A07: Identification and Authentication Failures

OWASP TOP 10 - Series

Presenter – Sanchay, Jalaj

@ null-meet, Airtel Centre, Gurgaon

26 August, 2023

>_whoami (Jalaj)

Blue Teamer by Day! Red Teamer by Night!

- Cyber security geek
- CTF Player
- CRAC research group : CVE Analysis and Cloud Security
- Cloud Security and Threat Hunting
- MMA
- Telegram: @senditfast

>_whoami (Sanchay)

Founding member of HackersVilla CyberSecurity. With over 6-7 years of professional experience in the field, I have worked with many top researchers. Mentored numerous students across the globe. Worked with Upgrad Campus, designed their security training programs and have given numerous talks at many Security conferences in India.

sanchayofficial

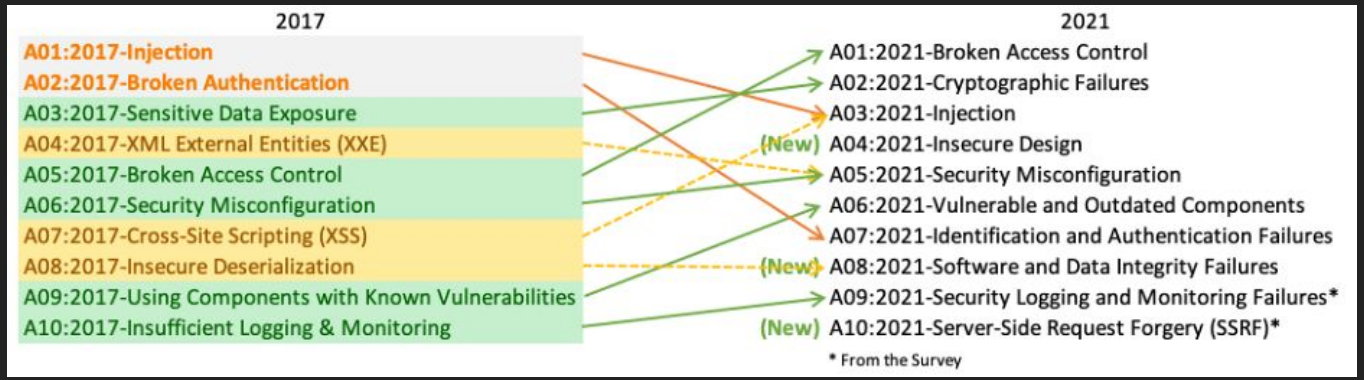
@sanchayofficial

sanchayofficial@gmail.com

Sanchay Singh

CYBERSECURITY EXPERT | CORPORATE TRAINER | PUBLIC SPEAKER

Intro to OWASP TOP 10



The OWASP Top 10 is a widely recognized list of the ten most critical security risks for web applications. It helps developers and security professionals prioritize their efforts to address common vulnerabilities like injection, broken authentication, and cross-site scripting.

A07: Auth Failures

When an application's login and session management systems are poorly implemented, allowing attackers to gain unauthorized access. Weak passwords, ineffective session handling, and lack of multi-factor authentication are common vulnerabilities that can lead to compromised user accounts and data breaches. Proper authentication security is crucial to prevent these issues.

Previously known as Broken Authentication, this category slid down from the second position and now includes Common Weakness Enumerations (CWEs) related to identification failures.

Common Weakness Enumerations

- *CWE-255 Credentials Management Errors*
- *CWE-259 Use of Hard-coded Password*
- *CWE-287 Improper Authentication*
- *CWE-288 Authentication Bypass Using an Alternate Path or Channel*
- *CWE-290 Authentication Bypass by Spoofing*
- *CWE-294 Authentication Bypass by Capture-replay*
- *CWE-295 Improper Certificate Validation*
- *CWE-297 Improper Validation of Certificate with Host Mismatch*
- *CWE-300 Channel Accessible by Non-Endpoint*
- *CWE-302 Authentication Bypass by Assumed-Immutable Data*
- *CWE-304 Missing Critical Step in Authentication*
- *CWE-306 Missing Authentication for Critical Function*
- *CWE-307 Improper Restriction of Excessive Authentication Attempts*
- *CWE-346 Origin Validation Error*
- *CWE-384 Session Fixation*
- *CWE-521 Weak Password Requirements*
- *CWE-613 Insufficient Session Expiration*
- *CWE-620 Unverified Password Change*
- *CWE-640 Weak Password Recovery Mechanism for Forgotten Password*
- *CWE-798 Use of Hard-coded Credentials*
- *CWE-940 Improper Verification of Source of a Communication Channel*
- *CWE-1216 Lockout Mechanism Errors*

What exactly is A07?

Identification

Failures

- Doesn’t prevents automated attacks like credential stuff or brute forcing to guess passwords
- Has flaws in the password reset or recovery flows
- Doesn’t handles (invalidates or rotates) session identifiers after email/password update, logout, inactivity, re-login

Some common scenarios based on the 3 failures

1. Use of Hard-coded Password

```
6     private static String username = "root";
7     private static String password = "securePassword";
8
9    public static void main(String args[])
10   {
11    try
12    {
       Class.forName("com.mysql.jdbc.Driver");
       Connection con=DriverManager.getConnection(
        "jdbc:mysql://localhost:3306/db", username, password);

     Statement stmt=con.createStatement();
     ResultSet rs=stmt.executeQuery("select * from users");

   while(rs.next())
    System.out.println(rs.getInt(1)+"  "+rs.getString(2)+"  "+rs.getString(3));

  con.close();
```

2. Missing Critical Step in Authentication

MicrosoftDocs/azure-docs

#66335 **Critical Step Missing for enabling Azure Active Directory...**

5 comments

awsles opened on November 19, 2020

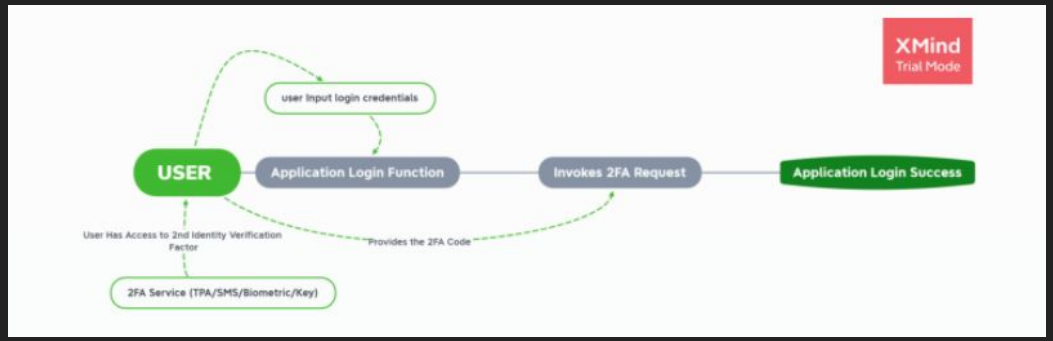
Vulnerability in bookwyrm-social / bookwyrm

Missing Critical Step in Authentication

by Akshay Ravi – @akshayravic09yc47

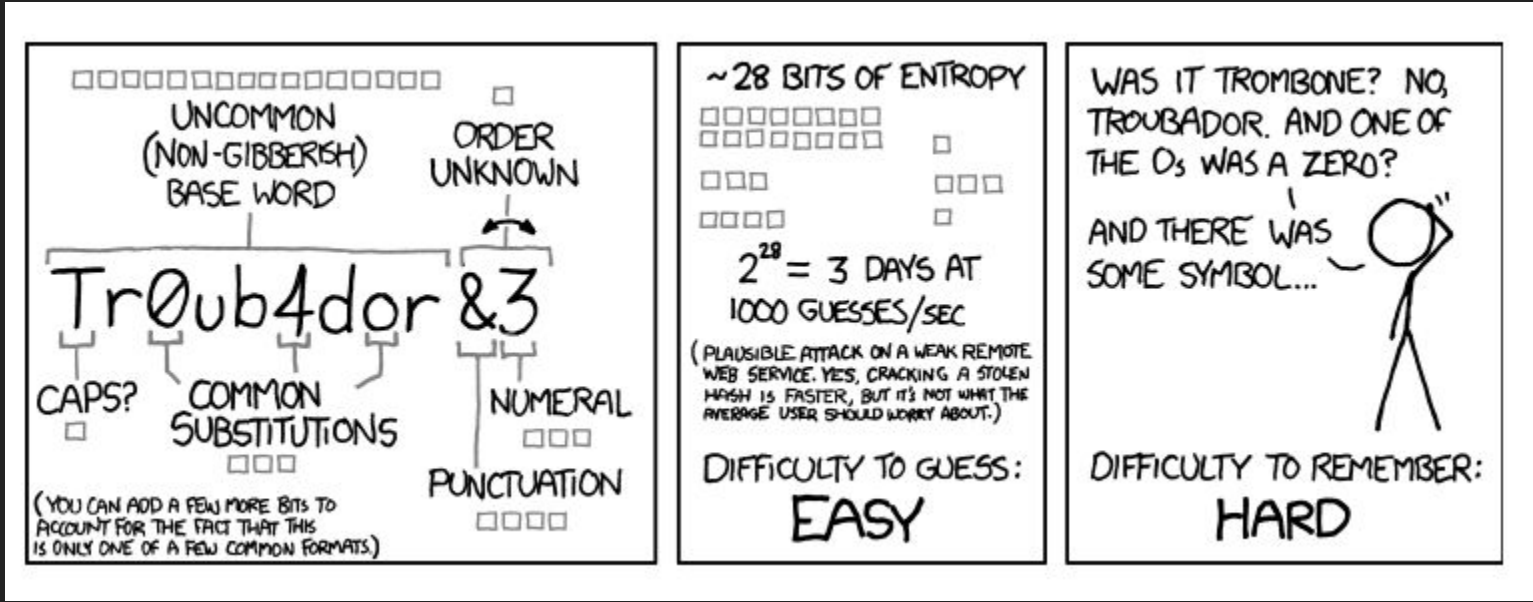
Top 34%	0/5	0	CVE-2022-35925
Popularity	Severity	Occurences	

3. MFA Bypass

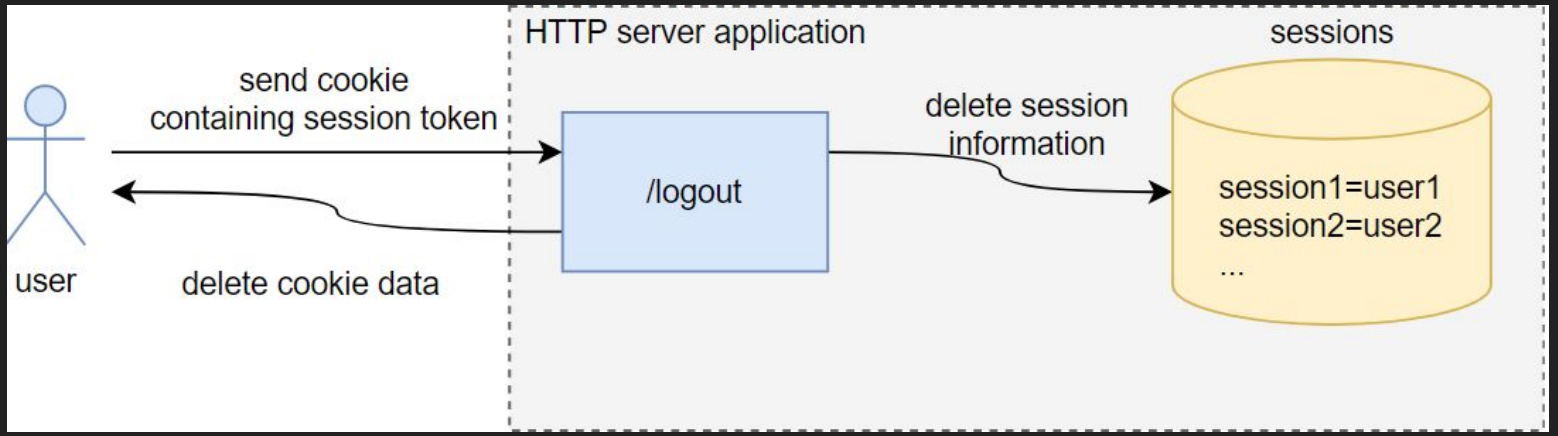


Could be done through Response Manipulation, CSRF, Forceful browsing, OTP Cached in Dynamic JS Files, Missing Integrity Check on OTP, etc.

4. Weak Password Requirements



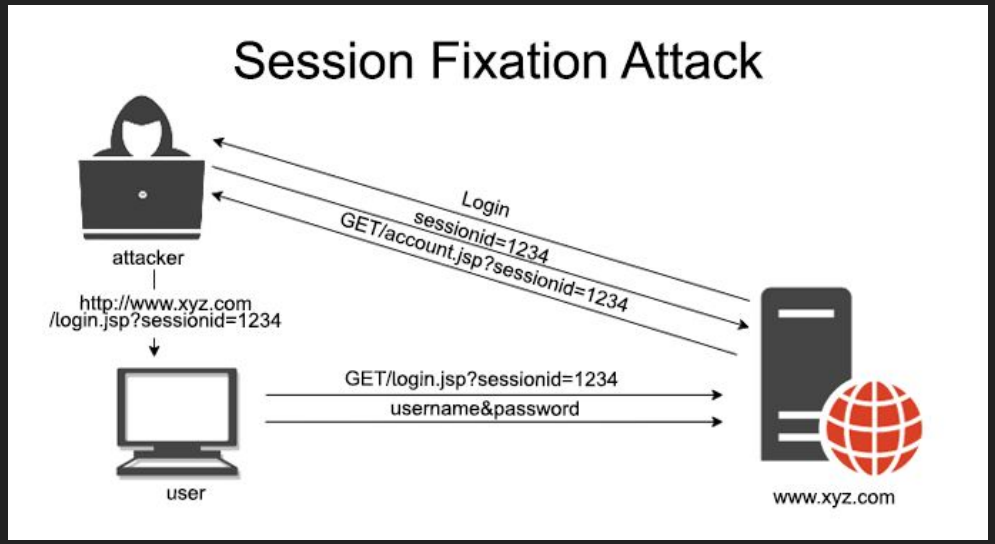
5. Logging out doesn't expire session cookie



Some important case scenarios to be discussed

1. Session Fixation

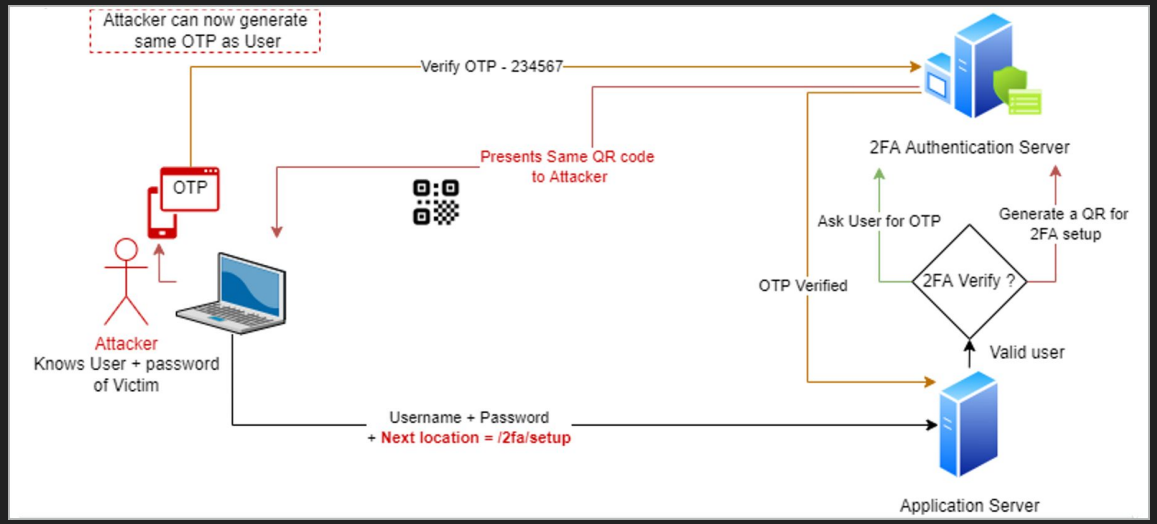
An attack that occurs when a malicious user sets up a fake session before the legitimate users are able to log in.

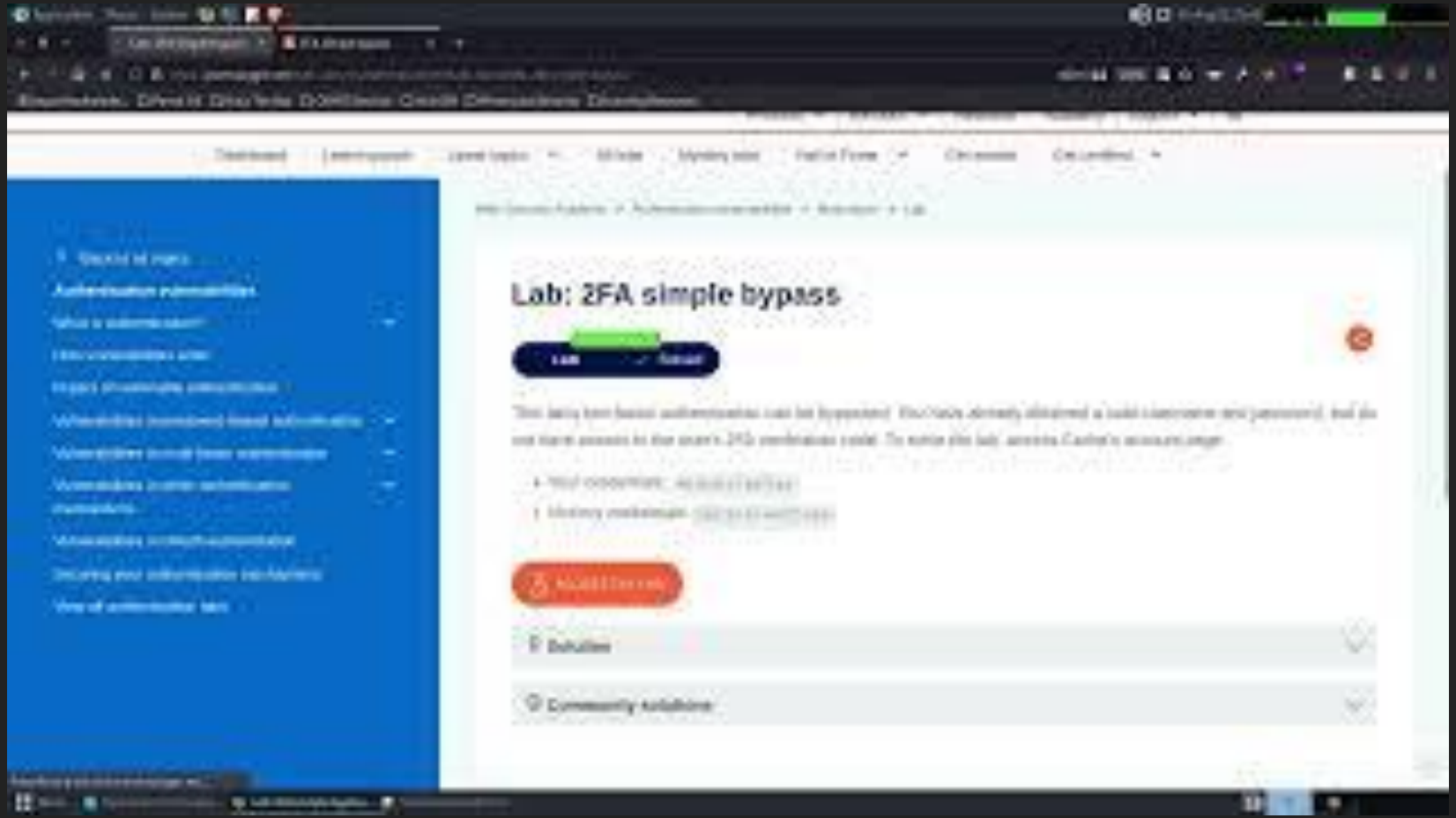


Let us understand how Session Fixation works

2. 2FA Bypass

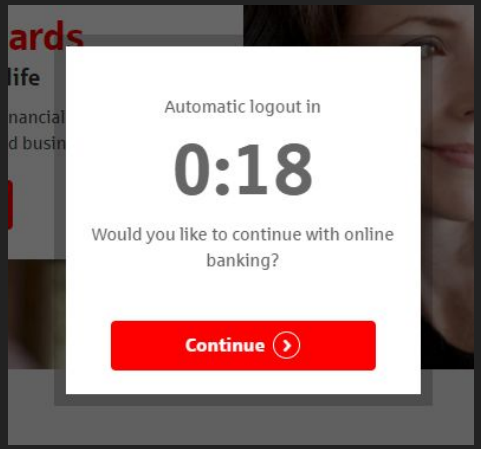
Involves circumventing the additional security layer, often through social engineering or technical vulnerabilities, allowing attackers to access accounts even with 2FA enabled.

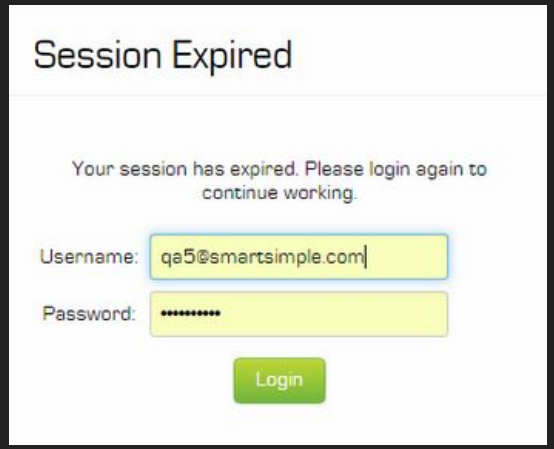



Lab: 2FA simple bypass

3. Session Timeout

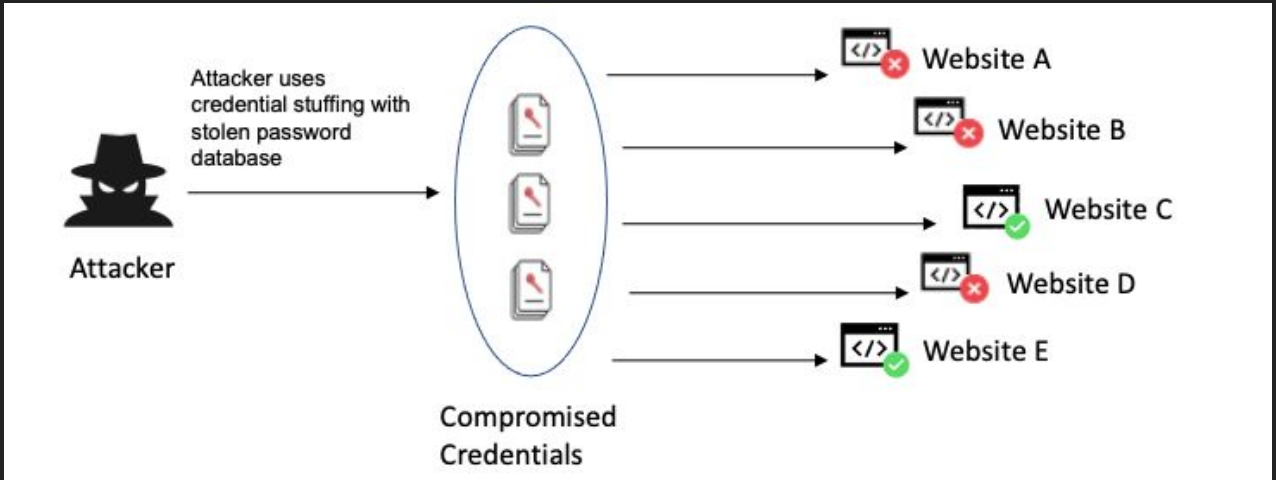
A security feature that automatically logs out a user after a period of inactivity, reducing the risk of unauthorized access to their active session and sensitive data.





4. Credential Stuffing

A cyberattack where attackers use previously stolen usernames and passwords to gain unauthorized access to multiple user accounts, exploiting the practice of reusing credentials across different platforms.



So....
Mitigations?

1. Enable and enforce MFA
2. Ensure that default passwords are only for one-time use and are updated as the user logins
3. Enforce a password policy to prevent users from setting weak passwords
4. Rate limit the critical endpoints
5. Session Cookies should get refreshed after every login and expired after every logout
6. Get your applications pentester and any code being pushed to production must be reviewed and well tested against such issues
7. **Use a Framework!!**

Thank You