

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>

Set-Cookie Demo with HTTPCookie.py

HTTPCookie.py

```
import webapp2
from paste import httpserver
import random

def GetAllHeaders(headers) :
    header_response = 'HTTP Headers Received:\n'
    for k, v in headers.items() :
        header_response += "%s : %s\n"% (k,v)

    return header_response

class RootCookie(webapp2.RequestHandler):

    def get(self):
        self.response.content_type = 'text/plain'
        header_response = GetAllHeaders(self.request.headers)

        # Not checking if cookie value is preset, simply overwrite existing

        self.response.set_cookie(
            'root_session_id',
            str(random.getrandbits(128)),
            max_age = 1200,
            path= '/' )

        self.response.set_cookie(
            'blog_session_id',
            str(random.getrandbits(128)),
            max_age = 1800,
            path= '/blog' )

        self.response.write(header_response)
```

Cookie.py

Install

```
PentesterAcademy# apt-get install python-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-pip is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 79 not upgraded.
PentesterAcademy#
PentesterAcademy#
PentesterAcademy# pip install webob paste webapp2
Requirement already satisfied (use --upgrade to upgrade): webob in /u
Requirement already satisfied (use --upgrade to upgrade): paste in /u
Requirement already satisfied (use --upgrade to upgrade): webapp2 in
Cleaning up...
PentesterAcademy# █
```

Assumption – you are running Kali Linux

Set a Cookie for “/”

← → ↻ 📄 192.168.1.8:8080

HTTP Headers Received:

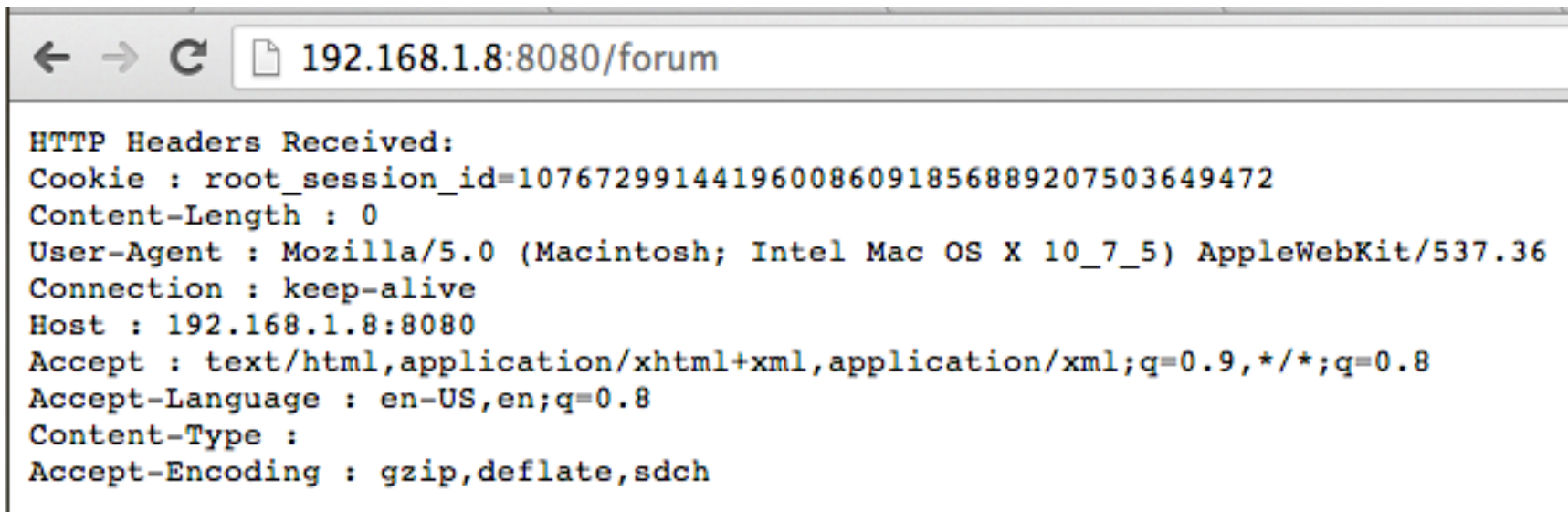
```
Cookie : root_session_id=282696174887011378294458518951940515678
Content-Length : 0
User-Agent : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36
Connection : keep-alive
Host : 192.168.1.8:8080
Cache-Control : max-age=0
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language : en-US,en;q=0.8
Content-Type :
Accept-Encoding : gzip,deflate,sdch
```

Cookie for “/blog”



```
← → ↻ 192.168.1.8:8080/blog
HTTP Headers Received:
Cookie : blog_session_id=295169252041865966514396790476656539981; root_session_id=107672991441960086091856889207503649472
Content-Length : 0
User-Agent : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.65 Safari/537.36
Connection : keep-alive
Host : 192.168.1.8:8080
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language : en-US,en;q=0.8
Content-Type :
Accept-Encoding : gzip,deflate,sdch
```

Cookie for “/forum”



```
← → ↻ 📄 192.168.1.8:8080/forum
HTTP Headers Received:
Cookie : root_session_id=107672991441960086091856889207503649472
Content-Length : 0
User-Agent : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36
Connection : keep-alive
Host : 192.168.1.8:8080
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language : en-US,en;q=0.8
Content-Type :
Accept-Encoding : gzip,deflate,sdch
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS PRICING WHY SUBSCRIBE [MEMBER ACCESS](#)



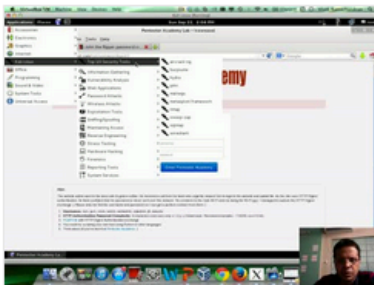
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

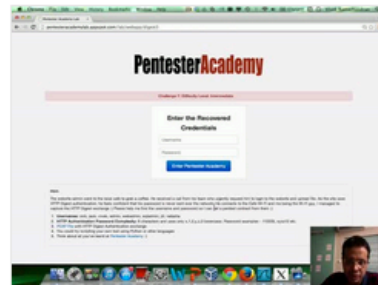
[Start Learning Today!](#)

Latest Videos

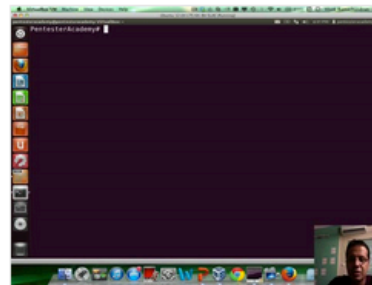
New content added weekly!



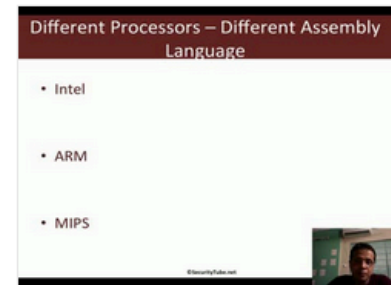
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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

Twitter and Facebook



Security Tube

@SecurityTube

Comprehensive, Hands-on, Practical and Affordable infosec training. Join students from 73+ Countries:

PentesterAcademy.com Securitytube-Training.com

CyberSpace · securitytube.net

19,964
TWEETS

8,576
FOLLOWING

37,554
FOLLOWERS



Edit profile



SecurityTube

✓ Like

You like this.

You and 36,320 others like SecurityTube.