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

XMLHttpRequest Basics

XMLHttpRequest

XMLHttpRequest

`XMLHttpRequest` is a JavaScript object that was designed by Microsoft and adopted by Mozilla, Apple, and Google. It's now being standardized in the W3C. It provides an easy way to retrieve data from a URL without having to do a full page refresh. A Web page can update just a part of the page without disrupting what the user is doing. `XMLHttpRequest` is used heavily in AJAX programming.

https://developer.mozilla.org/en-US/docs/Web/API/XMLHttpRequest

Origin Policies

- Same origin policy
  - resource sharing allowed only if from same origin
  - Origin based on Protocol, Port and Host combination
  - https://developer.mozilla.org/en-US/docs/Web/JavaScript/Same_origin_policy_for_JavaScript
- Cross Origin Resource Sharing
  - https://developer.mozilla.org/en/docs/HTTP/Access_control_CORS
  - server decides based on origin domain
  - http://stackoverflow.com/questions/2533049/cross-origin-resource-sharing-cors-am-i-missing-something-here

Structure of XHR

```
<script>

var req = new XMLHttpRequest();

req.onreadystatechange=function()
  {
  if (req.readyState==4 && req.status==200)
    {
     response =req.responseText;
    }
  };


req.open("GET", "/lab/webapp/jfp/14/email?name=john", true);

req.send();


</script>
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

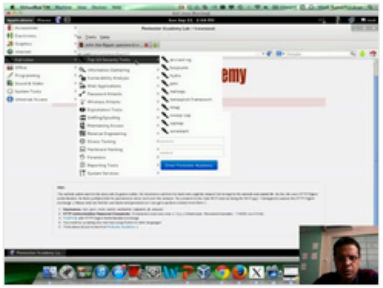
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

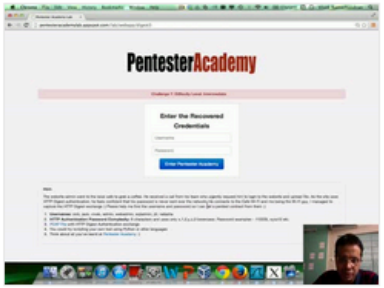
Start Learning Today!

Latest Videos

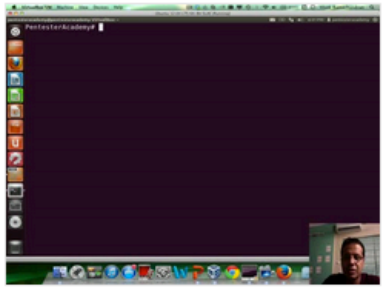
New content added weekly!



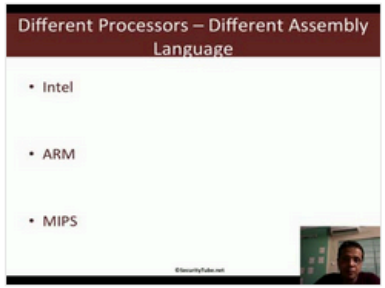
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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