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

- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY

core

of system and data
Key Security Requirements

- AUTHENTICATION
- ACCESS CONTROL
- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY

of system and data
Key Security Requirements

- INTEGRITY
- CONFIDENTIALITY
- AVAILABILITY
- AUTHENTICATION
- ACCESS CONTROL

Functional

Core

Meta-process

Mitigation of vulnerabilities and violations

of system and data
Authentication

Who are you?
Authentication

Who are you?

strongly relies on

AUTHENTICATION  ACCESS CONTROL  CONFIDENTIALITY  INTEGRITY  AVAILABILITY

MITIGATION OF VULNERABILITIES AND VIOLATIONS

OWASP
Open Web Application Security Project

3
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, ...
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, ...

Reset password

Fill in one of the fields to receive a temporary password via email.

⚠️ There is no user by the name "admin". Usernames are case sensitive. Check your spelling, or create a new account.

Username:
admin

Email address:
admin@owasp.org

Reset password
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, ...

impersonation
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, ...

impersonation

credentials

AUTHENTICATION

bypass

ACCESS CONTROL
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, ...

credentials bypass

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

MITIGATION OF VULNERABILITIES AND VIOLATIONS

INTEGRITY
CONFIDENTIALITY
AVAILABILITY
ACCESS CONTROL
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, ...
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)
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)
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)

impersonation

suspicious auth

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)

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

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

Access Denied

You don't have permission to access "http://www.paypal.com/signin?" on this server.
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
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

MITIGATION OF 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
- Strong data encryption and hashing
- No caching

**INTEGRITY**
**CONFIDENTIALITY**
**AVAILABILITY**
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

Authentication

Access Control

Integrity

Availability

Mitigation of vulnerabilities and violations

INTEGRITY
CONFIDENTIALITY
AVAILABILITY
AUTHENTICATION
ACCESS CONTROL

MITIGATION OF VULNERABILITIES AND VIOLATIONS

CONNECT.
LEARN.
GROW.

violate

access

discovery
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**

**OWASP Top 10-2017 A6-Security Misconfiguration**
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 interpreted as code!
Integrity

TOP 10 threats 2017
• Injection
• XML External Entities
• Cross-Site Scripting
• Insecure Deserialization

Is there a common root cause for all the above integrity threats?
– Yes, inadequate or missing input handling
  • Input data can be arbitrarily interpreted as code!

Other threats (examples)
• Unvalidated Redirects and Forwards
• HTTP Response Splitting
• Malicious File Execution
• Buffer Overflow
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 interpreted as code!
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 interpreted 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

Normal Data → Code functionalities

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

Integrity

Normal Data ➔ Code functionalities
• E.g. Google URL redirect service
  – used to track “clicks”


Click!
redirect

https://www.pluribus-one.it
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

Indirizzo IP, Luogo: 180.162.205.30, China – Shanghai

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

Se recentemente 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](https://www.google.com/url?q=http://phishing.url).

Cordiali saluti,

Supporto Apple
Normal Data $\rightarrow$ 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?

Secure API (code)

Contextual data

Secure API (code)
Integrity

How to deal with Data $\rightarrow$ Code threats?

Contextual data

Secure API (code)

Interpreter

Authorized only

data $\rightarrow$ code

MITIGATION OF VULNERABILITIES AND VIOLATIONS

INTEGRITY

AUTHENTICATION

ACCESS CONTROL

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

Secure API

Interpreter

Authorized only

any security requirement

How to deal with Data $\rightarrow$ 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
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
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

Mitigation of vulnerabilities

Mitigation of violations
Mitigation of vulnerabilities and violations

A6:2017 - Security Misconfiguration

Mitigation of vulnerabilities

Mitigation of violations
Mitigation of vulnerabilities and violations

A6:2017 - Security Misconfiguration
A9:2017 - Using Components with Known Vulnerabilities

Mitigation of vulnerabilities

Mitigation of violations
Mitigation of vulnerabilities and violations

- Mitigation of violations: A10:2017 – Insufficient Logging & Monitoring
- Mitigation of vulnerabilities:
  - A6:2017 - Security Misconfiguration
  - A9:2017 - Using Components with Known Vulnerabilities
Mitigation of vulnerabilities and violations

- **Authentication**
- **Access Control**
- **Confidentiality**
- **Integrity**
- **Availability**

**A6:2017** - Security Misconfiguration

**A9:2017** - Using Components with Known Vulnerabilities

**A10:2017** – Insufficient Logging & Monitoring

Anomaly-based detection

Mitigation of vulnerabilities

Mitigation of violations
Mitigation of vulnerabilities and violations

**A6:2017** - Security Misconfiguration

**A9:2017** - Using Components with Known Vulnerabilities

Mitigation of vulnerabilities

Mitigation of violations

**A10:2017** – Insufficient Logging & Monitoring

Anomaly-based detection

Smart Load Balancing

Web Application Firewall
## TOP 10 Threats and Key Security Violations

<table>
<thead>
<tr>
<th>TOP 10 Threat 2017</th>
<th>Security Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Injection</td>
<td>Integrity (Data→Code)</td>
</tr>
<tr>
<td>2. Broken Authentication</td>
<td>Authentication</td>
</tr>
<tr>
<td>3. Sensitive Data Exposure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>4. XML External Entities (XXE)</td>
<td>Integrity (Data→Code)</td>
</tr>
<tr>
<td>5. Broken Access Control</td>
<td>Access Control</td>
</tr>
<tr>
<td>6. Security Misconfiguration</td>
<td>Mitigation of vulnerabilities &amp; violations</td>
</tr>
<tr>
<td>7. Cross-Site Scripting (XSS)</td>
<td>Integrity (Data→Code)</td>
</tr>
<tr>
<td>8. Insecure Deserialization</td>
<td>Integrity (Data→Code)</td>
</tr>
<tr>
<td>9. Using Components with Known Vulnerabilities</td>
<td>Mitigation of vulnerabilities &amp; violations</td>
</tr>
<tr>
<td>10. Insufficient Logging &amp; Monitoring</td>
<td>Mitigation of vulnerabilities &amp; violations</td>
</tr>
</tbody>
</table>
# Key Security Violations and TOP 10 Threats

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

(*) 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