OWASP
Open Web Application Security Project

<Are you focusing on the root causes?/>

A unified framework for web security

Igino Corona, PhD
Computer Security Researcher & CTO @ Pluribus One
https://www.pluribus-one.it

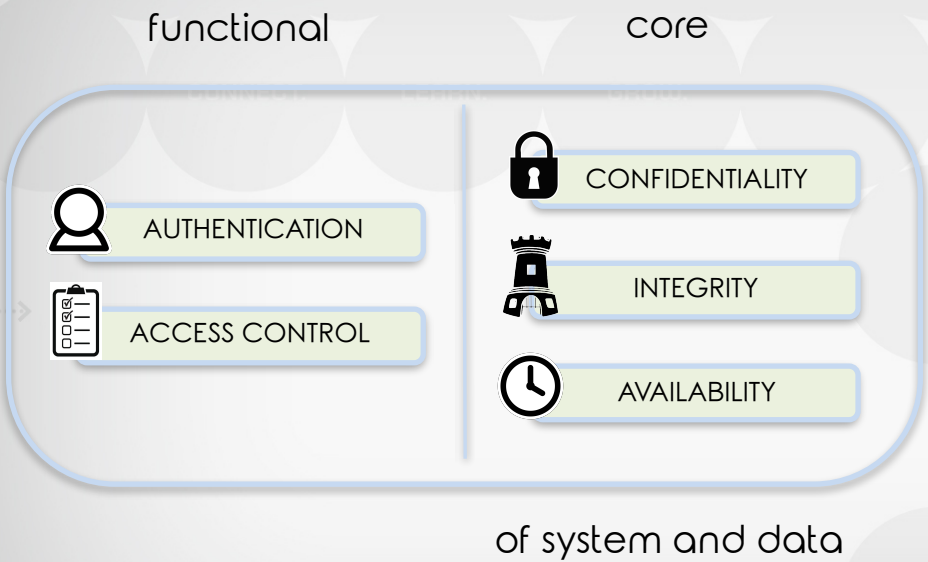
OWASP Italy Day
Cagliari, 19th October 2018

Key Security Requirements

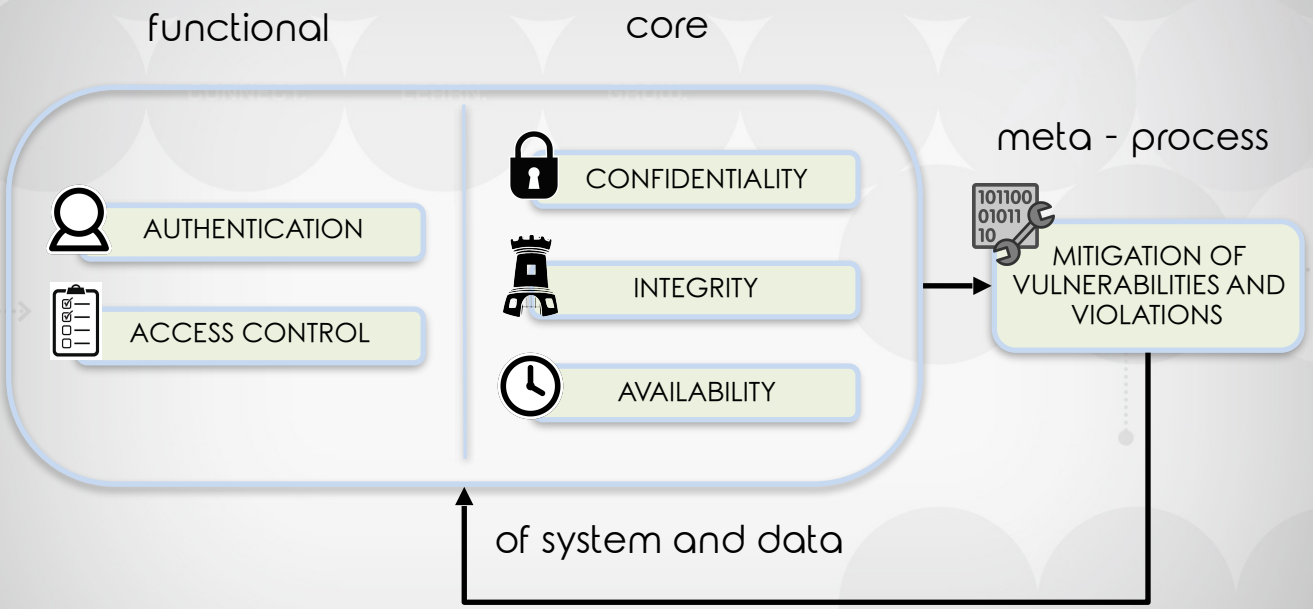
core

of system and data

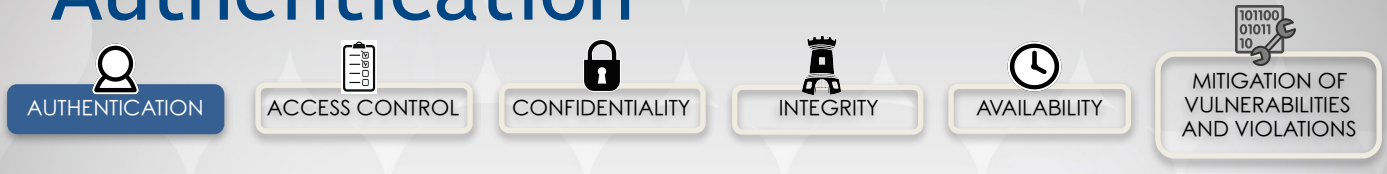
Key Security Requirements



Key Security Requirements



Authentication



Who are you?

Authentication

Who are you?

Authentication

Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …

Authentication

Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …

Authentication

Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …

OWASP Top 10-2017
A2-Broken Authentication

Authentication

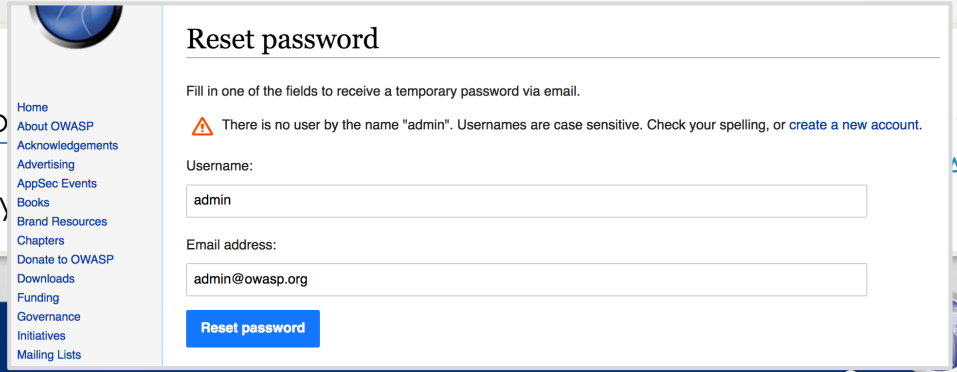
Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …



Authentication

Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …

Authentication

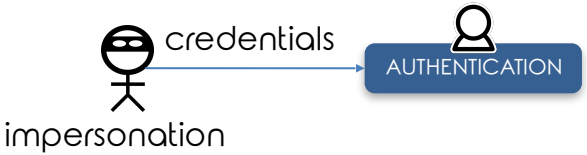
Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …



Authentication

Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …

Authentication

Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …

1. Contextual Information
2. Anomaly detection
3. Notifications and logging

Authentication

Who are you?

The answer strongly relies on

- **confidential (Security through obscurity!)**
- and/or **unique**

information of an user (credentials)

- username, password, session id, biometrics, private key, telephone number, …

È appena stato eseguito l'accesso al tuo Account Google da un nuovo dispositivo: Windows. Ti abbiamo inviato questa email per assicurarci che si tratti di un accesso eseguito da te.

CONTROLLA L'ATTIVITÀ

Access Control

Who can do what?

Access Control

Who can do what?

- needs authentication first (who are you?)

Access Control

Who can do what?

- needs authentication first (who are you?)

Access Control

Who can do what?

- needs authentication first (who are you?)
- necessary to protect all core security properties

Access Control

Who can do what?

- needs authentication first (who are you?)
- necessary to protect all core security properties
- key step also for recent EU privacy regulation (GDPR)

Access Control

Who can do what?

- needs authentication first (who are you?)
- necessary to protect all core security properties
- key step also for recent EU privacy regulation (GDPR)

OWASP Top 10-2017
A5-Broken Access Control

Access Control

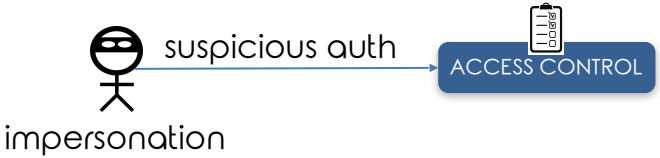
Who can do what?

- needs authentication first (who are you?)
- necessary to protect all core security properties
- key step also for recent EU privacy regulation (GDPR)

Access Control

Who can do what?

- needs authentication first (who are you?)
- necessary to protect all core security properties
- key step also for recent EU privacy regulation (GDPR)



Access Control

Who can do what?

- needs authentication first (who are you?)
- necessary to protect all core security properties
- key step also for recent EU privacy regulation (GDPR)

Account protection and notification

Access Control

Who can do what?

- needs authentication first (who are you?)
- necessary to protect all core security properties
- key step also for recent EU privacy regulation (GDPR)

È stato bloccato un tentativo di accesso al tuo Account Google collegato

Confidentiality

Data must be accessed by authorized parties only

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification

Confidentiality

CONNECT. LEARN. GROW.

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

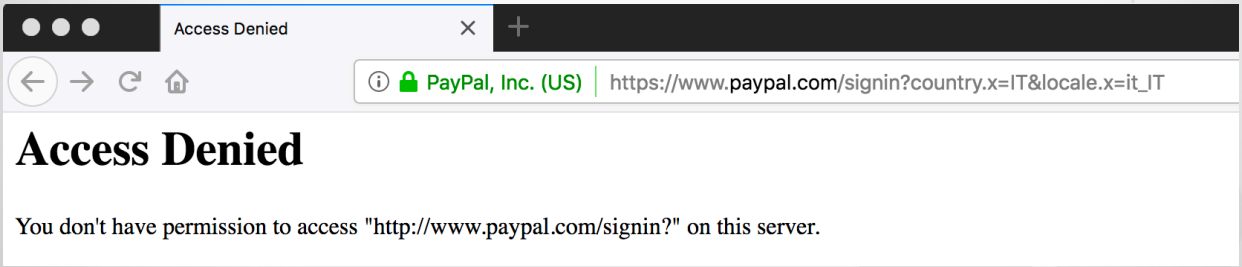
- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations



Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations
- Authentication & Access Control

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations
- Authentication & Access Control
- Strong data encryption and hashing

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations
- Authentication & Access Control
- Strong data encryption and hashing
- No caching

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations
- Authentication & Access Control
- Strong data encryption and hashing
- No caching

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

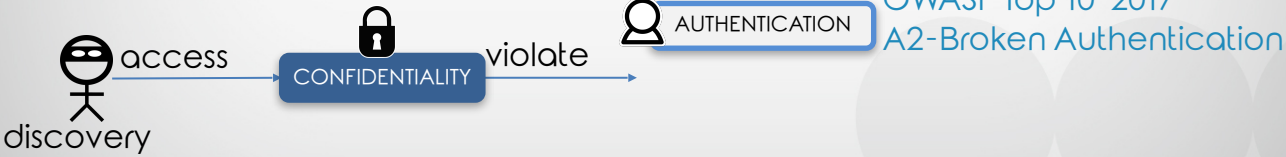
- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations
- Authentication & Access Control
- Strong data encryption and hashing
- No caching

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations
- Authentication & Access Control
- Strong data encryption and hashing
- No caching



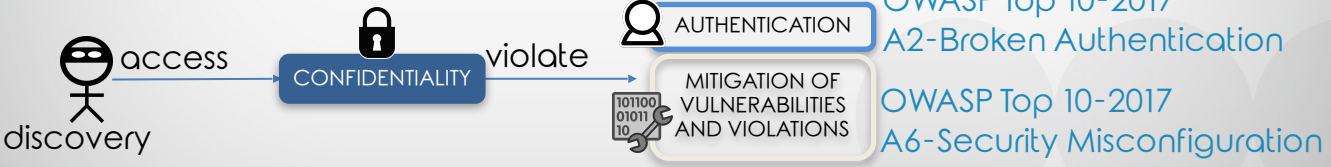
OWASP Top 10-2017 A2-Broken Authentication

Confidentiality

Data must be accessed by authorized parties only

OWASP Top 10-2017 A3-Sensitive Data Exposure

- Sensitive Data classification
  - We should also include information about the system itself
  - Useful to increase the cost of (information gathering) attacks
    - i.e., mitigate vulnerabilities and violations
- Authentication & Access Control
- Strong data encryption and hashing
- No caching



Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

System integrity violation

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

System integrity violation

Unauthorized modification of code and/or system functionalities

Integrity

Data, Code, System functionalities can be modified by authorized parties only

Are you aware of any attack whose root security violation is integrity?

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

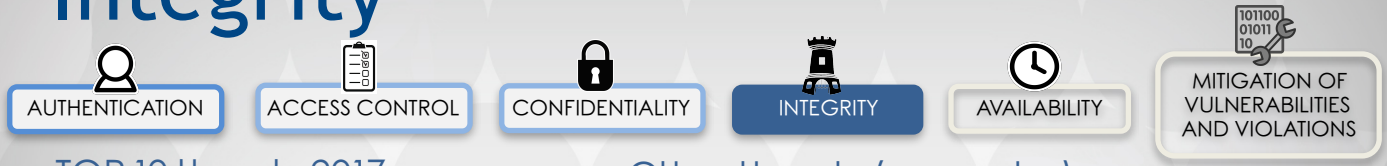
Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

System integrity violation

Unauthorized modification of code and/or system functionalities

Integrity



TOP 10 threats 2017

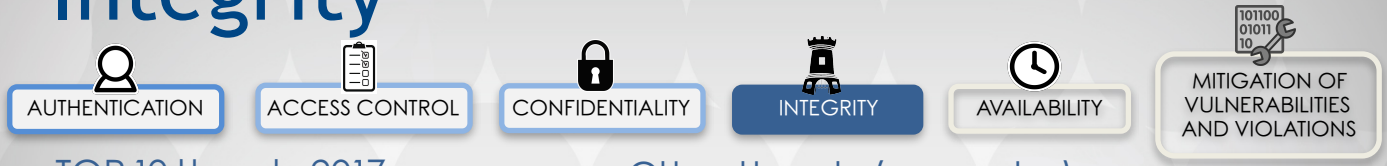
- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Is there a common root cause for all the above integrity threats?

Integrity



TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

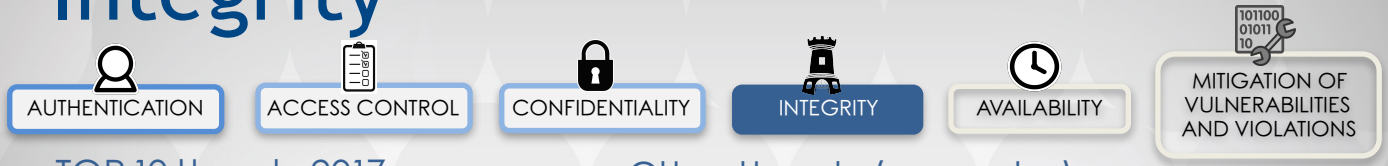
Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Is there a common root cause for all the above integrity threats?

– Yes, inadequate or missing input handling

Integrity



TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Is there a common root cause for all the above integrity threats?

- Yes, inadequate or missing input handling
  - Input data can be arbitrarily intepreted as code!

Integrity

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | **INTEGRITY** | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

TOP 10 threats 2017

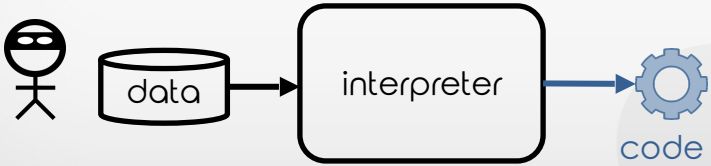
- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Is there a common root cause for all the above integrity threats?

- Yes, inadequate or missing input handling
  - Input data can be arbitrarily intepreted as code!



Integrity

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | **INTEGRITY** | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

TOP 10 threats 2017

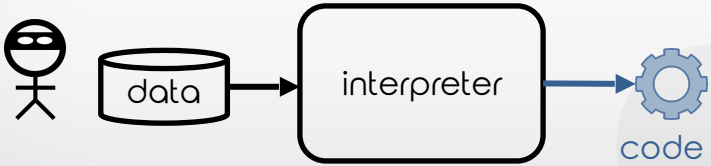
- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Is there a common root cause for all the above integrity threats?

- Yes, inadequate or missing input handling
  - Input data can be arbitrarily intepreted as code!



Integrity

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | **INTEGRITY** | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

TOP 10 threats 2017

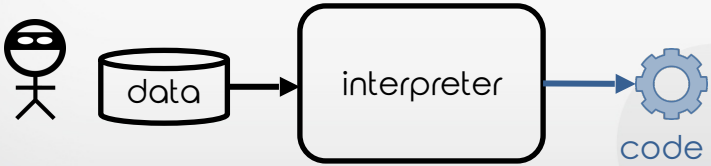
- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Is there a common root cause for all the above integrity threats?

- Yes, inadequate or missing input handling
  - Input data can be arbitrarily intepreted as code!



Let's call them as: Data→Code threats

Integrity

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Main difference between these Data→Code threats?

Integrity

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Main difference between these Data→Code threats?

- Targeted interpreter

Integrity

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Main difference between these Data→Code threats?

- Targeted interpreter
  - Database, Web application, Operating System, XML parser, HTML parser, JavaScript engine, HTTP Client, HTTP Server, CPU, …

Integrity

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Main difference between these Data→Code threats?

- Targeted interpreter
  - Database, Web application, Operating System, XML parser, HTML parser, JavaScript engine, HTTP Client, HTTP Server, CPU, …
- BE AWARE

Integrity

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Main difference between these Data→Code threats?

- Targeted interpreter
  - Database, Web application, Operating System, XML parser, HTML parser, JavaScript engine, HTTP Client, HTTP Server, CPU, …
- BE AWARE
  - New interpreter = New Data→Code instance!

Integrity

TOP 10 threats 2017

- Injection
- XML External Entities
- Cross-Site Scripting
- Insecure Deserialization

Other threats (examples)

- Unvalidated Redirects and Forwards
- HTTP Response Splitting
- Malicious File Execution
- Buffer Overflow

Main difference between these Data→Code threats?

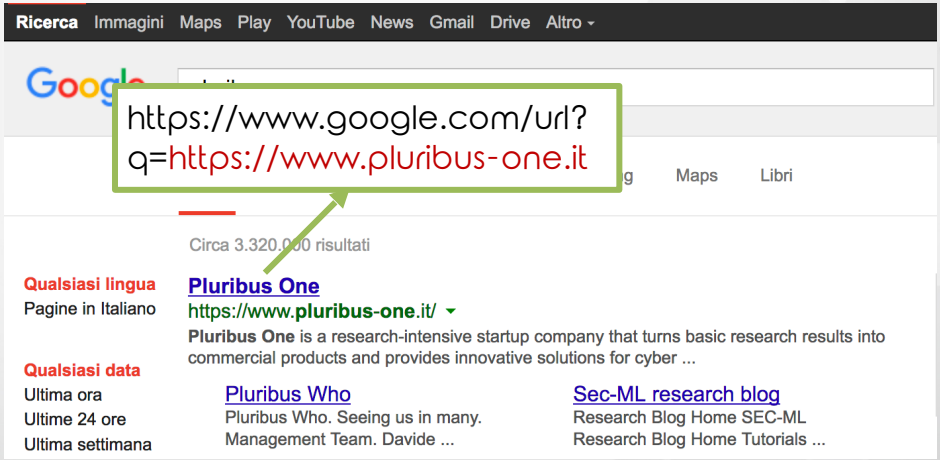
- Targeted interpreter
  - Database, Web application, Operating System, XML parser, HTML parser, JavaScript engine, HTTP Client, HTTP Server, CPU, …
- BE AWARE
  - New interpreter = New Data→Code instance!

Integrity

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | **INTEGRITY** | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

Normal Data→Code functionalities

- E.g. Google URL redirect service
  - used to track “clicks”

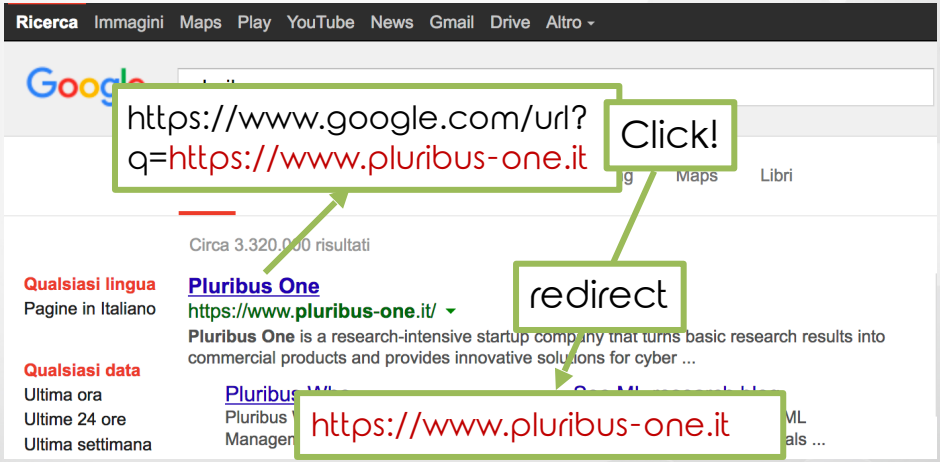


Integrity

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | INTEGRITY | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

Normal Data→Code functionalities

- E.g. Google URL redirect service
  - used to track “clicks”



Integrity

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | **INTEGRITY** | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

Gentile Cliente,

il tuo ID Apple è stato utilizzato per accedere a iCloud da un browser web.

Data e ora: 19 febbraio 2018, 08:48 PDT

Indirizio IP , Luogo: 180.162.205.30, China – Shanghai

Se recententemente hai eseguito l'accesso a iCloud, puoi ignorare questa email.

Se recententemente non hai eseguito l'accesso a iCloud e ritieni che qualcun altro possa aver eseguito l'accesso al tuo account, clicca sul link seguente per riavviare il informazioni Il mio ID Apple.

Cordiali saluti,

Supporto Apple

https://www.google.com/url?q=http://phishing.url

REAL-WOLD PHISHING EMAIL AGAINST APPLE USERS!

Integrity

Normal Data→Code functionalities may be abused!

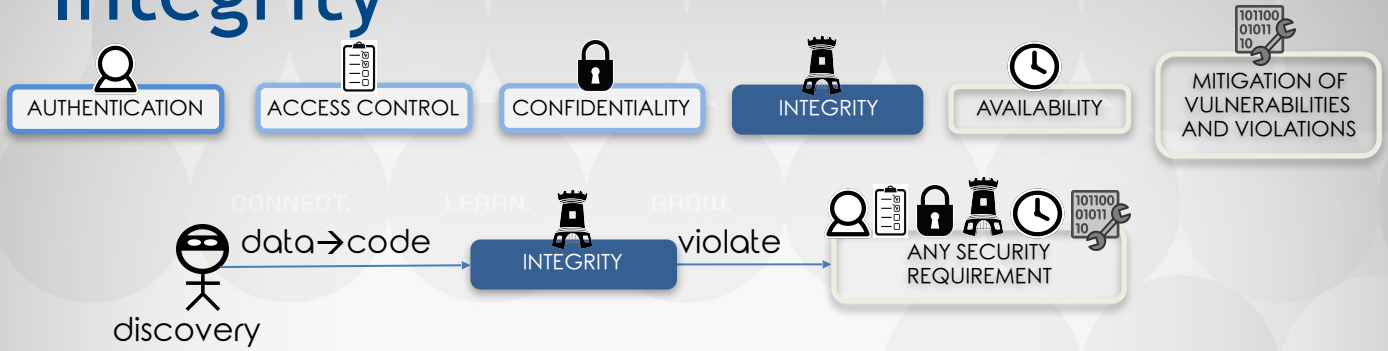
- Google URL redirect **service** used to track clicks
  - exposed to ”Unvalidated Redirects and Forwards - TOP 10 2013”

may be **abused** to bypass spam filters
  - Thanks to Google URLs reputation

- Mitigation measures require **contextual data**
  - E.g., in this case, Google might look at
    - referer URL
    - cookies

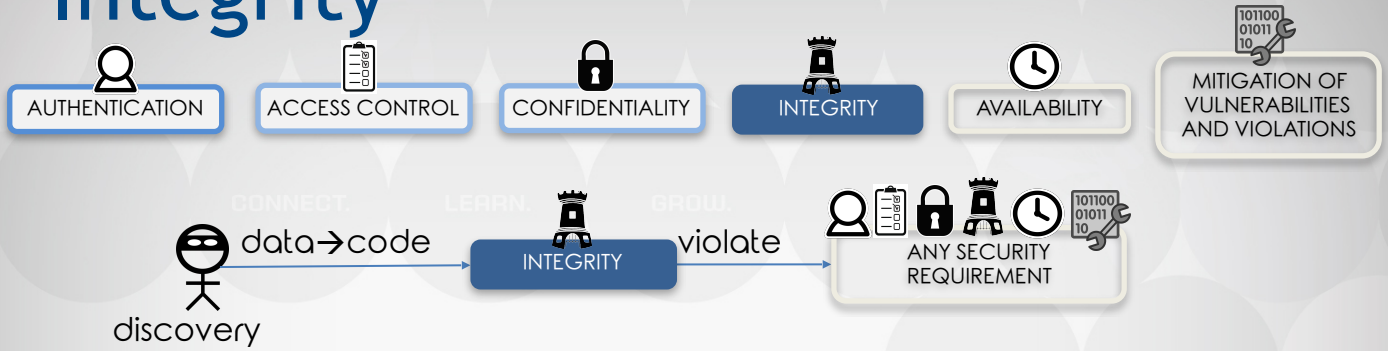
    to assess if the user is actually coming from a search page or not

Integrity



How to deal with Data→Code threats?

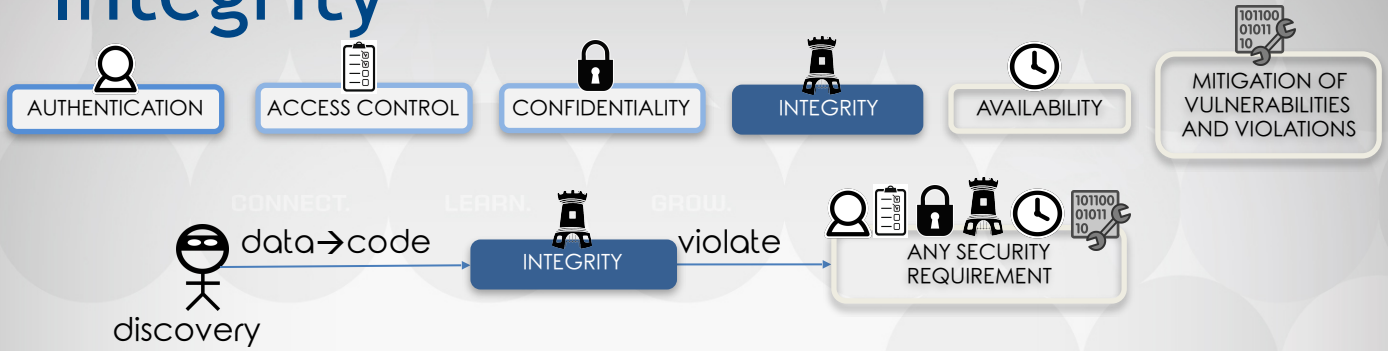
Integrity



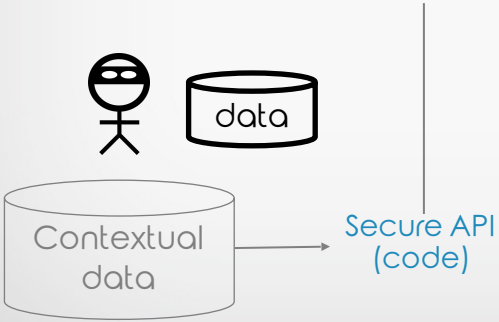
How to deal with Data→Code threats?

Secure API (code)

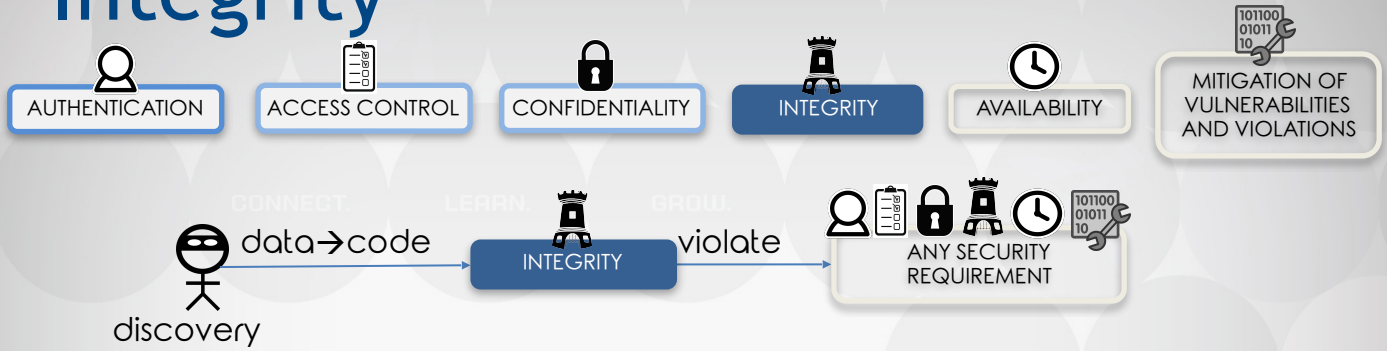
Integrity



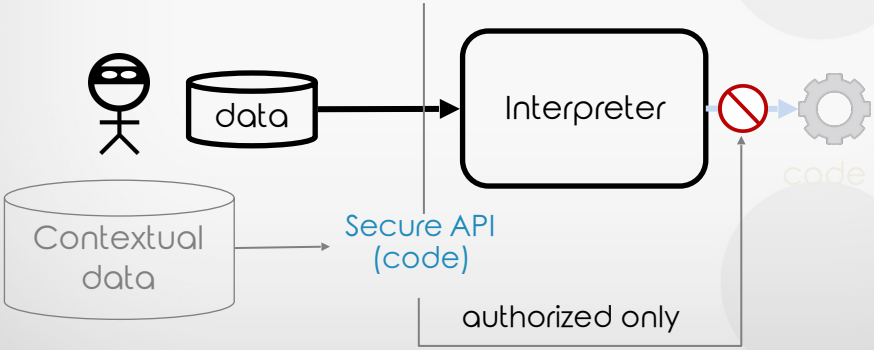
How to deal with Data→Code threats?



Integrity



How to deal with Data→Code threats?



Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery
- Resource limit per user

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery
- Resource limit per user
- Max number of concurrent users

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery
- Resource limit per user
- Max number of concurrent users
- Access control and Traffic prioritization

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery
- Resource limit per user
- Max number of concurrent users
- Access control and Traffic prioritization
  - E.g., authenticated sessions may be prioritized

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery
- Resource limit per user
- Max number of concurrent users
- Access control and Traffic prioritization
  - E.g., authenticated sessions may be prioritized
  - E.g., users during a payment process may be prioritized

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery
- Resource limit per user
- Max number of concurrent users
- Access control and Traffic prioritization
  - E.g., authenticated sessions may be prioritized
  - E.g., users during a payment process may be prioritized
- Headchecks and performance measures to detect SLA violations

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery
- Resource limit per user
- Max number of concurrent users
- Access control and Traffic prioritization
  - E.g., authenticated sessions may be prioritized
  - E.g., users during a payment process may be prioritized
- Headchecks and performance measures to detect SLA violations
- Non-repudiation mechanisms vs account protection

Availability

Data and services can be accessed (in a reasonable time) by *authorized* parties when requested

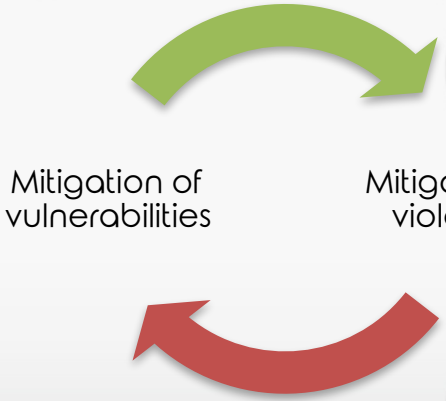
NOT in TOP 10 2017, but **fundamental for any service**!

- Regular data backups for recovery
- Resource limit per user
- Max number of concurrent users
- Access control and Traffic prioritization
  - E.g., authenticated sessions may be prioritized
  - E.g., users during a payment process may be prioritized
- Headchecks and performance measures to detect SLA violations
- Non-repudiation mechanisms vs account protection

- OWASP Denial of Service Cheat Sheet (DRAFT)

Mitigation of vulnerabilities and violations

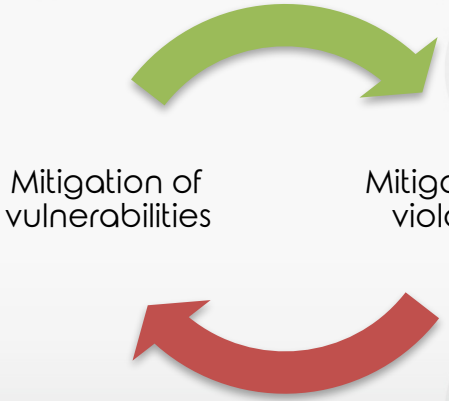
AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | INTEGRITY | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS



Mitigation of vulnerabilities and violations

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | INTEGRITY | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

A6:2017 - Security Misconfiguration

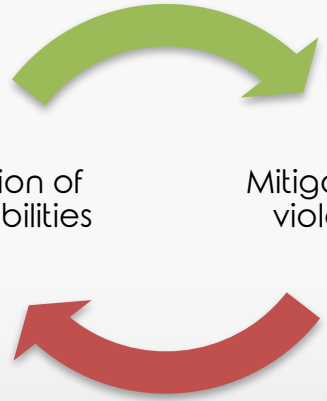


Mitigation of vulnerabilities and violations

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | INTEGRITY | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

A6:2017 - Security Misconfiguration

A9:2017 - Using Components with Known Vulnerabilities



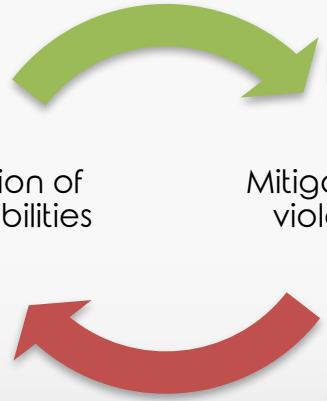
Mitigation of vulnerabilities and violations

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | INTEGRITY | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

A10:2017 – Insufficient Logging & Monitoring

A6:2017 - Security Misconfiguration

A9:2017 - Using Components with Known Vulnerabilities

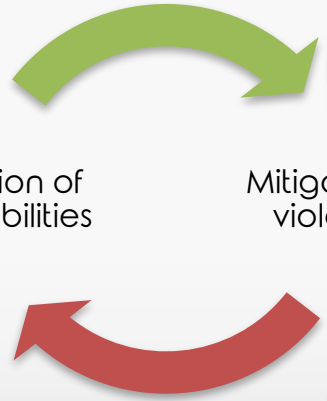


Mitigation of vulnerabilities and violations

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | INTEGRITY | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

A6:2017 - Security Misconfiguration

A9:2017 - Using Components with Known Vulnerabilities



A10:2017 – Insufficient Logging & Monitoring

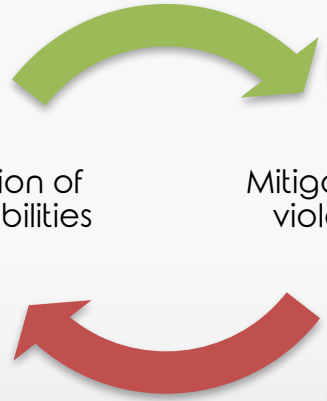
Anomaly-based detection

Mitigation of vulnerabilities and violations

AUTHENTICATION | ACCESS CONTROL | CONFIDENTIALITY | INTEGRITY | AVAILABILITY | MITIGATION OF VULNERABILITIES AND VIOLATIONS

A6:2017 - Security Misconfiguration

A9:2017 - Using Components with Known Vulnerabilities



A10:2017 – Insufficient Logging & Monitoring

Anomaly-based detection

Smart Load Balancing Web Application Firewall

TOP 10 Threats and Key Security Violations

TOP 10 Threat 2017	Security Violation
1. Injection	 Integrity (Data→Code)
2. Broken Authentication	 Authentication
3. Sensitive Data Exposure	 Confidentiality
4. XML External Entities (XXE)	 Integrity (Data→Code)
5. Broken Access Control	 Access Control
6. Security Misconfiguration	 Mitigation of vulnerabilities & violations
7. Cross-Site Scripting (XSS)	 Integrity (Data→Code)
8. Insecure Deserialization	 Integrity (Data→Code)
9. Using Components with Known Vulnerabilities	 Mitigation of vulnerabilities & violations
10. Insufficient Logging & Monitoring	 Mitigation of vulnerabilities & violations

Key Security Violations and TOP 10 Threats

Security Violation	TOP 10 Threat 2017
Integrity (Data→Code)	 1. Injection
	 4. XML External Entities (XXE)
	 7. Cross-Site Scripting (XSS)
	 8. Insecure Deserialization
Authentication	 2. Broken Authentication
Confidentiality	 3. Sensitive Data Exposure
Access Control	 5. Broken Access Control
Mitigation of vulnerabilities & violations	 6. Security Misconfiguration
	 9. Using Components with Known Vulnerabilities
	 10. Insufficient Logging & Monitoring
Availability	 - (*)

(*) Last appearance in 2004: A9. Application Denial of Service

Thanks!

Questions are more than welcome

igino.corona <at> pluribus-one.it

Pluribus One

seeing one in many

Pluribus One S.r.l.
Via Vincenzo Bellini 9, Cagliari (CA), Italy
Via Emilio Segrè, 17, Elmas (CA), Italy
www.pluribus-one.it