Cross-site access for XMLHttpRequest()

tlr@w3.org

XMLHttpRequest

http://www.w3.org/TR/XMLHttpRequest

"The XMLHttpRequest object can be used by scripts to programmatically connect to their originating server via HTTP."

"If stored url is non same-origin the user agent should raise a **SECURITY_ERR** exception and terminate these steps."

GET POST **HEAD** PUT DELETE **OPTIONS**

Enabling Read Access for Web Resources

http://www.w3.org/TR/access-control

HTTP Header

XML Processing Instruction

Access-Control: allow <*.example.org> exclude <*.public.example.org>

Access-Control: allow <webmaster.public.example.org>

<?acces-control allow="public.example.com"?>

Processing Model

GET (HEAD)

Safe HTTP method, not designed for side effects.

Don't use for selfdestruction, might be prefetched (and then cached)...



Don't use for selfdestruction, might be prefetched (and then cached)...

Goal

Authorize some data access, prevent unauthorized data access.

Goal?

Prevent HTTP GET requests.

Not a goal.

Prevent HTTP GET requests.

Retrieve resource

Check HTTP header

Check Processing Instruction, if XML

If access not allowed, throw exception

POST PUT DELETE



Unsafe HTTP methods, may have side effects.

Goal

Authorize some side effects, prevent unauthorized side effects and data access.

Retrieve resource with **GET**

(with additional HTTP header to identify target method)

Check HTTP header

Check Processing Instruction, if XML

Check HTTP Allow: header

If access not allowed, raise exception

Otherwise, HTTP request with original method

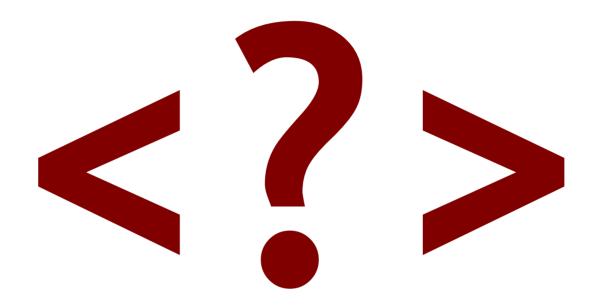
(Currently under discussion, likely to change.)

"access-control" is implemented in Firefox3.

Background links

http://www.w3.org/TR/access-controlhttp://www.w3.org/TR/XMLHttpRequest

Public comments make a difference, see "Status of this Document" for details on how to submit them.



tlr@w3.org