CORS

http://cors.kojo.ru

Константин Якушев

MoscowJS 14, 28.08.2014

CORS IN ACTION

Creating and consuming cross-origin APIs

Monsur Hossain

MEAP

MANNING

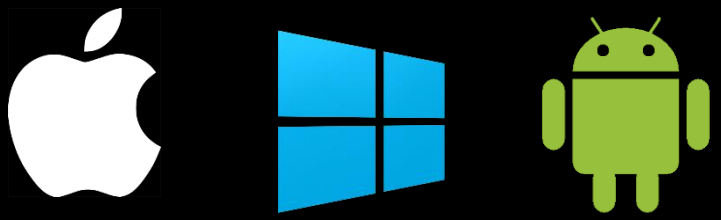

Скидка 44% по
промо-коду
corscftw
RS
ION
cross-origin APIs
Monsur Hossain
MEAP
MANNING

http://api.ya.ru

http://api.ya.ru



http://api.ya.ru



http://m.ya.ru?

```
function Fetch()
{
    var Url = "http://api.ya.ru/";
    var xhr = new XMLHttpRequest();
    xhr.onreadystatechange =
ProcessResponse;
    xhr.open("GET", Url);
    xhr.send(null);
}
```

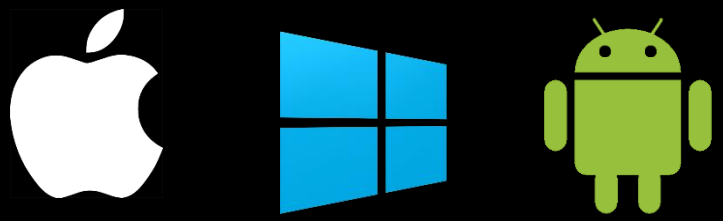
```
function Fetch()
{
    var Url = "http://api.ya.ru/";
    $.get(Url, ProcessResponse);
}
```

Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource at http://api.ya.ru/. This can be fixed by moving the resource to the same domain or enabling CORS.

2

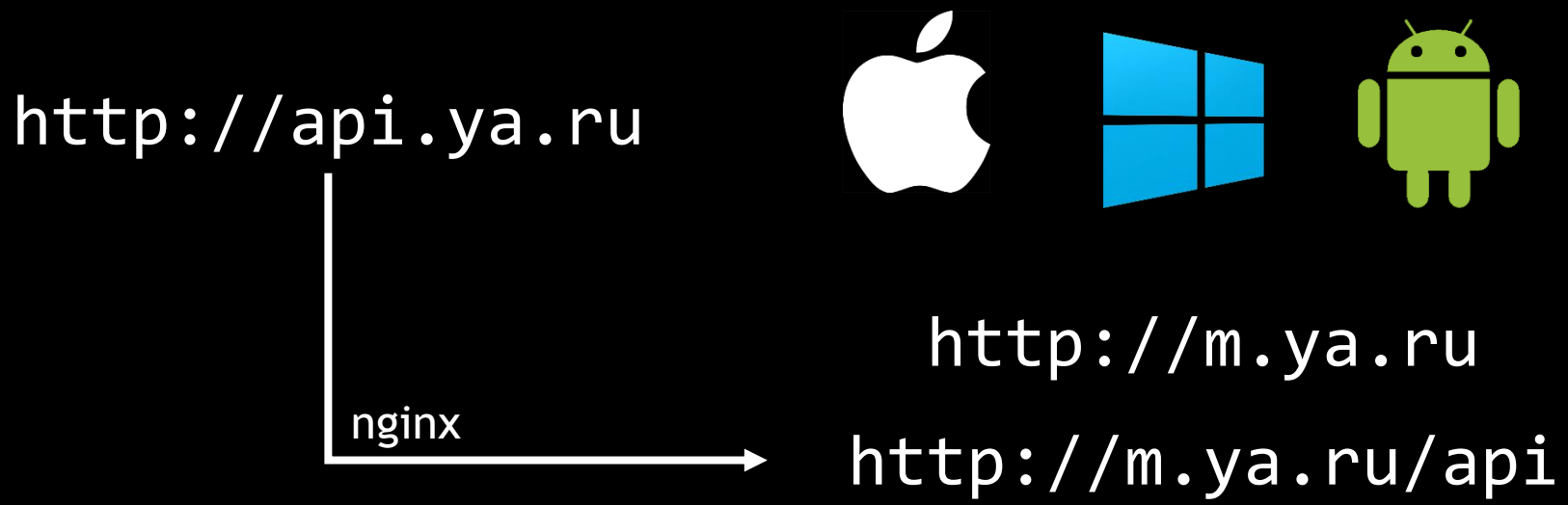
moving the resource to the same domain

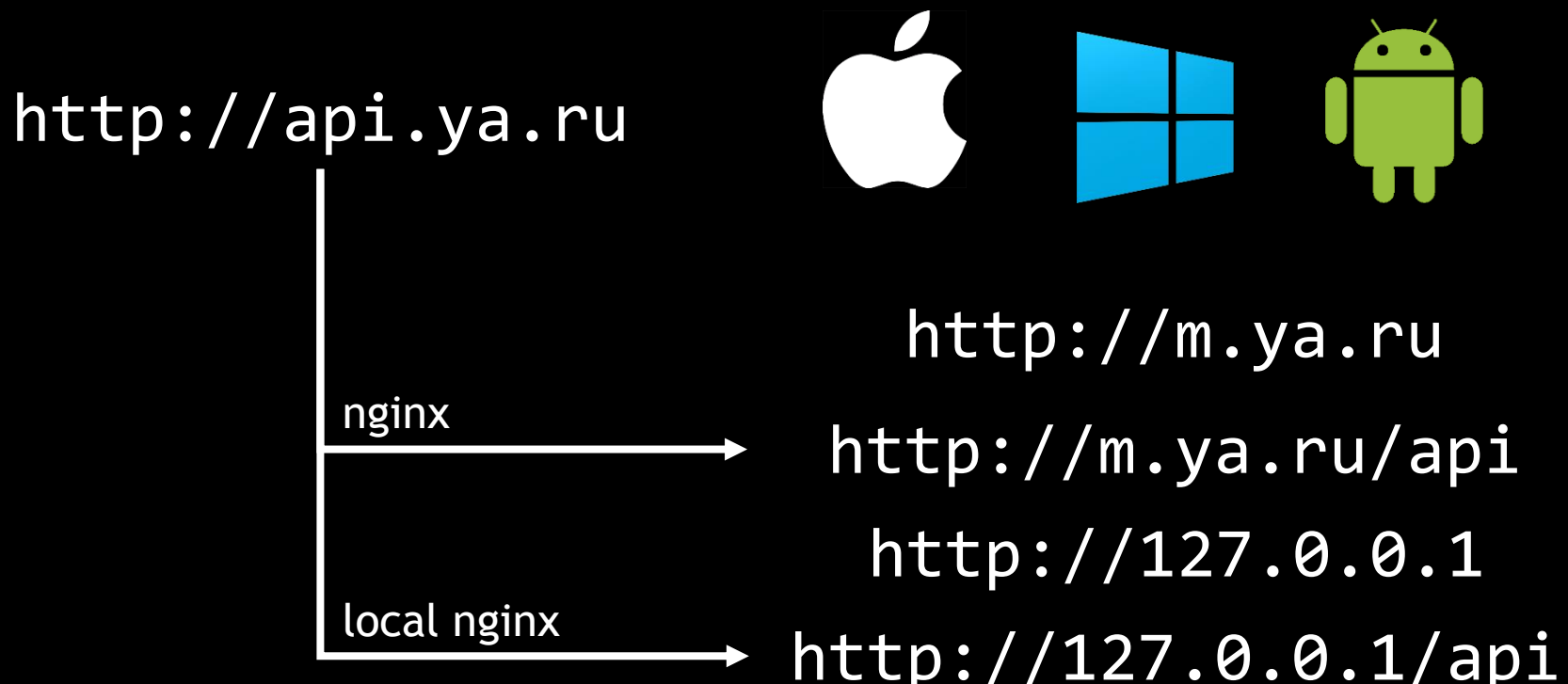
http://api.ya.ru



~~http://m.ya.ru~~

http://api.ya.ru/m


http://api.ya.ru
nginx
http://m.ya.ru
http://m.ya.ru/api


http://api.ya.ru
nginx
local nginx
http://m.ya.ru
http://m.ya.ru/api
http://127.0.0.1
http://127.0.0.1/api

Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource at http://api.ya.ru/. This can be fixed by moving the resource to the same domain or enabling CORS.

2

enabling CORS.

XHR
m.ya.ru

browser

api.ya.ru

without
CORS

XHR
m.ya.ru

GET /data

browser

api.ya.ru

without
CORS

XHR
m.ya.ru

GET /data

browser

GET /data
Origin: http://m.ya.ru

api.ya.ru

without
CORS

XHR
m.ya.ru

GET /data

browser

GET /data
Origin: http://m.ya.ru

<Content>

api.ya.ru

without
CORS

XHR
m.ya.ru

GET /data

ERROR

browser

GET /data
Origin: http://m.ya.ru

<Content>

api.ya.ru

without
CORS

```
header("Access-Control-Allow-Origin: *");
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Origin: http://ya.ru
Access-Control-Allow-Origin: null
~~Access-Control-Allow-Origin: ya.ru, www.ru~~
~~Access-Control-Allow-Origin: http://*.ya.ru~~
```

XHR
m.ya.ru

browser

api.ya.ru

with
CORS

XHR
m.ya.ru

GET /data

browser

api.ya.ru

with
CORS

XHR
m.ya.ru

GET /data

browser

GET /data
Origin: http://m.ya.ru

api.ya.ru

with
CORS

XHR
m.ya.ru

GET /data

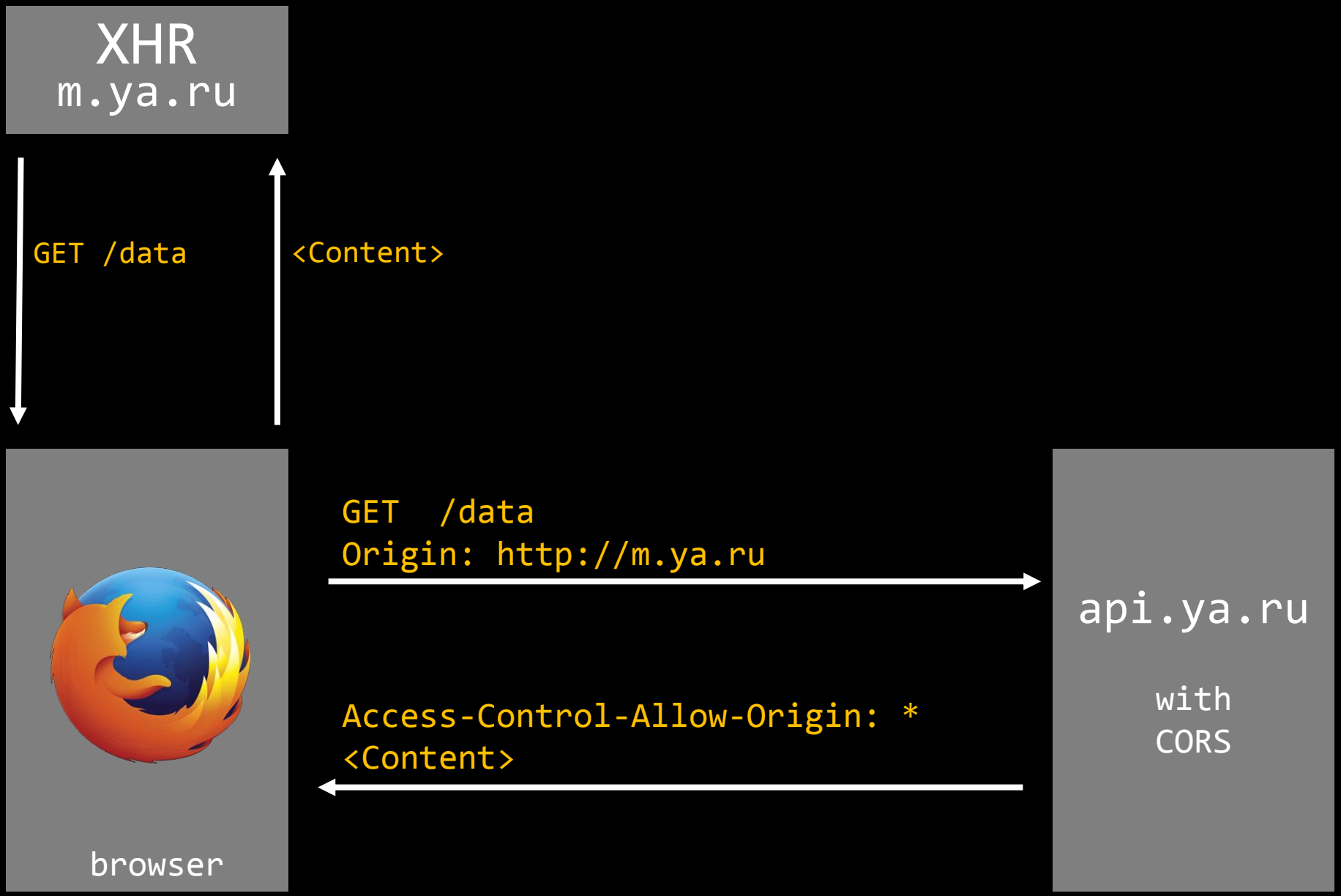
browser

GET /data
Origin: http://m.ya.ru

Access-Control-Allow-Origin: *
<Content>

api.ya.ru

with
CORS


XHR
m.ya.ru
GET /data
<Content>
GET /data
Origin: http://m.ya.ru
Access-Control-Allow-Origin: *
<Content>
browser
api.ya.ru
with
CORS

XHR
m.ya.ru

browser

api.ya.ru

without
CORS

XHR
m.ya.ru

POST /new

browser

api.ya.ru

without
CORS

XHR
m.ya.ru

POST /new

browser

```
OPTIONS  /new
Origin: http://m.ya.ru
Access-Control-Request-Method: POST
```

api.ya.ru

without
CORS

XHR
m.ya.ru

POST /new

browser

OPTIONS /new
Origin: http://m.ya.ru
Access-Control-Request-Method: POST

o_O

api.ya.ru

without
CORS

XHR
m.ya.ru

POST /new

<ERROR>

browser

OPTIONS /new
Origin: http://m.ya.ru
Access-Control-Request-Method: POST

o_O

api.ya.ru

without
CORS

```
Access-Control-Allow-Methods: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Methods: DELETE
Access-Control-Allow-Methods: POST, PUT
Access-Control-Allow-Methods: P*
```

```
header("Access-Control-Allow-Origin: *");
if(request_is_options()) {
    header("Access-Control-Allow-Methods:
POST");
}
```

XHR
m.ya.ru

browser

api.ya.ru

with
CORS

XHR
m.ya.ru

POST /new

browser

api.ya.ru

with
CORS

XHR
m.ya.ru

POST /new

browser

```
OPTIONS  /new
Origin: http://m.ya.ru
Access-Control-Request-Method: POST
```

api.ya.ru

with
CORS

XHR
m.ya.ru

POST /new

browser

OPTIONS /new
Origin: http://m.ya.ru
Access-Control-Request-Method: POST

Access-Control-Allow-Methods: POST

api.ya.ru

with
CORS

XHR
m.ya.ru

POST /new

browser

OPTIONS /new
Origin: http://m.ya.ru
Access-Control-Request-Method: POST

Access-Control-Allow-Methods: POST

POST /new

api.ya.ru

with
CORS

XHR
m.ya.ru

POST /new

browser

OPTIONS /new
Origin: http://m.ya.ru
Access-Control-Request-Method: POST

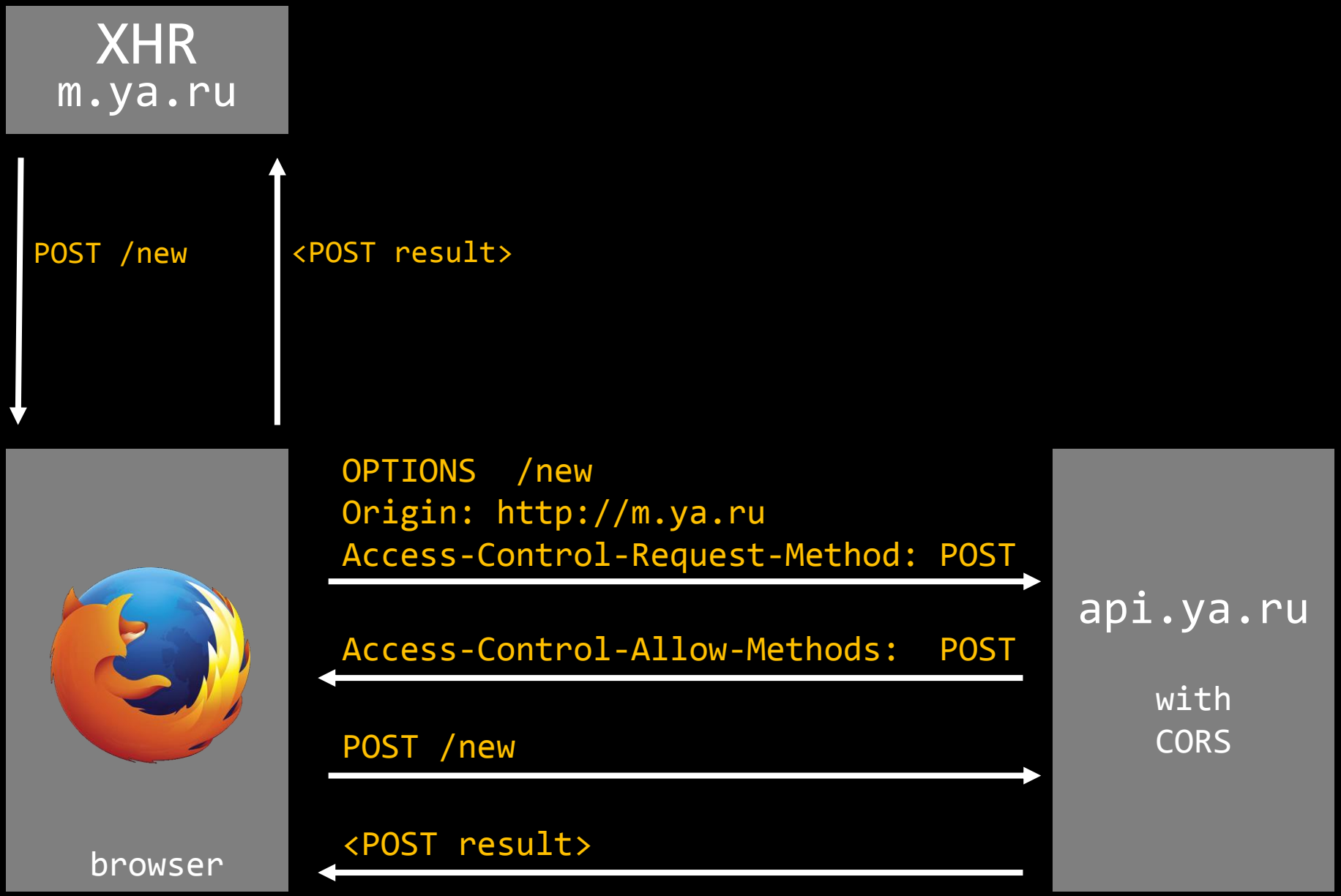
Access-Control-Allow-Methods: POST

POST /new

<POST result>

api.ya.ru

with
CORS


XHR
m.ya.ru
POST /new
<POST result>
OPTIONS /new
Origin: http://m.ya.ru
Access-Control-Request-Method: POST
Access-Control-Allow-Methods: POST
POST /new
<POST result>
browser
api.ya.ru
with
CORS

~~Access-Control-Allow-Headers: *~~

Access-Control-Allow-Headers: x-header

Access-Control-Allow-Headers: x-smpl

Access-Control-Allow-Headers: x-he, x-smpl

~~Access-Control-Allow-Headers: x-*~~

~~Access-Control-Expose-Headers: *~~

Access-Control-Expose-Headers: x-header

Access-Control-Expose-Headers: x-smpl

Access-Control-Expose-Headers: x-he, x-smpl

~~Access-Control-Expose-Headers: x-*~~

```
function Add()
{
    var Url = "http://api.ya.ru/new";
$.ajax({
    url: Url,
    data: { name:'foo' },
    type: 'POST',
    xhrFields: {
       withCredentials: true
    });
}
```

```
header("Access-Control-Allow-Credentials:
true");
```

```
header("Access-Control-Allow-Origin: *");
header("Access-Control-Allow-Credentials: true");
if(request_is_options()) {
    header("Access-Control-Allow-Methods: POST");
}
```

```
header("Access-Control-Allow-Origin: *");
header("Access-Control-Allow-Credentials: true");
if(request_is_options()) {
    header("Access-Control-Allow-Methods: POST");
}
```

```
header("Access-Control-Allow-Origin:
http://m.ya.ru");
header("Access-Control-Allow-Credentials:
true");
if(request_is_options()) {
    header("Access-Control-Allow-Methods:
POST");
}
```

8+

10+

http://cors.kojo.ru

Константин Якушев
kojo@kojo.ru
MoscowJS 14, 28.08.2014

Бонус-трэк!
XSRF и JSONP

```
<html><head>
    <script
src="http://ya.ru/?script"></script>
    <link rel="stylesheet"
href="http://ya.ru/?css">
</head>
<body>
<img src="http://ya.ru/?img">
<form action=" http://ya.ru/" method="get">
    <input type="text" name="test">
    <input type="submit">
</form>
</body></html>
```

C:/Users...esktop/test.html

ile:///C:/Users/Konstantin/Desktop/test.html

Co... Ins... Deb... Style ... P... Ne...

✓	Method	File	Domain	Type
●	GET	/?script	ya.ru	html
●	GET	/?css	ya.ru	html
●	GET	/?img	ya.ru	html
●	GET	/?css	ya.ru	html
●	GET	/?img	ya.ru	html

Headers | Cookies | Params | Response | Timings

Filter cookies

Request cookies

yandexuid: "75923203114084217

All HTML CSS JS XHR Fonts Images Media Flash Other

```
<script type="text/javascript">
     function parseQuote(response)
     {alert(response);}
</script>


<script type="text/javascript"
src="http://api.forismatic.com/api/1.0/?met
hod=getQuote&format=jsonp&jsonp=parseQuote"
></script>
```

```
Response:

parseQuote({"quoteText":"Text", "quoteAuthor":"Author"})
```

http://cors.kojo.ru

Константин Якушев
kojo@kojo.ru
MoscowJS 14, 28.08.2014