امنیت وب

NETWORK RESEARCH LABORATORY

آزمایشگاه تحقیقاتی شبکه های کامپیوتری
دانشکده مهندسی دانشگاه فردوسی مشهد
Engineering School
Ferdowsi University of Mashhad

STANFORD

دانشگاه فردوسی مشهد

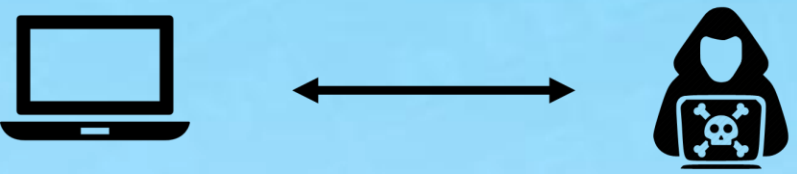
Email: Alireza.sazegar@um.ac.ir Home Page : https://Alireza-sazegar.github.io

اهداف امنیت وب

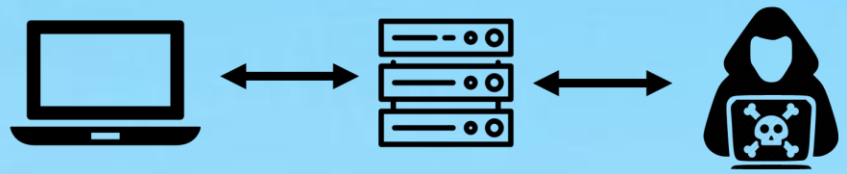
با خیال راحت در مواجهه با مهاجمان، وب را مرور کنید
از یک وب‌سایت (از جمله سایت‌های مخرب!) بدون آسیب دیدن بازدید کنید
سایت A نمی‌تواند داده‌ها را از دستگاه شما بدزدد، بدافزار نصب کند، به دوربین دسترسی پیدا کند و غیره
سایت A نمی‌تواند روی جلسه سایت B تأثیر بگذارد یا در سایت B استراق سمع کند
از برنامه‌های وب امن و با کارایی بالا پشتیبانی کنید مثلاً Google Meet
برنامه‌های بومی کمتر که کد غیرقابل اعتماد اجرا می‌کنند، بهتر است!

انواع حمله وب

Malicious Website



Malicious External Resource



Network Attacker

پروتکل HTTP

پروتکل بر مبنا ASCII از سال ۱۹۸۹ که امکان دریافت منابع (به عنوان مثال، فایل HTMLرا از یک سرور فراهم می کند.

- دو پیام: درخواست و پاسخ
- پروتکل Stateless فراتر از یک پاسخ و درخواست

هر منبع یک URLدارد:

آناتومی درخواست

GET /index.html HTTP/1.1

Accept: image/gif, image/x-bitmap, image/jpeg, */*

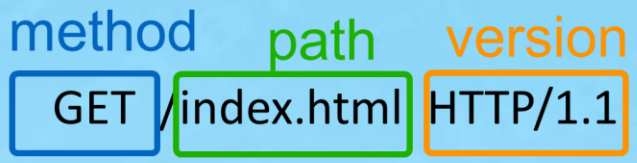
Accept-Language: en

Connection: Keep-Alive

User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)

Host: www.example.com

Referer: http://www.google.com?q=dingbats



Accept: image/gif, image/x-bitmap, image/jpeg, */*

Accept-Language: en

Connection: Keep-Alive

User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)

Host: www.example.com

Referer: http://www.google.com?q=dingbats

اناتومی پاسخ

HTTP/1.0 200 OK

status code

Date: Sun, 21 Apr 1996 02:20:42 GMT
Server: Microsoft-Internet-Information-Server/5.0
Content-Type: text/html
Last-Modified: Thu, 18 Apr 1996 17:39:05 GMT
Content-Length: 2543

headers

<html>Some data... announcement! ... </html>

body

تفاوت GETو POST

method path version

POST /index.html HTTP/1.1

Accept: image/gif, image/x-bitmap, image/jpeg, */*

Accept-Language: en

User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)

Host: www.example.com

Referer: http://www.google.com?q=dingbats

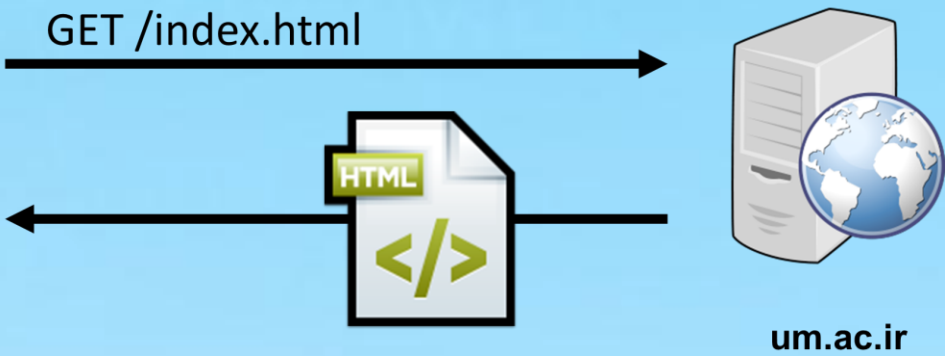
headers

Name: John Smith

Organization: Ferdowsi University

body

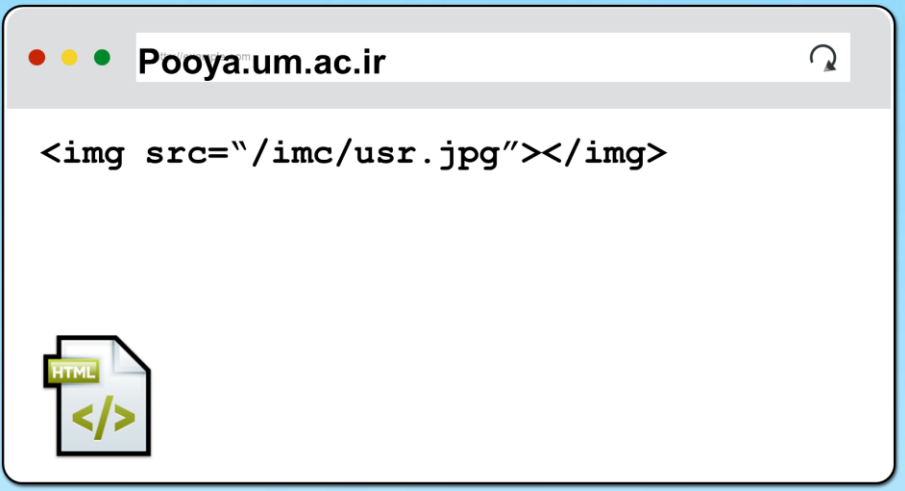
وقتی سایتی را بارگذاری می‌کنید، مرورگر وب شما یک درخواست GETبه آن وب‌سایت ارسال می‌کند



بارگیری منابع

بارگیری منابع

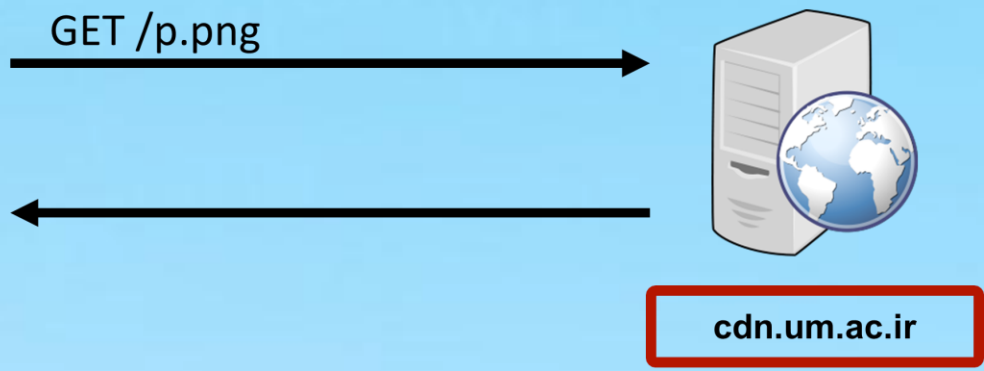
صفحه HTMLریشه می تواند شامل منابع اضافی مانند تصاویر، فیلم ها، فونت ها باشد
پس از تجزیه صفحه HTML، مرورگر شما آن منابع اضافی را درخواست می کند



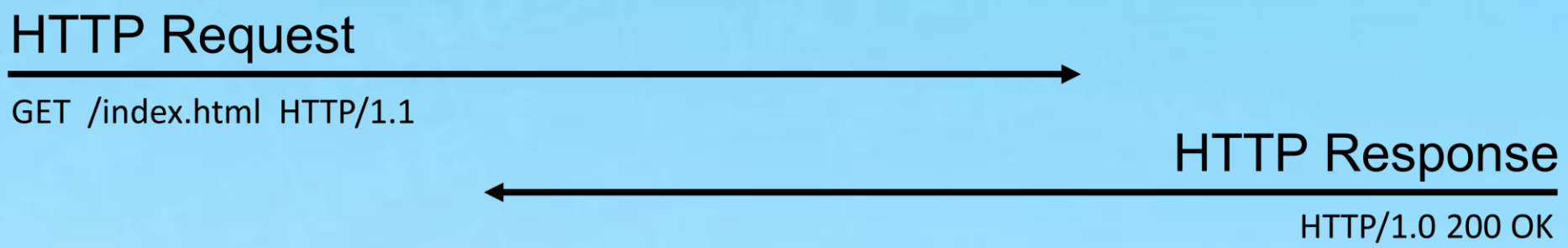
Pooya.um.ac.ir

منابع خارجی

هیچ محدودیتی برای بارگیری منابعی مانند تصاویر وجود ندارد
هیچ چیز شما را از اضافه کردن تصاویر در یک دامنه دیگر منع نمی کند



HTTP یک پروتکل Stateless است



اگر HTTPیک پروتکل Statelessاست .چگونه در وبسایت ها Sessionداریم؟

Cookies

کوکی :قطعه کوچکی از داده که یک سرور به مرورگر وب ارسال می‌کند.
مرورگر ممکن است ذخیره کند و در درخواست‌های بعدی به آن سایت ارسال کند.
مدیریت جلسه
ورود به سیستم، سبد خرید، امتیازات بازی یا هر وضعیت جلسه دیگر
شخصی‌سازی
تنظیمات برگزیده کاربر، تم‌ها و سایر تنظیمات
ردیابی
ضبط و تجزیه و تحلیل رفتار کاربر

تنظیم کردن کوکی

HTTP Response

HTTP/1.0 200 OK

Date: Sun, 21 Apr 1996 02:20:42 GMT

Server: Microsoft-Internet-Information-Server/5.0

Connection: keep-alive

Content-Type: text/html

Set-Cookie: trackingID=3272923427328234

Set-Cookie: userID=F3D947C2

Content-Length: 2543

<html>Some data... whatever ... </html>

ارسال کوکی

HTTP Request

GET /index.html HTTP/1.1

Accept: image/gif, image/x-bitmap, image/jpeg, */*

Accept-Language: en

Connection: Keep-Alive

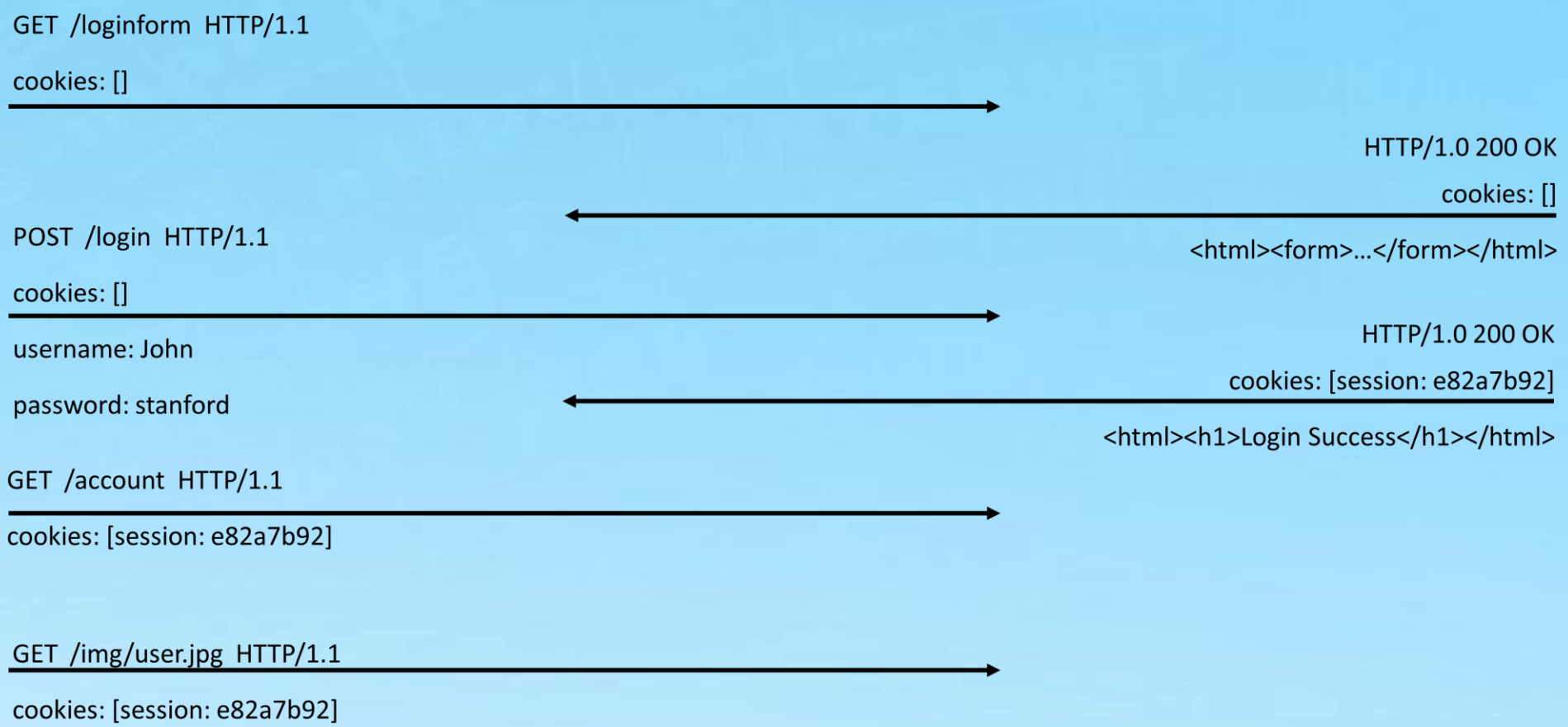
User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)

Cookie: trackingID=3272923427328234

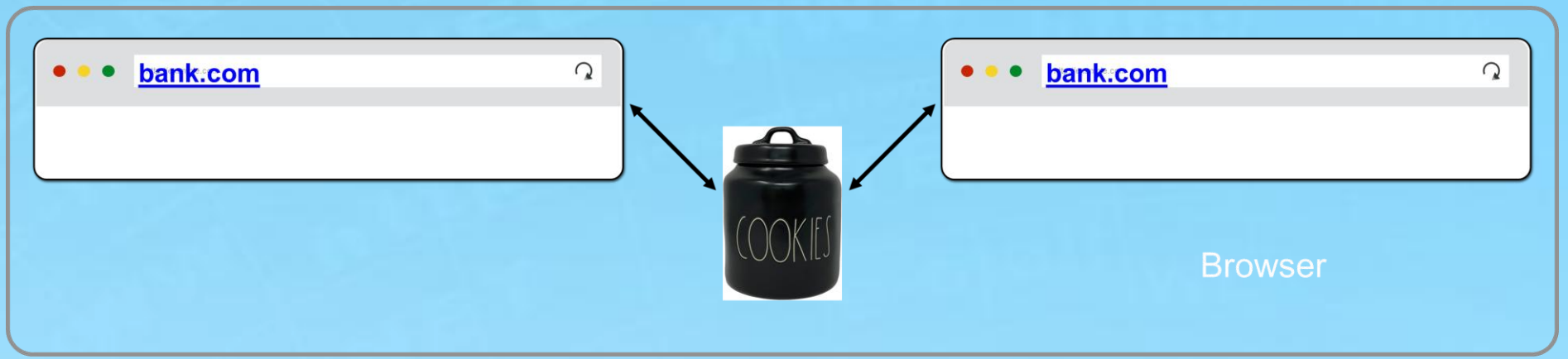
Cookie: userID=F3D947C2

Referer: http://www.google.com?q=dingbats

Login Session



ظرف کوکی مشترک



هر دو برگه منشا یکسانی دارند و به کوکی‌های یکدیگر دسترسی دارند

(۱) Tab 1 به bank.com وارد می شود و یک کوکی دریافت می کند (۲) درخواست Tab 2 های همچنین کوکی های دریافت شده توسط Tab 1 را به bank.com ارسال می کند.

Same Origin Policy
(Origins)

Web Isolation

با خیال راحت وب را مرور کنید

از یک وب سایت (از جمله سایت های مخرب!) بدون آسیب دیدن بازدید کنید

سایت Aنمی تواند داده ها را از دستگاه شما بدزدد، بدافزار نصب کند، به دوربین دسترسی پیدا کند و غیره.

سایت Aنمی تواند بر جلسه سایت Bتأثیر بگذارد یا استراق سمع در سایت B انجام دهد.

از برنامه های وب با کارایی بالا و ایمن پشتیبانی کنید

برنامه های کاربردی مبتنی بر وب (به عنوان مثال، Google Meet)باید دارای ویژگی های امنیتی مشابه یا بهتر از برنامه های دسکتاپ بومی باشند.

یادآوری

مدل امنیتی UNIX

افراد (چه کسی؟)
- کاربران، فرآیندها

اشیاء (چی؟)
- فایل ها، دایرکتوری ها
- فایل ها: سوکت ها، لوله ها، دستگاه های سخت افزاری، اشیاء هسته، داده های پردازش

عملیات دسترسی (چگونه؟)
- بخوان، بنویس، اجرا کن

مدل امنیت وب

Subjects

"Origins" — a unique **scheme://domain:port**

Objects

DOM tree, DOM storage, cookies, javascript namespace, HW permission

خط مشی مبدا یکسان SOP

هدف: جداسازی محتوایی با ریشه های مختلف

- محرمانه بودن: اسکریپت در evil.comنباید bank.chرا بخواند
- صحت: evil.comنباید بتواند محتوای bank.chرا تغییر دهد

مثال هایی درباره مبدا

Origin defined as scheme://domain:port

All of these are different origins

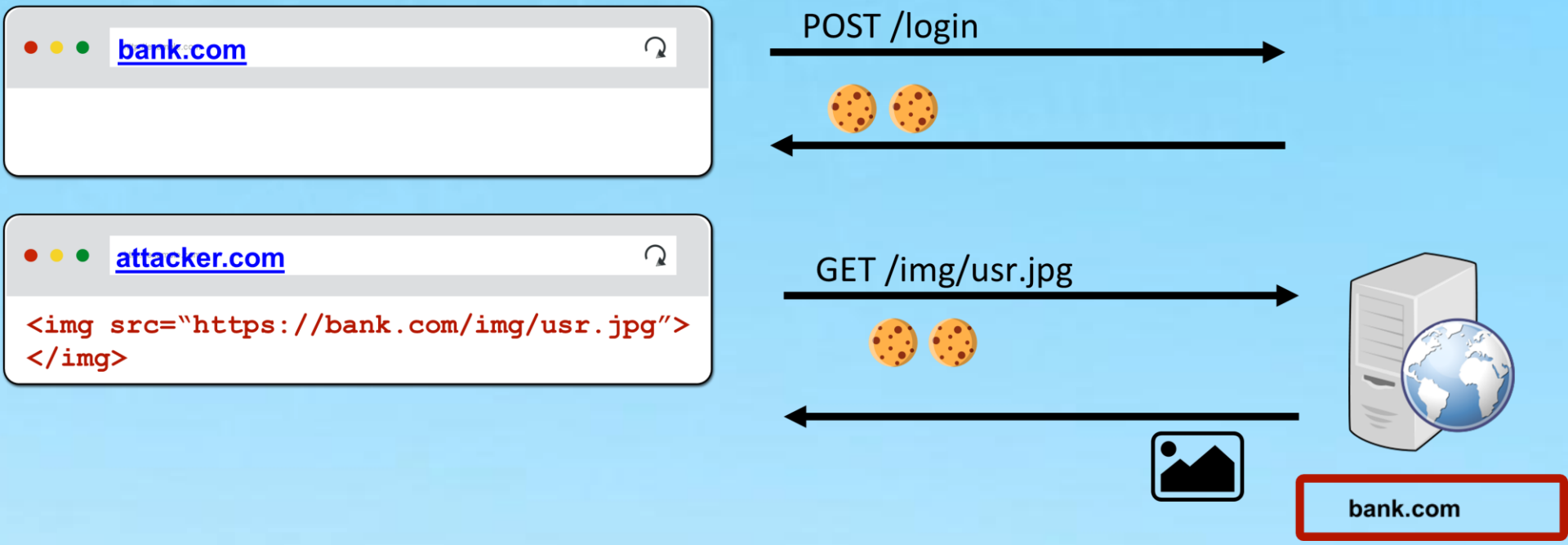
- http://um.ac.ir
- http://**www.**um.ac.ir
- http://um.ac.ir**:8080**
- **https**://um.ac.ir

These origins are the same

- https://um.ac.ir
- https://um.ac.ir:80
- https://um.ac.ir/cs

HTTP Same Origin Policy (SOP)

مبدا و کوکی ها



مرورگر کوکی bank.comرا ارسال می کند

SOP attacker.comرا از بازرسی تصویر و کوکی bank.comمسدود می‌کند

CORS

فرض کنید یک برنامه وب دارید که در app.company.comاجرا می شود و می خواهید با درخواست به api.company.comبه داده های JSONدسترسی داشته باشید.

به طور پیش فرض، این امکان پذیر نیست - app.company.comو api.company.comمبدا متفاوتی دارند

CORS Success

```
Origin: app.c.com

$.post({url: "api.c.com/x",
  success: function(r){
    $("#div1").html(r);
  }
});
```

POST /x

OPTIONS /x

Origin:
api.c.com

Header:
Access-Control-Allow-Origin:
http://app.c.com

POST /x

DATA

Wildcard Origins

```
Origin: app.c.com

$.post({url: "api.c.com/x",
  success: function(r){
    $("#div1").html(r);
  }
});
```

Header:
Access-Control-Allow-Origin: *

Origin:
api.c.com

DATA

CORS Failure

```
Origin: app.c.com

$.post({url: "api.c.com/x",
  success: function(r){
    $("#div1").html(r);
  }
});
```

POST /x

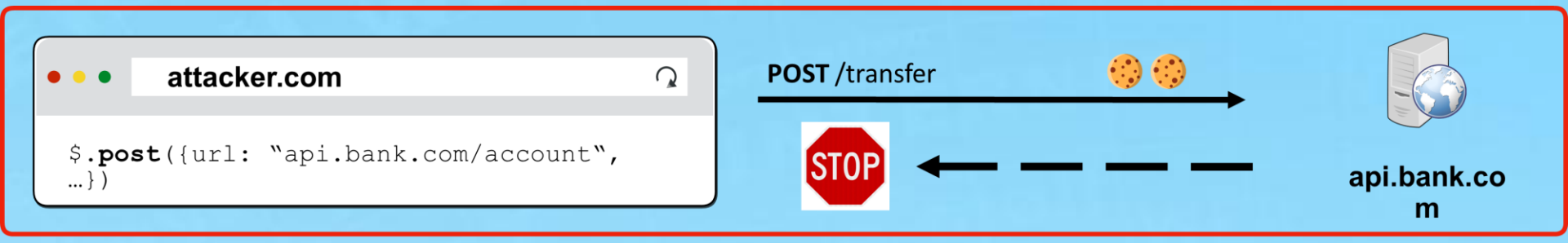
OPTIONS /x

Origin:
api.c.com

```
Header:
Access-Control-Allow-Origin:
  https://www.c.com
```

ERROR

CSRF



حملات جعل درخواست متقابل CSRF نوعی سوء استفاده از وب است که در آن یک وب‌سایت دستورات غیرمجاز را به عنوان کاربری که سرور به آن اعتماد دارد ارسال می‌کند.

در یک حمله CSRF، کاربر فریب داده می شود تا یک درخواست وب ناخواسته (اغلب محقق نشده) به یک وب سایت ارسال کند - معمولاً از کوکی های جلسه استفاده می کند.

برای محافظت در برابر حملات CSRF باید به طور فعال دفاعی را در برنامه های وب ایجاد کنید

به کوکی‌ها برای نشان دادن اینکه آیا یک برنامه مجاز درخواست ارسال کرده است اعتماد نکنید، زیرا آنها در هر درخواست (در محدوده) گنجانده شده‌اند.

تکنیک های مقابله با CSRF

- Referer Header Validation
- Secret Validation Token
- Custom HTTP Header
- sameSite Cookies

Custom HTTP Header

معمولاً هنگام دسترسی به APIهای RESTاستفاده می شود (زیرا به هر حال هدر فقط با استفاده از جاوا اسکریپت قابل تنظیم است)

Secret Validation Token

برای هر گونه تعامل متداول HTML (به عنوان مثال، فرم ورود به سیستم که وقتی کاربر روی ارسال کلیک می کند، به URLپست می شود) استفاده می شود