Broken Authentication: What it means, and what you can do

hassan.abudu@owasp.org

OWASP
The Open Web Application Security Project

OWASP
The Open Web Application Security Project

OWASP Top 10 Vulnerabilities - 2017

Rank	Name
1	Injection
2	Broken Authentication
3	Sensitive Data Exposure
4	XML External Entities
5	Broken Access Control
6	Security Misconfiguration
7	Cross-Site Scripting
8	Insecure Deserialization
9	Using Components with Known Vulnerabilities
10	Insufficient Logging & Monitoring

OWASP
The Open Web Application Security Project

Broken Authentication

An important lesson: Anyone in your organization could be a weak link

What is it?

- It is when your password authentication isn't sufficiently secure.
- When that happens, it fails to protect your organizations assets.
- It isn't an exploit in itself, but when a hacker can just log in as a member of your organization, you're in big trouble

OWASP
The Open Web Application Security Project

Broken Authentication

Q: How do hackers exploit authentication vulnerabilities?

A: Often through password cracking. These are some sources of vulnerabilities

- **Having weak or inadequate password policies**
- **Allowing an unlimited amount of login attempts**
- **Providing information back to an attacker on failed logins**
- **Sending credentials over insecure channels**
- **Weakly hashing passwords**

OWASP
The Open Web Application Security Project

Broken Authentication

Eliminating Password Vulnerabilities

Passwords should have:

- At least 1 uppercase character (A-Z)
- At least 1 lowercase character (a-z)
- At least 1 digit (0-9)
- At least 1 special character including punctuation marks & spaces
- Be at least 10 characters long.

OWASP
The Open Web Application Security Project

Broken Authentication

Any questions?