

Enterprise Security

API

ESAPI





parler haut
interagir librement



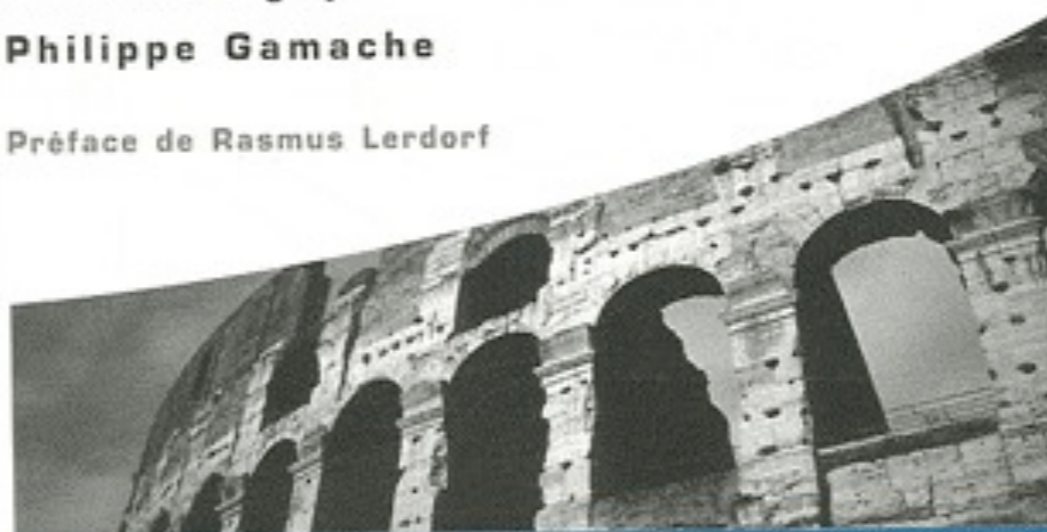
Sécurité PHP 5 et MySQL

2^e édition

Damien Seguy

Philippe Gamache

Préface de Rasmus Lerdorf



EYROLLES

 parler haut
interagir librement





I answer question



parler haut
interagir librement

The problems



The problems

- Input Validation and Output Encoding
- Authentication and Identity
- URL Access Control
- Business Function Access Control
- Data Layer Access Control



The problems

- Presentation Layer Access Control
- Errors, Logging, and Intrusion Detection
- Encryption, Hashing, and Randomness



OWASP TOP 10

A1 – Injection

A2 – Cross-Site Scripting
(XSS)

A3 – Broken Authentication
and Session Management

A4 – Insecure Direct
Object References

A5 – Cross-Site Request
Forgery (CSRF)

A6 – Security
Misconfiguration

A7 – Insecure
Cryptographic Storage

A8 - Failure to Restrict
URL Access

A9 - Insufficient Transport
Layer Protection

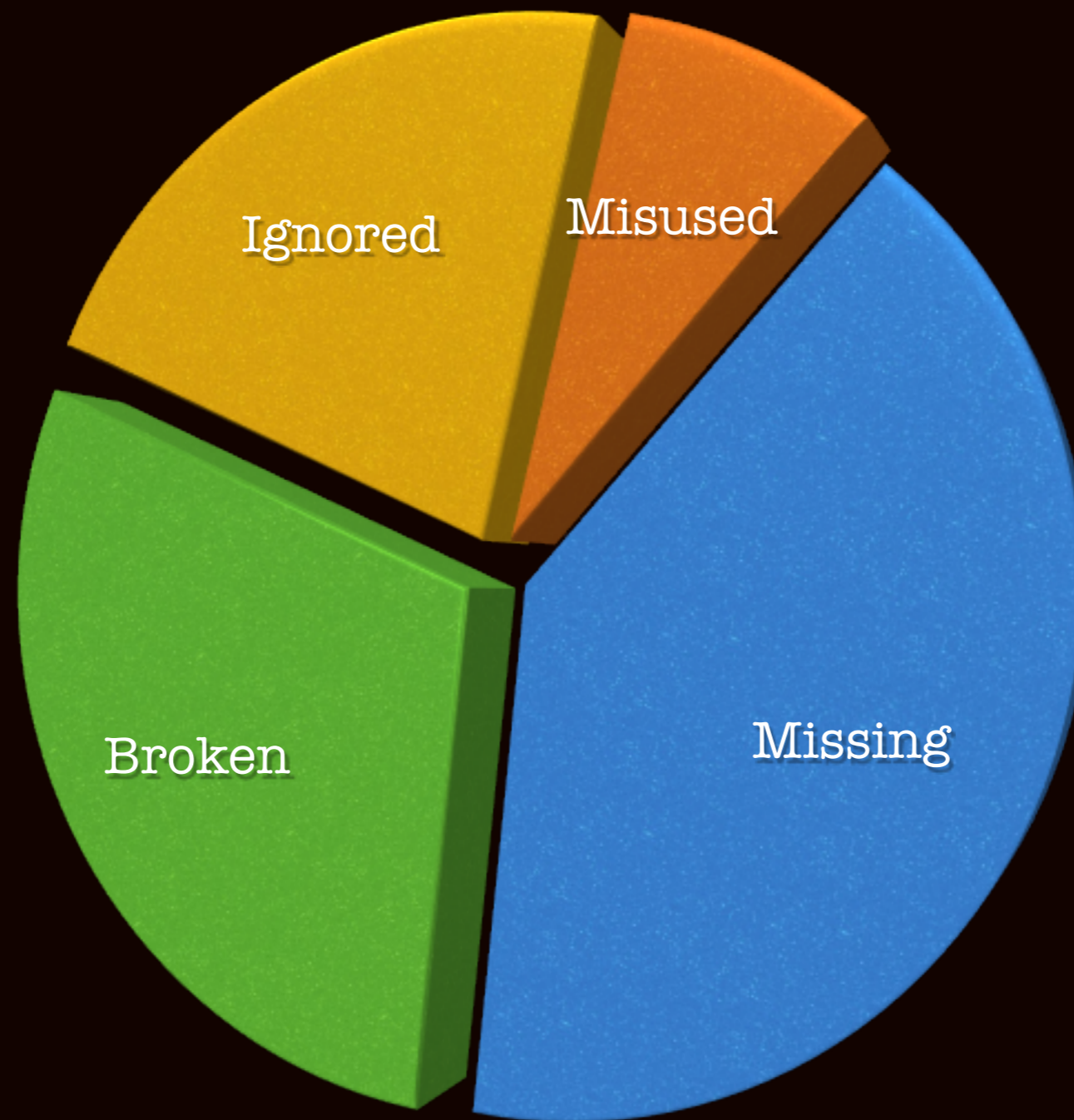
A10 – Unvalidated
Redirects and Forwards



And over 300
others security
problems types

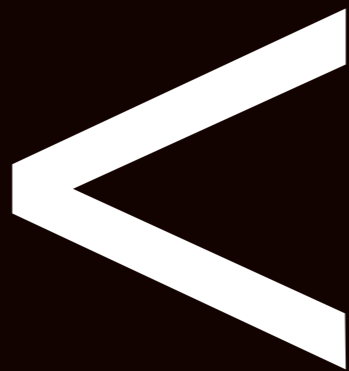


Vulnerabilities and Security Controls



Why Input Validation Is Hard?





 parler haut
interagir librement

Percent (url) Encoding

- %3c
- %3C



HTML Entity Encoding

- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`



HTML Entity Encoding

- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`



HTML Entity Encoding

- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`



HTML Entity Encoding

- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`



HTML Entity Encoding

- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`
- `<`



HTML Entity Encoding

- <
- <
- <
- <
- <
- <
- <
- <
- <
- <
- <
- <



JavaScript Escape

- `<`
- `\x3c`
- `\X3c`
- `\u003c`
- `\U003c`
- `\x3C`
- `\X3C`
- `\u003C`
- `\U003C`



CSS Escape

- `\3c`
- `\03c`
- `\003c`
- `\0003c`
- `\00003c`
- `\3C`
- `\03C`
- `\003C`
- `\0003C`
- `\00003C`



UTF-7 vs UTF-8

- +ADw-
- %c0%bc
- %e0%80%bc
- %f0%80%80%bc
- %f8%80%80%80%bc
- %fc%80%80%80%80%bc



1,677,721,600,000,000

ways to encode <script>



The Solutions?



What is Enterprise Security API?



ESAPI Community

Communauté ESAPI

Library

Wiki

Mailing List

Users

Developers



Objective-C

ESAPI Community

Communauté ESAPI

Library

Wiki

Mailing List

Users

Developers



Objective-C

ESAPI Community

Communauté ESAPI

Library

Wiki

Mailing List

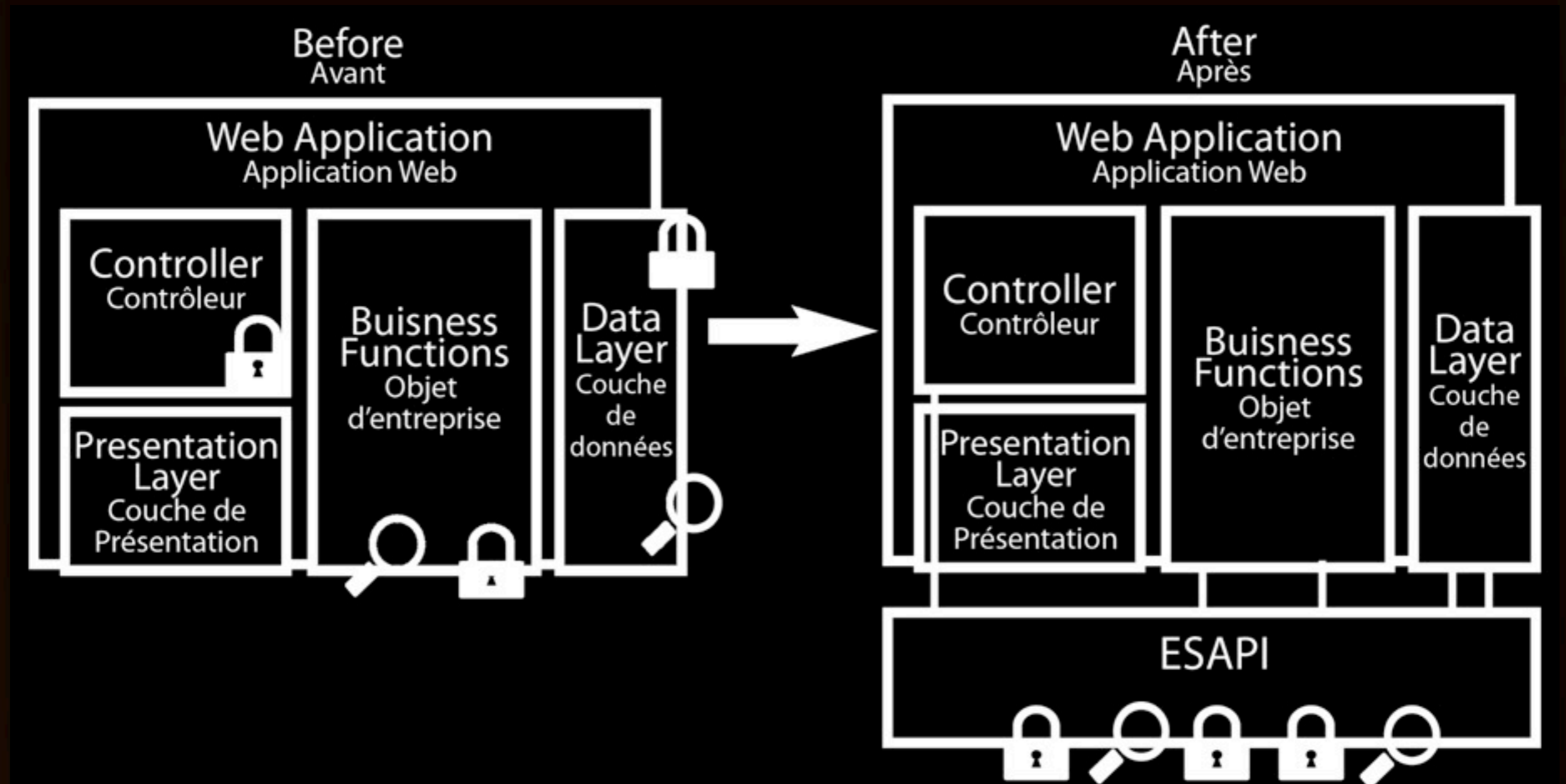


Users

Developers



Overview of the Architectural Impact



Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration



Entreprise Security API

Authenticator

User

AccessController

AccessReferenceMap

`isAuthorizedForData()`
`isAuthorizedForFile()`
`isAuthorizedForFunction()`
`isAuthorizedForService()`
`isAuthorizedForURL()`

Validator

Encoder

HTTPUtilities

Encoder

EncryptedReference

Randomizer

ExceptionHandler

Logger

IntrusionDetector

SecurityConfiguration



Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration



Entreprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

```
<?php echo $ESAPI  
->validator()  
->getValidInput(  
    String $context,  
    String $input,  
    String type,  
    int $maxLength,  
    boolean allowNull,  
    ValidationErrorList  
    $errorList);
```

?>

IntrusionDetector

SecurityConfiguration



Entreprise Security API

interface
ValidationRule



abstract
BaseValidationRule



CreditCard
ValidationRule

Validator

```
assertIsValidHttpRequest()  
assertIsValidHttpRequest  
ParameterSet()  
assertIsValidFileUpload()  
  
getValidDate()  
getValidDouble()  
getValidDirectoryPath()  
getValidDouble()  
getValidFileContent()  
getValidFileName()
```



Entreprise Security API

interface
ValidationRule



abstract
BaseValidationRule



CreditCard
ValidationRule

Validator

```
isValidCreditCard()  
isValidDataFromBrowse()  
isValidDirectoryPath()  
isValidFileContent()  
isValidFileName()  
isValidHTTPRequest()  
isValidListItem()  
isValidRedirectLocation()  
isValidSafeHTML()  
isValidPrintable()  
safeReadLine()
```

IntrusionDetector

SecurityConfiguration

Entreprise Security API

encodeForCSS
encodeForDN
encodeForHTML
encodeForLDAP
encodeForSQL
encodeForURL
encodeForXML
encodeForXPath

Encoder

```
<?php echo $ESAPI  
->encoder()  
->encodeForHTML($name)  
>
```

encodeForJavaScript
encodeForHTMLAttribute
encodeForVBScript
encodeForXMLAttribute
encodeForXPath



Entreprise Security API

- Add Safe Header
- No Cache Headers
- Set Content Type
- Add Safe Cookie
- Kill Cookie
- Change SessionID
- CSRF Tokens

HTTPUtilities

- **isSecureChannel**
- Safe Request Logging
- Safe File Uploads
- **sendSafeForward**
- **sendSafeRedirect**
- Encrypt State in Cookie
- Hidden Field Encryption
- Querystring Encryption



Enterprise Security API

```
<?php $encrypted =  
$ESAPI->encryptor()-  
->encrypt($text)
```

Encryptor

- Integrity Seals
- Strong GUID
- Random Tokens
- Encryption
- Digital Signatures
- Salted Hash

- Safe Config Details
- Timestamp



Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration



Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration



Entreprise Security API

- `AccessControlException`
- `AuthenticationException`
- `AvailabilityException`
- `EncodingException`
- `EncryptionException`
- `ExecutorException`
- `IntegrityException`
- `IntrusionException`
- `ValidationException`

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration



Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration



Entreprise Security API

- Configurable Thresholds
- Responses
 - Log Intrusion
 - Logout User
 - Disable Account

Authenticator

AccessController

AccessRuleReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration



Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration



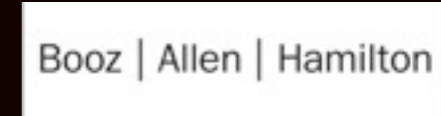
OWASP TOP 10	ESAPI
A1: Injection	Encoder
A2: Cross Site Scripting (XSS)	Encoder, Validator
A3: Broken Authentication and Session Management	Authenticator, User, HTTPUtilities
A4: Insecure Direct Object Reference	AccessReferenceMap, AccessController
A5: Cross Site Request Forgery (CSRF)	User (CSRF Token)
A6: Security Misconfiguration	SecurityConfiguration
A7: Insecure Cryptographic Storage	Encryptor
A8: Failure to Restrict URL Access	AccessController
A9: Insufficient Transport Layer Protection	HTTPUtilities (Secure Cookie, Channel)
A10: Unvalidated Redirects and Forwards	AccessController



										Objective -C
Authentication	2.0	1.4	1.4	1.4						
Identity	2.0	1.4	1.4	1.4						
Access Control	2.0	1.4	1.4	1.4	1.4					
Input Validation	2.0	1.4	1.4	1.4	1.4	1.4	2.0			
Output Escaping	2.0	1.4	1.4	1.4		1.4	2.0			
Canonicalization	2.0	1.4	1.4	1.4		1.4	2.0			
Encryption	2.0	1.4	1.4	1.4	1.4					
Random Numbers	2.0	1.4	1.4	1.4	1.4					
Exception Handling	2.0	1.4	1.4	1.4	1.4	1.4	2.0			
Logging	2.0	1.4	1.4	1.4	1.4	1.4	2.0			
Intrusion Detection	2.0	1.4	1.4	1.4						
Security Configuration	2.0	1.4	1.4	1.4	1.4	1.4	2.0			
WAF	2.0									



Adopters




Additional Resources

- OWASP Home Page
<http://www.owasp.org>
- ESAPI Project Page
<http://www.esapi.org>
- ESAPI-Users Mailing List
[https://lists.owasp.org/mailman/
listinfo/esapi-users](https://lists.owasp.org/mailman/listinfo/esapi-users)
- ESAPI-Dev Mailing List
[https://lists.owasp.org/mailman/
listinfo/esapi-dev](https://lists.owasp.org/mailman/listinfo/esapi-dev)



Questions ?

- philippe@ph-il.ca
- <http://www.ph-il.ca>
- @SecureSymfony 
- <http://www.ph-il.ca/en/conferences>
- <http://www.ph-il.ca/fr/conferences>



You are free:



to **Share** — to copy, distribute and transmit the work

Under the following conditions:



Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).



Noncommercial. You may not use this work for commercial purposes.



No Derivative Works. You may not alter, transform, or build upon this work.

- For any reuse or distribution, you must make clear to others the licence terms of this work.
- Any of the above conditions can be waived if you get permission from the copyright holder.
- The author's moral rights are retained in this licence.

