Solving Real-World Problems with an Enterprise Security API (ESAPI)

Jim Manico
OWASP Board Member

OWASP
AppSec 2103

Solving Real World Problems with An Enterprise Security API (ESAPI)

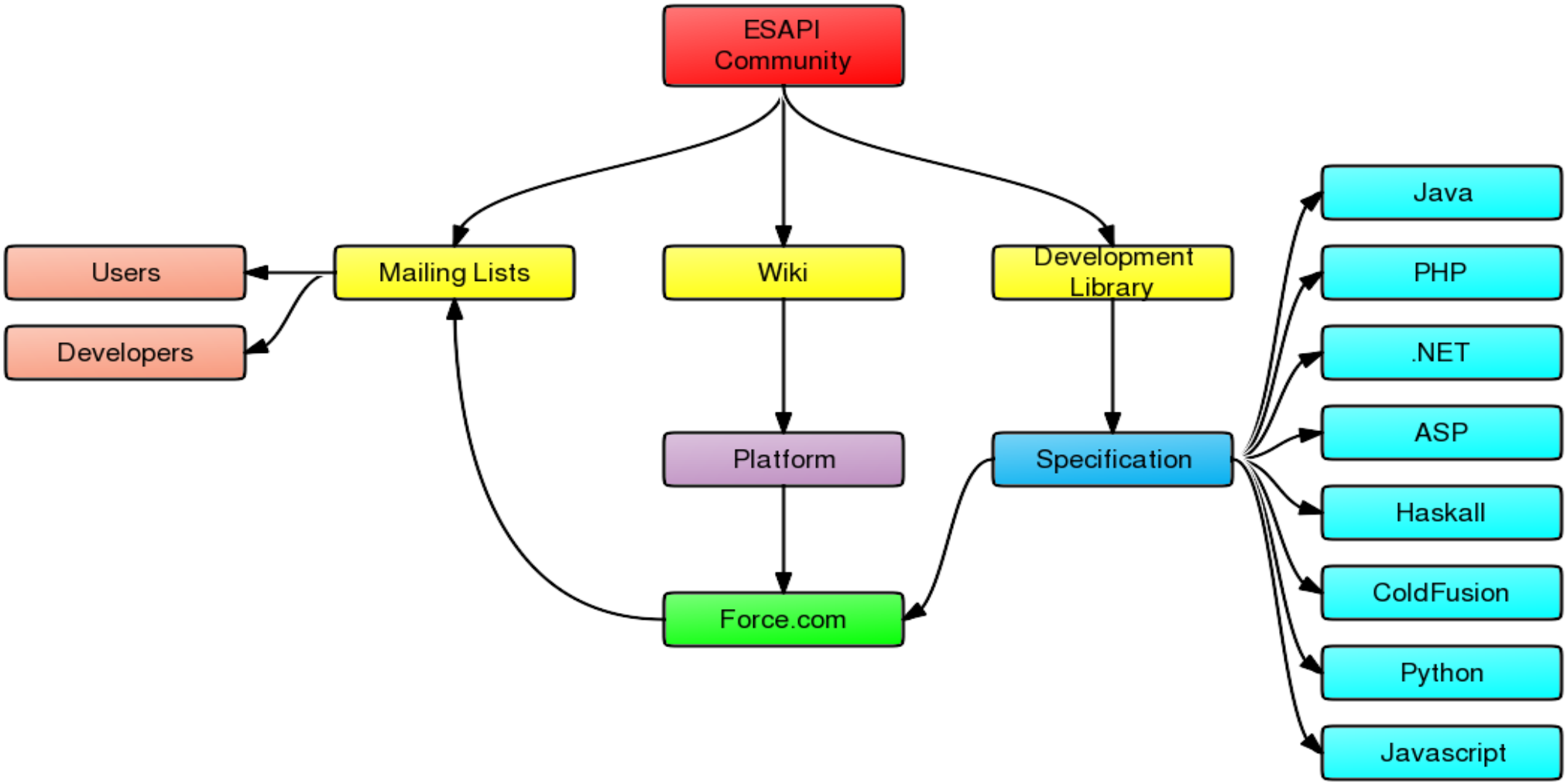
- What is an ESAPI?
- Using OWASP ESAPI
- Case Study: Cross Site Scripting
- Case Study: Direct Object Reference
- Case Study: Yours!
- Additional Resources
- Questions?

Solving Real World Problems with An Enterprise Security API (ESAPI)

- **What is an ESAPI?**

What is an Enterprise Security API?

The ESAPI Family Community Breakdown



What is an Enterprise Security API?

- High-Level API that provides access to common security functions as services to the calling code.
- Centrally configured to keep configuration separate from implementation.
- Developers don't have to focus on writing custom security controls for components.
- Compliments a Secure Software Development Environment and Secure Coding Conventions
- Enforces a common API (interfaces) but also allows customization or extension to adapt to specific environments.

What is an Enterprise Security API?

Addressing The OWASP Top Ten

OWASP Top Ten	OWASP 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
A10: Unvalidated Redirects and Forwards	AccessController

Solving Real World Problems with An Enterprise Security API (ESAPI)

- What is an ESAPI?
- **Using OWASP ESAPI**

Solving Real World Problems with An Enterprise Security API (ESAPI)

Getting OWASP's ESAPI (Java)

Download from Google Code:

http://owasp-esapi-java.googlecode.com

Use Maven:

```
<dependencies>
   <dependency>
      <groupId>org.owasp.esapi</groupId>
      <artifactId>esapi</artifactId>
   </dependency>
</dependencies>
```

Solving Real World Problems with An Enterprise Security API (ESAPI)

Basics

OWASP ESAPI Uses a Service Locator class to access implementations of core interfaces. This locator is currently configured via the ESAPI.properties file.

- ESAPI.encoder()
- ESAPI.encryptor()
- ESAPI.validator()
- ESAPI.accessController()
- ESAPI.logger()
- ESAPI.authenticator()
- ESAPI.randomizer()
- ESAPI.httpUtilities()

Solving Real World Problems with An Enterprise Security API (ESAPI)

- What is an ESAPI?
- Using OWASP ESAPI
- **Case Study: Cross Site Scripting**

Solving Real World Problems with An Enterprise Security API (ESAPI)

The Problem

Contact Form is vulnerable to XSS

The Solution

```
<% String fullname = StringUtilities.replaceNull( request.getParameter( “firstname” ), “” ); %>
<form action=“/SubmitContactInformation” method=“POST”>
  <input type=“text” name=“fullname” id=“full-name” value=“<%=ESAPI.encoder().encodeForHTMLAttribute(fullname)%>”>
  <label for=“full-name”>Full Name</label>
</form>
```

Solving Real World Problems with An Enterprise Security API (ESAPI)

- What is an ESAPI?
- Using OWASP ESAPI
- Case Study: Cross Site Scripting
- **Case Study: Direct Object Reference**

Solving Real World Problems with An Enterprise Security API (ESAPI)

The Problem

Direct Reference to File allows writing to Filesystem

Behavior:

1. Servlet POSTs to /save.action
2. Filename is stored in a hidden form field
3. Content is entered through a textfield on the page

Post looks like:

```
POST /save.action HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 35

filename=user-info.txt&content=test
```

Solving Real World Problems with An Enterprise Security API (ESAPI)

The Solution

```
class SaveFileServlet extends HttpServlet {
   // List of accessible files
   static Set<String> VALID_FILES = new HashSet<String>();
   // add file paths to set

   public void doPost( … ) {
      AccessReferenceMap<String> filemap = ESAPI.httpUtilities().getSessionAttribute(“valid-files”);
      if ( filemap == null ) {
         filemap = new RandomAccessReferenceMap();
         filemap.addAll(VALID_FILES);
         request.setAttribute(“valid-files”, filemap);
      } else {
         String fileToken = request.getParameter(“fileToken”);
         String filename = filemap.get(filetoken);
         if ( filename == null ) {
            throw new EnterpriseSecurityException(…);
         } else {
            String content = request.getParameter(“content”);
            if ( ESAPI.validator().isValidInput( “SaveFile”, content, “FileContent”, 512, true ) ) {
               // .. Save file
            } else {
               throw EnterpriseSecurityException(…);
            }
         }
      }
   }
}
```

Solving Real World Problems with An Enterprise Security API (ESAPI)

The Solution - Continued

```
<%
   AccessReferenceMap<String> validFiles = ESAPI.httpUtilities().getRequestAttribute("valid-files");
   String fileToken = validFiles.getIndirectReference("user-info.txt");
   String existingContent = FileHelper.readFile( validFiles.getDirectReference(fileToken));
%>
<form action="/save.action" method="POST">
   <input type="hidden" name="fileToken" value="<%=ESAPI.encoder().encodeForHTMLAttribute(fileToken)%>"/>
   <textarea cols="50" rows="4" name="content">
      <%=ESAPI.encoder().encodeForHTML(existingContent)%>
   </textarea>
   <input type="submit"/>
</form>
```

Solving Real World Problems with An Enterprise Security API (ESAPI)

- What is an ESAPI?
- Using OWASP ESAPI
- Case Study: Cross Site Scripting
- Case Study: Direct Object Reference
- **Case Study: Yours!**

Solving Real World Problems with An Enterprise Security API (ESAPI)

The Problem

YOU TELL ME!

Describe a problem or requirement that you have encountered and let's discuss how using an ESAPI you could resolve the issue, or meet the requirement.

Solving Real World Problems with An Enterprise Security API (ESAPI)

- What is an ESAPI?
- Using OWASP ESAPI
- Case Study: Cross Site Scripting
- Case Study: Direct Object Reference
- Case Study: Yours!
- **Additional Resources**

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
- **ESAPI-Dev Mailing List**
  - https://lists.owasp.org/mailman/listinfo/esapi-dev
- **E-Mail Me**
  - chris.schmidt@aspectsecurity.com
- **Follow me on Twitter**
  - http://twitter.com/carne

Solving Real World Problems with An Enterprise Security API (ESAPI)

- What is an ESAPI?
- Using OWASP ESAPI
- Case Study: Cross Site Scripting
- Case Study: Direct Object Reference
- Case Study: Yours!
- Additional Resources
- **Questions?**