Javascript for Pentesters

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

XHR and HTML Parsing

Why HTML Parsing?

- XSS can be used to traverse the application
- HTML Pages might need to be processed
  - extract tokens
- Text based treatment is painful
- DOM based Parsing is required

HTML in XHR

HTML in XMLHttpRequest

The W3C XMLHttpRequest specification adds HTML parsing support to `XMLHttpRequest`, which originally supported only XML parsing. This feature allows Web apps to obtain an HTML resource as a parsed DOM using `XMLHttpRequest`.

Limitations

To discourage the synchronous use of `XMLHttpRequest`, HTML support is not available in the synchronous mode. Also, HTML support is only available if the `responseType` property has been set to `"document"`. This limitation avoids wasting time parsing HTML uselessly when legacy code uses `XMLHttpRequest` in the default mode to retrieve `responseText` for `text/html` resources. Also, this limitation avoids problems with legacy code that assumes that `responseXML` is null for HTTP error pages (which often have a `text/html` response body).

Usage

Retrieving an HTML resource as a DOM using `XMLHttpRequest` works just like retrieving an XML resource as a DOM using `XMLHttpRequest`, except you can't use the synchronous mode and you have to explicitly request a document by assigning the string `"document"` to the `responseType` property of the `XMLHttpRequest` object after calling `open()` but before calling `send()`.

https://developer.mozilla.org/en-US/docs/HTML_in_XMLHttpRequest

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

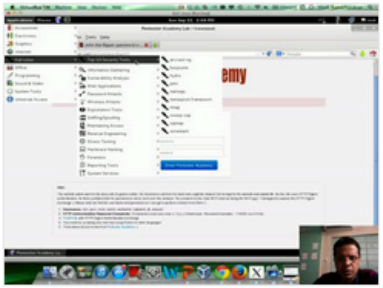
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

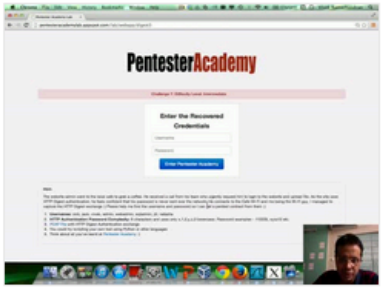
Start Learning Today!

Latest Videos

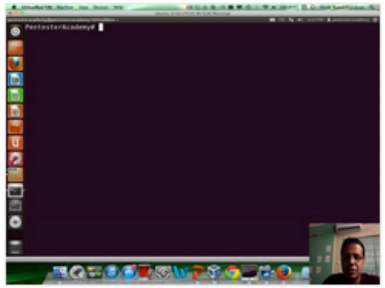
New content added weekly!



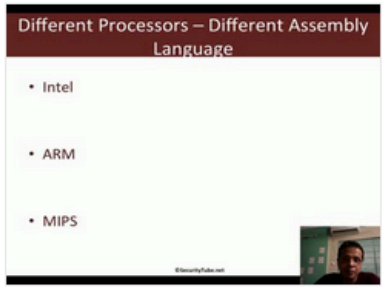
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux