer ☐ User Agent ☐ Cookies

Add Header

[Clear All](#)

01 工具使用

Firefox

◆ 题1:

Hackergame 2018 签到题

<http://114.212.190.28:20000/t1/>

01 工具使用

burpsuite

- ◆ Web集成攻击套件

- 报文拦截

- 请求重放

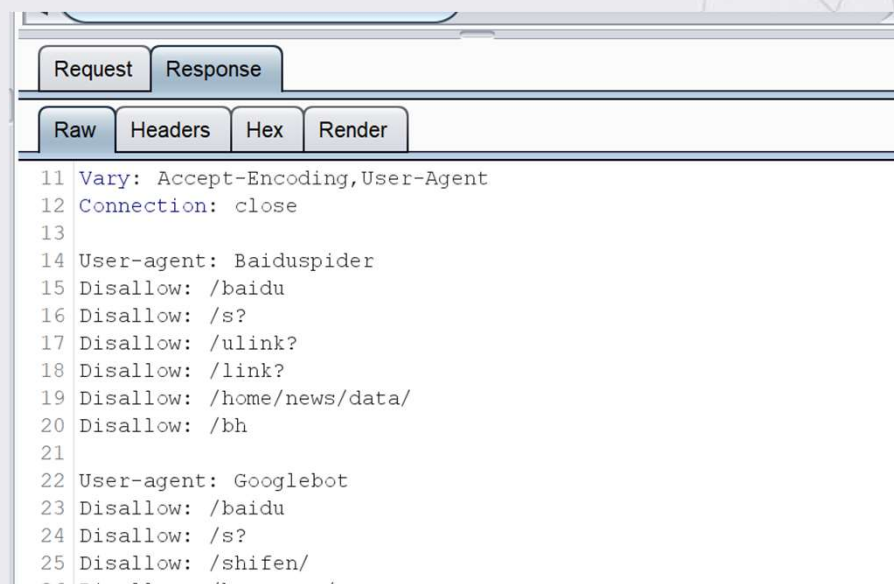
- 简易爆破

-

01 工具使用

Burpsuite -抓包 (报文拦截)

1. 浏览器设置代理
2. 安装burpsuite的证书到浏览器 (可选)
3. Proxy操作:
 1. Forward
 2. Send to repeater
 3. Send to target/scanner/scope/inducer



Baidu的robots.txt

01 工具使用

Burpsuite - repeater

重放报文
简易爬虫

题目：

黑曜石浏览器

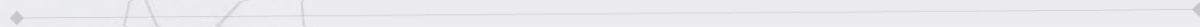
<http://114.212.190.28:20000/heicore/index.php>

单身21年的手速

<http://114.212.190.28:20000/speed1/Index.php>

01 工具使用

白嫖万方



01 工具使用

为什么不能白嫖知网

Request

RawParamsHeadersHex

1 GET /TopLogin/api/loginapi/get?type=top&returnurl=https%3a%2f%2fwww.cnki.net%2f%2flocalCSS= HTTP/1.1
2 Host: login.cnki.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
4 Accept: */*
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: https://www.cnki.net/
10 Cookie: ASP.NET_SessionId=4thjog4qnr02jgo34cc0tfg; SID=020199
11 Pragma: no-cache
12 Cache-Control: no-cache
13
14

Response

RawHeadersHexRender

Name	Value
HTTP/1.1	200 OK
Cache-Control	public, max-age=1200
Content-Length	11126
Content-Type	text/plain; charset=utf-8
Server	Microsoft-IIS/7.5
Access-Control-Allow-Origin	*
Access-Control-Allow-Methods	GET, PUT, POST, DELETE, OPTIONS
Access-Control-Allow-Credentials	true
X-AspNet-Version	4.0.30319
X-Powered-By	ASP.NET
Date	Sat, 07 Nov 2020 08:01:38 GMT
Connection	close

1 document.write("<script >var lang='zh-CN'</script>");
2 document.write("<script
src='//login.cnki.net/TopLogin/Scripts/jquery-1.11.3.min.js' ></script>");
3 document.write("<script src='//login.cnki.net/TopLogin/Scripts/jquery.cookie.js'
></script>");
4 document.write("<script src='//login.cnki.net/TopLogin/Scripts/jquery.md5.js'
></script>");
5 document.write("<script src='//login.cnki.net/TopLogin/Scripts/json2-min.js'
></script>");
6 document.write("<script
src='//login.cnki.net/TopLogin/Scripts/topLogin2.js?v=201020' ></script>");
7 document.write("<script

状态	方法	域名	文件	发起者	类型	传输	大小	耗时
200	GET	www.cnki.net	/	BrowserTabChild.js:102 (docu...	html	62.67 KB	62.6...	5991 毫

状态	方法	域名	文件	发起者	类型	传输	大小	耗时
200	GET	www.cnki.net	/	BrowserTabChild.js:1...	html	62.67 KB	6...	...
200	GET	login.cnki.net	lpLoginFlush?callback=jQuery111301846943527565672_1604736055642&_...	jquery-1.11.3.min.js:5 (...	json	480 字节	4...	...
200	GET	login.cnki.net	get?type=top&returnurl=https://www.cnki.net/&localCSS=	script	plain	10.90 KB	1...	...
200	GET	search.cnki.net	topk.ashx?jsonvar=top_Words_json&v=1507789236929&td=1507789236929	script	plain	207 字节	1...	...
200	GET	search.cnki.net	topk.ashx?jsonvar=top_Words_json&v=1604736056119&td=1604736056119	cnkisug.min.js:1 (script)	plain	207 字节	1...	...
200	GET	track.cnki.net	tracking?action_name=中国知网&idsite=&rec=1&r=818042&h=16&m=0&s=	piwik.js:3166 (img)	plain	39 字节	0

消息头

Cookie

请求

响应

耗时

安全性

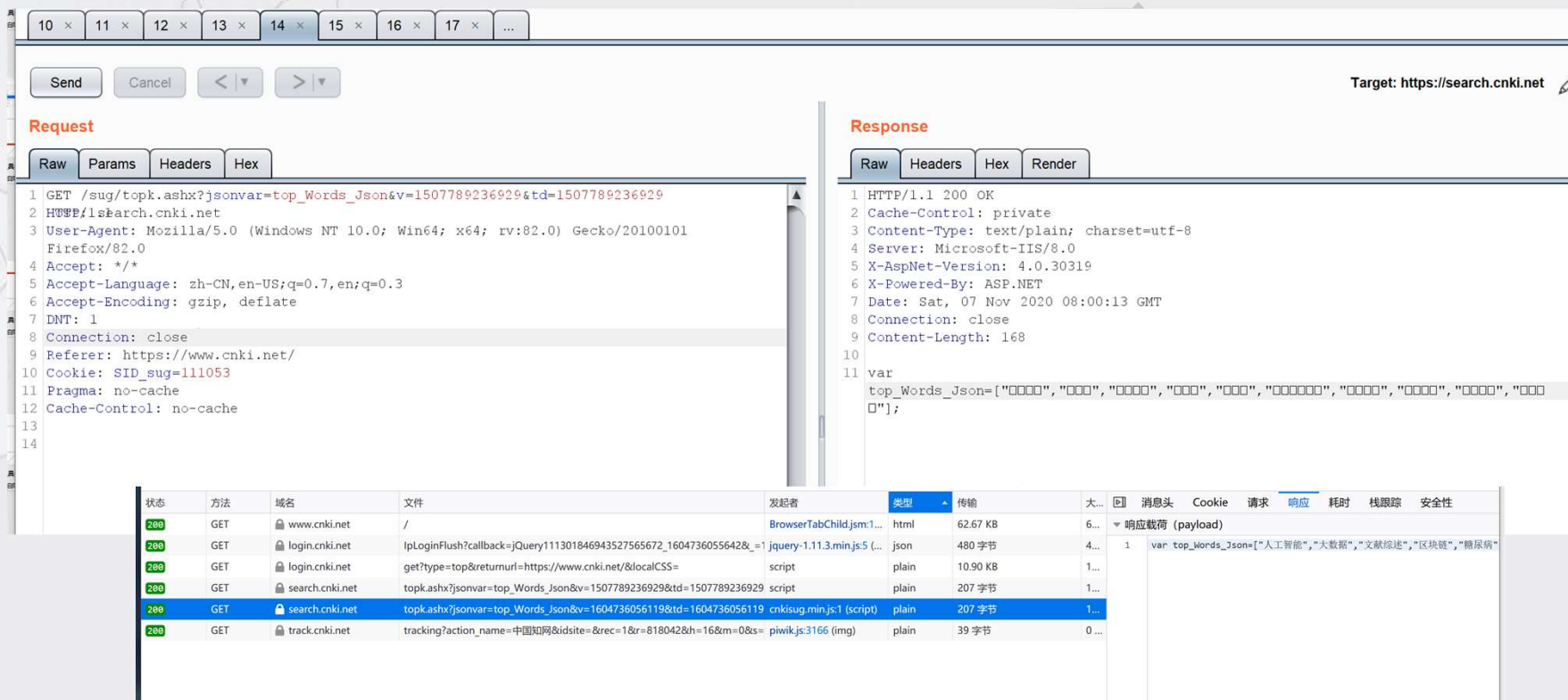
响应载荷 (payload)

1 document.write("<script >var lang='zh-CN'</script>");
2 document.write("<script src='//login.cnki.net/TopLogin/Scripts/jq
3 document.write("<script src='//login.cnki.net/TopLogin/Scripts/jq
4 document.write("<script src='//login.cnki.net/TopLogin/Scripts/jq
5 document.write("<script src='//login.cnki.net/TopLogin/Scripts/js
6 document.write("<script src='//login.cnki.net/TopLogin/Scripts/to
7 document.write("<script src='//login.cnki.net/TopLogin/Scripts/jq
8 document.write("<script src='//login.cnki.net/TopLogin/Scripts/re
9 document.write("<script src='//login.cnki.net/TopLogin/Scripts/re
10 function IncludeCss(path){ var a=document.createElement('link');
11 IncludeCss('//login.cnki.net/TopLogin/Content/TopLogin.css?v=2010
12 document.write("<div class='ecp_top-nav'> <div class='ecp_tn-hea
13

01

工具使用

为什么不能白嫖知网



01 工具使用

为什么不能白嫖知网

RawParamsHeadersHex

1 GET /TopLogin/api/loginapi/IpLoginFlush?callback=jQuery111301846943527565672_1604736055642&_=1604736055643 HTTP/1.1
2 Host: login.cnki.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
4 Accept: */*
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: https://www.cnki.net/
10 Cookie: ASP.NET_SessionId=4thjcg4qrnr02jgo34cc0tfg; SID=020199
11 Pragma: no-cache
12 Cache-Control: no-cache
13
14

RawHeadersHex

1 HTTP/1.1 200 OK
2 Cache-Control: no-cache
3 Pragma: no-cache
4 Content-Length: 441
5 Content-Type: application/json; charset=utf-8
6 Expires: -1
7 Server: Microsoft-IIS/7.5
8 Access-Control-Allow-Origin: *
9 Access-Control-Allow-Methods: GET, PUT, POST, DELETE, OPTIONS
10 Access-Control-Allow-Credentials: true
11 X-AspNet-Version: 4.0.30319
12 Set-Cookie: Ecp_ClientId=2201107160202705234; domain=cnki.net; expires=Thu, 07-Nov-2120
13 Set-Cookie: Ecp_LoginStuts={"IsAutoLogin":false,"UserName":"sh0301","ShowName":"%e5%8d%97
14 Set-Cookie: c_m_LinID=LinID=WEEvREcwSIJHSldSdmVqMDh6aSs3ZC9PYVdZblk3cVdIVXV3U0MweGc0WT0=\$
15 Set-Cookie: LID=WEEvREcwSIJHSldSdmVqMDh6aSs3ZC9PYVdZblk3cVdIVXV3U0MweGc0WT0=\$9A4hF_YAuvQ5
16 Set-Cookie: c_m_expire=2020-11-07 16:22:21; domain=cnki.net; expires=Sat, 07-Nov-2020 08
17 Set-Cookie: Ecp_IpLoginFail; domain=cnki.net; expires=Thu, 07-Nov-2019 08:02:21 GMT; pa
18 Set-Cookie: Ecp_session=1; domain=cnki.net; path=/
19 X-Powered-By: ASP.NET

状态	方法	域名	文件	发起者	类型	传输	大小	消息头	Cookie	请求	响应	耗时	栈跟踪	安全性
200	GET	www.cnki.net	/	BrowserTabChild.js:1...	html	62.67 KB	6...	过滤属性						
200	GET	login.cnki.net	IpLoginFlush?callback=jQuery111301846943527565672_1604736055642&_=1	jquery-1.11.3.min.js:5 (...)	json	480 字节	4...	JSONP → 回调 jQuery111301846943527565672_1604736055642()						
200	GET	login.cnki.net	get?type=top&returnurl=https://www.cnki.net/&localCSS=	script	plain	10.90 KB	1...	IsSuccess: true						
200	GET	search.cnki.net	topk.ashx?jsonvar=top_Words_Json&v=1507789236929&td=1507789236929	script	plain	207 字节	1...	Msg: "登录成功"						
200	GET	search.cnki.net	topk.ashx?jsonvar=top_Words_Json&v=1604736056119&td=1604736056119	cnkisug.min.js:1 (script)	plain	207 字节	1...	ErrorCode: 1						
200	GET	track.cnki.net	tracking?action_name=中国知网&idsite=&rec=1&r=818042&h=16&m=0&s=	piwik.js:3166 (img)	plain	39 字节	0 ...	ErrorMsg: null						
								Uid: "WEEvREcwSIJHSldSdmVqMDh6aSs3ZC9PYVdZblIMWHPMTIUcEdM cFdIOD0=\$9A4hF_YAuvQ5obgVAqNKPCYcEjKensW4IQMowwHtwkF4 VYPoHbKxJw!!"						
								UserName: "sh0301"						
								ShowName: "南京大学"						
								UserType: "bk"						
								BUserName: ""						

01 工具使用

为什么不能白嫖知网

Raw	Params	Headers	Hex
1 GET /tracking?action_name=%E4%B8%AD%E5%9B%BD%E7%9F%A5%E7%BD%91&idsite=&rec=1&r=818042&h=16&m=0&s=57&url=https%3A%2F%2Fwww.cnki.net%2F&_id=6e5da2c0-38cd-4bb7-9aff-c0f088b3924e&_idts=1604736058&_idvc=1&_idn=1&_refts=0&_views=1604736058&send_image=0&pdf=0&qt=0&realp=0&wma=0&dir=0&fla=1&java=0&gears=0&ag=0&cookie=1&res=3840x2160>_ms=5985 HTTP/1.1			
2 Host: track.cnki.net			
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0			
4 Accept: image/webp, */*			
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3			
6 Accept-Encoding: gzip, deflate			
7 DNT: 1			
8 Connection: close			
9 Referer: https://www.cnki.net/			
0 Cookie: SID_track=020100; ASP.NET_SessionId=kkmjqliyg0gvthkyzve0t2pk			
1 Pragma: no-cache			
2 Cache-Control: no-cache			
3			

Raw	Headers	Hex
1 HTTP/1.1 200 OK		
2 Cache-Control: private		
3 Server: Microsoft-IIS/8.5		
4 X-AspNetMvc-Version: 4.0		
5 X-AspNet-Version: 4.0.30319		
6 X-Powered-By: ASP.NET		
7 Date: Sat, 07 Nov 2020 08:13:59 GMT		
8 Connection: close		
9 Content-Length: 0		
10		
11		

01 一些补充

一个web请求的完整流程

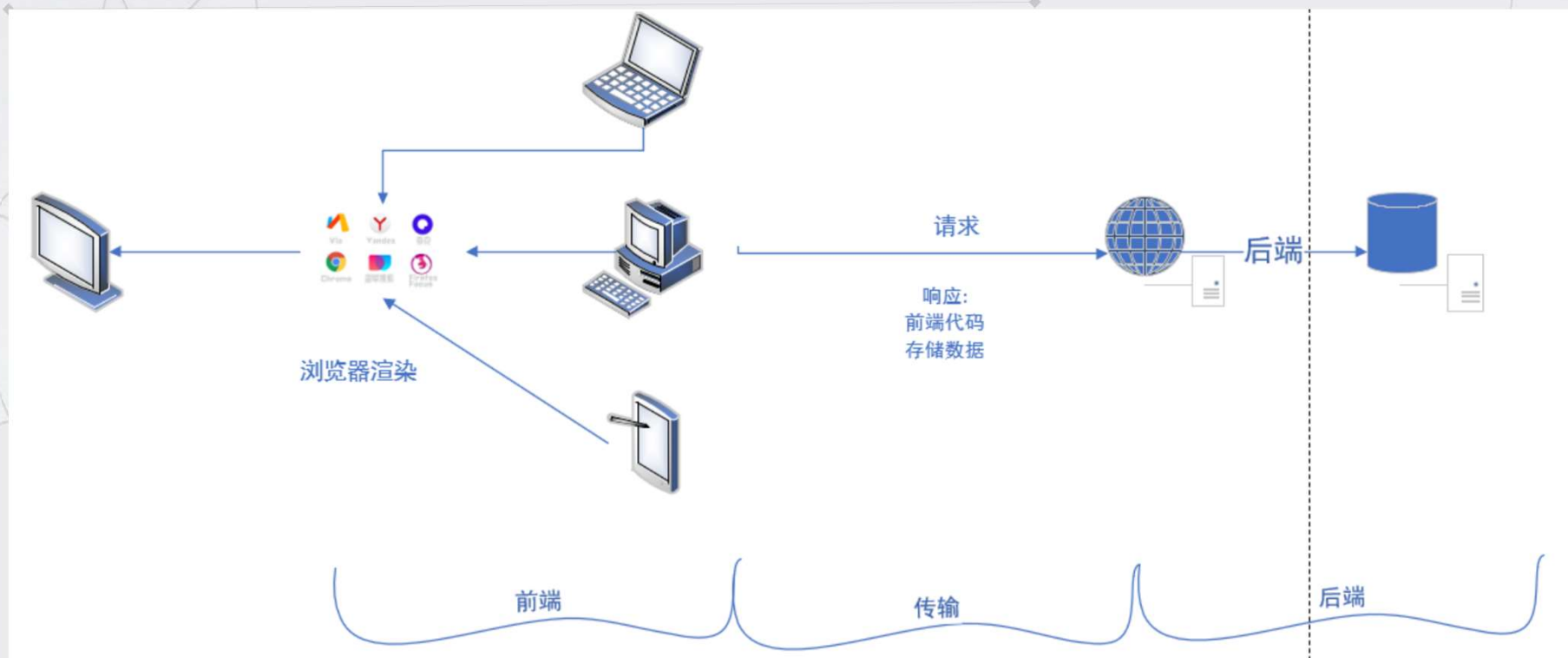
- ◆ client browser 网络层 ---- apache/nginx/java/python/CGI 后端 数据库
- client browser --- apache 只涉及前端
- client browser --- apache PHP 涉及后端，在加载网页完成后有与服务器交互
- client browser 网络层 ---- apache/nginx/java/python/CGI 后端 数据库

02

前端入门

02 前端入门

Overview



02 前端入门

HTML

- **Hyper Text Markup Language** 超文本标记语言
- 与XML语法有相似之处
- Tag: 标签
 - 由尖括号包围
 - tag大部分都是成对的, 以显示范围
 - `<h1>标题</h1>`
 - 标签可以带有属性
 - `<p>段落</p>` ``
 - Tag可以包含子tag

常见的HTML标签:

`<h1></h1>` 标题

...

`<h6></h6>`

`<p></p>` 段落

`<a>` 标记

`<html></html>` 标记了一个HTML文档

`<head></head>` 网页头, 包含一些基本信息

`<body></body>` 网页的主体

`<div></div>` 块元素

02 前端入门

HTML

- 值得注意的几个标签及其属性
- `<script >`
 - `Alert("1");`
- `</script>`
- `<script src= "xxx" > </script>`
- ``
- `<form action= "handler.php" >`这个表单交由handler.php处理
- `<input type= "submit" onclick= "submit()" >` 点击的时候调用最外层作用域的submit函数

02 前端入门

CSS

- 层叠样式表 (**C**ascading **S**tyle **S**heets)
- 用于描述如何显示HTML
- 主要语法：选择器，声明



02 前端入门

javascript

- 与HTML、css交互
- 操作DOM
- 动态地改变页面
- 语句：
 - 多个语句需要用;隔开
- 变量：
 - 必须先声明再使用
 - 所有的变量都用var声明，但JavaScript有基本类型
 - Var tmp = 1;
 - Int, str, NaN,array,function,object
 - 弱类型，相当于把变量名“贴”到内存地址上
- 函数
 - 关键字 function
 - Function tmp (arg1,arg2) {}
 - 一个函数也是一个变量，也可以赋值
 - Var t= function (){};
 - 匿名函数
 - (function(arg1, arg2){})() 直接调用
- 回调函数
 - 异步设计
 - 当某个事件发生时，调用这个函数
 - <input type= "submit" onclick= "submit()" >

02 前端入门

javascript

- Document对象

```
>> document
< HTMLDocument https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&tn=monline_7_dg&wd=JavaScript&oq=HTML&rsv_pq=a9605aa300102bd6&rsv_t=70cb%2F0kksd
rsv_btype=t&inputT=2559&rsv_sug3=5&rsv_sug1=5&rsv_sug7=100&rsv_sug2=0&rsv_sug4=3408
  URL: "https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&tn=monline_7_d...&rsv_sug3=5&rsv_sug1=5&rsv_sug7=100&rsv_sug2=0&rsv_sug4=3408"
  ▶ __evaluate: function evaluate()
  ▶ activeElement: <input id="su" class="bg s_btn" type="submit" value="百度一下">
  ▶ addEventListener: function addEventListener(d, h, q)
  ▶ alinkColor: ""
  ▶ all: HTMLAllCollection { 0: html, 1: head, 2: script, ... }
  ▶ anchors: HTMLCollection { 0: a, 1: a, 2: a, ... }
  ▶ applets: HTMLCollection { length: 0 }
  ▶ baseURI: "https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&tn=monline_7_d...&rsv_sug3=5&rsv_sug1=5&rsv_sug7=100&rsv_sug2=0&rsv_sug4=3408"
  ▶ bgColor: ""
  ▶ body: <body link="#0000cc">
  ▶ characterSet: "UTF-8"
```

比较重要的:

如 document.cookie, document.baseURI, document.domain等

02 前端入门

javascript

- 与DOM交互:
 - `Document.getElementById`
- JQuery:
 - `$('#su')`

02 前端入门

定义

所有能在前端或者只要绕过前端限制就能得到flag的都是trick

除了有时会考察浏览器pwn之类的高难度题目之外，只在签到题出现

Header里藏hint

在返回的响应头里藏hint，使用burpsuite查看响应头

注释里藏flag

对应到实际开发中，就是可能会有一些开发者不注重前端安全，比如将测试数据或者业务逻辑写到注释中

Js代码混淆

Js代码可以经过不可逆的混淆，来让人难以读懂而解释器仍然能够正常执行。比如生产环境和使用环境中使用的各种框架js



前端
Trick

02 前端入门

前端trick

- 一道题目
- <http://114.212.190.28:20000/trick1/>

03

前端安全

03 前端安全

XSS

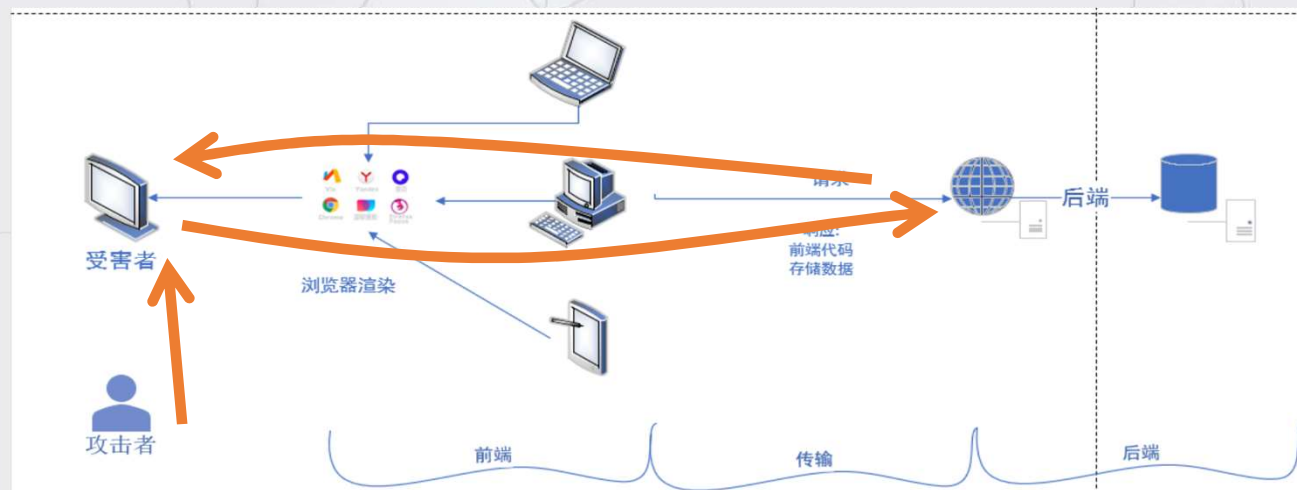
- Cross site script 跨站脚本
- 利用网页开发时的漏洞，巧妙地注入恶意指令到网页，使用户加载并执行攻击者制造的网页程序
- 反射型XSS
- 存储型XSS

03

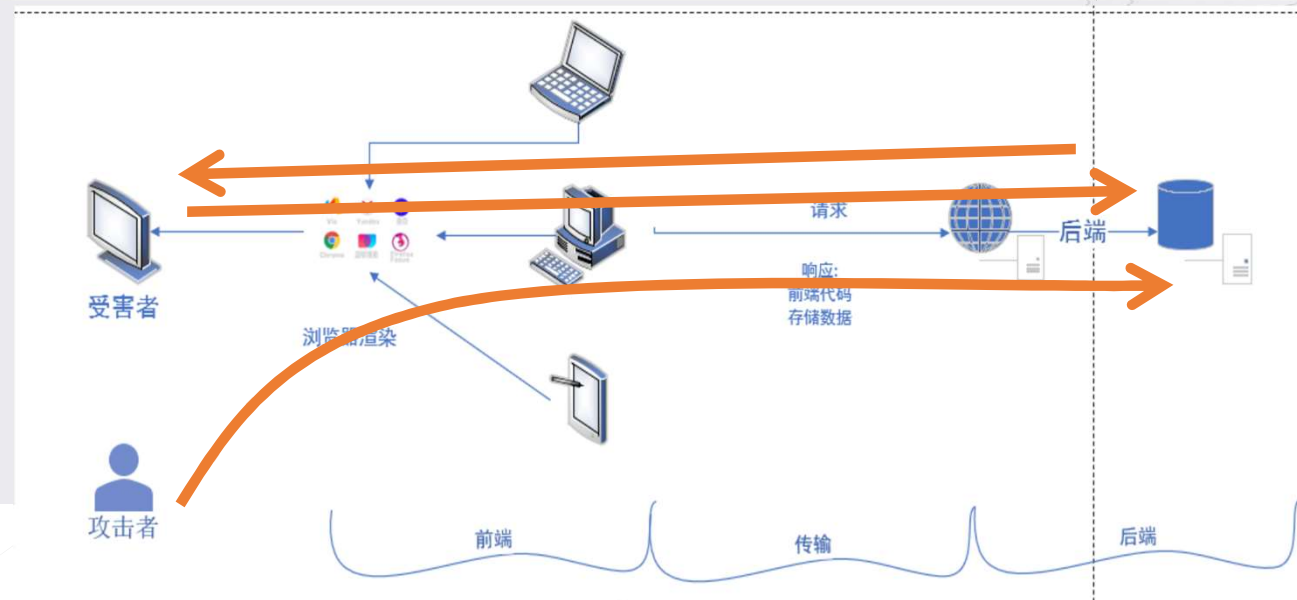
前端安全

XSS

反射型XSS 恶意代码流向



存储型XSS 恶意代码流向



03 前端安全

XSS

- 最关键的技术：
 - 闭合标签
 - JavaScript解析引擎只把文本当成代码，按照预定的规则解析
 - 当闭合标签后，就可以在DOM树中加新的节点，比如<script>
- 一道题目
- http://114.116.226.11:20000/xss_reflect/
- 1"</from></div><script>alert(1)</script>

03 前端安全

XSS

- 简单的绕过
- 服务器用黑名单方法过滤:
- 大小写绕过: SCriPt
- 双写绕过: SCripTscRipt => script
- 其他的奇技淫巧:
 - 注入到标签的事件中 onerror="alert(1)"
 - 不能用() <script>alert`xss`</script>
 - 不能用引号 <script>alert(/xss/)</script>

Explore more:

<http://xss-quiz.int21h.jp/>