Web Service Security Cheat Sheet

From OWASP

Contents

Introduction

This article is focused on providing guidance to securing web services and preventing web services related attacks.

1. Transport Confidentiality

All communication with and between web services containing sensitive features, an authenticated session, or transfer of sensitive data must be encrypted using well configured TLS. For more information see Transport Layer Protection Cheat Sheet

2. Transport Authentication

3. Transport Encoding

4. Message Authentication

5. Message Integrity

6. Message Confidentiality

7. Authorization

Web services need to authorize web service clients the same way web applications authorize users. A web service needs to make sure a web service client is authorized to perform a certain action.

RULE - A web service should authorize its clients whether they have access to the method in question. This can be done using one of the following methods:

- Having clients authorize to the web service using username and password
- Having clients authorize to the web service using client certificates

8. Schema Validation

Schema validation enforces constraints, syntax and semantics defined by the schema.

RULE - Web services must validate SOAP payloads against the web service schema.

9. Content Validation

RULE - Like any web application, web services need to validate input before consuming it. Content validation include:

- Validation against malformed XML entities
- Validation against XML Bomb attacks
- Validating inputs using a strong white list
- Validating against external entity attacks

10. Output Encoding

Web services need to ensure that output sent to clients is encoded to be consumed as data and not as scripts. This gets pretty important when web service clients use the output to render HTML pages either directly or indirectly using AJAX objects.

RULE - All the rules of output encoding applies as per XSS (Cross_Site_Scripting) Prevention CheatSheet

11. Virus Protection

SOAP provides the ability to attach files and document to SOAP messages. This gives the opportunity for hackers to attach viruses and malware to these SOAP messages.

RULE - SOAP messages must be scanned against viruses and malware.

12. Message Size

Web services like web applications could be a target for DOS attacks by automatically sending the web services thousands of large size SOAP messages. This either cripples the application making it unable to respond to legitimate messages or it could take it down entirely.

RULE - SOAP Messages size should be limited to an appropriate size limit. Larger size limit (or no limit at all) increases the chances of a successful DOS attack.

13. Message Throughput

14. Identity, key, cert, provisioning

15. Endpoint Security Profile

16. Audit Logging

18. Software Engineering Assurance

19. XML Denial of Service Protection

20. Testing

Other Articles in the OWASP Cheat Sheet Series

- Authentication Cheat Sheet
- Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet
- Cryptographic Storage Cheat Sheet
- Input Validation Cheat Sheet
- DOM based XSS Prevention Cheat Sheet
- Forgot Password Cheat Sheet
- HTML5 Security Cheat Sheet
- SQL Injection Prevention Cheat Sheet
- Security Architecture Cheat Sheet
- Session Management Cheat Sheet
- Transport Layer Protection Cheat Sheet
- XSS (Cross Site Scripting) Prevention Cheat Sheet
- **Web Service Security Cheat Sheet**

Retrieved from "https://www.owasp.org/index.php
/Web_Service_Security_Cheat_Sheet"
Category: Cheatsheets