CHAPTER 1

INTRODUCTION

1.1 GENERAL

Nowadays, users are more focused on web applications for doing their day to day activities such as Bank, Insurance, and Education etc. Web applications are prevalent because of the presence of web programs and the accommodation of utilizing a web program as a customer. Current web applications are becoming more important in corporate, public and Government services today. The rapid growth in web application deployment has created more complex, distributed IT infrastructures that is harder to secure.

Although web applications can provide convenience and efficiency, there are also a number of new security threats. These threats originate from non-trusted client access points, session-less protocols, the general complexity of web technologies and network-layer insecurity. With web applications, client software usually cannot always be controlled by the application owner. Therefore, input from a client running the software cannot be completely trusted and processed directly.

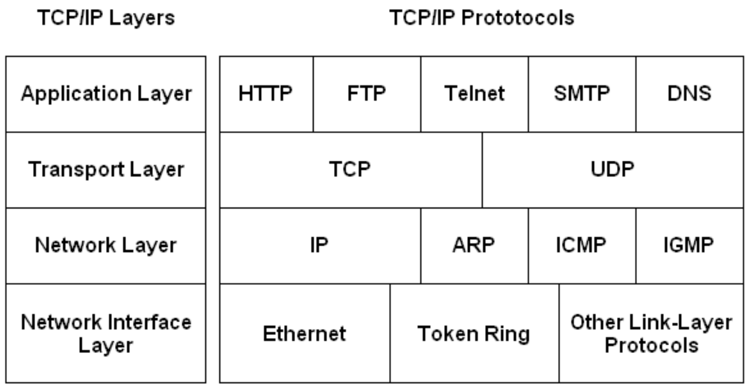
Hypertext Transport Protocol (HTTP) is a session-less protocol and is susceptible to replay and injection attacks. HTTP messages can easily be modified, spoofed and sniffed. Organizations must understand and be fully aware of the threats to properly implement appropriate defensive strategies. Additional security controls, both technical and administrative may be required to reinforce the protection of vital infrastructure in response to the deployment of web applications. These threats will cause significant risks to Organizational Security. However, traditional network security measures and technologies may not be sufficient to safeguard web applications from new threats since attacks are now specifically targeting security flaws in the design of web applications. For more than a decade, organizations have been dependent upon security measures at the network such as firewalls. However more attacks are targeting security flaws in the design of web applications such as injection flaws, buffer overflow and weak session ID

New security measures, both technical and administrative, need to be implemented alongside the development of web applications. In order to tackle the threats related to these new application services, it is essential to understand the vulnerabilities commonly found in web applications. Basic web applications incorporate webmail, online retail deals, online barters, wikis and numerous different domains. The components of the network are as follows

(i) Routers
(ii) Switches
(iii) Antennas
(iv) Transceivers
(v) Power Amplifier

1.2 ARCHITECTURE OF TCP / IP MODEL

Architecture of TCP / IP model defines the layers and the corresponding protocols in the layers to work across the networks.



TCP/IP Layers	TCP/IP Prototocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP	UDP			
Network Layer	IP	ARP	ICMP	IGMP	
Network Interface Layer	Ethernet	Token Ring	Other Link-Layer Protocols		

Fig.1.1 TCP / IP model

1.3 LAYERS OF TCP / IP MODEL

TCP / IP model has five layers. They are as follows,

(i) Physical layer
(ii) Data link layer
(iii) Network layer
(iv) Transport layer
(v) Application layer

1.3.1 PHYSICAL LAYER

Physical layer is used to establish the physical connection with the network devices. The functions of the physical layer are as follows,

(i) Encoding
(ii) Signaling
(iii) Transmission of data
(iv) Reception of data
(v) Specification of Hardware’s
(vi) Design of physical network

1.3.2 DATALINK LAYER

Data link layer is divided into Logical Link Control (LLC) and Media Access Control (MAC). The functions of data link layer are as follows,

(i) Logical Link Control
(ii) Media Access Control
(iii) Framing the data
(iv) Addressing
(v) Handling of errors
(vi) Detection of errors

1.3.3 NETWORK LAYER

The functions of network layer are as follows,

(i) Logical addressing

(ii) Route discovery

(iii) Encapsulation of datagram

(iv) Data fragmentation

(v) Reassembly

1.3.4 TRANSPORT LAYER

The functions of network layer are as follows,

(i) Transmission of data

(ii) Connection oriented service

(iii) Connection less service

1.3.5 APPLICATION LAYER

The functions of network layer are as follows,

(iv) Various application service

(v) File Transfer

(vi) Remote login to hosts

(vii) Electronic Mail Transfer

1.4 VULNERABILITIES OF WEB APPLICATION

Web applications are strongly vulnerable to a variety of attacks because of its weak security. Among the layers of TCP/IP architecture, most of the hackers target the application layer to launch their attacks. Positive Technologies (www.ptsecurity.com) is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients across 30 countries consists of world's most advanced specialist researchers, renowned security experts and highly skilled programmers. Table 1.1 shows the percentage of web application vulnerabilities as per the report of Positive Technologies, Massachusetts, U.S.A.

Table.1.1 Web application Vulnerabilities

No	Web application vulnerability	Percentage
1	Session hijack Attacks	70 %
2	Content Tampering	6 %
3	SQL Injection Attack	5 %
4	Predictable Resource Locator	5 %
5	Information Leakage	4 %
6	HTTP response splitting	5 %
7	Others	5 %

The following Table.1.2 shows the percentage of web application vulnerabilities as per the report of Positive Technologies, Massachusetts, U.S.A. The Table.1.2 shows that asp, aspx and jsp web pages have the highest number of vulnerabilities.

Table.1.2 Vulnerabilities based on web page URL

No	URL extension	Percentage of web pages	Percentage of vulnerabilities
1	Asp	27 %	26 %
2	Aspx	22 %	10 %
3	Jsp	8 %	7 %
4	Php	5 %	2 %
5	Html	4 %	2 %
6	Dll	4 %	3 %
7	Cfm	3 %	3 %
8	Xml	7 %	3 %
9	Do	7 %	4 %
10	Old	4 %	2 %
11	Unknown	9 %	38 %

The number of attacks presented in the NExTWORK CONFERENCE, New York, June 2011 by the survey conducted by Ponemon Research Institute and Juniper Networks on 583 American companies it was found that almost 90% of the US company web sites are hacked in anyway. The survey results are given in Table.1.3

Table.1.3 Number of Attacks on US Companies

No of attacks	Percentage
NIL attacks	10 %
1 attack	21%
2-3 attacks	32%
4-5 attacks	18%
More than 5 attacks	9%
Do not know	10%

1.5 OWASP TOP 10 VULNERABILITIES

Open Web Application Security Project (OWASP) is the nonprofit organization developed for analyzing the security of web applications. Every year, OWASP will release the Top 10 vulnerabilities. OWASP Top 10 vulnerabilities for the year 2013 is listed in the Table.1.4

Table.1.4 OWASP Top 10 vulnerabilities

Sl.No	Name of the Attack
1	SQL Injection attack
2	Session Hijack attack
3	Cross Site Scripting attack
4	Insecure Object References
5	Misconfiguration of Security
6	Data exposure
7	Missing of functions
8	Cross Site Request Forgery
9	Known vulnerabilities
10	Invalidated redirect

1.6 NETWORK ATTACK GROUPS

All the attacks executed in the networks are classified in to four network attack groups. They are as follows

(i) Denial of Service (DoS)
(ii) User to Root attacks (U2R)
(iii) Remote to Local (R2L)
(iv) Probe attacks

1.6.1 GENERIC FEATURE SET

Massachusetts Institute of Technology (MIT) Lincoln Lab, USA has conducted the "1998 DARPA Intrusion Detection Evaluation Program". The generic features set uses the original data set managed with DARPA Intrusion Detection Program. Generic Feature Set contains totally 31 features. The generic feature set is grouped into three types such as
i) Basic features of TCP connections
ii) Content features within a connection
iii) Computed traffic features

1.6.2 INDIVIDUAL FEATURE SET FOR EACH ATTACK GROUP

The four network attack groups such as DoS, U2R, R2L and Probe attacks are executed in different ways. So it is necessary to fix the individual feature set for each network attack group. So features are selected for each layer based on the attacks executed in each layer.

1.6.3 INDIVIDUAL FEATURE SET FOR PROBE ATTACKS:

Probe attack is an attempt to gain the access to the system. So the following features are selected for probe attacks.

(i) duration

(ii) protocol_type

(iii) src_bytes

(iv) service

Example of Probe attacks : Session Hijack attacks

1.6.4 INDIVIDUAL FEATURE SET FOR DOS ATTACKS

A denial-of-service attack (DoS attack) is an attempt to make a computer or network resource unavailable to its intended users. So the following traffic features are selected for DoS attacks.

(i) duration

(ii) protocol_type

(iii) src_bytes

(iv) count

(v) dst_host_same_servicerate

(vi) dst_host_serror_rate

(vii) dst_host_srv_serror_rate

(vii) dst_host_reerror_rate

Example of DoS attacks: pod, smurf attacks

1.6.5 INDIVIDUAL FEATURE SET FOR R2L ATTACKS

Remote to Local (R2L) attacks are unauthorized access from a remote machine. As R2L attacks deal with network level and host level, features related to both network and host levels are considered for R2L attacks.

(i) duration

(ii) protocol_type

(iii)src_bytes
(iv)num_failed_logins
(v) num_compromised
(vi)num_file_creations
(vii) num_shells
(viii) num_access_file
(ix) is_host_login
(x) is_guest_login

Example R2L attacks : password, imap, phf, spy attacks

1.6.6 INDIVIDUAL FEATURE SET FOR U2R ATTACKS

User to Root (U2R) attacks are unauthorized access to local root privileges. As U2R attacks involve with the content of the connection, content features within connection are considered for U2R attacks.

(i) num_compromised
(ii) root_shell
(iii) num_root
(iv) num_file_creations
(v) num_access_files
(vi) is_host_login

Example U2R attacks: buffer overflow and root kit attacks

1.7 SESSION HIJACK ATTACK

Web applications are widely used in the areas of education, Information Technology and communication, entertainment and commercial applications. At the same time, web applications are weakly secured against variety of attacks such as Denial of Service, brute force attack and session Hijack attacks

Most of the web applications involves in creating the session with the client. HTTP is the default protocol responsible for establishing the session in the application layer. The web session is the data transfer and communication between the client and web server for the specific time period. All the web applications initiate the session with the user and web server. Session hijack attack is easy to launch and it is difficult to detect. Session hijack attack is the most severe attack in web applications. HTTP is the default protocol in the application layer.

In session hijack, the hacker or attacker sniffs the network traffic and takes over the active session between the client and server by means of cracking the session ID. Takeover of a web session from the client by the attacker is called as session hijack attacks. Session hijack attacks in web applications can occur in three types of modes. The three types of modes are as follows,

(i) Active mode
(ii) Passive mode
(iii) Hybrid mode

In case of Active mode, the hacker disconnects the client and takes over the session. In Passive mode, the hacker simply sits back and observes the network traffic between the client and server. In passive mode, client will not be disconnected. Hybrid mode is the combination of active and passive modes of session hijack attacks.

Server side web sessions cannot handle the congestion perfectly. In client side web sessions, session cookies are used to maintain the state of the web applications. A Session Identifier is a unique ID assigned by the web server to each web session when a session is established between client and server. HTTP is a stateless protocol. Each and every request is independent. HTTP does not monitor the requests. Session attributes are used to maintain the state of the web applications. The difference between the active, passive and hybrid modes of session hijacking attacks are tabulated in Table.1.5

Table.1.5 Session Hijack Modes

ACTIVE	PASSIVE	HYBRID
The non legitimate user identifies the active session between legitimate client and server and then takes over the session and also pretend to be legitimate client thereby communication occurs.	The non legitimate user identifies the session but just watch the traffic flow between legitimate client and server.	Combination of active and passive attack.
Session replaced by non legitimate client.	Session monitored by non legitimate client.	The non legitimate user keeps listening to active session and then takes over the session when needed.
The attacker uses client side scripting tool. The attacker tears down the connection between legitimate users sequence number need to be predicted before tearing down connection.	Sniffers are used by attacker to gather the details of legitimate client to logon later as legitimate client.	

1.7.1 TYPES OF COOOKIES

Cookies are used to store the session IDs. There are several types of cookies available to maintain the state of the web applications that are listed in Table.1.6

Table.1.6 Types of Cookies

S.No	Cookie	Functionality & Behavior
1	Session Cookie	Session cookies gets deleted from the browser when the user closes the browser
2	Persistent Cookie	The persistent cookies get deleted after the time period is expired.
3	Secure Cookie	Cookies are encrypted when it was transmitted
4	HTTP only Cookie	Cookie will be used only for http or https protocol
5	Third party Cookies	Third party cookies are set by multiple domain names
6	Super Cookie	To track the technology that is not rely on HTTP cookies
7	Zombie Cookie	The cookie automatically recreated

Based on the survey conducted by SANS Security Institute in December 2012 on 50 web applications that belongs to national and international companies, the percentage of web application vulnerabilities are analyzed and listed in Table.1.7

Table.1.7 Percentage of Web Application Vulnerabilities

S.No	Vulnerabilities	Percentage
1	SQL Injection	30%
2	Session Hijacking	28%
3	Cross Site Scripting	18%
4	Distributed DoS attack	8%
5	Phishing attack	8%
6	Cloning attack	4%
7	Others	4 %

There are several vulnerabilities that attack the current web application and they are listed in Table.1.8

Table.1.8 Session Vulnerabilities in Web Application

Sino	Vulnerability	Description
1	Session sniffing	Unauthorized way of viewing the session's data during data transmission
2	HTTP Packet sniffing	Sniffing the http packet of a web application session established between client and server
3	Session prediction	Predicting the session ID of a web session by using brute force attack
4	Session Fixing	Session ID is fixed by the attacker before the client establish the session with the server
5	Session Hijacking	Session ID is sniffed & Session is hijacked after the client established the session with the server

1.7.2 TYPES OF SESSION HIJACK ATTACKS

Session hijacking is the technique of hijacking the web application session between trusted client and the target server. The types of session hijacking are,

(i) Session Fixing attack
(ii) Session Hijacking attack
(iii)Cross Site Scripting attack

1.7.2.1 SESSION FIXING ATTACK

Session fixing attack can be done by installing proxy server. It's the primary type of Session hijacking. It is similar to man in the middle attack, where the attacker gets in the middle of the session and capture the information such as session ID, sequence number, IP address, port number…etc. The attacker convinces the server as legitimate client and it can alter, delete the information. The attacker often breaks the connection between the client and server.

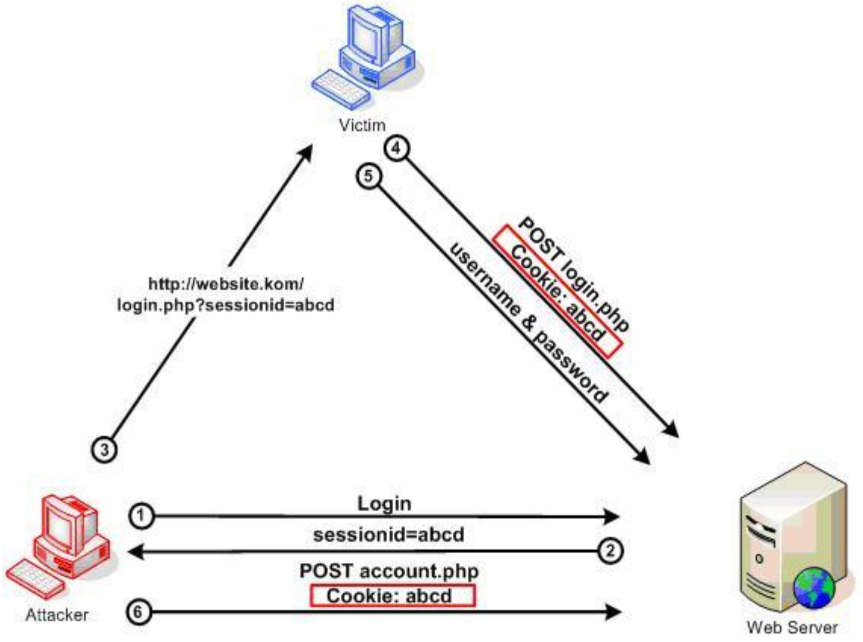


Fig.1.2 Session Fixing attack

1.7.2.2 SESSION HIJACKING ATTACK

Hacker captures the network traffic between the two users by sniffing over the network. The purpose is to capture the session cookie which consists session ID. Attacker disconnects the client (by sending Reset (RST) or Finished (FIN) packets) and take over the session. When an authenticated user login in with his username and password in a face book account. The face book server will provide a cookie for the authenticated user. The rest of the communication relies on the cookies for identifying the authenticated user. If the attacker steals the cookie then he will start accessing the session with that cookie.

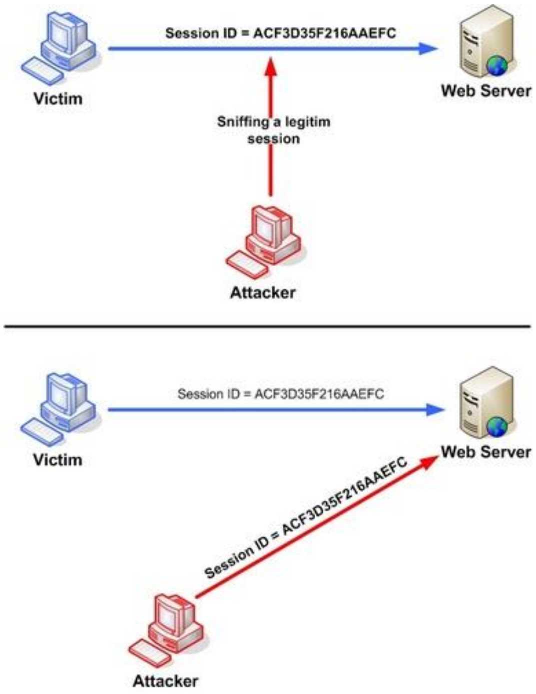

Session ID = ACF3D35F216AAEFC
Victim
Web Server
Sniffing a legitim session
Attacker
Session ID = ACF3D35F216AAEFC
Victim
Web Server
Session ID = ACF3D35F216AAEFC
Attacker

Fig.1.3 Session Hijacking attack

1.7.2.3 CROSS SITE SCRIPTING ATTACK

Today’s web applications act as an interface between client and server to perform client’s requirement over the internet. 2011 web application security report clearly states that most of the web applications are hacked against vulnerabilities.

The two important and most severe attacks are Structured Query Language (SQL) injection attacks where hackers modifies the SQL query and Cross Site Scripting attacks where hacker injects malicious java scripts into the web applications. The primary aim of Cross Site Scripting attack is to hijack the web applications or to modify the web page contents by stealing the session cookies. Three conditions for XSS attacks.

i) A web application accepts the user's input
ii) The input is used to create dynamic content
iii) The input is insufficiently validated

Attackers are able to inject client-side script (java script) into web applications.

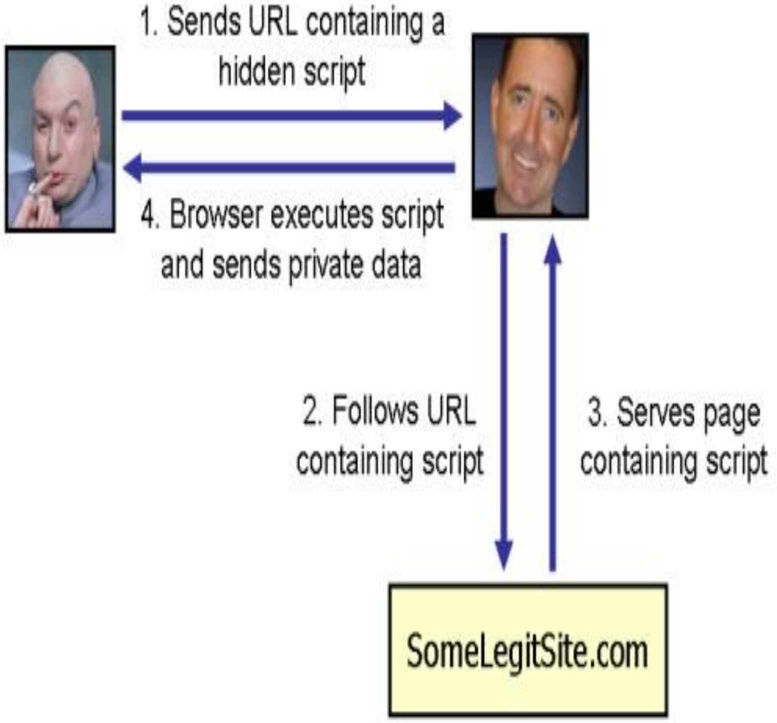

1. Sends URL containing a hidden script
4. Browser executes script and sends private data
2. Follows URL containing script
3. Serves page containing script
SomeLegitSite.com

Fig.1.4 Cross Site Scripting attack

The steps for executing the cross site scripting attack are as follows

(i) Attacker send the Uniform Resource Locator (URL) that contains the hidden script
(ii) User follows the URL containing the script
(iii)Web server serves the corresponding pages
(iv)User's browser executes the script and send the private data

The following Table.1.9 shows the suspected entities to launch the Cross Site Scripting (XSS attack).

Table.1.9 Cross Site Scripting attack Executors

S.No	XSS Executors	Specific entities/persons
1.	Attacker	i)Anonymous internet user ii)Malicious internet user
2.	Company's web server	i)Internal Ex: Employee self-service portal ii)External Ex: Commercial servers
3.	Client	i)Any type of customer ii)Anonymous user accessing the web server

1.7.2.4 BRUTE FORCE ATTACK

The non legitimate user use brute force technique and tries all possibilities of session id until the exact match is found. If the user clicks some link which open another site. The attacker finds the session ID in that URL.

1.8 LAYER WISE SESSION HIJACK ATTACKS

Session Hijack attack can be executed in the two layers of TCP/ IP model

(i) TCP Session Hijacking

(ii) HTTP Session Hijacking

1.8.1 TCP SESSION HIJACKING ATTACKS

Several methods are used to hijack the TCP session. They are as follows

(i) IP Spoofing
(ii) Blind hijacking
(iii) User Datagram Protocol (UDP) Hijacking

1.8.1.1 IP SPOOFING

Attacker uses the legitimate client's IP address to take over the TCP session. IP spoofing otherwise called IP address fraud, is a seizing the system in which the assailant takes on the appearance of a trusted host to disguise his personality, seize programs or get access to a system. Fig.1.5 shows the method of IP spoofing.

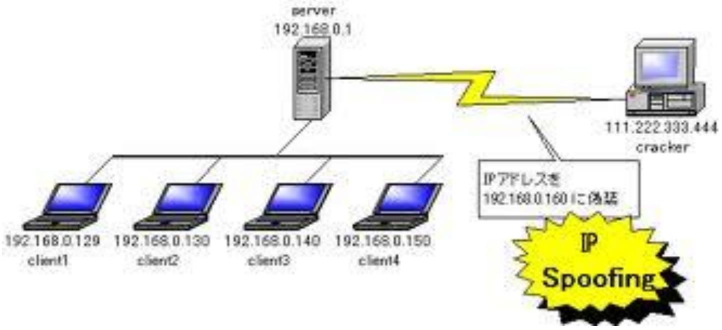


Fig.1.5   IP spoofing

1.8.1.2 BLIND HIJACKING

Attacker can inject the malicious command to the TCP traffic to modify the confidential data to the client. Since the attacker can't see the traffic content, it is called as blind hijacking attack.

1.8.1.3 UDP HIJACKING

Attacker takes over the UDP session is called as UDP session hijacking. It is simpler than TCP to seize UDP session. UDP request from the client to the server can be forged by the attacker to execute the UDP hijacking.

1.8.2 HTTP SESSION HIJACKING ATTACKS

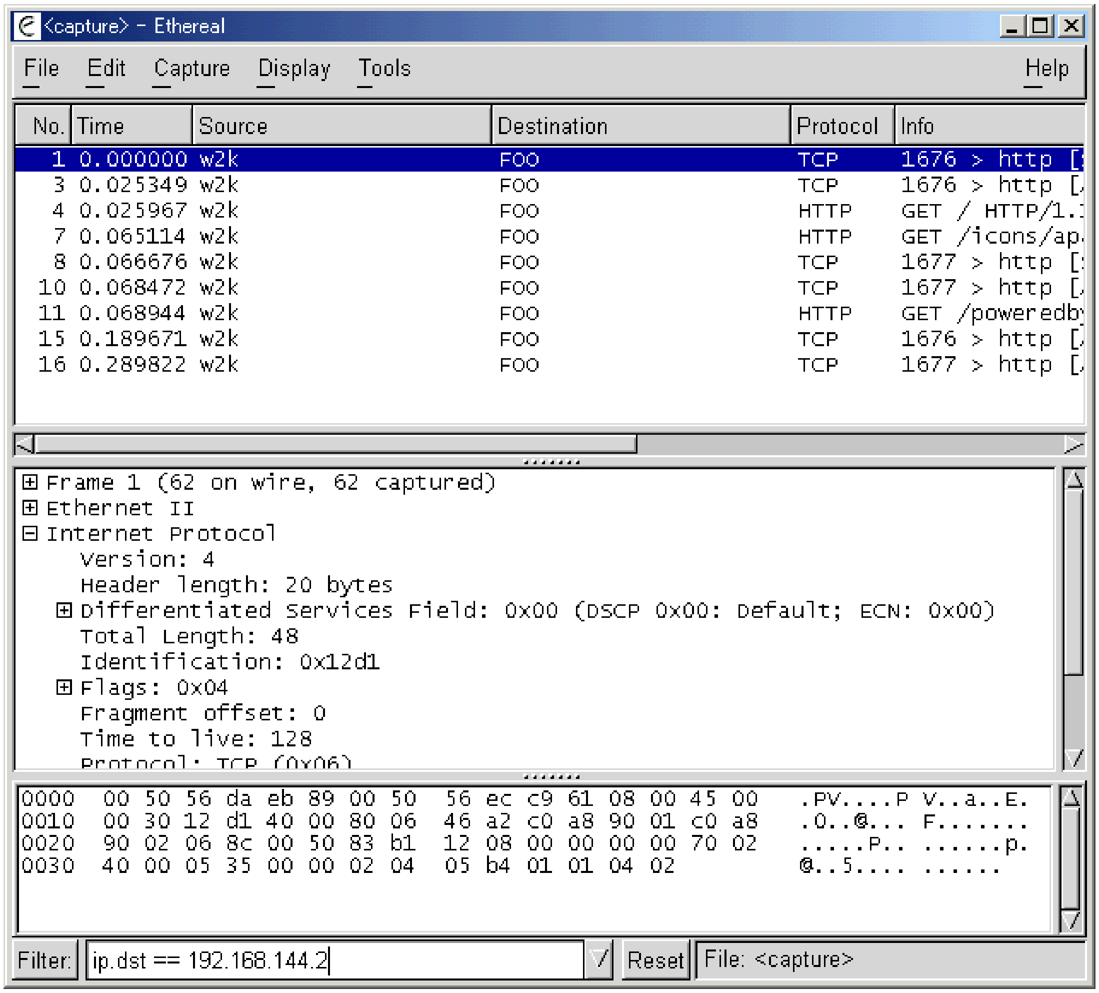
Attacker can use the following techniques to hijack the http web application session.

(i) Network Sniffing attack

(ii) Brute Force attack

1.8.2.1 NETWORK SNIFFING ATTACK

A sniffer is used to capture network packets. Attacker can use the sniffer tools such as Wireshark, Snort, etc to capture the network packets. Sniffers are able to read the data between the client and server. Wireshark is the popular tool that is used by the attackers to steal the cookies which contains the session ID to execute the HTTP session hijacking attack. The Fig.1.6 shows the packet capturing by Wireshark.



```
No. Time      Source  Destination  Protocol  Info
 1 0.000000  w2k     FOO          TCP       1676 > http [
 3 0.025349  w2k     FOO          TCP       1676 > http [
 4 0.025967  w2k     FOO          HTTP      GET / HTTP/1.
 7 0.065114  w2k     FOO          HTTP      GET /icons/ap
 8 0.066676  w2k     FOO          TCP       1677 > http [
10 0.068472  w2k     FOO          TCP       1677 > http [
11 0.068944  w2k     FOO          HTTP      GET /poweredb
15 0.189671  w2k     FOO          TCP       1676 > http [
16 0.289822  w2k     FOO          TCP       1677 > http [
```

```
⊞ Frame 1 (62 on wire, 62 captured)
⊞ Ethernet II
⊟ Internet Protocol
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 48
    Identification: 0x12d1
  ⊞ Flags: 0x04
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
```

```
0000  00 50 56 da eb 89 00 50  56 ec c9 61 08 00 45 00   .PV....P V..a..E.
0010  00 30 12 d1 40 00 80 06  46 a2 c0 a8 90 01 c0 a8   .0..@... F.......
0020  90 02 06 8c 00 50 83 b1  12 08 00 00 00 00 70 02   .....P.. ......p.
0030  40 00 05 35 00 00 02 04  05 b4 01 01 04 02         @..5.... ......
```

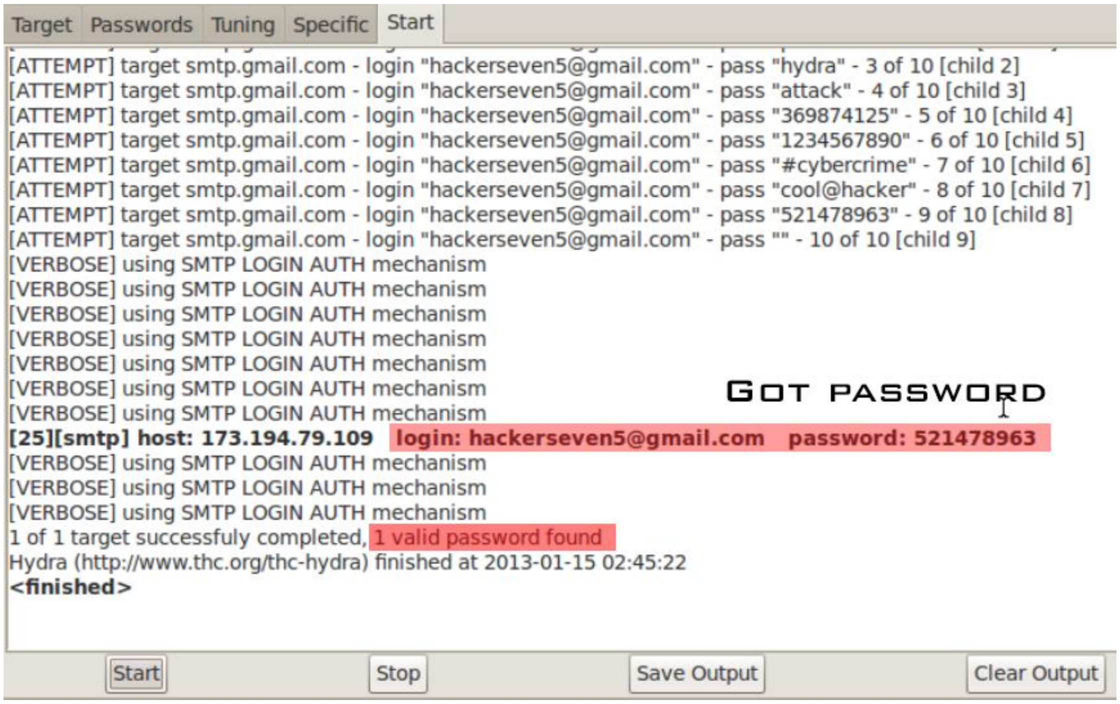
Filter: ip.dst == 192.168.144.2 Reset File: <capture>

Fig.1.6 Packet Sniffing

1.8.2.2 BRUTE FORCE ATTACK

Brute force attack is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys through exhaustive effort (using brute force) rather than using intellectual strategies. The attacker might crack the login credentials by trying many possible combinations. The brute force attack application proceeds through all possible combinations of legal characters in sequence.

Brute force is considered to be an infallible and time-consuming approach. Attacker tries various possibilities of password or session ID using the combinations of permutation and combinations. When key guessing, the key length used in the cipher determines the practical feasibility of performing a brute-force attack. A cipher with a key length of N bits can be broken in a worst-case time proportional to 2N and an average time of half that. Brute-force attacks are the application of brute-force search which is used to crack the session ID of the web applications.



```
[ATTEMPT] target smtp.gmail.com - login "hackerseven5@gmail.com" - pass "hydra" - 3 of 10 [child 2]
[ATTEMPT] target smtp.gmail.com - login "hackerseven5@gmail.com" - pass "attack" - 4 of 10 [child 3]
[ATTEMPT] target smtp.gmail.com - login "hackerseven5@gmail.com" - pass "369874125" - 5 of 10 [child 4]
[ATTEMPT] target smtp.gmail.com - login "hackerseven5@gmail.com" - pass "1234567890" - 6 of 10 [child 5]
[ATTEMPT] target smtp.gmail.com - login "hackerseven5@gmail.com" - pass "#cybercrime" - 7 of 10 [child 6]
[ATTEMPT] target smtp.gmail.com - login "hackerseven5@gmail.com" - pass "cool@hacker" - 8 of 10 [child 7]
[ATTEMPT] target smtp.gmail.com - login "hackerseven5@gmail.com" - pass "521478963" - 9 of 10 [child 8]
[ATTEMPT] target smtp.gmail.com - login "hackerseven5@gmail.com" - pass "" - 10 of 10 [child 9]
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[25][smtp] host: 173.194.79.109   login: hackerseven5@gmail.com   password: 521478963
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-01-15 02:45:22
<finished>
```

Fig.1.7 Brute Force attack

1.9 RESEARCH OBJECTIVES

The primary objective of this thesis is to prevent the Session Hijack attack in web applications. The main objectives of this thesis are listed below.

(i) To design the prevention model to prevent the session hijack attacks using Message Authentication Code (MAC) appended session ID.

(ii) To develop the architecture of encrypted session ID to prevent the session Hijack attacks.

(iii) To design the prevention model for healthcare web applications against session hijack attacks.

(iv) To develop the four tier validation system to prevent the session hijack attacks by defending the cross site scripting attacks.

1.10 SCOPE OF THE THESIS

In count to this introductory chapter, the dissertation is organized as follows.

Chapter 2 presents a complete literature survey about prevention mechanisms for session hijack attacks.

Chapter 3 presents a prevention model to prevent the session hijack attacks using MAC appended Session ID.

Chapter 4 presents the prevention model to prevent the session hijack attacks using encrypted Session ID.

Chapter 5 describes the prevention model to prevent the session hijack attacks in healthcare web applications using distributed Session ID.

Chapter 6 explains about the four tier validation system to prevent the session hijack attacks by defending the cross site scripting attacks.