DAY 5 : Web Security Owasp

—Map Web Architecture :

Serverless :

In some cases, the use of serverless code may be indicated by the presence of specific HTTP headers .For ex, AWS lambda functions return the following headers :

```
X-Amz-Invocation-Type

X-Amz-Log-Type

X-Amz-Client-Context
```

Static Storage :

Many applications store static content on dedicated storage platforms, rather than hosting it directly on the main web server.The two most comman storage platforms are Azure S3 Buckets and Azure Storage accounts and it can easily identified by domain names:

- BUCKET.s3.amazonaws.com or s3.REGION.amazonaws.com/BUCKET for Amazon S3 Buckets
- ACCOUNT.blob.core.windows.net for Azure Storage Accounts

Database :

Most of web application use some kind of database to store dynamic contents. Way to determine database :

1)Port scanning where open port are related to database

2)Triggering SQL and NoSQL error messages

Some applications uses database as :

1)Windows, IIS and ASP.NET use Microsoft SQL server

2)Embedded system use SQLite

3)PHP used MySQL and PostgreSQL

4)APEX uses Oracle

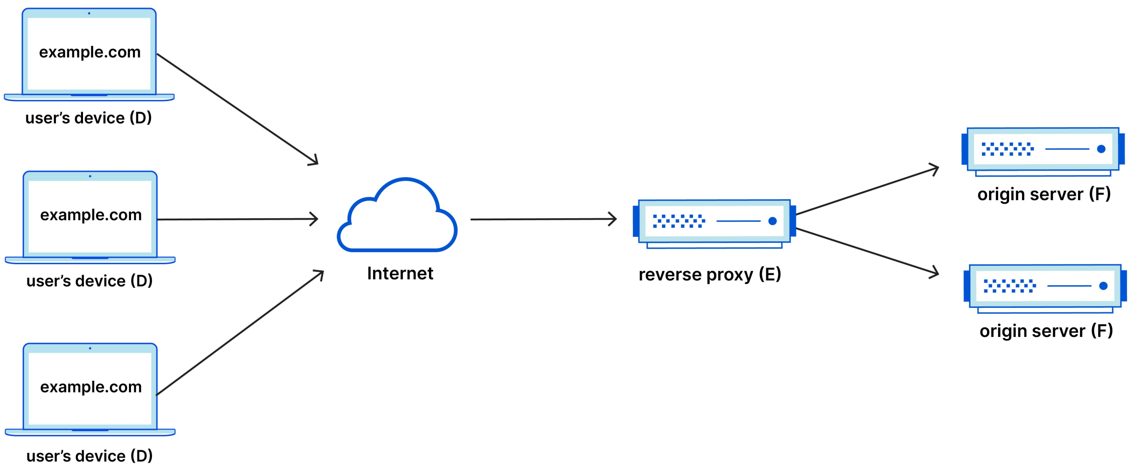
Network Components :

Network components in web architecture :

User — CDN — Load balancer — Reverse proxy — Application server — Database

1)Reverse Proxy :

Reverse proxies sits in front of application server and forward the client requests to it.



Reverse Proxy Flow

How To Detect :

Check HTTP headers :

Server: nginx

Via:

X-Forwarded-For:

X-Real-Ip:

Reverse Proxy can introduce :

—Header Injection issues

—IP spoofing via X-Forwarded-For

—Misconfigured Routing

—Access control bypass

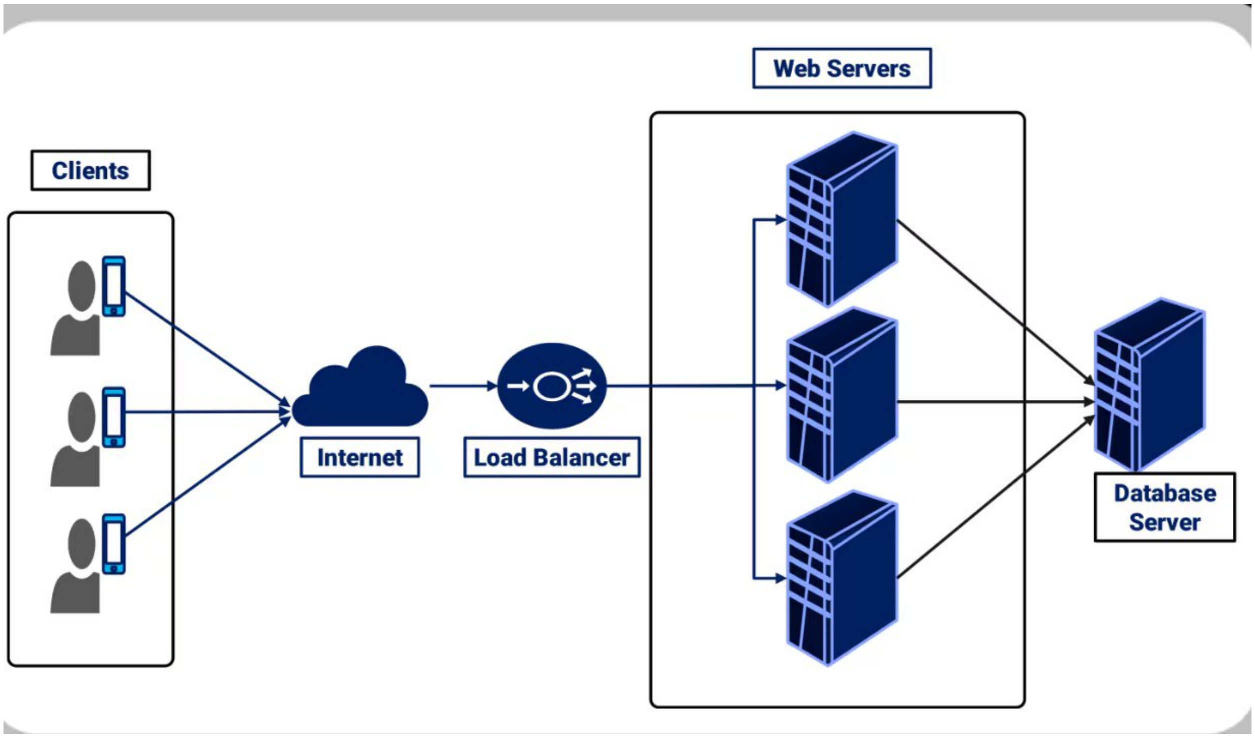
—Hidden internal endpoints

Ex: If proxy trusts : X-Forwarded-For: 127.0.0.1

You might bypass IP-based restrictions

2)load balancer :

Load balancers distributed traffic across multiple backend servers.It is used for high-availability, Scalability and fault-tolerance.



Comman load balancer :

- AWS ELB / ALB
- HAProxy
- Nginx
- F5
- Cloud-based providers

How to detect :

- Different responses on repeated requests
- Session inconsistency
- Changing Set-Cookie
- IP address resolves to cloud provider
- Headers like:

  X-Forwarded-For , X-Amzn-Trace-Id

Load balancer may introduce :

- Session handling issues
- Sticky session misconfigurations
- Race conditions
- WAF bypass opportunities
- Different security configs on backend nodes

Ex : server A patched and server B vulnerable then load balancer route traffic — inconsistent behaviour — possible exploit

3)Content Delivery network :

CDN caches content and serves it from geographically distributed edge servers and improves speed, availability and Ddos protection.

Common CDNs :

- Cloudflare
- Akamai
- Fastly
- Cloudfront

How To Detect :

CF-Ray:
CF-Cache-Status:
Server: cloudflare
X-Cache:
Via:

CDNs can:

- Hide real server IP
- Act as WAF

- Cache sensitive data
- Allow origin IP bypass

If you find backend IP ,you may bypass WAF, rate limiting and IP restrictions