status codes

-- 100-199 informational responses

-- 200-299 Successful respoinses

-- 300-399 Redirection messages

-- 400-499 Client responses

-- 500-599 Server error responses

curl --proxy localhost:8080 -x GET example.com -k -d 'testet'

types of Authentication:

common types of Authentication

- Password-based authentication
- Multi-factor authentication
- Application behaivour / side-channel analysis

common weaknesses

- Lack of brute-force protection
- logic flaws

Cenbtral Process

- Map the entire authentication attack surface
- Create multiple accounts
- check for lack of brute-force protection
- Is the application using a standard library/framework

- check for logic issues

- inspect tokens

==========

Brute-force Attack

Watch for changes in:

-- Status codes

-- Error messages

-- Content length

-- Response times

wordlists

Use wordlists to save us time

-- Assetnote

-- Seclists

-- Custom

==========

ffuf -request req.txt -request-proto https -mode clusterbomb -w /home/kali/usernames/.txt:FUZZUSER -w /home/kali/passwrods.txt:FUZZPASS -mc 302

==========

X-Real-Ip:1.2.3.6

X-Forwarded-For:1.2.3.6

X-originating-Ip:1.2.3.6

Client-Ip: 1.2.3.6

True-Client: 1.2.3.6

==========

Multi-factor Authentication

Things we might try:

--Forceful browsing

--Changing parameters & body content

--Brute-forcing codes

--Testing for predictability

--Testing backup codes

--Testing codes multiple times or against different accounts

--Triggering errors or erroneous behaviour

--Test other functionality like enrolment

==========

What is the Access Control?

--Also known as "Authorization"

--In a nutshell:it's what you're allowed to do

--Common finding in modern and complex application

--Different types of access controls exist;

horizonal,vertical and context-dependent.

==========

Typical Access Control Issues:

--Forceful browsing

--IDOR/BOLA/BFLA

--Trusting user input

==========

IDOR-Insecure Direct Object Refrence

Sometimes applications use user-ssupplied input to accesss objects directly.

--Often used to access information of other objects

--Many need to be combined with another weakness if the object ID is not easy to quess or brute-force

--can also inpact files and work in various other contexts

--Known as BOLA in APIs

==========

What is SSRF?

--SSRF occurs when a server-side application

--makes requests on our behalf for example, with an SSRF payload we can potentially make an external-facing that we have no direct access to.

==========

what is SQL Injection?

SQL injection allows us to manipulate queries that are made to a database and typically leads to:

--Exposure of sensitive data

--Data manipulation

--Denial of service

==========

Dynamic queries:

```
$query = "SELECT id,name,price FROM products";

$result = mysqli_query($connection,$query);
```

```
String query = "SELECT id,name,price FROM products";

Statement Assads = connection.creatStatement();

ResultSet Assads = statement.executeQuery(query);
```

```
const query = "SELECT id,name,price FROM products";

connection.query(query,(error,results,fields) => {
        if (error) throw error;
        //process results


});
```

==========

Parametrised queries/Prepared statements

```
$query = "SELECT id, name, price FROM products WHERE category=?";

$stmt = $pdo->prepare(query);
```

$stmt->execute([$category]);

String query = "SELECT id, name,price FROM products WHERE category=?";

PrepareStatement Assads = connection.prepareStatment(query);

prepareStatement.setString(1,category);

ResultSet Assads = prepareStatement.executeQuery();

---

const query = "SELECT id,name,price FROM products WHERE category=?";

connection.query(query,[category],(error,result,fields)=>{

    if (error) throw error;

});

==========

ORM(object relational mapping)

ORM is a programming technique that allows developers to manipulate database data as objects rather than dealing with SQl queries directly.

ORM act as a bridge between the object-oriented world of application code and the relational world of database,automating the tedious task of converting data between different systems.

=sqlmap www.example.com --dbs

=sqlmap www.example.com -D public --tables --batch

=sqlmap www.example.com -D public -T users --batch --dump

==========

Blind SQL Injection

The target application is vulberable to SQL injection however, the response does not contain the results of the query.

UNION attacks become ineffective as wwe rely on seeing the rsults.Instead, we can use conditional responses to extract information.

==========

Boolean-based Blind SQLi

'AND 1=1 -- -

'and 1=2 -- -

==========

Timebased Blind SQLi

SELECT SLEEP(10)

here , sleep(10) forces the database to wait for 10 seconds if the condition is true, if the response from the application is delayed by about 10 seconds, it indicates the injection worked.

Error-based Blind SQLi

' OR(SELCET CASE WHEN (ASCII(SUBSTRING((SELECT databse()),1,1) = 'a')) THEN CAST('' AS INT) ELSE 'a' END) -- '';

==========

what is File Inclusion?

Modular Design:

Modern applications are designed in a modular fashion for maintainability,scalability,and efficiency

Instead of a single , monoilithic script, appl;ications are broken down into multiple components or modules. This modular design involves seperating the code into different files based on functionality

==========

What is XXE injection?

When application use XML(Extensible Markup Language) to transfer data we can try yo use potentially dangerous features of the XML specification.These featues are supporeted by standard parsers even if they are not used by the application.

Using XXE we can potentially:

--View files on the target server

--SSRF(server-side request forgery)

--Exfiltrate sensetive information

==========

What XSS?

XSS allows us to execute code in the client/browser which can potentially lead to:

--Impresonate a user & carry out actionson their behalf

--Steal data(including user input)

==========

What is Mass Assignment?

Mass Assignment occurs when applications(often frameworks)automatically bind parameters to objects.

How do we identify these parameters?

--Fuzzing

--Code review

--JWWT tokens

--Leaky API endpoints

--Front-end code

==========

What are WebSockets?

--A protocol providing full-duplex

--commuunication channels over a single TCP connection.

--Enables interaction between a web browser

and a web server with lower overheads, facilitating real-time data transfer.

==========

What is an Open Redirect?

open redirect occur when an application accepts untrusted input that could cause a redirection to an external URL.

==========

What is a Race Condition?

Race condition occur whwen requests are processed concurrently.

can lead to multiple threads interacting with the same data at the same time causing a collision.

As attackers,we can use carefully timed requests to cause collisions and exploit the resulting behaviour.

==========

Multi-Endpoint Race Conditions

Testing Multiple endpoints

--Aseries of actions or requests that make up the application flow or businesslogic.

--For example: the checkout in an application, the time it takes to verify a payment,and the confirmation

--Could we add more times to the bacsket during this window between checkout and confirmation?

Methodology:

--Test the application functinality

--Think about the logic the application and the steps follows to carry a task

--Test your theory

==========

Shodan Switch:

#shodan init (APIKEY)

#shodan submit ipaddress

#shodan scan submit --filname scan-result.json.gz ipaddress

#sahodan stats ftp/bigip