www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #2 Broken Session Management

By @isaacsabas

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

www.pandoralabs.net

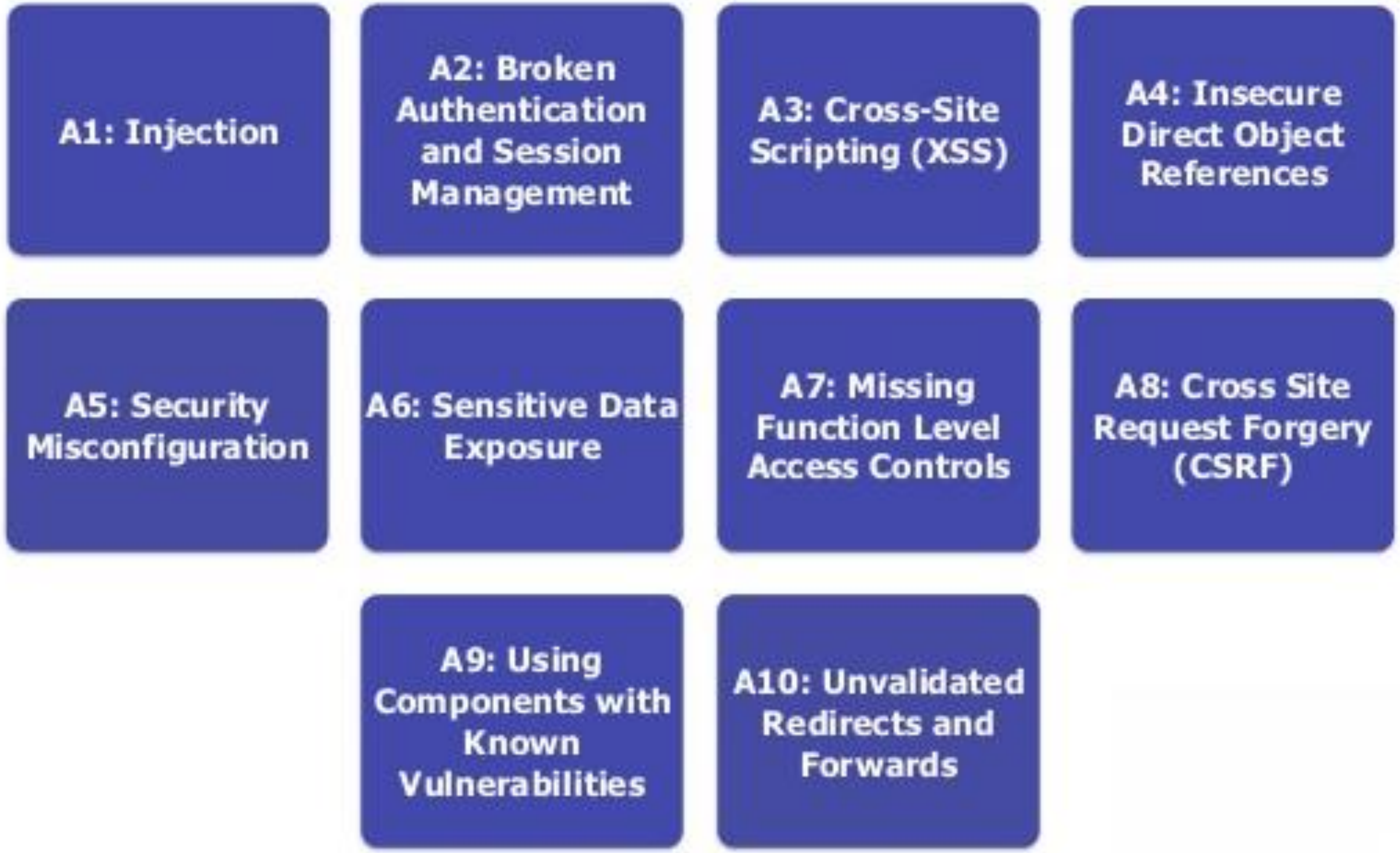
We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

OWASP

Open Web Application
Security Project



A1: Injection

A2: Broken Authentication and Session Management

A3: Cross-Site Scripting (XSS)

A4: Insecure Direct Object References

A5: Security Misconfiguration

A6: Sensitive Data Exposure

A7: Missing Function Level Access Controls

A8: Cross Site Request Forgery (CSRF)

A9: Using Components with Known Vulnerabilities

A10: Unvalidated Redirects and Forwards

OWASP #2

Broken Session Management

OWASP Top 10 Vulnerabilities

A vulnerability that allows the bypass of authentication or access control mechanisms used to protect systems against unauthorized access.

What is Broken Session Management?

Where it all began.

Ways How Session Management Is Exploited

1. Unencrypted connection
2. Predictable login credentials
3. Session value does not timeout (or does not expire after logout)
4. Weak user credential storage
5. Session IDs are used in the URL

WEB APP
LOGIN

Let's walk through the steps that are performed when logging into a web application.

Authentication Steps

1. Input user credentials **(usually username/email and password)**
   - e.g. username ***jsmith***, password ***12345***
2. The credentials are then submitted to the web app for validation and then a **session ID** is generated to link to the credentials
   - e.g. *sessionid=3gXXLeNPGbksjielqidkfpoksle19k9l1k234b70kskeols*

1. Unencrypted Connections

- All information that is being sent/received between user’s browser and web application can be intercepted without your knowledge
- This eventually fails to safely transmit the username, password and session ID of the user to the web application
- You can solve this by using encryption (HTTPS), enabling SSL.

2. Predictable Login Credentials

- Username and password values that are easy to guess due to frequent usage or no password change policy
- Allows web application to be susceptible to brute force login attacks
- This can be solved by enforcing:
  - Strong password policy
  - Password update policy

3. Session ID Does Not Expire/Invalidate

- The web application doesn’t discard the session IDs issued after logout or after a certain period of time.
- Allows users to steal session IDs to hijack a session
- This can be solved by setting auto session ID expiration period.

4. Weak User Credential Storage

- The web application doesn’t encrypt the user credentials that is stored within the database.
- Allows attackers to get user credentials in clear text.
- This can be solved by salting and hashing passwords of users, in addition to encrypting the database.

5. Session IDs are Used In The URL

- The web application transmits the session ID through the URL which can be easily seen by anyone.
  - e.g. *http://www.example.com/login.php?**sessionid=abcd1234***
- This can be solved by transmitting sensitive information via **POST** request, **not GET** requests.

Go to http://demo.testfire.net

EXPLOIT DEMO

How simple it is to test for a Broken Session Management vulnerability.

Demo

1. Login without using HTTPS
2. Brute force login

TIME FOR Q&A

OWASP Top 10 - Injection

Go download WebGoat

https://github.com/WebGoat/WebGoat-Legacy

TRY IT YOURSELF

Some homework for you to learn a bit more.

WebGoat Installation How-To

1. Download Java VM, JDK 1.7
2. Download WebGoat: https://webgoat.atlassian.net/builds/browse/WEB-WGM/latestSuccessful/artifact/shared/WebGoat-Embedded-Tomcat/WebGoat-6.0.1-war-exec.jar
3. Run the .jar file:
   1. java -jar WebGoat-6.0-exec-war.jar
4. Then navigate in your browser to: (http://localhost:8080/WebGoat)
5. Login using guest account
6. Go to: Authentication Flaws and complete the following exercises:
   1. Password Strength
   2. Forgot Password
7. Go to: Session Management Flaws and complete the following exercises:
   1. Hijack a Session

OWASP #2

Broken Session Management

OWASP Top 10 Vulnerabilities

www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #2 Broken Session Management

By @isaacsabas