Session Extending - Session Extension - Websecurity (English translation)

Session Extending - продовження сесії - Websecurity - MustLive, websecurity.com.ua.

- Title in English: Session Extending - Session Extension - Websecurity
- Published: date not stated
- Original: <http://websecurity.com.ua/2233/>
- Preserved from: http://websecurity.com.ua/2233/ (stored) on 2026-08-11
- Licence: unknown

Content (translated into English)

Machine translation of `websecurity-com-ua-session-extending-websecurity.md` *, which holds the source's own words. Code, payloads, type names, URLs and CVE identifiers were masked before translating and restored after, so they are byte-identical to the original.*

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Session Extending - Session Extension - Websecurity - Web Security

---

Session Extending - Session Extension

22:48 03.07.2008

When carrying out Cross-Site Scripting attacks that steal cookies for later use to gain access to an account (particularly an administrator account), session duration is an important factor. This applies when a session cookie is used for identification (rather than a password or hash—because in that case there will be no problems with session duration, and if there is no limit on the cookie's lifetime, the attack will be successful a priori). The success of the attack directly depends on the session duration. If the session expires, that cookie (that session) will be useless.

Therefore, when carrying out an XSS attack, it is necessary to pay attention to the session duration. If the site is vulnerable to Insufficient Session Expiration, the attack will encounter no complications and the session will remain active for a long time (from several hours to an unlimited length of time). This is enough time to carry out an account takeover successfully.

If, however, the site has no Insufficient Session Expiration vulnerabilities (the site's administrators have taken care of this aspect), it will be necessary either to carry out the account takeover procedure very quickly (while the session is active) or to resolve the issue in another way. In

particular, this problem can be solved by extending the session, and for this purpose I developed my own method—the MustLive Session Extending Method.

My method, which I developed in 2006, is intended to extend a captured session and can be used when carrying out XSS attacks. This method has been successfully tested in practice many times [image: ;-)] .

The essence of the method is to send requests to the site being attacked. The requests are sent periodically, and the interval can be set arbitrarily; the main requirement is that it be shorter than the session lifetime (which is determined experimentally). The request itself is sent to the site together with the captured cookie, thereby extending its session. Using this method, a captured session (or several sessions) can be extended for any length of time (as long as necessary).

Web developers and site administrators should therefore remember that session-duration limits can be bypassed. Even the absence of Insufficient Session Expiration vulnerabilities will not protect against an attack by a professional. Consequently, the only way to counter Cross-Site Scripting attacks is to fix all XSS holes on the site.

This entry was posted on 22:48 03.07.2008 and is filed under Articles. You can follow any responses to this entry through the RSS 2.0 feed.

Leave a Reply

You must be logged in to post a comment.
