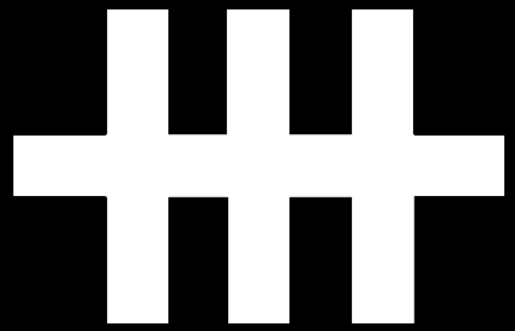


ConSecuty

Applikationssäkerhet för testare

ConSecuty

- Säkerhet är allas jobb. Utvecklare, kravanalytiker, testare och produktägare måste förstå grunderna i säkerhet och veta hur man bygger in säkerhet i programvara och tjänster för att göra produkterna säkrare.

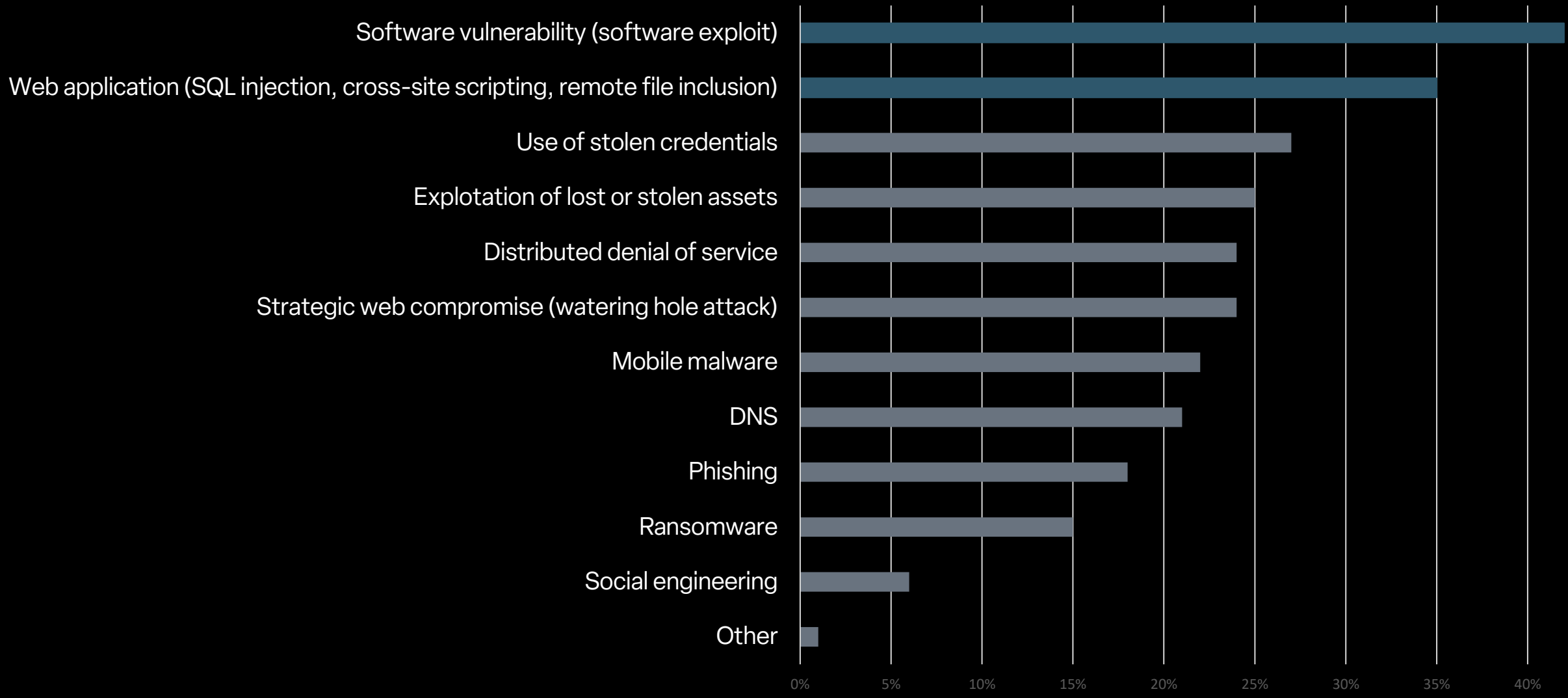
- Alla behöver inte vara säkerhetsexperter eller sträva efter att bli en skicklig penetrationstestare för att kunna bidra i säkerhetsarbetet.

Viktor Laszlo - ConSecuty

Jobbat med utveckling i 25+ år. Fokus på QA och Säkerhet.

ConSecuty

Hur genomfördes det externa hacket?



Vilken åtgärd ger störst effekt?

40% Utbildning

20% Hotmodellering

4% Minskad attackyta

2% Fuzz Testing

ConSecuty

Säkerhetsutbildning

ConSecuty

Säkerhetsutbildning

- Alla i organisationen deltar
- Olika typer av hot och attacker
- Regler och policies
- Säker utveckling
- Informationssäkerhet och informationsklassificering
- Ökat medvetande och säkerhetsfokus
- Förnyas årligen

ConSecuty

Hotmodellering

Hotmodellering

Systematiskt lista alla möjliga sätt hur en applikation kan attackeras.

Hotmodellering

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

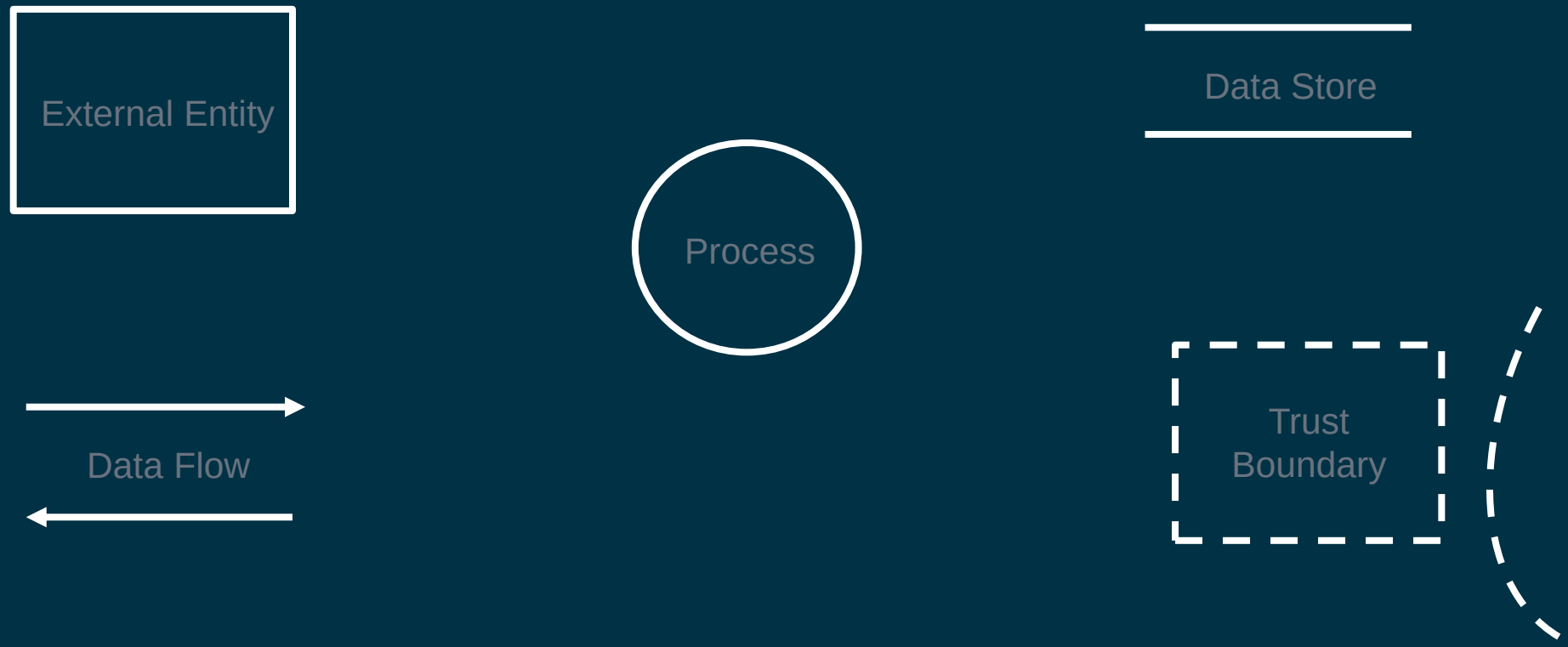
Elevation of Privilege

ConSecuty

Hotmodellering - STRIDE

Property	Threat	Definition	Example
Authentication	Spoofing	Impersonating something or someone else.	Pretending to be any of billg, microsoft.com or ntdll.dll
Integrity	Tampering	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the LAN.
Non-repudiation	Repudiation	Claiming to have not performed an action.	“I didn’t send that email,” “I didn’t modify that file,” “I certainly didn’t visit that web site, dear!”
Confidentiality	Information Disclosure	Exposing information to someone not authorized to see it	Allowing someone to read the Windows source code; publishing a list of customers to a web site.
Availability	Denial of Service	Deny or degrade service to users	Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole.
Authorization	Elevation of Privilege	Gain capabilities without proper authorization	Allowing a remote internet user to run commands is the classic example, but going from a limited user to admin is also EoP.

Hotmodellering - Element

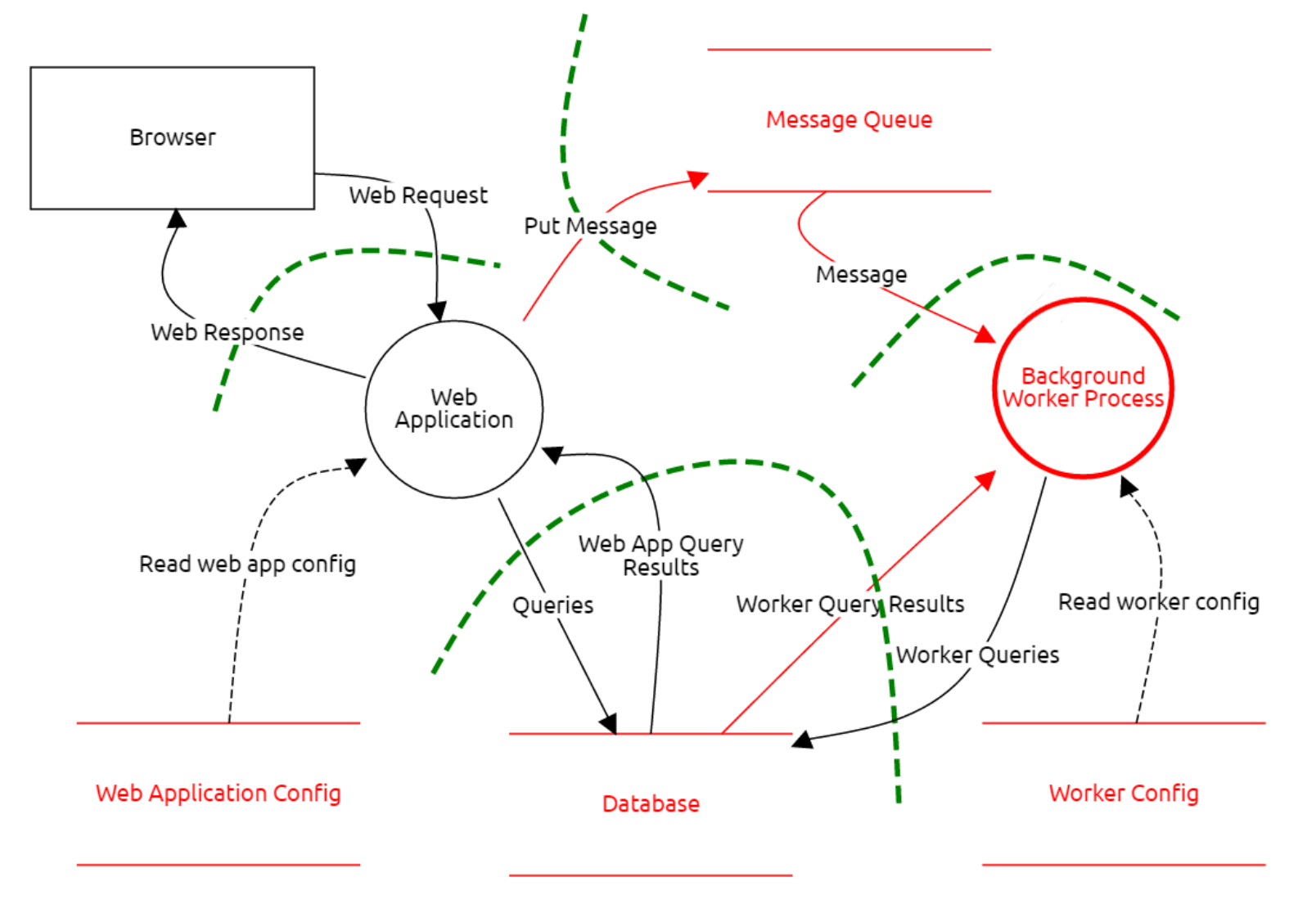


ConSecuty

STRIDE per Element

Element	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store		✓	✓	✓	✓	
Dataflow		✓		✓	✓	

Hotmodellering - Diagram



Minska Attackytan

Attackyta

Minskad attackyta

Säkerhetstester

ConSecuty

OWASP Application Security Verification Standard

- Första applikationssäkerhetsstandarden av utvecklare, för utvecklare.
- Varje objekt är ett enda koncept.
- Helt öppen källkod och delningsbar.

ConSecuty

Level 1 - Bara grunderna

- 136 Kontroller (Krav)
- Lätt automatiserad.
- Lägsta godtagbar säkerhet.
- Otillräckligt för att bygga en säker applikation.
- Lätt att automatisera med hjälp av verktyg.

ConSecuty

Level 2 – Rekommenderad nivå

- 267 Kontroller (Krav)
- Vissa kontroller är engångsaktiviteter.
  - Ha en SDL (säker SDLC)
  - Använd versionshanteringssystem (scv)
  - Använd en defekt tracker.
  - Använd repeterbar, säker deployment
- De flesta kan enhets- och/eller integrationstestas.

Level 3 - För appar som kan döda dig eller förstöra ekonomin

- 286 Kontroller (Krav)
- Lämplig för:
  - Medicinska applikationer och apparater.
  - OT – kraft, vatten, avlopp, kemiska anläggningar, kärnkraftverk m.m.
  - Finansiella applikationer som kan förstöra ekonomin.
- Säkerhetsnivån är maximal.
- Nivån av paranoia är hög.

Application Security Verification Standard 4.0.3

October 2021

1. Architecture, Design and Threat Modeling
2. Authentication
3. Session Management
4. Security Verification Requirements
5. Validation, Sanitization and Encoding
6. Stored Cryptography
7. Error Handling and Logging
8. Data Protection
9. Communication
10. Malicious Code
11. Business Logic
12. Files and Resources
13. API and Web Service
14. Configuration

ConSecuty

2. Authentication

V2.1 Password Security
V2.2 General Authenticator Security
V2.3 Authenticator Lifecycle
V2.4 Credential Storage
V2.5 Credential Recovery
V2.6 Look-up Secret Verifier
V2.7 Out of Band Verifier
V2.8 One Time Verifier
V2.9 Cryptographic Verifier
V2.10 Service Authentication

ConSecuty

V2.1 Password Security

Passwords, called "Memorized Secrets", include passwords, PINs, unlock patterns, pick the correct kitten or another image element, and passphrases.

They are generally considered "something you know", and often used as single-factor authenticators.

Applications should strongly encourage users to enroll in multi-factor authentication, or link to a credential service provider that provides multi-factor authentication.

V2.1 Password Security

#	Description	L1	L2	L3	CWE
2.1.1	Verify that user set passwords are at least 12 characters in length (after multiple spaces are combined). (C6)	✓	✓	✓	521
2.1.2	Verify that passwords of at least 64 characters are permitted, and that passwords of more than 128 characters are denied. (C6)	✓	✓	✓	521
2.1.3	Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space. (C6)	✓	✓	✓	521
2.1.4	Verify that any printable Unicode character, including language neutral characters such as spaces and Emojis are permitted in passwords.	✓	✓	✓	521
2.1.5	Verify users can change their password.	✓	✓	✓	620
2.1.6	Verify that password change functionality requires the user's current and new password.	✓	✓	✓	620
2.1.7	Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password. (C6)	✓	✓	✓	521
2.1.8	Verify that a password strength meter is provided to help users set a stronger password.	✓	✓	✓	521
2.1.9	Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters. (C6)	✓	✓	✓	521
2.1.10	Verify that there are no periodic credential rotation or password history requirements.	✓	✓	✓	263
2.1.11	Verify that "paste" functionality, browser password helpers, and external password managers are permitted.	✓	✓	✓	521
2.1.12	Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as built-in functionality.	✓	✓	✓	521

CWE-521: Weak Password Requirements

Description:

The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

Related Attack Patterns:

CAPEC-112	Brute Force
CAPEC-16	Dictionary-based Password Attack
CAPEC-49	Password Brute Forcing
CAPEC-509	Kerberoasting
CAPEC-55	Rainbow Table Password Cracking
CAPEC-555	Remote Services with Stolen Credentials
CAPEC-561	Windows Admin Shares with Stolen Credentials
CAPEC-565	Password Spraying
CAPEC-70	Try Common or Default Usernames and Passwords

CAPEC-112: Brute Force

Description

In this attack, some asset (information, functionality, identity, etc.) is protected by a finite secret value. The attacker attempts to gain access to this asset by using trial-and-error to exhaustively explore all the possible secret values in the hope of finding the secret (or a value that is functionally equivalent) that will unlock the asset.

Typical Severity

High

Prerequisites

The attacker must be able to determine when they have successfully guessed the secret. As such, one-time pads are immune to this type of attack since there is no way to determine when a guess is correct.

Skills Required

[Level: Low]

The attack simply requires basic scripting ability to automate the exploration of the search space. More sophisticated attackers may be able to use more advanced methods to reduce the search space and increase the speed with which the secret is located.

viktor@consecuty.com

ConSecuty