PHP - Sessions - Security

Asked 16 years, 2 months ago Modified 9 years, 11 months ago

Viewed 788 times Part of PHP Collective

3

How secure are php Sessions? I am planning to use the native PHP sessions to authenticate users. Can users modify session data like they can $_POST and $_GET data?

PHP php session

Share

Improve this question

Follow

asked Oct 20, 2008 at 21:13

user29772

1,467 ● 7 ● 21 ● 26

2 Answers

Sorted by: Highest score (default)

6

Data only goes into a session when you as the developer have the user put it into the session via the code you write. Therefore, sessions are as secure as the data you allow into them, and how you trust and use that data. Further, sessions are based on a sessionID that the client uses to identify the session user. If someone hijacks a sessionID, then they can emulate being the user whose session ID they stole. This can happen in non SSH communication. So don't trust a session ID for identifying

a user (for important stuff) unless they have logged in and the sessionID has only been transmitted in secure mode.

The next question of security would be the "guessability" of a sessionID you sent off to the user. If you handle the stuff I mention above, by the time you get through it and the documentation you will understand how "guessable" PHP sessionIDs are.

Finally watch out for XSS attacks. There are several posts across the internet that explain how to minimize the incidence of XSS.

Share Improve this answer

Follow

answered Oct 20, 2008 at 21:20

Zak

25.2k ● 11 ● 41 ● 68

3

PHP sessions are as secure as the session cookie given to the user. All the data in the session is stored server-side, so users can't arbitrarily modify them except through whatever functionality your site provides. However, PHP session cookies are a common target for cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. Just the same, sessions are a good way to do user authentication as long as you're aware of the potential risks.

Some Wikipedia links:

CSRF

XSS

Share Improve this answer

Follow

answered Oct 20, 2008 at 21:20

Randy

4,023 ● 21 ● 25

How else can you do authentication? $_SESSION is the only way anyone ever talks about. – Robert K Oct 20, 2008 at 21:26

The only other way I've done it was long ago in Perl by storing username/hashed password cookies on the client machine and reading those in at each page load. A bit risky; someone accessing the cookies on the machine after you could then access your account at any time if they copy your cookie. – Randy Oct 20, 2008 at 21:31

In some environments, you could also potentially do IP-based server side authentication (e.g., when you get valid login credentials, store the IP and an expiration timestamp in the server's database). This obviously doesn't work well with NATs or proxy servers though. – Randy Oct 20, 2008 at 21:33