SESSION HIJACKING AT SHOPFAST E-COMMERCE PLATFORM

Bakka Ramyasree

What exactly this session hijacking means whean a legitimate user login to a website it generally creates and entry with the data base and gives session id or cookie.

These are unique identifiers for logging session and they are randomly generated.

There are many methods for Session hijacking
Commonly

- Sesssion sniffing
- Man int the browser
- Session side jacking
- Session fixation…….

I used session sniffing for implemenatinf this attack

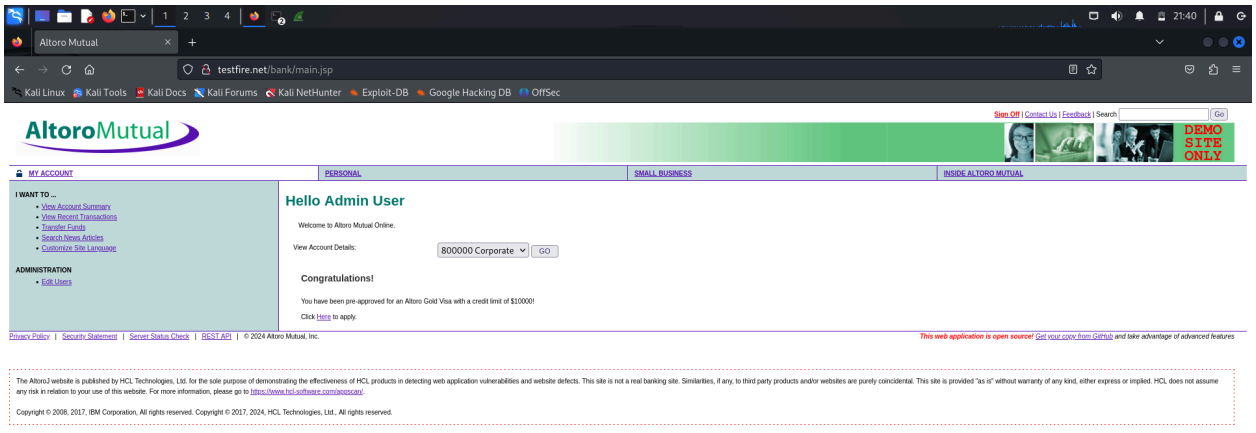
Tools commonly used are

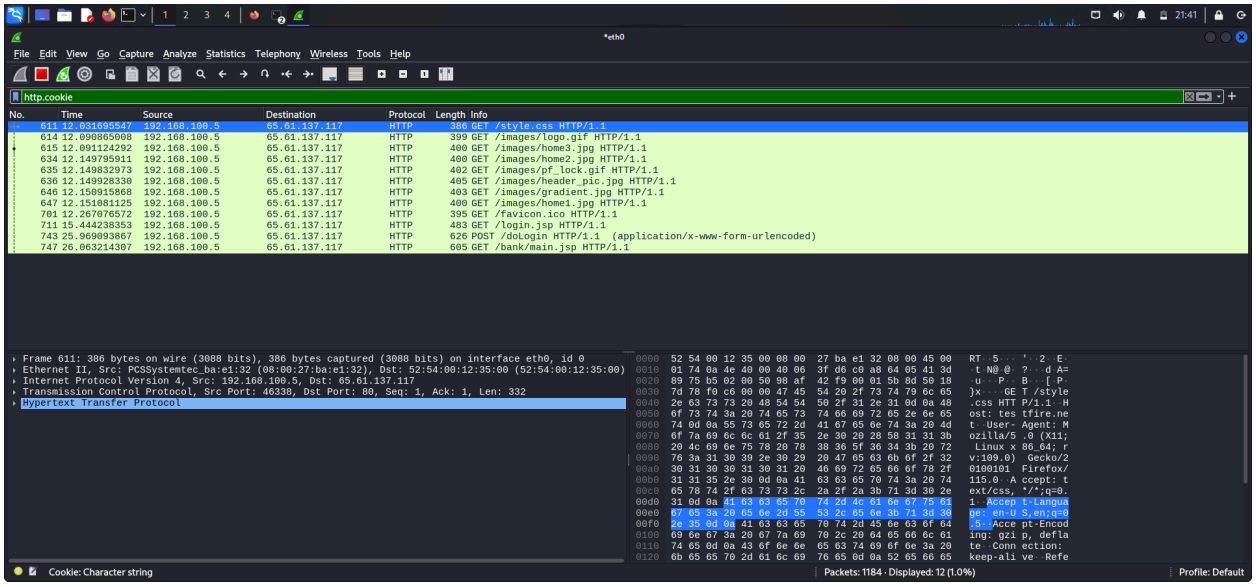
- Wireshark
- Ettercap
- Brupsuite
- ZAP proxy..

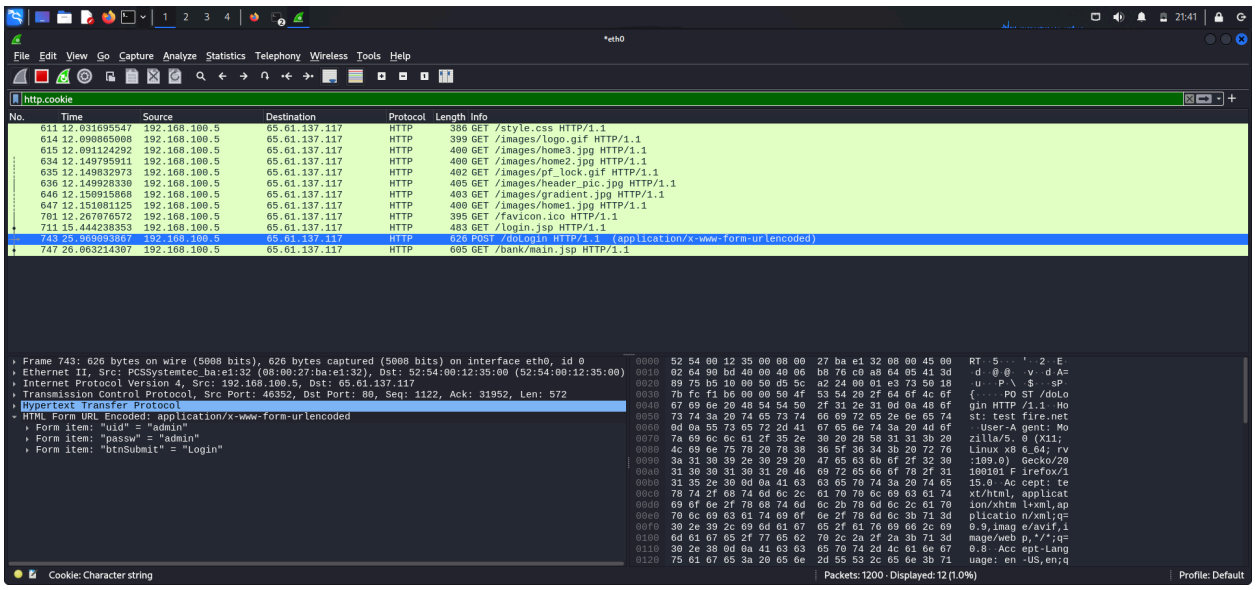
I have done this with wireshark and ettercap

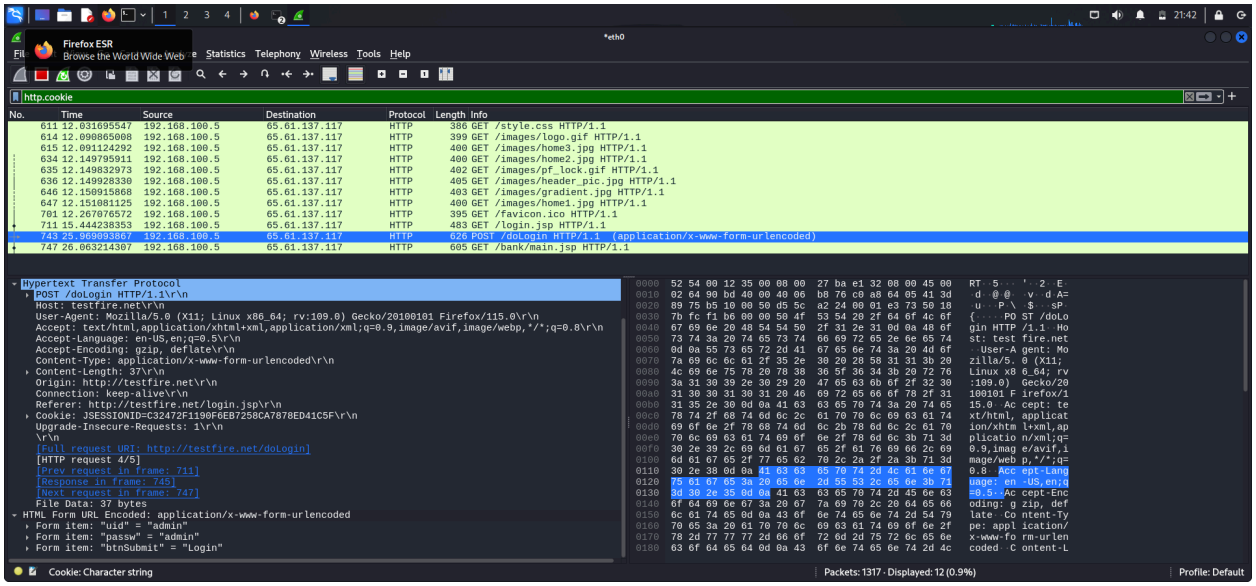
USING WIRESHARK

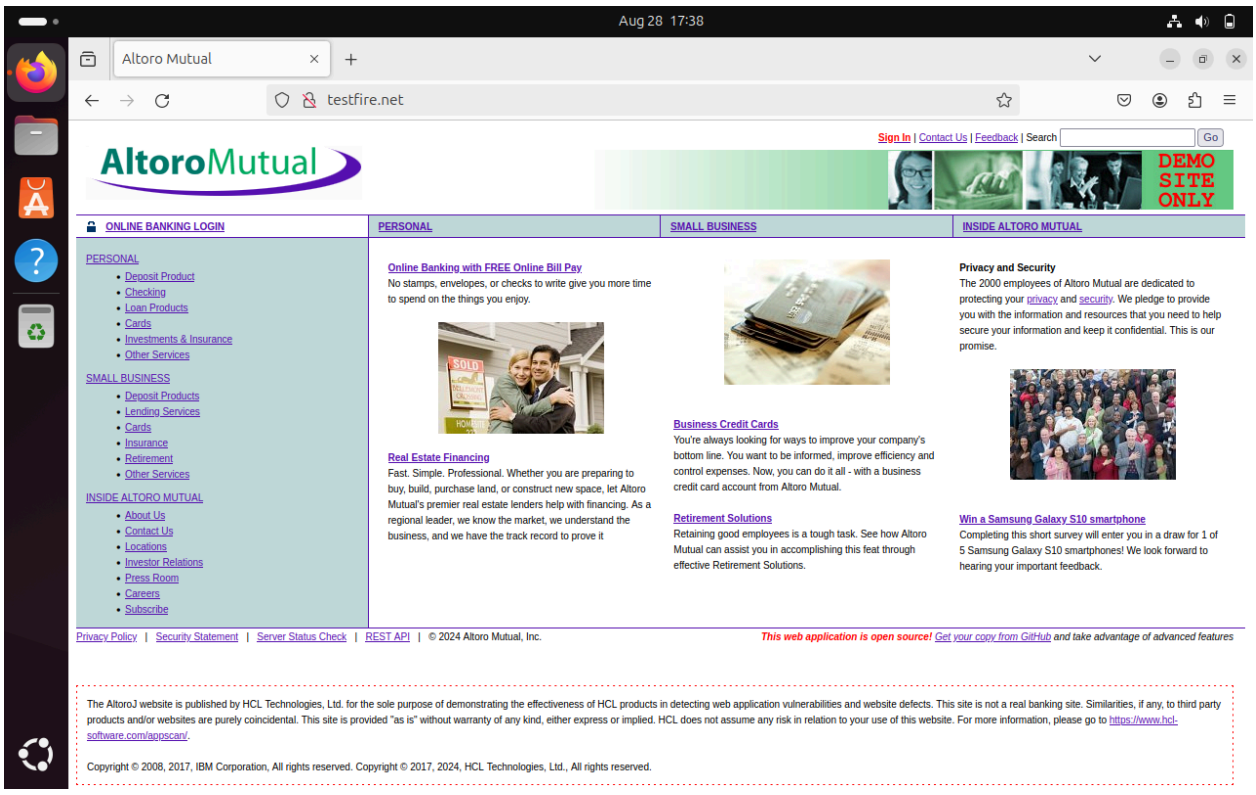
This is the demo website testfire.net

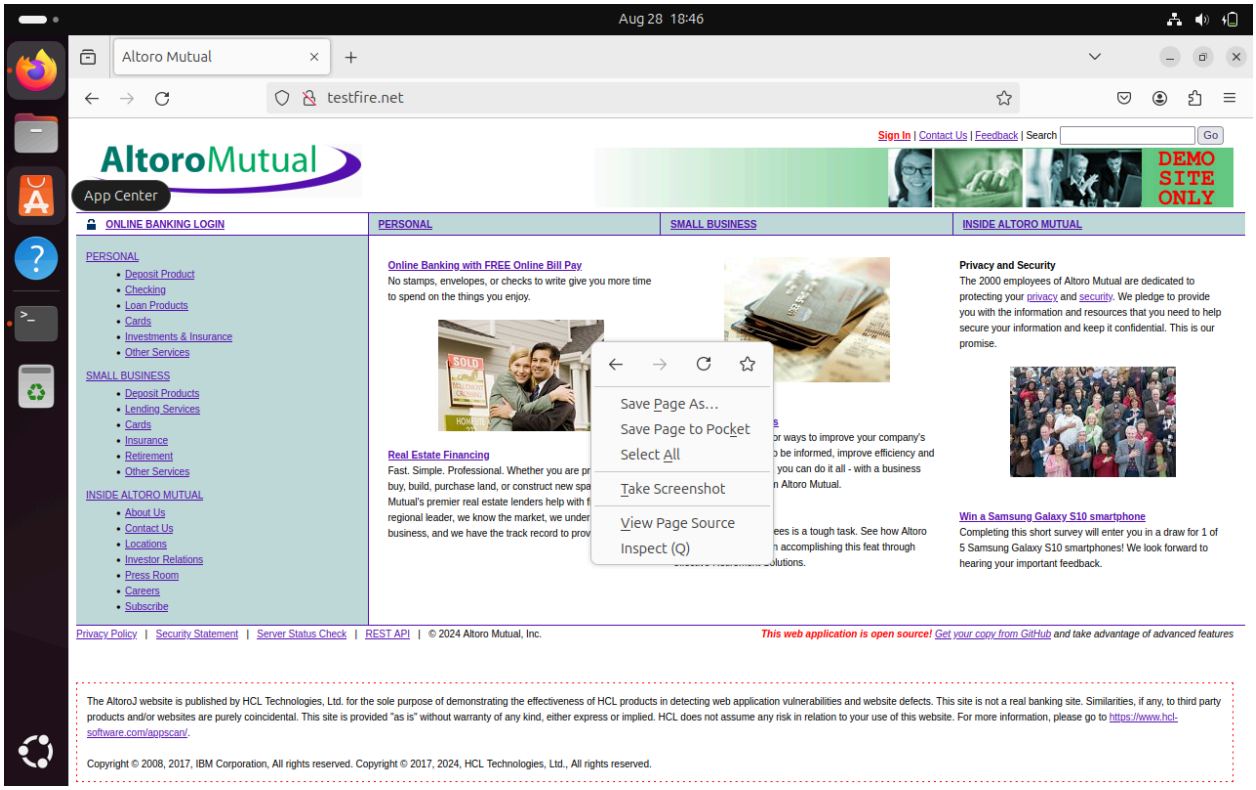


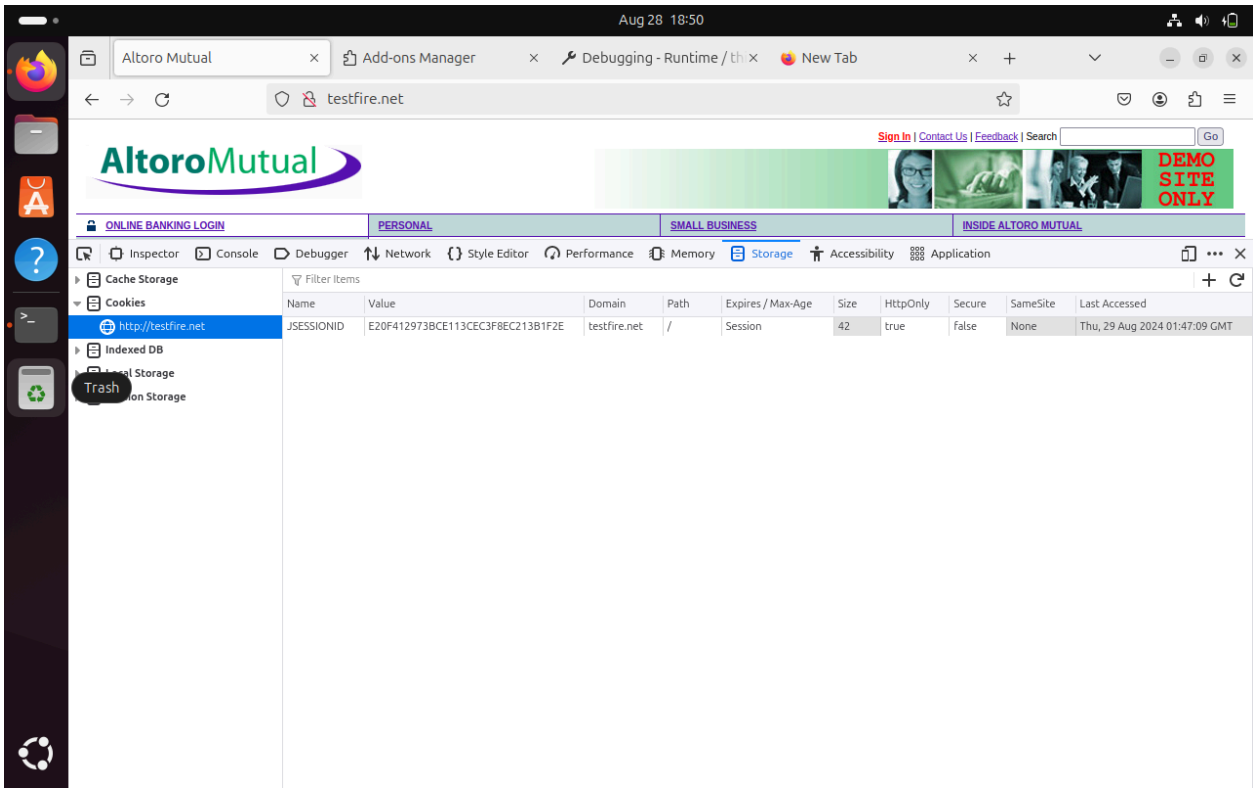

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.cookie
No. Time Source Destination Protocol Length Info
611 12.031695547 192.168.100.5 65.61.137.117 HTTP 386 GET /style.css HTTP/1.1
614 12.090865008 192.168.100.5 65.61.137.117 HTTP 399 GET /images/logo.gif HTTP/1.1
615 12.091124292 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home3.jpg HTTP/1.1
634 12.149795911 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home2.jpg HTTP/1.1
635 12.149832973 192.168.100.5 65.61.137.117 HTTP 402 GET /images/pf_lock.gif HTTP/1.1
636 12.149928330 192.168.100.5 65.61.137.117 HTTP 405 GET /images/header_pic.jpg HTTP/1.1
646 12.150915868 192.168.100.5 65.61.137.117 HTTP 403 GET /images/gradient.jpg HTTP/1.1
647 12.151081125 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home1.jpg HTTP/1.1
701 12.267076572 192.168.100.5 65.61.137.117 HTTP 395 GET /favicon.ico HTTP/1.1
711 15.444238353 192.168.100.5 65.61.137.117 HTTP 483 GET /login.jsp HTTP/1.1
743 25.969093867 192.168.100.5 65.61.137.117 HTTP 626 POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
747 26.063214307 192.168.100.5 65.61.137.117 HTTP 605 GET /bank/main.jsp HTTP/1.1
Frame 611: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 46338, Dst Port: 80, Seq: 1, Ack: 1, Len: 332
Hypertext Transfer Protocol
Cookie: Character string
Packets: 1184 · Displayed: 12 (1.0%)
Profile: Default

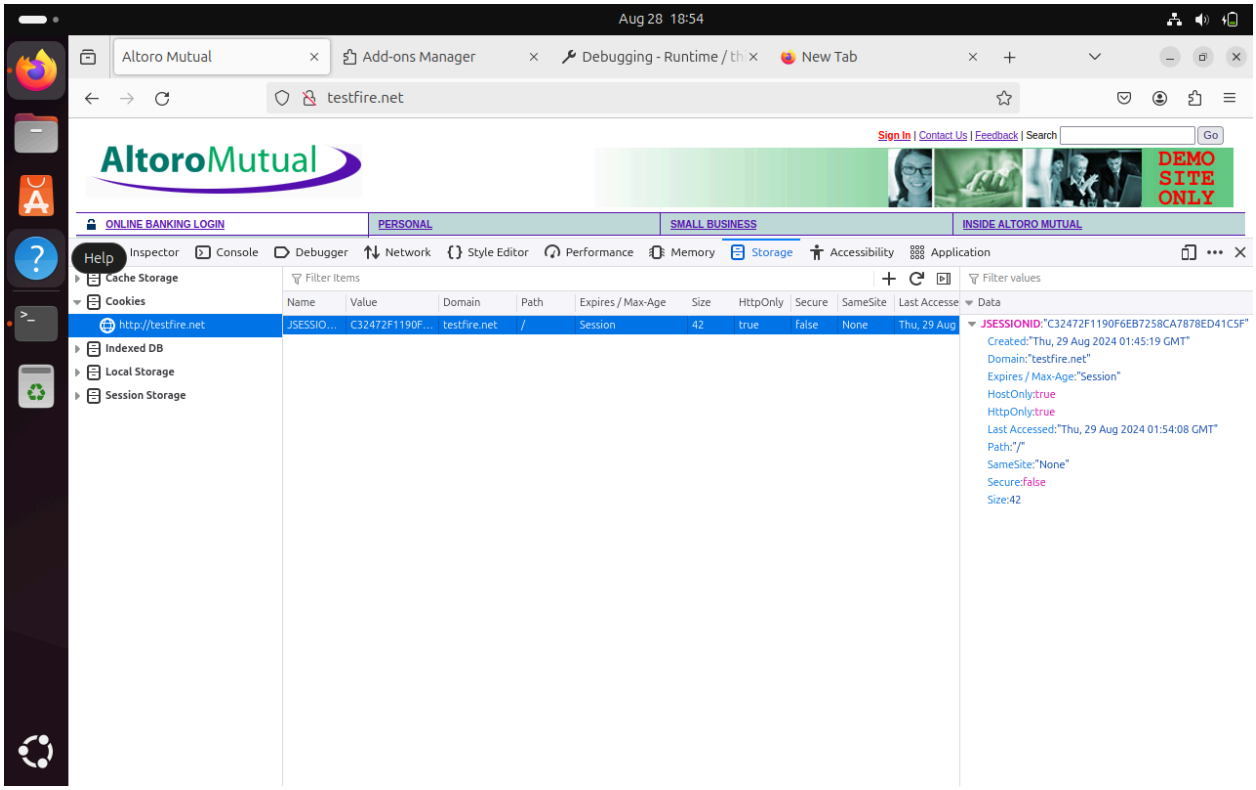

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.cookie
No. Time Source Destination Protocol Length Info
611 12.031695547 192.168.100.5 65.61.137.117 HTTP 386 GET /style.css HTTP/1.1
614 12.090865008 192.168.100.5 65.61.137.117 HTTP 399 GET /images/logo.gif HTTP/1.1
615 12.091124292 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home3.jpg HTTP/1.1
634 12.149795911 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home2.jpg HTTP/1.1
635 12.149832973 192.168.100.5 65.61.137.117 HTTP 402 GET /images/pf_lock.gif HTTP/1.1
636 12.149928330 192.168.100.5 65.61.137.117 HTTP 405 GET /images/header_pic.jpg HTTP/1.1
646 12.150915868 192.168.100.5 65.61.137.117 HTTP 403 GET /images/gradient.jpg HTTP/1.1
647 12.151081125 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home1.jpg HTTP/1.1
701 12.267076572 192.168.100.5 65.61.137.117 HTTP 395 GET /favicon.ico HTTP/1.1
711 15.444238353 192.168.100.5 65.61.137.117 HTTP 483 GET /login.jsp HTTP/1.1
743 25.969093867 192.168.100.5 65.61.137.117 HTTP 626 POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
747 26.063214307 192.168.100.5 65.61.137.117 HTTP 605 GET /bank/main.jsp HTTP/1.1
Frame 743: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 46352, Dst Port: 80, Seq: 1122, Ack: 31952, Len: 572
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uid" = "admin"
Form item: "passw" = "admin"
Form item: "btnSubmit" = "Login"
Cookie: Character string
Packets: 1200 · Displayed: 12 (1.0%)
Profile: Default

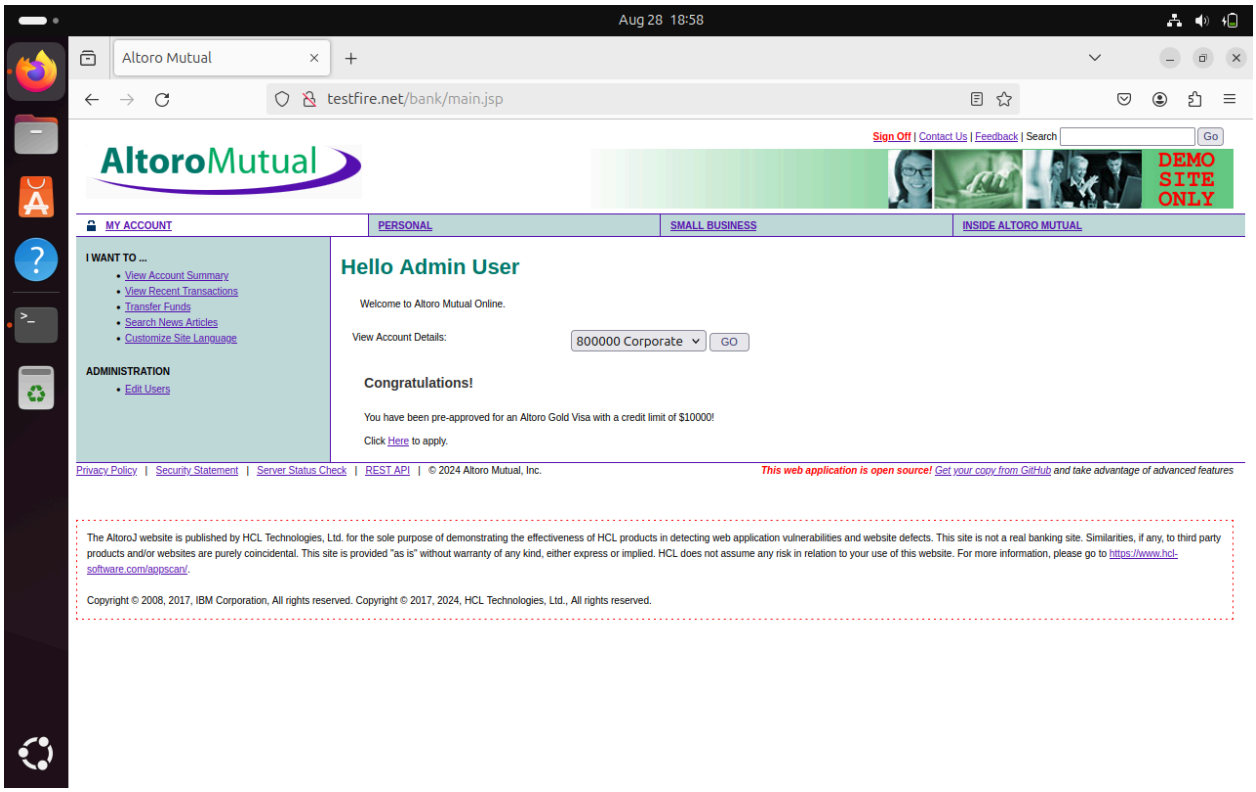

Firefox ESR
Browse the World Wide Web
*eth0
Statistics Telephony Wireless Tools Help
http.cookie
No. Time Source Destination Protocol Length Info
611 12.031695547 192.168.100.5 65.61.137.117 HTTP 386 GET /style.css HTTP/1.1
614 12.090865008 192.168.100.5 65.61.137.117 HTTP 399 GET /images/logo.gif HTTP/1.1
615 12.091124292 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home3.jpg HTTP/1.1
634 12.149795911 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home2.jpg HTTP/1.1
635 12.149832973 192.168.100.5 65.61.137.117 HTTP 402 GET /images/pf_lock.gif HTTP/1.1
636 12.149928330 192.168.100.5 65.61.137.117 HTTP 405 GET /images/header_pic.jpg HTTP/1.1
646 12.150915868 192.168.100.5 65.61.137.117 HTTP 403 GET /images/gradient.jpg HTTP/1.1
647 12.151081125 192.168.100.5 65.61.137.117 HTTP 400 GET /images/home1.jpg HTTP/1.1
701 12.267076572 192.168.100.5 65.61.137.117 HTTP 395 GET /favicon.ico HTTP/1.1
711 15.444238353 192.168.100.5 65.61.137.117 HTTP 483 GET /login.jsp HTTP/1.1
743 25.969093867 192.168.100.5 65.61.137.117 HTTP 626 POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
747 26.063214307 192.168.100.5 65.61.137.117 HTTP 605 GET /bank/main.jsp HTTP/1.1
Hypertext Transfer Protocol
POST /doLogin HTTP/1.1\r\n
Host: testfire.net\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 37\r\n
Origin: http://testfire.net\r\n
Connection: keep-alive\r\n
Referer: http://testfire.net/login.jsp\r\n
Cookie: JSESSIONID=C32472F1190F6EB7258CA7878ED41C5F\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://testfire.net/doLogin]
[HTTP request 4/5]
[Prev request in frame: 711]
[Response in frame: 745]
[Next request in frame: 747]
File Data: 37 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uid" = "admin"
Form item: "passw" = "admin"
Form item: "btnSubmit" = "Login"
Cookie: Character string
Packets: 1317 · Displayed: 12 (0.9%)
Profile: Default


Aug 28 17:38
Altoro Mutual
testfire.net
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

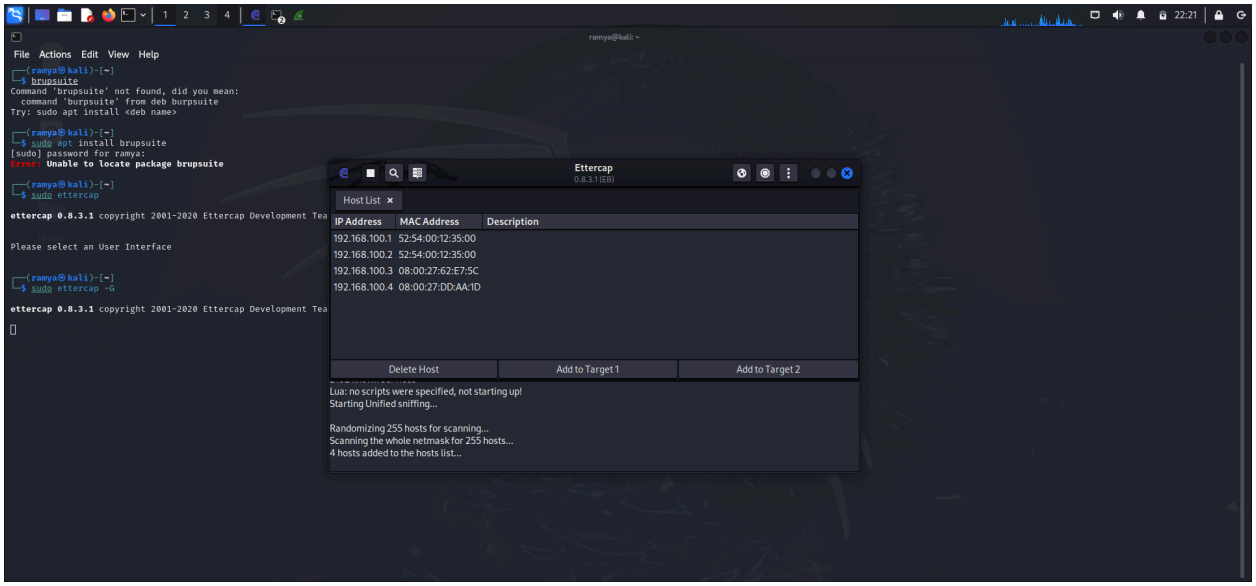

Aug 28 18:46
Altoro Mutual
testfire.net
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
App Center
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Real Estate Financing
Fast. Simple. Professional. Whether you are pr
buy, build, purchase land, or construct new spa
Mutual's premier real estate lenders help with f
regional leader, we know the market, we under
business, and we have the track record to prov
Save Page As...
Save Page to Pocket
Select All
Take Screenshot
View Page Source
Inspect (Q)
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

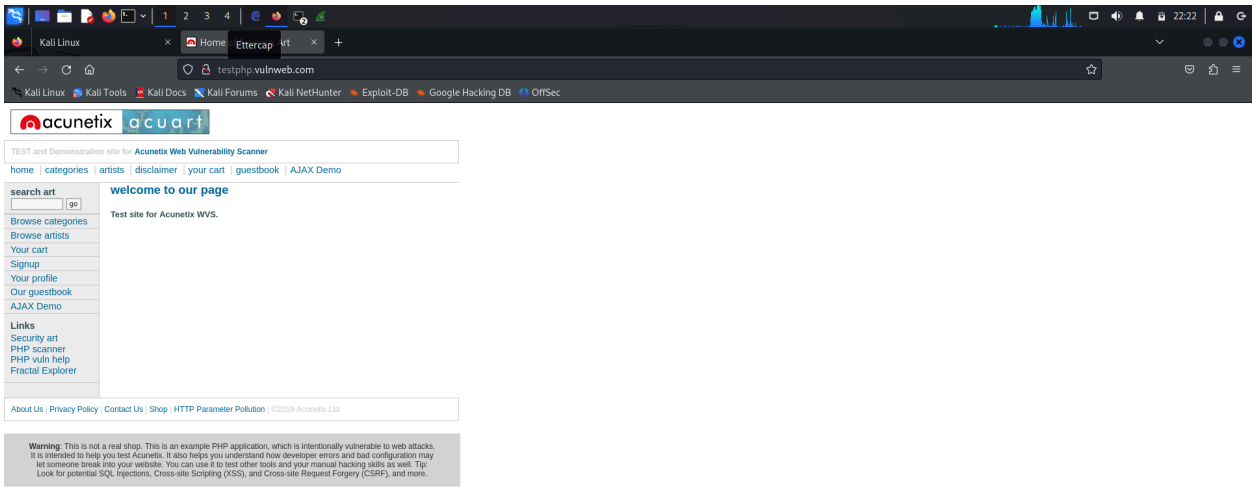

Aug 28 18:50
Altoro Mutual
Add-ons Manager
Debugging - Runtime / th
New Tab
testfire.net
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
http://testfire.net
Indexed DB
Filter Items
Name
Value
Domain
Path
Expires / Max-Age
Size
HttpOnly
Secure
SameSite
Last Accessed
JSESSIONID
E20F412973BCE113CEC3F8EC213B1F2E
testfire.net
/
Session
42
true
false
None
Thu, 29 Aug 2024 01:47:09 GMT
Trash

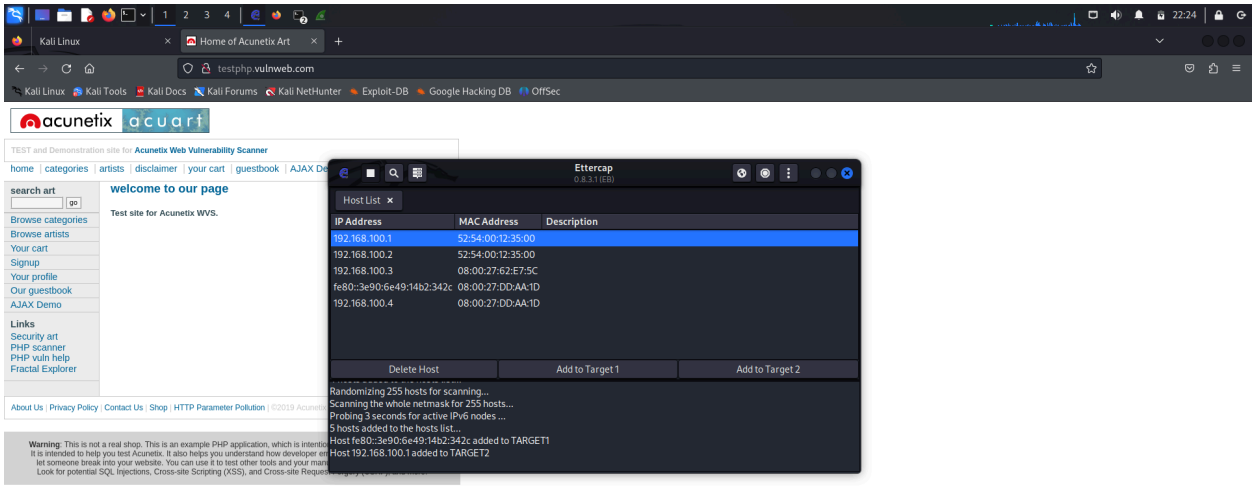


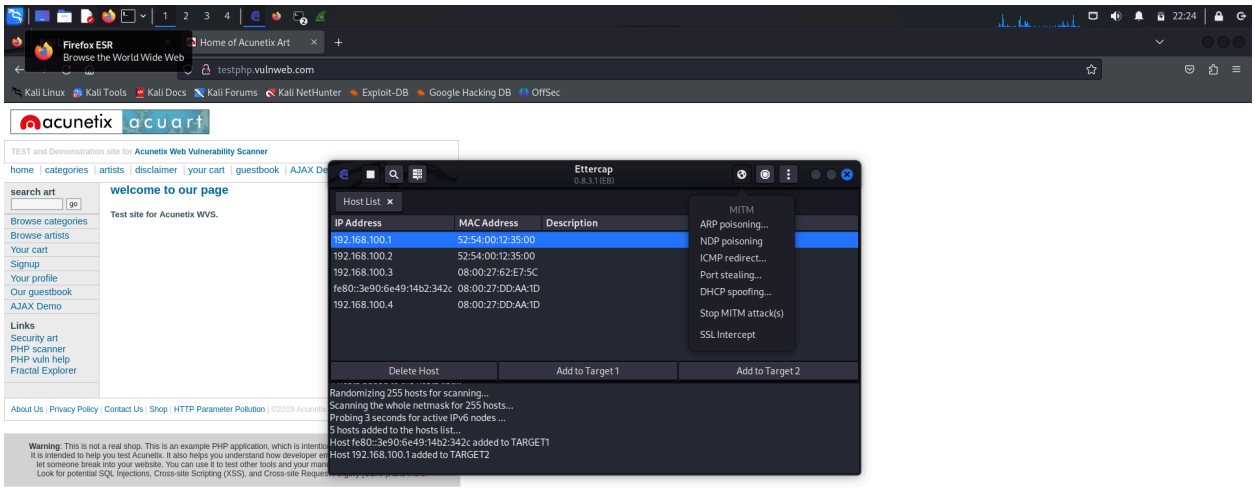


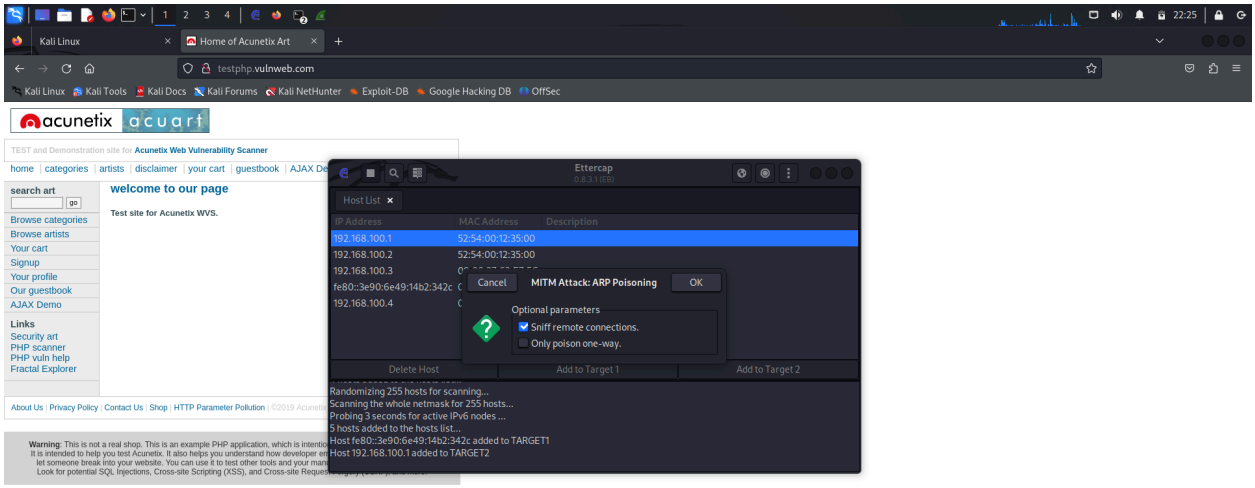
USING ETTERCAP

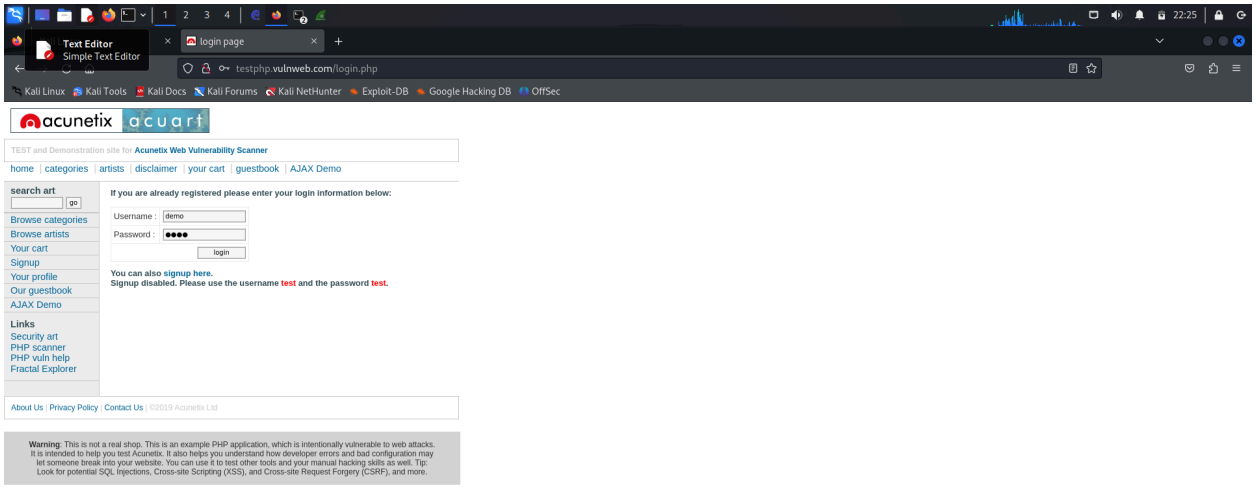

File Actions Edit View Help
(ramya㉿kali)-[~]
$ brupsuite
Command 'brupsuite' not found, did you mean:
command 'burpsuite' from deb burpsuite
Try: sudo apt install <deb name>
(ramya㉿kali)-[~]
$ sudo apt install brupsuite
[sudo] password for ramya:
Error: Unable to locate package brupsuite
(ramya㉿kali)-[~]
$ sudo ettercap
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Tea
Please select an User Interface
(ramya㉿kali)-[~]
$ sudo ettercap -G
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Tea
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.1 52:54:00:12:35:00
192.168.100.2 52:54:00:12:35:00
192.168.100.3 08:00:27:62:E7:5C
192.168.100.4 08:00:27:DD:AA:1D
Delete Host
Add to Target 1
Add to Target 2
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...

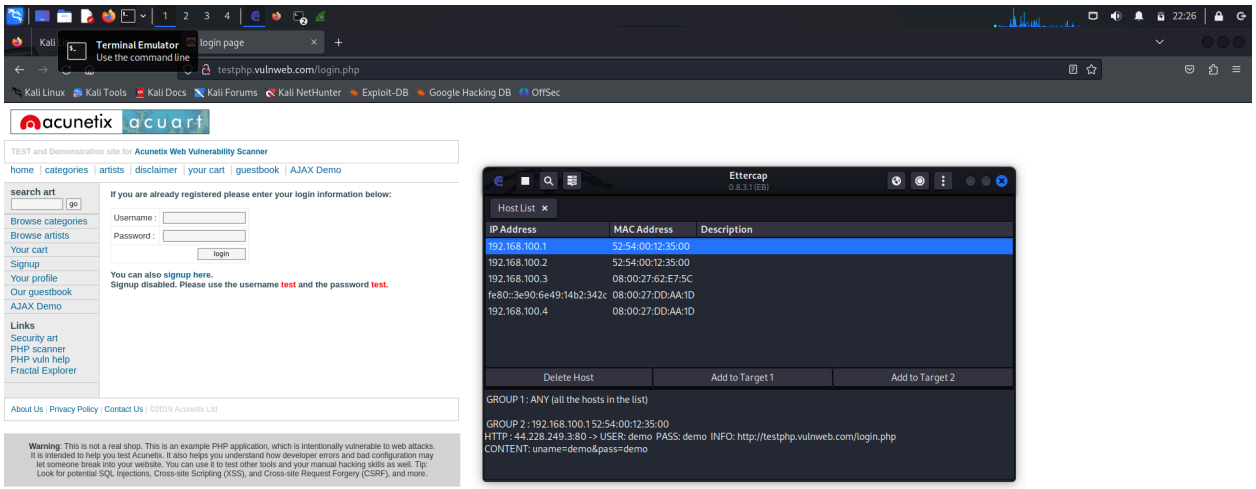

Kali Linux
Home
Ettercap
testphp.vulnweb.com
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
welcome to our page
Test site for Acunetix WVS.
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.
It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may
let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip:
Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.


Kali Linux
Home of Acunetix Art
testphp.vulnweb.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX De
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
welcome to our page
Test site for Acunetix WVS.
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution
Warning: This is not a real shop. This is an example PHP application, which is intentio
It is intended to help you test Acunetix. It also helps you understand how developer er
let someone break into your website. You can use it to test other tools and your mant
Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Reques
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.1 52:54:00:12:35:00
192.168.100.2 52:54:00:12:35:00
192.168.100.3 08:00:27:62:E7:5C
fe80::3e90:6e49:14b2:342c 08:00:27:DD:AA:1D
192.168.100.4 08:00:27:DD:AA:1D
Delete Host
Add to Target 1
Add to Target 2
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
Probing 3 seconds for active IPv6 nodes ...
5 hosts added to the hosts list...
Host fe80::3e90:6e49:14b2:342c added to TARGET1
Host 192.168.100.1 added to TARGET2


Firefox ESR
Browse the World Wide Web
Home of Acunetix Art
testphp.vulnweb.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX De
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
welcome to our page
Test site for Acunetix WVS.
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution
Warning: This is not a real shop. This is an example PHP application, which is intentio
It is intended to help you test Acunetix. It also helps you understand how developer er
let someone break into your website. You can use it to test other tools and your mant
Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Reques
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.1 52:54:00:12:35:00
192.168.100.2 52:54:00:12:35:00
192.168.100.3 08:00:27:62:E7:5C
fe80::3e90:6e49:14b2:342c 08:00:27:DD:AA:1D
192.168.100.4 08:00:27:DD:AA:1D
MITM
ARP poisoning...
NDP poisoning
ICMP redirect...
Port stealing...
DHCP spoofing...
Stop MITM attack(s)
SSL Intercept
Delete Host
Add to Target 1
Add to Target 2
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
Probing 3 seconds for active IPv6 nodes ...
5 hosts added to the hosts list...
Host fe80::3e90:6e49:14b2:342c added to TARGET1
Host 192.168.100.1 added to TARGET2


Kali Linux
Home of Acunetix Art
testphp.vulnweb.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX De
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
welcome to our page
Test site for Acunetix WVS.
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution
Warning: This is not a real shop. This is an example PHP application, which is intentio
It is intended to help you test Acunetix. It also helps you understand how developer er
let someone break into your website. You can use it to test other tools and your mani
Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Reques
Ettercap
Host List
IP Address
MAC Address
Description
192.168.100.1 52:54:00:12:35:00
192.168.100.2 52:54:00:12:35:00
192.168.100.3
fe80::3e90:6e49:14b2:342c
192.168.100.4
Cancel
MITM Attack: ARP Poisoning
OK
Optional parameters
Sniff remote connections.
Only poison one-way.
Delete Host
Add to Target 1
Add to Target 2
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
Probing 3 seconds for active IPv6 nodes ...
5 hosts added to the hosts list...
Host fe80::3e90:6e49:14b2:342c added to TARGET1
Host 192.168.100.1 added to TARGET2


Text Editor
Simple Text Editor
login page
testphp.vulnweb.com/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username : demo
Password : ••••
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.


Terminal Emulator
Use the command line
login page
testphp.vulnweb.com/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username :
Password :
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.1 52:54:00:12:35:00
192.168.100.2 52:54:00:12:35:00
192.168.100.3 08:00:27:62:E7:5C
fe80::3e90:6e49:14b2:342c 08:00:27:DD:AA:1D
192.168.100.4 08:00:27:DD:AA:1D
Delete Host
Add to Target 1
Add to Target 2
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : 192.168.100.1 52:54:00:12:35:00
HTTP : 44.228.249.3:80 -> USER: demo PASS: demo INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=demo&pass=demo