

File System API with HTML5

File System API with HTML5 - shreeraj, shreeraj.blogspot.com.

- Published: date not stated
- Original:
<<https://web.archive.org/web/20170903113359/http://shreeraj.blogspot.com/2012/08/file-system-api-with-html5-juice-for-xss.html>>
- Current location:
<<https://web.archive.org/web/20190110045801/http://shreeraj.blogspot.com/2012/08/file-system-api-with-html5-juice-for-xss.html>>
- Preserved from:
<https://web.archive.org/web/20190110045801/http://shreeraj.blogspot.com/2012/08/file-system-api-with-html5-juice-for-xss.html> (live) on 2026-08-10
- Capture timestamp: 20170903113359
- Licence: unknown

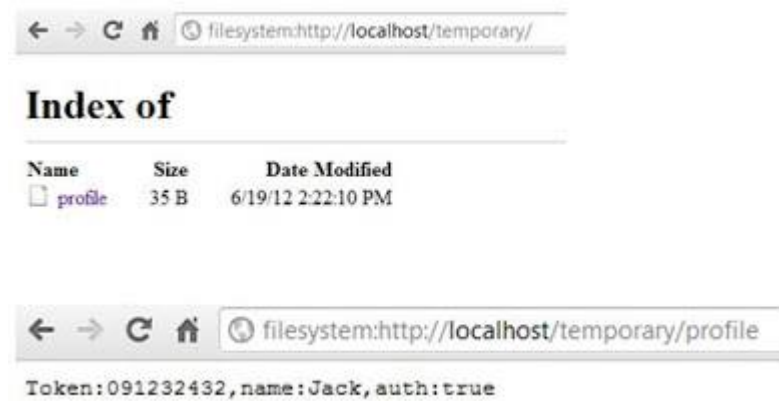
Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

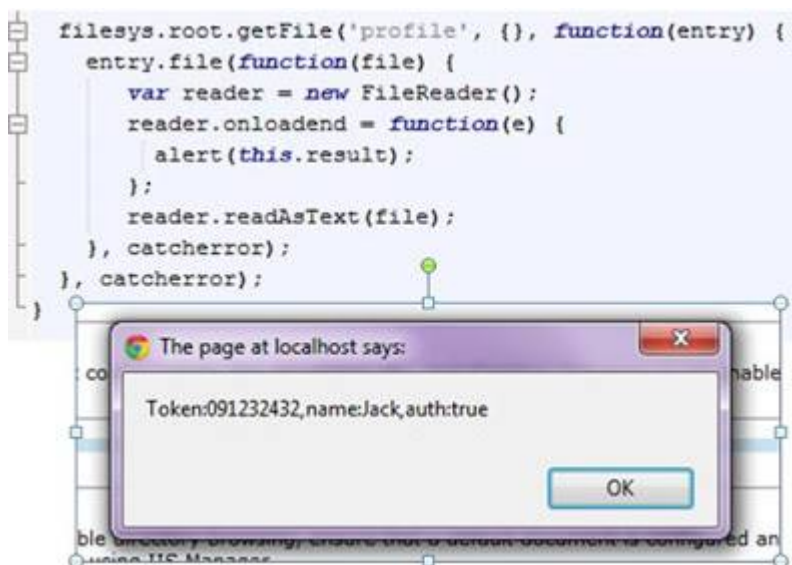
UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

HTML5 has come up with several APIs and one of them is File System API (<http://www.w3.org/TR/file-system-api/>). Browsers are implementing it and it is covering both directories and files under this API. Hence, now web application can create a mini file system and dump files inside the browser. These files can be accessed at any point in time by the browser with the same domain context. These files can be permanent or temporary. The browser is acting like a mini OS and exposing the surface. If XSS is found it is easy to extract full file system created by the application.

For example, if an application has created a token file on the file system using the API. We can see files by following URI on chrome.



In above figure we can see files are being created in the browser. Now assuming XSS is found, it is easy to exploit by hooking into the file system and extracting the content. Following code can be part of the access routine.



Bottom-line, lot is getting added to HTML5 and strong JavaScript analysis and look around would be needed from security professional. Looks like developer community is still playing around with these APIs but the days are not far where we will start seeing these types of application in production and landing for review at the door steps.