RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -17

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

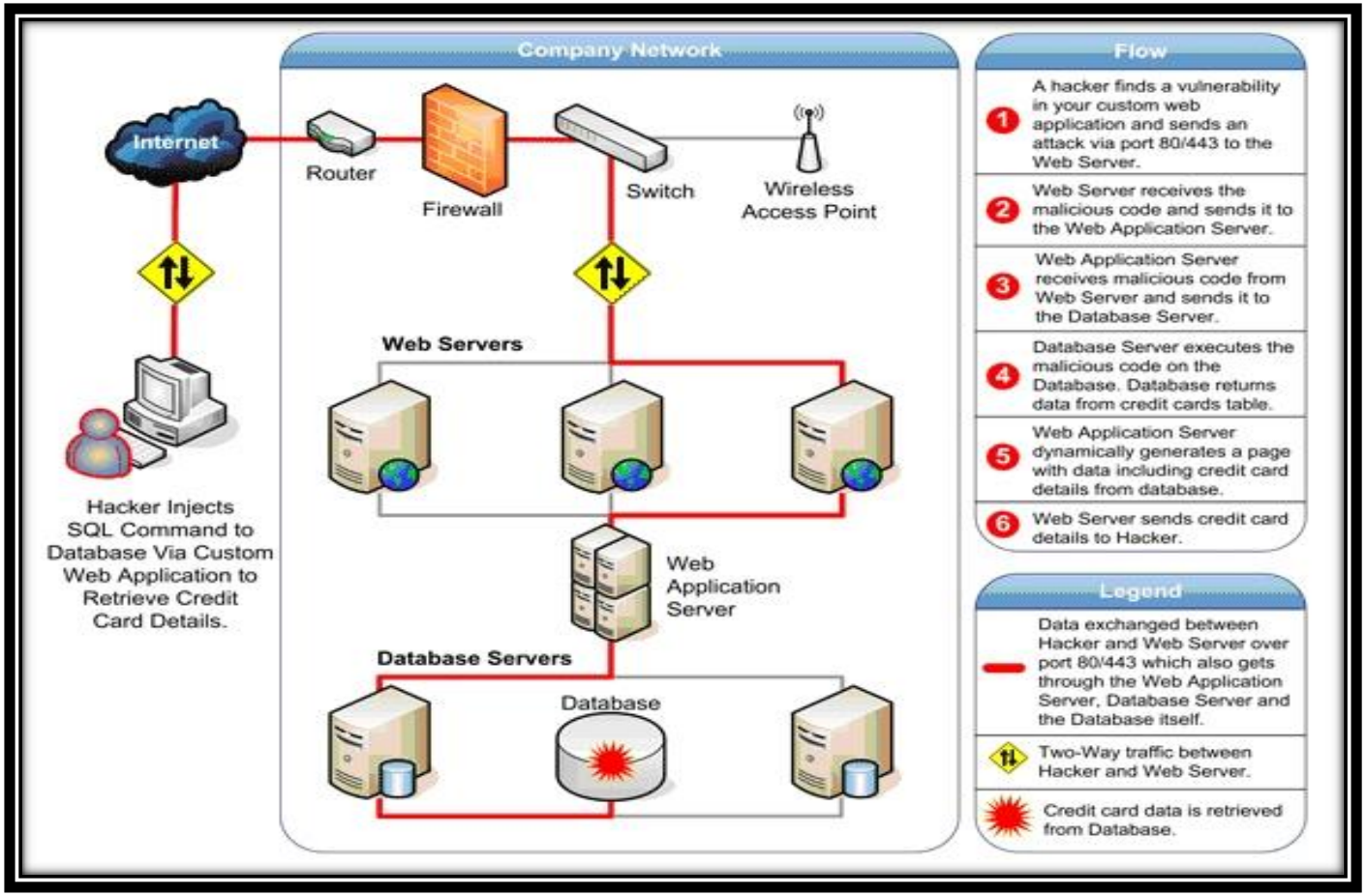
- Web Application Attack
- URL Interpretation attacks
- MCQ
- References

Web Application Attack

- Let us now look at types of attacks on web applications. Despite their advantages, web applications do raise a number of security concerns stemming from improper coding. Serious weaknesses or vulnerabilities allow criminals to gain direct and public access to databases in order to churn sensitive data – this is known as a web application attack. Many of these databases contain valuable information (e.g. personal data and financial details) making them a frequent target of attacks. Although such acts of vandalism (often performed by the so-called script kiddies) as defacing corporate websites are still commonplace, nowadays attackers prefer gaining access to the sensitive data residing on the database server because of the immense pay-offs in selling the results of data breaches. In the framework described above, it is easy to see how a criminal can quickly access the data residing on the database through a dose of creativity and, with luck, negligence or human error, leading to vulnerabilities in the web applications.

WEB APPLICATION ATTACK

Web Application Attack



URL Interpretation attacks

- The web server fails to parse the URL properly.
- e.g. the Unicode / Superfluous decode attack.
- Mismatched resource mappings in the configuration.
- e.g. +.htr, .JSP, Java remote command execution, etc.

The URL (Uniform Resource Locator) of a web application is the vector that makes it possible to indicate the requested resource. It is a string of printable ASCII characters that is divided into five parts:

Countermeasures:

- Usually require a vendor supplied fix.
- Thorough inspection of the web server configuration and bindings.

URL Interpretation attacks

1. **The name of the protocol:**

This is in some sorts the language used to communicate on the network. The most widely used protocol is the HTTP protocol (Hypertext Transfer Protocol), which makes it possible to exchange web pages in HTML format. A variety of other protocols may also be used (FTP, News, Mailto, etc.)

2. **ID and password:**

makes it possible to specify the parameters required to access a secure server. This option is not recommended since the password circulates unscrambled in the URL

3. **The name of the server:**

This is the domain name of the computer hosting the requested resource. Note that it is possible to use the server's IP address

URL Interpretation attacks

4. The port number:

This is a number associated with a service that tells the server what type of resource is being requested. The port that is associated with the protocol by default is port number 80. When the server's web service is associated with port number 80, specification of the port number is optional.

5. The access path to the resource:

This last part tells the server where the resource is located, that is, in general, the location (directory) and the requested file name.

- **A URL has the following structure:**

Protocol	Password (optional)	Server name	Port (optional if 80)	Path
http://	user:password@	www.commentcamarche.net	:80	/glossair/glossair.php3

MCQ

6. A firewall protects which of the following attacks?
   a) Phishing
   b) Dumpster diving
   c) Denial of Service (DoS)
   d) Shoulder surfing

7. There are _____ types of firewall.
   a) 5
   b) 4
   c) 3
   d) 2

8. Packet filtering firewalls are deployed on _____
   a) routers
   b) switches
   c) hubs
   d) repeaters

9. In the _____ layer of OSI model, packet filtering firewalls are implemented.
   a) Application layer
   b) Session layer
   c) Presentation layer
   d) Network layer

10. The _____ defines the packet filtering firewall rules.
   a) Access Control List
   b) Protocols
   c) Policies
   d) Ports

REFERENCES

- https://ccm.net/contents/31-url-manipulation-attacks