Is it possible to set a cookie for a site /server other than you own?

Asked 15 years, 10 months ago Modified 15 years, 1 month ago

Viewed 1k times Part of PHP Collective

2

Here's the quick version of my question:

Is it possible to set a cookie somehow into a client's browser when the cookie is for use with a different server (in this case an Exchange mail server)? In this scenario the server trying to set the cookie is at "intranet.myschool.edu" and the exchange server is at "owa_server.myschool.edu".

Here's the full question:

I have a php script that uses cURL to make an HTTP POST to our Exchange server that has Forms Based Authentication enabled.

When I make a successful HTTP POST (which includes the user/pass in the posted url), the Exchange Server (or more specifically, the https://my.school.edu/exchweb/bin/auth/owaauth.dll file) outputs cookies. Specifically, it outputs a "sessionid" and a "cadata" id.

With these cookie ids written to a text file on the server, cURL/PHP can reference it and then request data (via webdav and such) from the Exchange/OWA server.

That part works. The problem I'd like to solve is now passing the cookie ids to a clients browser, so that they can use these cookie ids to auto-login to their own OWA account.

In essence I would like our users to log into our intranet with their Active Directory IDs, and see a snapshot of their recent emails. Then, if they need to, I'd give them a little link to switch over to the full OWA web application. When this switch happens, I don't want them to have to login to the OWA manually. Since they already submitted their Active Directory UserName and password at the front of the intranet, I'd like them to be auto-logged into the OWA.

I should note that using Windows Authentication to try to do single sign on is not possible since we have a mix of Mac OS, Windows, and Linux.

I had thought that I would be able to do a "setcookie" and assign the cookie ids that cURL got and put them into the clients browser.

Is this not possible? Is it not possible to "spoof" Exchange/OWA (or any other site) this way. I have legitimate cookie ids that cURL captured. Is there no way to pass these to a client browser on a different computer?

In a worst case scenario, would using Javascript to just auto paste the username and password into the OWA login page be my only hope? Does anyone have any other ideas on how to avoid my double login problem with Exchange/OWA?

Thanks for any help provided!

PHP php cookies curl exchange-server logonserver

Share

Improve this question

Follow

asked Jan 29, 2009 at 22:00

Chain

627 ● 3 ● 9 ● 24

7 Answers

Sorted by: Highest score (default)

5

From RFC 2965 (NB HDN = "host domain name)

> Host A's name domain-matches host B's if
>
> ```
> *  their host name strings string-compare equal;
>
> * A is a HDN string and has the form NB, where N
>   name string, B has the form .B', and B' is a
>   x.y.com domain-matches .Y.com but not Y.com.)
> ```
>
> Note that domain-match is not a commutative operation: a.b.c.com domain-matches .c.com, but not the reverse.

So using `.myschool.edu` as the domain should work. NB the leading . is essential

Share Improve this answer

Follow

answered Jan 29, 2009 at 22:18

barrowc

10.7k ● 2 ● 44 ● 56

Overlaps with Alnitak's answer above :(– barrowc Jan 29, 2009 at 22:19

3

You *may* be able to set a cookie with a domain part of '.myschool.edu'. In theory that's then sent to any other site hosted under a subdomain of 'myschool.edu'.

In practise however, your client software may decide that the cookie's scope is too wide, and refuse to send it back.

Share Improve this answer

Follow

answered Jan 29, 2009 at 22:12

Alnitak

340k ● 71 ● 418 ● 502

1

I think this would be a serious security loophole if it were possible...

Share Improve this answer

Follow

answered Jan 29, 2009 at 22:05

Scott Evernden

39.9k ● 15 ● 80 ● 84

1

> In this scenario the server trying to set the cookie is at "intranet.myschool.edu" and the exchange server is at "owa_server.myschool.edu".

You should be able to do that.

I do this on my site (which I will change the names for the purpose of the example):

I have a web app at url

webapp.domain.com

And when users login, I set the cookie of the PunBB forum package which is at:

forum.domain.com

By setting/clearing the PunBB forum cookie, I can automatically login/logout my users on their forum account for convenience (this of course assumes that the registrations are syncrhonized, in my case I removed the forum registration and the main site registration creates the forum account for the user).

All you need to do is in subdomain#1 to set the cookie path to **"/"** (the default), and set the cookie domain to "domain.com". Then your app in subdomain#2 should see the cookie.

EDIT: I see **barrowc** has answered, I've seen the ".domain.com" pattern in some examples, my site uses "domain.com" for the cookie domain and it works too (maybe php set_cookie adds the leading dot if missing?)

Share Improve this answer

Follow

answered Jan 29, 2009 at 23:39

user58777

> Section 3.2.2 of RFC 2965 says: "The value of the Domain attribute specifies the domain for which the cookie is valid. If an explicitly specified value does not start with a dot, the user agent supplies a leading dot" – barrowc Jan 30, 2009 at 0:13

> Thanks! :) Section 3.3.2 of the RFC shows some good examples. – user58777 Jan 30, 2009 at 10:16

0

Your browser gets to decide that... but usually no, you cannot. That is considered a type of XSS vulnerability.

Share Improve this answer

Follow

answered Jan 29, 2009 at 22:47

Keith

0

you could use an iframe to set the cookie, ie. have an iframe on your web server that makes a request to a page on your exchange http server (https://my.school.edu/exchweb/) with your wanted cookie

vars set as get or post variables. then use the vars to set the cookie for that domain, and redirect the user to the exchange server.

now, there could be logic on the backend of OWA that checks ip address, user agent, etc.... when registering the session that may invalidate this..... not sure

Share Improve this answer

Follow

answered Jan 31, 2009 at 4:36

Jason

2,049 ● 11 ● 13

0

We've been fighting this one hard for months, the best we can come up with is allowing the web server to get the cookie for Exchange at EVERY LOGIN. problem is, that without cookie affinity, we don't have a way to make sure that the cookie obtained by the web server came from the same load balanced node that the client connects to.

Share Improve this answer

Follow

answered Nov 6, 2009 at 19:46

phydroxide

1