吴空·第三场

深入浅出 CSRF

吴空 美团点评高级前端工程师

1. CSRF 是什么？CSRF 可以做什么？CSRF 攻击现状。
2. CSRF 攻击原理与防御、CSRF漏洞检测
3. 前端与服务器端如何在代码层面防范 CSRF 攻击

CODE A BETTER LIFE
一 行 代 码　亿 万 生 活

深入浅出CSRF

JTalk 第八期
前端安全大起底
美 团 点 评 技 术 团 队 专 场

吴空

美团高级前端开发工程师

深入浅出CSRF

1 你真的了解CSRF?

2 知道CSRF怎么防御?

CSRF是什么?

- Cross-site Request Forgery（跨站请求伪造），攻击者伪装成受信任用户攻击受信用网站!

CSRF攻击可以做什么？

- 伪造邮件
- 伪造消息
- 盗取账号
- 购买商品
- 银行转账

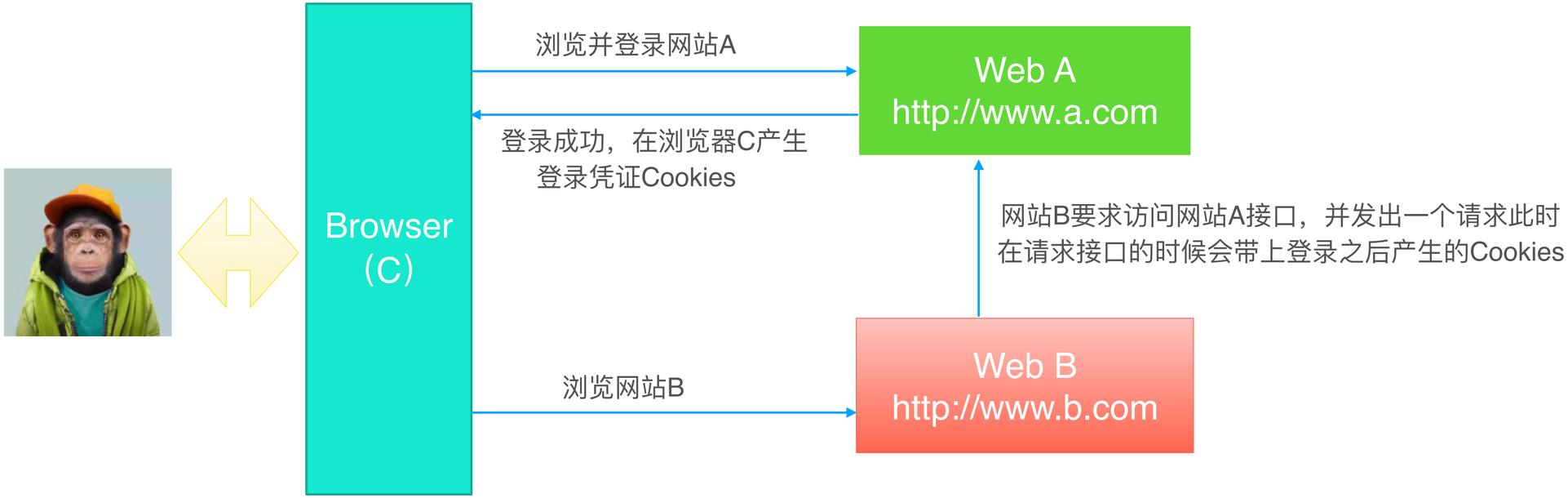
……

CSRF攻击现状

2000年国外的安全人员提出，06年国内才开始关注，08年国内外网站相继爆出CSRF漏洞

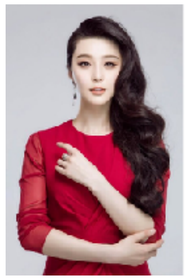
CSRF攻击.....

CSRF攻击原理


Browser
(C)
浏览并登录网站A
登录成功，在浏览器C产生
登录凭证Cookies
Web A
http://www.a.com
网站B要求访问网站A接口，并发出一个请求此时
在请求接口的时候会带上登录之后产生的Cookies
浏览网站B
Web B
http://www.b.com

CSRF常见的攻击方式

- 图片链接或a标签



```
<img src="http://www.a.com/trans.php?toBankId=10010&money=1000" />
```

第三次世界大战爆发

```
<a href="http://www.a.com/trans.php?toBankId=10010&money=1000">第三次世界大战爆发</a>
```

CSRF常见的攻击方式

- Form表单提交

```
<body>
  <form style="display:none" name="form" action="http://www.a.com/trans.php" method="post">
    <input type="hidden" name="toBankId" value="10010"/>
    <input type="hidden" name="money" value="1000"/>
    <input type="submit" value>
  </form>
  <script>
    document.forms.form.submit();
  </script>
</body>
```

CSRF常见的防御方式

- 表单包含随机值
- 不同表单包含不同的随机值
- 添加验证码
- 验证 HTTP Referer 字段
- 在 HTTP 头中自定义属性并验证

……

通过编码防御CSRF攻击

- 所有表单包含一个随机值

```
/**
 *  Nodejs
 *  服务器端渲染模版
 */
let express = require('express');
let crypto = require('crypto');
let app = express();

app.set('view engine', 'ejs');
app.get('/', function (req,res) {

  let csrf_token = crypto
                   .createHmac('sha1', '!@#$#')
                   .update(`abcd${ +new Date() }`)
                   .digest('base64');

  res.cookie('csrf_token', csrf_token);
  res.render('index');
})
```

通过编码防御CSRF攻击

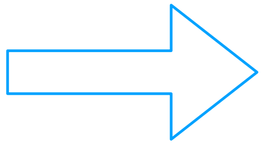
- 所有表单包含一个随机值

```
/**
 * 客户端统一封装异步请求
 */
import axios from 'axios'

export default async function fetchData (params) {

  let csrf_token = $.cookie.get('csrf_token');

  params.headers['CsrfToken'] = csrf_token;
  return await axios(params)
}
```

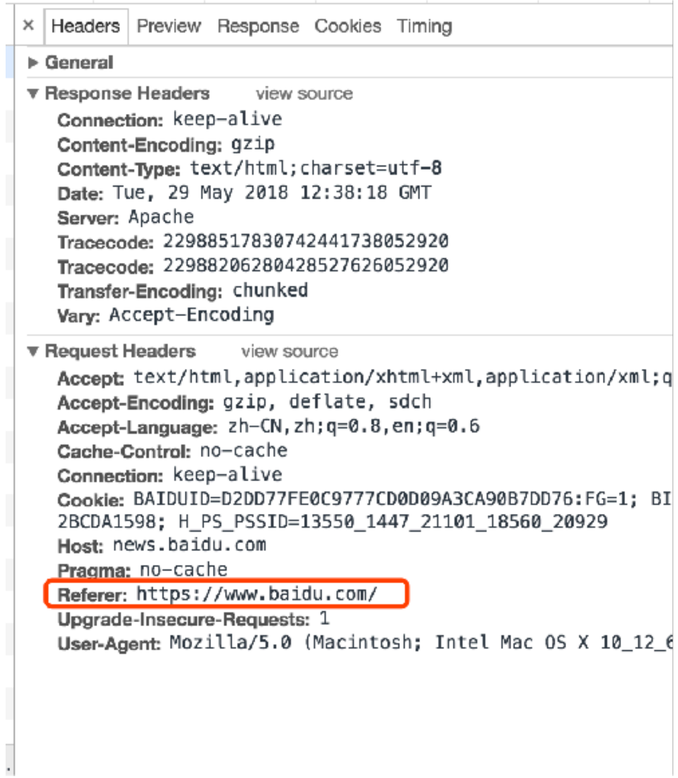


```
/**
 * Nodejs
 * 服务器端验证
 */
let header_token = request.headers.CsrfToken;
let cookie_token = request.cookies.csrf_token;

if (header_token &&
    cookie_token &&
    herader_token === cookie_token) {
  // 验证通过
} else {
  // 验证失败
}
```

通过编码防御CSRF攻击

- 验证 HTTP Referer 字段




```
let referer = request.headers.Referer;

if (referer && _.startsWith(referer, 'http://www.baidu.com')) {
  // 验证成功
} else {
  // 验证失败
}
```

```
const url = require('url');
const whiteList = [
  'google.com',
  'nodejs.org',
]

const referer = req.headers.referer || ''
const host = url.parse(referer).host

if (whiteList.some(h => h === host)) {
  console.log('验证成功')
} else {
   console.log('验证失败')
}
```

CSRF漏洞检测工具

- CSRF Tester

使用代理抓取我们在浏览器中访问过的所有的连接以及所有的表单等信息，通过在CSRFTester中修改相应的表单等信息，重新提交，相当于一次伪造客户端请求，如果修测试的请求成功被网站服务器接受，则说明存在CSRF漏洞，当然此款工具也可以被用来进行CSRF攻击

- CSRF Request Builder

在黑客圈指：观点验证程序，运行这个程序得到预期结果，就验证了这个观点

安全扫描工具

- Watchfire AppScan

是一款商业类的Web漏洞扫描程序。AppScan在应用程序的整个开发周期都提供安全测试，从而测试简化了部件测试和开发早期的安全保证。它可以扫描许多常见的漏洞，如跨站脚本攻击、HTTP响应拆分漏洞、参数篡改、隐式字段处理、后门/调试选项、缓冲区溢出等等。

- WebInspect
- WebScarab

……

如何做到线上安全

接入公司安全平台

自动化构建过程中接入

线上接口扫描

Q&A