Sparrow 분석 보고서

Sparrow Cloud

요약 정보

프로젝트 이름	Demo Project
분석 ID	5291
분석 유형	URL
분석 시작 일시	2025-02-05 22:52:55
분석 완료 일시	2025-02-05 23:00:35
분석 시간	7분 39초
총 이슈 수	28

위험도별 이슈 수

매우 높음	높음	보통	낮음	매우 낮음
1	4	11	4	8

■ 레퍼런스별 이슈 수

레퍼런스 이름	총 이슈 수
.NET framework design guideline	0
CWE 658 4.14	0
CWE 658 4.7	0
CWE 659 4.14	0
CWE 659 4.7	0
CWE 660 4.14	0
CWE 660 4.7	0
Code conventions for the Java Programming Language(Oracle)	0
JavaScript 시큐어코딩 가이드 2022	0
MISRA-C 2004	0
MISRA-C 2012	0
MISRA-C 2012 Amendment 2	0
MISRA-C 2012 Amendment 3	0
MISRA-C++ 2008	0
OWASP 2017	11
OWASP 2021	8
Python 시큐어코딩 가이드 2022	0
Rust ANSSI guide v1.0	0
무기체계 소프트웨어 보안약점 점검 목록	0
방위사업청 코딩규칙	0
소프트웨어 보안약점 진단가이드 2021	1
주요정보통신기반시설 취약점 분석·평가 기준	1

● .NET framework design guideline

레퍼런스 항목 이름	이슈 수
System.Xml 사용법	0
구조체 디자인	0
네임스페이스의 이름	0
리소스 이름 지정	0
매개변수 이름 지정	0
멤버 오버로드	0
보호된 멤버	0

봉인	0
예외 throw	0
예외 및 성능	0
인터페이스 디자인	0
일반 명명 규칙	0
컬렉션	0
클래스와 구조체 간의 선택	0
표준 예외 형식 사용	0

CWE 658 4.14

레퍼런스 항목 이름	이슈 수
119 - Improper Restriction of Operations within the Bounds of a Memory Buffer	0
120 - Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	0
121 - Stack-based Buffer Overflow	0
122 - Heap-based Buffer Overflow	0
123 - Write-what-where Condition	0
124 - Buffer Underwrite ('Buffer Underflow')	0
125 - Out-of-bounds Read	0
126 - Buffer Over-read	0
127 - Buffer Under-read	0
128 - Wrap-around Error	0
129 - Improper Validation of Array Index	0
131 - Incorrect Calculation of Buffer Size	0
1325 - Improperly Controlled Sequential Memory Allocation	0
1335 - Incorrect Bitwise Shift of Integer	0
134 - Use of Externally-Controlled Format String	0
1341 - Multiple Releases of Same Resource or Handle	0
135 - Incorrect Calculation of Multi-Byte String Length	0
14 - Compiler Removal of Code to Clear Buffers	0
170 - Improper Null Termination	0
188 - Reliance on Data/Memory Layout	0
191 - Integer Underflow (Wrap or Wraparound)	0
192 - Integer Coercion Error	0
194 - Unexpected Sign Extension	0
195 - Signed to Unsigned Conversion Error	0

196 - Unsigned to Signed Conversion Error	0
197 - Numeric Truncation Error	0
242 - Use of Inherently Dangerous Function	0
243 - Creation of chroot Jail Without Changing Working Directory	0
244 - Improper Clearing of Heap Memory Before Release ('Heap Inspection')	0
362 - Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	0
364 - Signal Handler Race Condition	0
366 - Race Condition within a Thread	0
375 - Returning a Mutable Object to an Untrusted Caller	0
401 - Missing Release of Memory after Effective Lifetime	0
415 - Double Free	0
416 - Use After Free	0
457 - Use of Uninitialized Variable	0
462 - Duplicate Key in Associative List (Alist)	0
463 - Deletion of Data Structure Sentinel	0
464 - Addition of Data Structure Sentinel	0
467 - Use of sizeof() on a Pointer Type	0
468 - Incorrect Pointer Scaling	0
469 - Use of Pointer Subtraction to Determine Size	0
476 - NULL Pointer Dereference	0
478 - Missing Default Case in Multiple Condition Expression	0
479 - Signal Handler Use of a Non-reentrant Function	0
480 - Use of Incorrect Operator	0
481 - Assigning instead of Comparing	0
482 - Comparing instead of Assigning	0
483 - Incorrect Block Delimitation	0
484 - Omitted Break Statement in Switch	0
558 - Use of getlogin() in Multithreaded Application	0
560 - Use of umask() with chmod-style Argument	0
562 - Return of Stack Variable Address	0
587 - Assignment of a Fixed Address to a Pointer	0
676 - Use of Potentially Dangerous Function	0
685 - Function Call With Incorrect Number of Arguments	0
690 - Unchecked Return Value to NULL Pointer Dereference	0
704 - Incorrect Type Conversion or Cast	0

733 - Compiler Optimization Removal or Modification of Security-critical Code	0
762 - Mismatched Memory Management Routines	0
783 - Operator Precedence Logic Error	0
785 - Use of Path Manipulation Function without Maximum-sized Buffer	0
787 - Out-of-bounds Write	0
789 - Memory Allocation with Excessive Size Value	0
805 - Buffer Access with Incorrect Length Value	0
806 - Buffer Access Using Size of Source Buffer	0
839 - Numeric Range Comparison Without Minimum Check	0
843 - Access of Resource Using Incompatible Type ('Type Confusion')	0
910 - Use of Expired File Descriptor	0

CWE 658 4.7

레퍼런스 항목 이름	이슈 수
Access of Resource Using Incompatible Type ('Type Confusion') - (843)	0
Addition of Data Structure Sentinel - (464)	0
Assigning instead of Comparing - (481)	0
Assignment of a Fixed Address to a Pointer - (587)	0
Buffer Access Using Size of Source Buffer - (806)	0
Buffer Access with Incorrect Length Value - (805)	0
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') - (120)	0
Buffer Over-read - (126)	0
Buffer Under-read - (127)	0
Buffer Underwrite ('Buffer Underflow') - (124)	0
Comparing instead of Assigning - (482)	0
Compiler Optimization Removal or Modification of Security-critical Code - (733)	0
Compiler Removal of Code to Clear Buffers - (14)	0
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - (362)	0
Creation of chroot Jail Without Changing Working Directory - (243)	0
Deletion of Data Structure Sentinel - (463)	0
Double Free - (415)	0
Duplicate Key in Associative List (Alist) - (462)	0
Function Call With Incorrect Number of Arguments - (685)	0
Function Call With Incorrect Variable or Reference as Argument - (688)	0

Heap-based Buffer Overflow - (122)	0
Improper Cleanup on Thrown Exception - (460)	0
Improper Clearing of Heap Memory Before Release ('Heap Inspection') - (244)	0
Improper Handling of Length Parameter Inconsistency - (130)	0
Improper Null Termination - (170)	0
Improper Restriction of Operations within the Bounds of a Memory Buffer - (119)	0
Improper Update of Reference Count - (911)	0
Improper Validation of Array Index - (129)	0
Incorrect Block Delimitation - (483)	0
Incorrect Calculation of Buffer Size - (131)	0
Incorrect Calculation of Multi-Byte String Length - (135)	0
Incorrect Pointer Scaling - (468)	0
Incorrect Type Conversion or Cast - (704)	0
Integer Coercion Error - (192)	0
Integer Underflow (Wrap or Wraparound) - (191)	0
Mismatched Memory Management Routines - (762)	0
Missing Default Case in Switch Statement - (478)	0
NULL Pointer Dereference - (476)	0
Numeric Range Comparison Without Minimum Check - (839)	0
Numeric Truncation Error - (197)	0
Omitted Break Statement in Switch - (484)	0
Operator Precedence Logic Error - (783)	0
Out-of-bounds Read - (125)	0
Out-of-bounds Write - (787)	0
Race Condition within a Thread - (366)	0
Reliance on Data/Memory Layout - (188)	0
Return of Pointer Value Outside of Expected Range - (466)	0
Return of Stack Variable Address - (562)	0
Signal Handler Race Condition - (364)	0
Signal Handler Use of a Non-reentrant Function - (479)	0
Signed to Unsigned Conversion Error - (195)	0
Stack-based Buffer Overflow - (121)	0
Unexpected Sign Extension - (194)	0
Unsigned to Signed Conversion Error - (196)	0
Use After Free - (416)	0
Use of Expired File Descriptor - (910)	0

Use of Externally-Controlled Format String - (134)	0
Use of Incorrect Operator - (480)	0
Use of Inherently Dangerous Function - (242)	0
Use of Pointer Subtraction to Determine Size - (469)	0
Use of Potentially Dangerous Function - (676)	0
Use of Uninitialized Variable - (457)	0
Use of getlogin() in Multithreaded Application - (558)	0
Use of sizeof() on a Pointer Type - (467)	0
Use of umask() with chmod-style Argument - (560)	0
Wrap-around Error - (128)	0
Write-what-where Condition - (123)	0

CWE 659 4.14

레퍼런스 항목 이름	이슈 수
119 - Improper Restriction of Operations within the Bounds of a Memory Buffer	0
120 - Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	0
121 - Stack-based Buffer Overflow	0
122 - Heap-based Buffer Overflow	0
123 - Write-what-where Condition	0
124 - Buffer Underwrite ('Buffer Underflow')	0
125 - Out-of-bounds Read	0
126 - Buffer Over-read	0
127 - Buffer Under-read	0
128 - Wrap-around Error	0
129 - Improper Validation of Array Index	0
130 - Improper Handling of Length Parameter Inconsistency	0
131 - Incorrect Calculation of Buffer Size	0
1325 - Improperly Controlled Sequential Memory Allocation	0
1335 - Incorrect Bitwise Shift of Integer	0
134 - Use of Externally-Controlled Format String	0
1341 - Multiple Releases of Same Resource or Handle	0
135 - Incorrect Calculation of Multi-Byte String Length	0
14 - Compiler Removal of Code to Clear Buffers	0
170 - Improper Null Termination	0
188 - Reliance on Data/Memory Layout	0

191 - Integer Underflow (Wrap or Wraparound)	0
192 - Integer Coercion Error	0
194 - Unexpected Sign Extension	0
195 - Signed to Unsigned Conversion Error	0
196 - Unsigned to Signed Conversion Error	0
197 - Numeric Truncation Error	0
242 - Use of Inherently Dangerous Function	0
243 - Creation of chroot Jail Without Changing Working Directory	0
244 - Improper Clearing of Heap Memory Before Release ('Heap Inspection')	0
248 - Uncaught Exception	0
362 - Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	0
364 - Signal Handler Race Condition	0
366 - Race Condition within a Thread	0
374 - Passing Mutable Objects to an Untrusted Method	0
375 - Returning a Mutable Object to an Untrusted Caller	0
396 - Declaration of Catch for Generic Exception	0
397 - Declaration of Throws for Generic Exception	0
401 - Missing Release of Memory after Effective Lifetime	0
415 - Double Free	0
416 - Use After Free	0
457 - Use of Uninitialized Variable	0
462 - Duplicate Key in Associative List (Alist)	0
463 - Deletion of Data Structure Sentinel	0
464 - Addition of Data Structure Sentinel	0
467 - Use of sizeof() on a Pointer Type	0
468 - Incorrect Pointer Scaling	0
469 - Use of Pointer Subtraction to Determine Size	0
476 - NULL Pointer Dereference	0
478 - Missing Default Case in Multiple Condition Expression	0
479 - Signal Handler Use of a Non-reentrant Function	0
480 - Use of Incorrect Operator	0
481 - Assigning instead of Comparing	0
482 - Comparing instead of Assigning	0
483 - Incorrect Block Delimitation	0
484 - Omitted Break Statement in Switch	0

493 - Critical Public Variable Without Final Modifier	0
495 - Private Data Structure Returned From A Public Method	0
496 - Public Data Assigned to Private Array-Typed Field	0
498 - Cloneable Class Containing Sensitive Information	0
500 - Public Static Field Not Marked Final	0
543 - Use of Singleton Pattern Without Synchronization in a Multithreaded Context	0
558 - Use of getlogin() in Multithreaded Application	0
562 - Return of Stack Variable Address	0
587 - Assignment of a Fixed Address to a Pointer	0
676 - Use of Potentially Dangerous Function	0
690 - Unchecked Return Value to NULL Pointer Dereference	0
704 - Incorrect Type Conversion or Cast	0
733 - Compiler Optimization Removal or Modification of Security-critical Code	0
762 - Mismatched Memory Management Routines	0
766 - Critical Data Element Declared Public	0
767 - Access to Critical Private Variable via Public Method	0
783 - Operator Precedence Logic Error	0
785 - Use of Path Manipulation Function without Maximum-sized Buffer	0
787 - Out-of-bounds Write	0
789 - Memory Allocation with Excessive Size Value	0
805 - Buffer Access with Incorrect Length Value	0
806 - Buffer Access Using Size of Source Buffer	0
839 - Numeric Range Comparison Without Minimum Check	0
843 - Access of Resource Using Incompatible Type ('Type Confusion')	0
910 - Use of Expired File Descriptor	0

CWE 659 4.7

레퍼런스 항목 이름	이슈 수
Access of Resource Using Incompatible Type ('Type Confusion') - (843)	0
Access to Critical Private Variable via Public Method - (767)	0
Addition of Data Structure Sentinel - (464)	0
Assigning instead of Comparing - (481)	0
Assignment of a Fixed Address to a Pointer - (587)	0
Buffer Access Using Size of Source Buffer - (806)	0
Buffer Access with Incorrect Length Value - (805)	0

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') - (120)	0
Buffer Over-read - (126)	0
Buffer Under-read - (127)	0
Buffer Underwrite ('Buffer Underflow') - (124)	0
Comparing instead of Assigning - (482)	0
Compiler Optimization Removal or Modification of Security-critical Code - (733)	0
Compiler Removal of Code to Clear Buffers - (14)	0
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - (362)	0
Creation of chroot Jail Without Changing Working Directory - (243)	0
Critical Public Variable Without Final Modifier - (493)	0
Declaration of Catch for Generic Exception - (396)	0
Declaration of Throws for Generic Exception - (397)	0
Deletion of Data Structure Sentinel - (463)	0
Double Free - (415)	0
Duplicate Key in Associative List (Alist) - (462)	0
Heap-based Buffer Overflow - (122)	0
Improper Cleanup on Thrown Exception - (460)	0
Improper Clearing of Heap Memory Before Release ('Heap Inspection') - (244)	0
Improper Handling of Length Parameter Inconsistency - (130)	0
Improper Null Termination - (170)	0
Improper Restriction of Operations within the Bounds of a Memory Buffer - (119)	0
Improper Update of Reference Count - (911)	0
Improper Validation of Array Index - (129)	0
Incorrect Block Delimitation - (483)	0
Incorrect Calculation of Buffer Size - (131)	0
Incorrect Calculation of Multi-Byte String Length - (135)	0
Incorrect Pointer Scaling - (468)	0
Incorrect Type Conversion or Cast - (704)	0
Integer Coercion Error - (192)	0
Integer Underflow (Wrap or Wraparound) - (191)	0
Mismatched Memory Management Routines - (762)	0
Missing Default Case in Switch Statement - (478)	0
NULL Pointer Dereference - (476)	0
Numeric Range Comparison Without Minimum Check - (839)	0
Numeric Truncation Error - (197)	0

Omitted Break Statement in Switch - (484)	0
Operator Precedence Logic Error - (783)	0
Out-of-bounds Read - (125)	0
Out-of-bounds Write - (787)	0
Passing Mutable Objects to an Untrusted Method - (374)	0
Public Data Assigned to Private Array-Typed Field - (496)	0
Race Condition within a Thread - (366)	0
Reliance on Data/Memory Layout - (188)	0
Return of Pointer Value Outside of Expected Range - (466)	0
Return of Stack Variable Address - (562)	0
Returning a Mutable Object to an Untrusted Caller - (375)	0
Signal Handler Race Condition - (364)	0
Signal Handler Use of a Non-reentrant Function - (479)	0
Signed to Unsigned Conversion Error - (195)	0
Stack-based Buffer Overflow - (121)	0
Uncaught Exception - (248)	0
Unexpected Sign Extension - (194)	0
Unsigned to Signed Conversion Error - (196)	0
Use After Free - (416)	0
Use of Expired File Descriptor - (910)	0
Use of Externally-Controlled Format String - (134)	0
Use of Incorrect Operator - (480)	0
Use of Inherently Dangerous Function - (242)	0
Use of Pointer Subtraction to Determine Size - (469)	0
Use of Potentially Dangerous Function - (676)	0
Use of Uninitialized Variable - (457)	0
Use of getlogin() in Multithreaded Application - (558)	0
Use of sizeof() on a Pointer Type - (467)	0
Wrap-around Error - (128)	0
Write-what-where Condition - (123)	0

CWE 660 4.14

레퍼런스 항목 이름	이슈 수
102 - Struts: Duplicate Validation Forms	0
103 - Struts: Incomplete validate() Method Definition	0

104 - Struts: Form Bean Does Not Extend Validation Class	0
106 - Struts: Plug-in Framework not in Use	0
109 - Struts: Validator Turned Off	0
110 - Struts: Validator Without Form Field	0
111 - Direct Use of Unsafe JNI	0
1235 - Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations	0
1335 - Incorrect Bitwise Shift of Integer	0
1336 - Improper Neutralization of Special Elements Used in a Template Engine	0
1341 - Multiple Releases of Same Resource or Handle	0
191 - Integer Underflow (Wrap or Wraparound)	0
192 - Integer Coercion Error	0
197 - Numeric Truncation Error	0
209 - Generation of Error Message Containing Sensitive Information	0
245 - J2EE Bad Practices: Direct Management of Connections	0
246 - J2EE Bad Practices: Direct Use of Sockets	0
248 - Uncaught Exception	0
362 - Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	0
366 - Race Condition within a Thread	0
374 - Passing Mutable Objects to an Untrusted Method	0
375 - Returning a Mutable Object to an Untrusted Caller	0
382 - J2EE Bad Practices: Use of System.exit()	0
383 - J2EE Bad Practices: Direct Use of Threads	0
396 - Declaration of Catch for Generic Exception	0
397 - Declaration of Throws for Generic Exception	0
460 - Improper Cleanup on Thrown Exception	0
470 - Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	0
476 - NULL Pointer Dereference	0
478 - Missing Default Case in Multiple Condition Expression	0
481 - Assigning instead of Comparing	0
484 - Omitted Break Statement in Switch	0
486 - Comparison of Classes by Name	0
487 - Reliance on Package-level Scope	0
491 - Public cloneable() Method Without Final ('Object Hijack')	0

492 - Use of Inner Class Containing Sensitive Data	0
493 - Critical Public Variable Without Final Modifier	0
495 - Private Data Structure Returned From A Public Method	0
496 - Public Data Assigned to Private Array-Typed Field	0
498 - Cloneable Class Containing Sensitive Information	0
500 - Public Static Field Not Marked Final	0
502 - Deserialization of Untrusted Data	0
537 - Java Runtime Error Message Containing Sensitive Information	0
567 - Unsynchronized Access to Shared Data in a Multithreaded Context	0
568 - finalize() Method Without super.finalize()	0
572 - Call to Thread run() instead of start()	0
574 - EJB Bad Practices: Use of Synchronization Primitives	0
575 - EJB Bad Practices: Use of AWT Swing	0
576 - EJB Bad Practices: Use of Java I/O	0
577 - EJB Bad Practices: Use of Sockets	0
578 - EJB Bad Practices: Use of Class Loader	0
579 - J2EE Bad Practices: Non-serializable Object Stored in Session	0
580 - clone() Method Without super.clone()	0
581 - Object Model Violation: Just One of Equals and Hashcode Defined	0
582 - Array Declared Public, Final, and Static	0
583 - finalize() Method Declared Public	0
594 - J2EE Framework: Saving Unserializable Objects to Disk	0
595 - Comparison of Object References Instead of Object Contents	0
607 - Public Static Final Field References Mutable Object	0
608 - Struts: Non-private Field in ActionForm Class	0
609 - Double-Checked Locking	0
7 - J2EE Misconfiguration: Missing Custom Error Page	0
766 - Critical Data Element Declared Public	0
917 - Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	0
95 - Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	0

CWE 660 4.7

레퍼런스 항목 이름	이슈 수

Array Declared Public, Final, and Static - (582)	0
Assigning instead of Comparing - (481)	0
Call to Thread run() instead of start() - (572)	0
Cloneable Class Containing Sensitive Information - (498)	0
Comparison of Classes by Name - (486)	0
Comparison of Object References Instead of Object Contents - (595)	0
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - (362)	0
Critical Public Variable Without Final Modifier - (493)	0
Declaration of Catch for Generic Exception - (396)	0
Declaration of Throws for Generic Exception - (397)	0
Deserialization of Untrusted Data - (502)	0
Direct Use of Unsafe JNI - (111)	0
Double-Checked Locking - (609)	0
EJB Bad Practices: Use of AWT Swing - (575)	0
EJB Bad Practices: Use of Java I/O - (576)	0
EJB Bad Practices: Use of Sockets - (577)	0
Finalize() Method Without super.finalize() - (568)	0
Improper Cleanup on Thrown Exception - (460)	0
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') - (95)	0
J2EE Bad Practices: Direct Management of Connections - (245)	0
J2EE Bad Practices: Direct Use of Sockets - (246)	0
J2EE Bad Practices: Direct Use of Threads - (383)	0
J2EE Bad Practices: Use of System.exit() - (382)	0
NULL Pointer Dereference - (476)	0
Numeric Truncation Error - (197)	0
Object Model Violation: Just One of Equals and Hashcode Defined - (581)	0
Omitted Break Statement in Switch - (484)	0
Passing Mutable Objects to an Untrusted Method - (374)	0
Public Data Assigned to Private Array-Typed Field - (496)	0
Public Static Field Not Marked Final - (500)	0
Public Static Final Field References Mutable Object - (607)	0
Reliance on Package-level Scope - (487)	0
Returning a Mutable Object to an Untrusted Caller - (375)	0
Uncaught Exception - (248)	0

Use of Inner Class Containing Sensitive Data - (492)	0

Code conventions for the Java Programming Language(Oracle)

레퍼런스 항목 이름	이슈 수
04.1 Line Length	0
04.2 Wrapping Lines	0
05.1.1 Block Comments	0
05.1.2 Single-Line Comments	0
05.1.3 Trailing Comments	0
05.1.4 End-Of-Line Comments	0
05.2 Documentation Comments	0
06.1 Number Per Line	0
06.2 Initialization	0
06.3 Placement	0
06.4 Class and Interface Declarations	0
07.1 Simple Statements	0
07.2 Compound Statements	0
07.3 return Statements	0
07.4 if, if-else, if else-if else Statements	0
07.5 for Statements	0
07.6 while Statements	0
07.7 do-while Statements	0
07.8 switch Statements	0
07.9 try-catch Statements	0
08.1 Blank Lines	0
08.2 Blank Spaces	0
09.1 Package	0
09.2 Classes or Interface	0
09.3 Methods	0
09.4 Variables	0
09.5 Constants	0
10.1 Providing Access to Instance and Class Variables	0
10.2 Refferring to Class Variables and Methods	0
10.3 Constants	0
10.4 Variable Assignments	0

10.5.1 Parentheses	0
10.5.2 Returning Values	0
10.5.3 Expressions before '?' in the Conditional Operator	0

JavaScript 시큐어코딩 가이드 2022

레퍼런스 항목 이름	이슈 수
01.01. SQL 삽입	0
01.02. 코드 삽입	0
01.03. 경로 조작 및 자원 삽입	0
01.04. 크로스사이트 스크립트(XSS)	0
01.05. 운영체제 명령어 삽입	0
01.08. 부적절한 XML 외부 개체 참조	0
01.11. 크로스사이트 요청 위조(CSRF)	0
02.04. 취약한 암호화 알고리즘 사용	0
02.07. 충분하지 않은 키 길이 사용	0
02.08. 적절하지 않은 난수 값 사용	0
02.14. 솔트 없이 일방향 해쉬 함수 사용	0
03.01. 종료되지 않는 반복문 또는 재귀 함수	0
04.01. 오류 메시지 정보 노출	0
06.02. 제거되지 않고 남은 디버그 코드	0

MISRA-C 2004

레퍼런스 항목 이름	이슈 수
1.02 (Required) : No reliance shall be placed on undefined or unspecified behaviour.	0
1.04 (Required) : The compiler/linker shall be checked to ensure that 31 character significance and case sensitivity are supported for external identifiers.	0
10.03 (Required) : The value of a complex expression of integer type may only be cast to a type that is narrower and of the same signedness as the underlying type of the expression.	0
10.04 (Required) : The value of a complex expression of floating type may only be cast to a narrower floating type.	0
10.05 (Required) : If the bitwise operators ~ and << are applied to an operand of underlying type unsigned char or unsigned short, the result shall be immediately cast to the underlying type of the operand.	0
10.06 (Required) : A "U" suffix shall be applied to all constants of unsigned type.	0

11.01 (Required) : Conversions shall not be performed between a pointer to a function and any type other than an integral type.	0
11.02 (Required) : Conversions shall not be performed between a pointer to object and any type other than an integral type, another pointer to object type or a pointer to void.	0
11.03 (Advisory) : A cast should not be performed between a pointer type and an integral type.	0
11.04 (Advisory) : A cast should not be performed between a pointer to object type and a different pointer to object type.	0
11.05 (Required) : A cast shall not be performed that removes any const or volatile qualification from the type addressed by a pointer.	0
12.01 (Advisory) : Limited dependence should be placed on C's operator precedence rules in expressions.	0
12.02 (Required) : The value of an expression shall be the same under any order of evaluation that the standard permits.	0
12.03 (Required) : The sizeof operator shall not be used on expressions that contain side effects.	0
12.04 (Required) : The right hand operand of a logical && or || operator shall not contain side effects.	0
12.05 (Required) : The operands of a logical && or || shall be primary-expressions.	0
12.06 (Advisory) : The operands of logical operators (&&, || and !) should be effectively Boolean. Expressions that are effectively Boolean should not be used as operands to operators other than (&&, || and !).	0
12.07 (Required) : Bitwise operators shall not be applied to operands whose underlying type is signed.	0
12.08 (Required) : The right hand operand of a shift operator shall lie between zero and one less than the width in bits of the underlying type of the left hand operand.	0
12.09 (Required) : The unary minus operator shall not be applied to an expression whose underlying type is unsigned.	0
12.10 (Required) : The comma operator shall not be used.	0
12.11 (Advisory) : Evaluation of constant unsigned integer expressions should not lead to wrap-around.	0
12.12 (Required) : The underlying bit representations of floating-point values shall not be used.	0
12.13 (Advisory) : The increment (++) and decrement (--) operators should not be mixed with other operators in an expression.	0
13.01 (Required) : Assignment operators shall not be used in expressions that yield a Boolean value.	0

13.02 (Advisory) : Tests of a value against zero should be made explicit, unless the operand is effectively Boolean.	0
13.03 (Required) : Floating-point expressions shall not be tested for equality or inequality.	0
13.04 (Required) : The controlling expression of a for statement shall not contain any objects of floating type.	0
13.05 (Required) : The three expressions of a for statement shall be concerned only with loop control.	0
13.06 (Required) : Numeric variables being used within a for loop for iteration counting shall not be modified in the body of the loop.	0
13.07 (Required) : Boolean operations whose results are invariant shall not be permitted.	0
14.01 (Required) : There shall be no unreachable code.	0
14.02 (Required) : All non-null statements shall either : a) have at least one side-effect however executed, or b) cause control flow to change.	0
14.03 (Required) : Before preprocessing, a null statement shall only occur on a line by itself; it may be followed by a comment provided that the first character following the null statement is a white-space character.	0
14.04 (Required) : The goto statement shall not be used.	0
14.05 (Required) : The continue statement shall not be used.	0
14.06 (Required) : For any iteration statement there shall be at most one break statement used for loop termination.	0
14.07 (Required) : A function shall have a single point of exit at the end of the function.	0
14.08 (Required) : The statement forming the body of a switch, while, do ... while or for statement shall be a compound statement.	0
14.09 (Required) : An if (expression) construct shall be followed by a compound statement. The else keyword shall be followed by either a compound statement, or another if statement.	0
14.10 (Required) : All if ... else if constructs shall be terminated with an else clause.	0
15.01 (Required) : A switch label shall only be used when the most closely-enclosing compound statement is the body of a switch statement.	0
15.02 (Required) : An unconditional break statement shall terminate every non-empty switch clause.	0
15.03 (Required) : The final clause of a switch statement shall be the default clause.	0
15.04 (Required) : A switch expression shall not represent a value that is effectively Boolean.	0
15.05 (Required) : Every switch statement shall have at least one case clause.	0

16.01 (Required) : Functions shall not be defined with a variable number of arguments.	0
16.02 (Required) : Functions shall not call themselves, either directly or indirectly.	0
16.03 (Required) : Identifiers shall be given for all of the parameters in a function prototype declaration.	0
16.04 (Required) : The identifiers used in the declaration and definition of a function shall be identical.	0
16.05 (Required) : The identifiers used in the declaration and definition of a function shall be identical.	0
16.06 (Required) : The number of arguments passed to a function shall match the number of parameters.	0
16.07 (Advisory) : A pointer parameter in a function prototype should be declared as pointer to const if the pointer is not used to modify the addressed object.	0
16.08 (Required) : All exit paths from a function with non-void return type shall have an explicit return statement with an expression.	0
16.09 (Required) : A function identifier shall only be used with either a preceding &, or with a parenthesised parameter list, which may be empty.	0
16.10 (Required) : If a function returns error information, then that error information shall be tested.	0
17.01 (Required) : Pointer arithmetic shall only be applied to pointers that address an array or array element.	0
17.02 (Required) : Pointer subtraction shall only be applied to pointers that address elements of the same array.	0
17.03 (Required) : >, >=, <, <= shall not be applied to pointer types except where they point to the same array.	0
17.04 (Required) : Array indexing shall be the only allowed form of pointer arithmetic.	0
17.05 (Advisory) : The declaration of objects should contain no more than 2 levels of pointer indirection.	0
17.06 (Required) : The address of an object with automatic storage shall not be assigned to another object that may persist after the first object has ceased to exist.	0
18.01 (Required) : All structure and union types shall be complete at the end of a translation unit.	0
18.02 (Required) : An object shall not be assigned to an overlapping object.	0
18.04 (Required) : Unions shall not be used.	0
19.01 (Advisory) : #include statements in a file should only be preceded by other preprocessor directives or comments.	0
19.02 (Advisory) : Non-standard characters should not occur in header file names in	

#include directives.	0
19.03 (Required) : The #include directive shall be followed by either a <filename> or "filename" sequence.	0
19.04 (Required) : C macros shall only expand to a braced initialiser, a constant, a parenthesised expression, a type qualifier, a storage class specifier, or a do-while-zero construct.	0
19.05 (Required) : Macros shall not be #define'd or #undef'd within a block.	0
19.06 (Required) : #undef shall not be used.	0
19.07 (Advisory) : A function should be used in preference to a function-like macro.	0
19.08 (Required) : A function-like macro shall not be invoked without all of its arguments.	0
19.09 (Required) : Arguments to a function-like macro shall not contain tokens that look like preprocessing directives.	0
19.10 (Required) : In the definition of a function-like macro each instance of a parameter shall be enclosed in parentheses unless it is used as the operand of # or ##.	0
19.11 (Required) : All macro identifiers in preprocessor directives shall be defined before use, except in #ifdef and #ifndef preprocessor directives and the defined() operator.	0
19.12 (Required) : There shall be at most one occurrence of the # or ## operators in a single macro definition.	0
19.13 (Advisory) : The # and ## operators should not be used.	0
19.14 (Required) : The defined preprocessor operator shall only be used in one of the two standard forms.	0
19.15 (Required) : Precautions shall be taken in order to prevent the contents of a header file being included twice.	0
19.16 (Required) : Preprocessing directives shall be syntactically meaningful even when excluded by the preprocessor.	0
2.01 (Required) : Assembly language shall be encapsulated and isolated.	0
2.02 (Required) : Source code shall only use /* ... */ style comments.	0
2.03 (Required) : The character sequence /* shall not be used within a comment.	0
20.01 (Required) : Reserved identifiers, macros and functions in the standard library, shall not be defined, redefined or undefined.	0
20.02 (Required) : The names of standard library macros, objects and functions shall not be reused.	0
20.04 (Required) : Dynamic heap memory allocation shall not be used.	0
20.05 (Required) : The error indicator errno shall not be used.	0

20.06 (Required) : The macro offsetof, in library <stddef.h>, shall not be used.	0
20.07 (Required) : The setjmp macro and the longjmp function shall not be used.	0
20.08 (Required) : The signal handling facilities of <signal.h> shall not be used.	0
20.09 (Required) : The input/output library <stdio.h> shall not be used in production code.	0
20.10 (Required) : The library functions atof, atoi and atol from library <stdlib.h> shall not be used.	0
20.11 (Required) : The library functions abort, exit, getenv and system from library <stdlib.h> shall not be used.	0
20.12 (Required) : The time handling functions of library <time.h> shall not be used.	0
21.1 (Required) : Minimisation of run-time failures shall be ensured by the use of at least one of a) static analysis tools/techniques; b) dynamic analysis tools/techniques; c) explicit coding of checks to handle run-time faults.	0
3.04 (Required) : All uses of the #pragma directive shall be documented and explained.	0
3.05 (Required) : If it is being relied upon, the implementation defined behaviour and packing of bitfields shall be documented.	0
4.01 (Required) : Only those escape sequences that are defined in the ISO C standard shall be used.	0
4.02 (Required) : Trigraphs shall not be used.	0
5.01 (Required) : Identifiers (internal and external) shall not rely on the significance of more than 31 characters.	0
5.02 (Required) : Identifiers in an inner scope shall not use the same name as an identifier in an outer scope, and therefore hide that identifier.	0
5.03 (Required) : A typedef name shall be a unique identifier.	0
5.04 (Required) : A tag name shall be a unique identifier.	0
5.05 (Advisory) : No object or function identifier with static storage duration should be reused.	0
5.06 (Advisory) : No identifier in one name space should have the same spelling as an identifier in another name space, with the exception of structure and union member names.	0
5.07 (Advisory) : No identifier name should be reused.	0
6.01 (Required) : The plain char type shall be used only for the storage and use of character values.	0
6.02 (Required) : Signed and unsigned char type shall be used only for the storage and use of numeric values.	0
6.03 (Advisory) : Typedefs that indicate size and signedness should be used in place of the basic types.	0

6.04 (Required) : Bit fields shall only be defined to be of type unsigned int or signed int.	0
6.05 (Required) : Bit fields of type signed int shall be at least 2 bits long.	0
7.01 (Required) : Octal constants (other than zero) and octal escape sequences shall not be used.	0
8.02 (Required) : Whenever an object or function is declared or defined, its type shall be explicitly stated.	0
8.03 (Required) : For each function parameter the type given in the declaration and definition shall be identical, and the return types shall also be identical.	0
8.04 (Required) : If objects or functions are declared more than once their types shall be compatible.	0
8.05 (Required) : There shall be no definitions of objects or functions in a header file.	0
8.06 (Required) : Functions shall be declared at file scope.	0
8.07 (Required) : Objects shall be defined at block scope if they are only accessed from within a single function.	0
8.08 (Required) : An external object or function shall be declared in one and only one file.	0
8.09 (Required) : An identifier with external linkage shall have exactly one external definition.	0
8.10 (Required) : All declarations and definitions of objects or functions at file scope shall have internal linkage unless external linkage is required.	0
8.11 (Required) : The static storage class specifier shall be used in definitions and declarations of objects and functions that have internal linkage.	0
8.12 (Required) : When an array is declared with external linkage, its size shall be stated explicitly or defined implicitly by initialisation.	0
9.01 (Required) : All automatic variables shall have been assigned a value before being used.	0
9.02 (Required) : Braces shall be used to indicate and match the structure in the non-zero initialisation of arrays and structures.	0
9.03 (Required) : In an enumerator list, the "=" construct shall not be used to explicitly initialise members other than the first, unless all items are explicitly initialised.	0

● MISRA-C 2012

레퍼런스 항목 이름	이슈 수
Directives 1.1	0

Directives 4.1	0
Directives 4.10	0
Directives 4.12	0
Directives 4.14	0
Directives 4.3	0
Directives 4.4	0
Directives 4.5	0
Directives 4.6	0
Directives 4.7	0
Directives 4.8	0
Directives 4.9	0
Rule 1.1	0
Rule 1.2	0
Rule 1.3	0
Rule 10.1	0
Rule 10.2	0
Rule 10.3	0
Rule 10.4	0
Rule 10.5	0
Rule 10.6	0
Rule 10.7	0
Rule 10.8	0
Rule 11.1	0
Rule 11.2	0
Rule 11.3	0
Rule 11.4	0
Rule 11.5	0
Rule 11.6	0
Rule 11.7	0
Rule 11.8	0
Rule 11.9	0
Rule 12.1	0
Rule 12.2	0
Rule 12.3	0
Rule 12.4	0
Rule 12.5	0

Rule 13.1	0
Rule 13.2	0
Rule 13.3	0
Rule 13.4	0
Rule 13.5	0
Rule 13.6	0
Rule 14.1	0
Rule 14.2	0
Rule 14.3	0
Rule 14.4	0
Rule 15.1	0
Rule 15.2	0
Rule 15.3	0
Rule 15.4	0
Rule 15.5	0
Rule 15.6	0
Rule 15.7	0
Rule 16.1	0
Rule 16.2	0
Rule 16.3	0
Rule 16.4	0
Rule 16.5	0
Rule 16.6	0
Rule 16.7	0
Rule 17.1	0
Rule 17.2	0
Rule 17.3	0
Rule 17.4	0
Rule 17.5	0
Rule 17.6	0
Rule 17.7	0
Rule 17.8	0
Rule 18.1	0
Rule 18.2	0
Rule 18.3	0
Rule 18.4	0

Rule 18.5	0
Rule 18.6	0
Rule 18.7	0
Rule 18.8	0
Rule 19.1	0
Rule 19.2	0
Rule 2.1	0
Rule 2.2	0
Rule 2.3	0
Rule 2.4	0
Rule 2.5	0
Rule 2.6	0
Rule 2.7	0
Rule 20.01	0
Rule 20.02	0
Rule 20.03	0
Rule 20.04	0
Rule 20.05	0
Rule 20.06	0
Rule 20.07	0
Rule 20.08	0
Rule 20.09	0
Rule 20.10	0
Rule 20.11	0
Rule 20.12	0
Rule 20.13	0
Rule 21.01	0
Rule 21.02	0
Rule 21.03	0
Rule 21.04	0
Rule 21.05	0
Rule 21.06	0
Rule 21.07	0
Rule 21.08	0
Rule 21.09	0
Rule 21.10	0

Rule 21.11	0
Rule 21.12	0
Rule 21.16	0
Rule 21.17	0
Rule 21.18	0
Rule 21.21	0
Rule 22.01	0
Rule 22.02	0
Rule 22.03	0
Rule 22.04	0
Rule 22.05	0
Rule 22.06	0
Rule 22.08	0
Rule 3.1	0
Rule 3.2	0
Rule 4.1	0
Rule 4.2	0
Rule 5.1	0
Rule 5.2	0
Rule 5.3	0
Rule 5.4	0
Rule 5.5	0
Rule 5.6	0
Rule 5.7	0
Rule 5.8	0
Rule 5.9	0
Rule 6.1	0
Rule 6.2	0
Rule 7.1	0
Rule 7.2	0
Rule 7.3	0
Rule 7.4	0
Rule 8.01	0
Rule 8.02	0
Rule 8.03	0
Rule 8.04	0

Rule 8.05	0
Rule 8.06	0
Rule 8.07	0
Rule 8.08	0
Rule 8.09	0
Rule 8.10	0
Rule 8.11	0
Rule 8.12	0
Rule 8.13	0
Rule 8.14	0
Rule 9.1	0
Rule 9.2	0
Rule 9.3	0
Rule 9.4	0
Rule 9.5	0

MISRA-C 2012 Amendment 2

레퍼런스 항목 이름	이슈 수
Directives 1.1	0
Directives 4.1	0
Directives 4.3	0
Directives 4.4	0
Directives 4.5	0
Directives 4.6	0
Directives 4.7	0
Directives 4.8	0
Directives 4.9	0
Rule 1.1	0
Rule 1.2	0
Rule 1.3	0
Rule 1.4	0
Rule 10.1	0
Rule 10.2	0
Rule 10.3	0
Rule 10.4	0

Rule 10.5	0
Rule 10.6	0
Rule 10.7	0
Rule 10.8	0
Rule 11.1	0
Rule 11.2	0
Rule 11.3	0
Rule 11.4	0
Rule 11.5	0
Rule 11.6	0
Rule 11.7	0
Rule 11.8	0
Rule 11.9	0
Rule 12.1	0
Rule 12.2	0
Rule 12.3	0
Rule 12.4	0
Rule 12.5	0
Rule 13.1	0
Rule 13.2	0
Rule 13.3	0
Rule 13.4	0
Rule 13.5	0
Rule 13.6	0
Rule 14.1	0
Rule 14.2	0
Rule 14.3	0
Rule 14.4	0
Rule 15.1	0
Rule 15.2	0
Rule 15.3	0
Rule 15.4	0
Rule 15.5	0
Rule 15.6	0
Rule 15.7	0
Rule 16.1	0

Rule 16.2	0
Rule 16.3	0
Rule 16.4	0
Rule 16.5	0
Rule 16.6	0
Rule 16.7	0
Rule 17.1	0
Rule 17.2	0
Rule 17.3	0
Rule 17.4	0
Rule 17.5	0
Rule 17.6	0
Rule 17.7	0
Rule 17.8	0
Rule 18.1	0
Rule 18.2	0
Rule 18.3	0
Rule 18.4	0
Rule 18.5	0
Rule 18.6	0
Rule 18.7	0
Rule 18.8	0
Rule 19.1	0
Rule 19.2	0
Rule 2.1	0
Rule 2.2	0
Rule 2.3	0
Rule 2.4	0
Rule 2.5	0
Rule 2.6	0
Rule 2.7	0
Rule 20.01	0
Rule 20.02	0
Rule 20.03	0
Rule 20.04	0
Rule 20.05	0

Rule 20.06	0
Rule 20.07	0
Rule 20.08	0
Rule 20.09	0
Rule 20.10	0
Rule 20.11	0
Rule 20.12	0
Rule 20.13	0
Rule 21.01	0
Rule 21.02	0
Rule 21.03	0
Rule 21.04	0
Rule 21.05	0
Rule 21.06	0
Rule 21.07	0
Rule 21.08	0
Rule 21.09	0
Rule 21.10	0
Rule 21.11	0
Rule 21.12	0
Rule 21.13	0
Rule 21.14	0
Rule 21.15	0
Rule 21.16	0
Rule 21.17	0
Rule 21.18	0
Rule 21.19	0
Rule 21.20	0
Rule 21.21	0
Rule 22.01	0
Rule 22.02	0
Rule 22.03	0
Rule 22.04	0
Rule 22.05	0
Rule 22.06	0
Rule 22.07	0

Rule 22.08	0
Rule 22.09	0
Rule 22.10	0
Rule 3.1	0
Rule 3.2	0
Rule 4.1	0
Rule 4.2	0
Rule 5.1	0
Rule 5.2	0
Rule 5.3	0
Rule 5.4	0
Rule 5.5	0
Rule 5.6	0
Rule 5.7	0
Rule 5.8	0
Rule 5.9	0
Rule 6.1	0
Rule 6.2	0
Rule 7.1	0
Rule 7.2	0
Rule 7.3	0
Rule 7.4	0
Rule 8.01	0
Rule 8.02	0
Rule 8.03	0
Rule 8.04	0
Rule 8.05	0
Rule 8.06	0
Rule 8.07	0
Rule 8.08	0
Rule 8.09	0
Rule 8.10	0
Rule 8.11	0
Rule 8.12	0
Rule 8.13	0
Rule 8.14	0

Rule 9.1	0
Rule 9.2	0
Rule 9.3	0
Rule 9.4	0
Rule 9.5	0

MISRA-C 2012 Amendment 3

레퍼런스 항목 이름	이슈 수
Directives 1.1	0
Directives 4.1	0
Directives 4.10	0
Directives 4.12	0
Directives 4.14	0
Directives 4.3	0
Directives 4.4	0
Directives 4.5	0
Directives 4.6	0
Directives 4.7	0
Directives 4.8	0
Directives 4.9	0
Rule 1.1	0
Rule 1.2	0
Rule 1.3	0
Rule 1.4	0
Rule 10.1	0
Rule 10.2	0
Rule 10.3	0
Rule 10.4	0
Rule 10.5	0
Rule 10.6	0
Rule 10.7	0
Rule 10.8	0
Rule 11.1	0
Rule 11.2	0
Rule 11.3	0

Rule 11.4	0
Rule 11.5	0
Rule 11.6	0
Rule 11.7	0
Rule 11.8	0
Rule 11.9	0
Rule 12.1	0
Rule 12.2	0
Rule 12.3	0
Rule 12.4	0
Rule 12.5	0
Rule 13.1	0
Rule 13.2	0
Rule 13.3	0
Rule 13.4	0
Rule 13.5	0
Rule 13.6	0
Rule 14.1	0
Rule 14.2	0
Rule 14.3	0
Rule 14.4	0
Rule 15.1	0
Rule 15.2	0
Rule 15.3	0
Rule 15.4	0
Rule 15.5	0
Rule 15.6	0
Rule 15.7	0
Rule 16.1	0
Rule 16.2	0
Rule 16.3	0
Rule 16.4	0
Rule 16.5	0
Rule 16.6	0
Rule 16.7	0
Rule 17.1	0

Rule 17.2	0
Rule 17.3	0
Rule 17.4	0
Rule 17.5	0
Rule 17.6	0
Rule 17.7	0
Rule 17.8	0
Rule 18.1	0
Rule 18.2	0
Rule 18.3	0
Rule 18.4	0
Rule 18.5	0
Rule 18.6	0
Rule 18.7	0
Rule 18.8	0
Rule 19.1	0
Rule 19.2	0
Rule 2.1	0
Rule 2.2	0
Rule 2.3	0
Rule 2.4	0
Rule 2.5	0
Rule 2.6	0
Rule 2.7	0
Rule 20.01	0
Rule 20.02	0
Rule 20.03	0
Rule 20.04	0
Rule 20.05	0
Rule 20.06	0
Rule 20.07	0
Rule 20.08	0
Rule 20.09	0
Rule 20.10	0
Rule 20.11	0
Rule 20.12	0

Rule 20.13	0
Rule 21.01	0
Rule 21.02	0
Rule 21.03	0
Rule 21.04	0
Rule 21.05	0
Rule 21.06	0
Rule 21.07	0
Rule 21.08	0
Rule 21.09	0
Rule 21.10	0
Rule 21.11	0
Rule 21.12	0
Rule 21.13	0
Rule 21.14	0
Rule 21.15	0
Rule 21.16	0
Rule 21.17	0
Rule 21.18	0
Rule 21.19	0
Rule 21.20	0
Rule 21.21	0
Rule 22.01	0
Rule 22.02	0
Rule 22.03	0
Rule 22.04	0
Rule 22.05	0
Rule 22.06	0
Rule 22.07	0
Rule 22.08	0
Rule 22.09	0
Rule 22.10	0
Rule 3.1	0
Rule 3.2	0
Rule 4.1	0
Rule 4.2	0

Rule 5.1	0
Rule 5.2	0
Rule 5.3	0
Rule 5.4	0
Rule 5.5	0
Rule 5.6	0
Rule 5.7	0
Rule 5.8	0
Rule 5.9	0
Rule 6.1	0
Rule 6.2	0
Rule 7.1	0
Rule 7.2	0
Rule 7.3	0
Rule 7.4	0
Rule 8.01	0
Rule 8.02	0
Rule 8.03	0
Rule 8.04	0
Rule 8.05	0
Rule 8.06	0
Rule 8.07	0
Rule 8.08	0
Rule 8.09	0
Rule 8.10	0
Rule 8.11	0
Rule 8.12	0
Rule 8.13	0
Rule 8.14	0
Rule 9.1	0
Rule 9.2	0
Rule 9.3	0
Rule 9.4	0
Rule 9.5	0

● MISRA-C++ 2008

레퍼런스 항목 이름	이슈 수
Rule 0-1-1	0
Rule 8-3-1	0
Rule0-1-10	0
Rule0-1-11	0
Rule0-1-12	0
Rule0-1-3	0
Rule0-1-4	0
Rule0-1-5	0
Rule0-1-6	0
Rule0-1-7	0
Rule0-1-8	0
Rule0-1-9	0
Rule0-2-1	0
Rule0-3-1	0
Rule10-1-1	0
Rule10-1-2	0
Rule10-1-3	0
Rule10-3-1	0
Rule10-3-2	0
Rule10-3-3	0
Rule11-0-1	0
Rule12-1-1	0
Rule12-1-2	0
Rule12-1-3	0
Rule12-8-1	0
Rule12-8-2	0
Rule14-5-1	0
Rule14-5-2	0
Rule14-5-3	0
Rule14-6-1	0
Rule14-6-2	0
Rule14-7-1	0
Rule14-7-3	0
Rule14-8-1	0

Rule14-8-2	0
Rule15-0-1	0
Rule15-0-2	0
Rule15-1-1	0
Rule15-1-2	0
Rule15-1-3	0
Rule15-3-1	0
Rule15-3-2	0
Rule15-3-3	0
Rule15-3-4	0
Rule15-3-5	0
Rule15-3-6	0
Rule15-3-7	0
Rule15-4-1	0
Rule15-5-1	0
Rule15-5-2	0
Rule15-5-3	0
Rule16-0-1	0
Rule16-0-2	0
Rule16-0-3	0
Rule16-0-4	0
Rule16-0-5	0
Rule16-0-6	0
Rule16-0-7	0
Rule16-0-8	0
Rule16-1-1	0
Rule16-2-1	0
Rule16-2-2	0
Rule16-2-3	0
Rule16-2-4	0
Rule16-2-5	0
Rule16-2-6	0
Rule16-3-1	0
Rule16-3-2	0
Rule17-0-1	0
Rule17-0-2	0

Rule17-0-3	0
Rule17-0-5	0
Rule18-0-1	0
Rule18-0-2	0
Rule18-0-3	0
Rule18-0-4	0
Rule18-0-5	0
Rule18-2-1	0
Rule18-4-1	0
Rule18-7-1	0
Rule19-3-1	0
Rule2-10-1	0
Rule2-10-2	0
Rule2-10-3	0
Rule2-10-4	0
Rule2-10-5	0
Rule2-10-6	0
Rule2-13-1	0
Rule2-13-2	0
Rule2-13-3	0
Rule2-13-4	0
Rule2-13-5	0
Rule2-3-1	0
Rule2-5-1	0
Rule2-7-1	0
Rule2-7-2	0
Rule2-7-3	0
Rule27-0-1	0
Rule3-1-1	0
Rule3-1-2	0
Rule3-1-3	0
Rule3-2-1	0
Rule3-2-2	0
Rule3-2-3	0
Rule3-2-4	0
Rule3-3-1	0

Rule3-3-2	0
Rule3-4-1	0
Rule3-9-1	0
Rule3-9-2	0
Rule3-9-3	0
Rule4-10-1	0
Rule4-10-2	0
Rule4-5-1	0
Rule4-5-2	0
Rule4-5-3	0
Rule5-0-1	0
Rule5-0-10	0
Rule5-0-11	0
Rule5-0-12	0
Rule5-0-13	0
Rule5-0-14	0
Rule5-0-15	0
Rule5-0-16	0
Rule5-0-17	0
Rule5-0-18	0
Rule5-0-19	0
Rule5-0-2	0
Rule5-0-20	0
Rule5-0-21	0
Rule5-0-3	0
Rule5-0-4	0
Rule5-0-5	0
Rule5-0-6	0
Rule5-0-7	0
Rule5-0-8	0
Rule5-0-9	0
Rule5-14-1	0
Rule5-18-1	0
Rule5-19-1	0
Rule5-2-1	0
Rule5-2-10	0

Rule5-2-11	0
Rule5-2-12	0
Rule5-2-2	0
Rule5-2-3	0
Rule5-2-4	0
Rule5-2-5	0
Rule5-2-6	0
Rule5-2-7	0
Rule5-2-8	0
Rule5-2-9	0
Rule5-3-1	0
Rule5-3-2	0
Rule5-3-3	0
Rule5-3-4	0
Rule5-8-1	0
Rule6-2-1	0
Rule6-2-2	0
Rule6-2-3	0
Rule6-3-1	0
Rule6-4-1	0
Rule6-4-2	0
Rule6-4-3	0
Rule6-4-4	0
Rule6-4-5	0
Rule6-4-6	0
Rule6-4-7	0
Rule6-4-8	0
Rule6-5-1	0
Rule6-5-2	0
Rule6-5-3	0
Rule6-5-4	0
Rule6-5-5	0
Rule6-5-6	0
Rule6-6-1	0
Rule6-6-2	0
Rule6-6-3	0

Rule6-6-4	0
Rule6-6-5	0
Rule7-1-1	0
Rule7-1-2	0
Rule7-2-1	0
Rule7-3-1	0
Rule7-3-2	0
Rule7-3-3	0
Rule7-3-4	0
Rule7-3-5	0
Rule7-3-6	0
Rule7-4-2	0
Rule7-4-3	0
Rule7-5-1	0
Rule7-5-2	0
Rule7-5-3	0
Rule7-5-4	0
Rule8-0-1	0
Rule8-4-1	0
Rule8-4-2	0
Rule8-4-3	0
Rule8-4-4	0
Rule8-5-1	0
Rule8-5-2	0
Rule8-5-3	0
Rule9-3-1	0
Rule9-3-2	0
Rule9-3-3	0
Rule9-5-1	0
Rule9-6-1	0
Rule9-6-2	0
Rule9-6-3	0
Rule9-6-4	0

OWASP 2017

레퍼런스 항목 이름	이슈 수
A1-Injection	0
A2-Broken Authentication	0
A3-Sensitive Data Exposure	2
A5-Broken Access Control	1
A6-Security Misconfiguration	8

OWASP 2021

레퍼런스 항목 이름	이슈 수
A03 Injection	0
A05 Security Misconfiguration	8
A07 Identification and Authentication Failures	0

Python 시큐어코딩 가이드 2022

레퍼런스 항목 이름	이슈 수
01.01. SQL 삽입	0
01.02. 코드 삽입	0
01.03. 경로 조작 및 자원 삽입	0
01.04. 크로스사이트 스크립트(XSS)	0
01.05. 운영체제 명령어 삽입	0
01.06. 위험한 형식 파일 업로드	0
01.07. 신뢰되지 않은 URL주소로 자동접속 연결	0
01.08. 부적절한 XML 외부 개체 참조	0
01.09. XML 삽입	0
01.10. LDAP 삽입	0
01.11. 크로스사이트 요청 위조(CSRF)	0
01.12. 서버사이드 요청 위조	0
01.13. HTTP 응답분할	0
01.14. 보안기능 결정에 사용되는 부적절한 입력값	0
01.15. 포맷 스트링 삽입	0
02.01. 적절한 인증 없는 중요 기능 허용	0
02.03. 중요한 자원에 대한 잘못된 권한 설정	0
02.04. 취약한 암호화 알고리즘 사용	0
02.06. 하드코드된 중요정보	0

02.07. 충분하지 않은 키 길이 사용	0
02.08. 적절하지 않은 난수 값 사용	0
02.09. 취약한 비밀번호 허용	0
02.10. 사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출	0
02.11. 주석문 안에 포함된 시스템 주요정보	0
02.12. 솔트 없이 일방향 해쉬 함수 사용	0
02.13. 무결성 검사없는 코드 다운로드	0
03.01. 경쟁조건: 검사시점과 사용시점(TOCTOU)	0
03.02. 종료되지 않는 반복문 또는 재귀 함수	0
04.01. 오류 메시지 정보노출	0
04.02. 오류상황 대응 부재	0
04.03. 부적절한 예외 처리	0
05.01. Null Pointer 역참조	0
05.02. 부적절한 자원 해제	0
05.03. 신뢰할 수 없는 데이터의 역직렬화	0
06.02. 제거되지 않고 남은 디버그 코드	0
06.03. Public 메소드로부터 반환된 Private 배열	0
06.04. Private 배열에 Public 데이터 할당	0

● Rust ANSSI guide v1.0

레퍼런스 항목 이름	이슈 수
R10 RULE - Don't use unsafe blocks	0
R11 RULE - Use appropriate arithmetic operations regarding potential overflows	0
R13 RECO - Use the ? operator and do not use the try! macro	0
R14 RULE - Don't use functions that can cause panic!	0
R15 RULE - Test properly array indexing or use the get method	0
R16 RULE - Handle correctly panic! in FFI	0
R17 RULE - Do not use forget	0
R19 RULE - Do not leak memory	0
R2 RULE - Keep default values for critical variables in cargo profiles	0
R20 RULE - Do release value wrapped in ManuallyDrop	0
R21 RULE - Always call from_raw on into_rawed value	0
R22 RULE - Do not use uninitialized memory	0
R32 RULE - Use only C-compatible types in FFI	0

● 무기체계 소프트웨어 보안약점 점검 목록

레퍼런스 항목 이름	이슈 수
CWE-119	0
CWE-134	0
CWE-170	0
CWE-190	0
CWE-209	0
CWE-22	0
CWE-259	0
CWE-285	0
CWE-306	0
CWE-307	0
CWE-312	0
CWE-319	0
CWE-321	0
CWE-327	0
CWE-330	0
CWE-367	0
CWE-369	0
CWE-390	0
CWE-400	0
CWE-404	0
CWE-415	0
CWE-416	0
CWE-457	0
CWE-467	0
CWE-469	0
CWE-476	0
CWE-489	0
CWE-494	0
CWE-495	0
CWE-496	0
CWE-497	0
CWE-521	0
CWE-562	0

CWE-587	0
CWE-59	0
CWE-615	0
CWE-628	0
CWE-676	0
CWE-732	0
CWE-755	0
CWE-759	0
CWE-78	0
CWE-89	0
CWE-99	0

방위사업청 코딩규칙

레퍼런스 항목 이름	이슈 수
1-01. Switch 구문에서 첫 번째 Label 전에 코드 구문이 존재하면 안된다.	0
1-02. 함수/변수 선언 시 type을 명시해야 한다.	0
1-03. 의미 없는 구문은 사용하지 말아야 한다.(side effect)	0
1-04. 함수의 Return Type에 맞는 return을 사용해야 한다.	0
1-05. 선언 없이 함수를 사용하지 말아야 한다.(묵시적 선언이 사용됨)	0
1-06. 매크로의 정의 여부를 확인하지 않고 해당 매크로에 대하여 #if, #elseif 표현을 사용하지 말아야 한다.	0
1-07. goto 문 사용은 최대한 자제한다.	0
1-08. 하나의 함수는 하나의 Exit Point를 가져야 한다.	0
1-09. switch~case 문은 default 문이 포함되어야 한다.	0
1-10. 한 줄에 하나의 명령문을 사용한다.	0
1-11. if - else if 문은 else 문도 포함시킨다.	0
2-01. String 배열의 초기화에서 배열의 마지막 인자는 NULL로 종료되어야 한다.	0
2-02. 초기화 되지 않은 변수를 사용하지 말아야 한다.	0
2-03. 설정되지 않은 포인터를 함수의 Read-only(const)로 사용하면 안된다.	0
3-01. external과 internal linkage 의 특성을 동시에 가질 수 없다.	0
3-02. external linkage scope 에서 선언된 함수나 Object의 이름은 유일해야 한다.	0
3-03. external linkage scope 에서 정의된 함수나 Object의 데이터 형은 선언 시 정의와 동일해야 한다.	0
3-04. 바깥 scope 의 식별자를 가리는 정의를 해서는 안된다.	0
4-01. float 자료형에서 동등성 비교연산을 수행하지 말아야 한다.	0

4-02. 조건문의 결과가 항상 True거나 False면 안된다.	0
4-03. switch의 case 조건을 만족할 수 없는 Label을 사용하지 않는다.	0
4-04. switch 구문에서 Expression을 논리적 연산으로 사용하지 말아야 한다.	0
4-05. 수행되지 않는 소스코드를 작성하지 말아야 한다.	0
5-01. 선언된 데이터 형으로 표현할 수 있는 숫자의 영역을 초과하는 값을 할당하지 말아야 한다.	0
5-02. 가변인수를 받는 함수의 Conversion 지시자와 Argument의 type은 동일해야 한다.	0
5-03. 가변인수를 받는 함수의 Conversion 지시자와 Argument의 개수는 동일해야 한다.	0
5-04. Object 저장값을 표현할 수 없는 데이터로의 형 변환을 하지말아야 한다.	0
5-05. 음수값을 unsigned type으로 변환을 자제해야 한다.	0
5-06. Character 문자열과 Wide character 문자열을 혼용하지 말아야 한다.	0
5-07. 포인터 Cast의 결과로 이전 포인터의 Const 특성의 상실을 유의해야 한다.	0
5-08. 포인터 Cast의 결과로 이전 포인터의 Volatile 특성의 상실을 유의해야 한다.	0
6-01. Null pointer를 참조하지 않는다.	0
6-02. 지역 변수의 주소값을 더 넓은 scope를 가진 변수에 할당하지 말아야 한다.	0
6-03. 지역 변수의 주소값을 함수의 리턴값으로 사용하지 말아야 한다.	0
6-04. 선언된 배열의 크기를 초과하는 인덱스 값을 사용하지 말아야 한다.	0
6-05. Null Pointer를 산술연산 하지 않는다.	0
7-01. 하나의 Sequence Point 내에서 하나의 Object Value를 두 번 이상 변경하지 않아야 한다.	0
7-02. 0 으로 나눗셈 연산을 하지 않는다.	0
7-03. 하나의 Sequence Point 내에서 Object의 값을 변경하고 Access 하지 않아야 한다.	0
7-04. 음수 값 또는 데이터 사이즈를 초과하는 값을 사용하여 Shift operator를 하지 않는다.	0
7-05. Underlying type이 부호 없는 정수일 경우 단행 빼기 연산(-)을 사용하여 결과를 대입하지 말아야 한다.	0
7-06. sizeof의 인자는 side effect를 가지지 말아야 한다.	0
7-07. Boolean 표현 값에 &&, ||, ! 연산자를 제외하고 다른 연산자를 사용하지 말아야 한다.	0
7-08. 조건문에 직접적인 대입 연산자를 사용하지 말아야 한다.	0
7-09. Signed Value에서 Bitwise연산자(<<, ~, |, ^ 등)로 인한 Negative Value를 유의해야 한다.	0
8-01. Scanf의 Argument 는 Object Value의 저장된 주소에 값이 입력되어야 한다.	0
8-02. #include 구문에서 표준에 맞지 않는 Character set을 사용하지 않아야 한다.	0
8-03. Allocated되는 메모리 블록의 크기는 Pointer에 의해서 Address 되는 완전한 하나의 multiple size여야 한다.	0
8-04. 함수의 Argument type과 개수는 함수의 Prototype, 선언, 정의가 모두 같아야 한다.	0
8-05. 구조체/배열의 초기화 시 default 초기화 값(0)을 제외하고, 구조에 맞게 '{}'를 사용하	

여 선언된 Size에 맞게 초기화 해야 한다.	0
9-01. 동적 할당된 데이터를 해제할 때, 잘못된 메소드를 이용하여 해제하면 안된다.	0
9-02. 지역 변수의 주소 값을 처리하는 handle을 return하지 말아야 한다.	0
9-03. 함수 parameter의 주소 값을 처리하는 handle을 return하지 말아야 한다.	0
9-04. 소멸자내에서 처리할 수 없는 예외 상황을 발생시키지 말아야 한다.	0
9-05. 사용되지 않는 예외 처리 문을 작성하지 말아야 한다.	0
9-06. exception specification에 기술되지 않은 모든 throw에 대하여 예외처리를 해야만 한다.	0
9-07. main 함수에서 처리되지 않는 throw를 작성하지 말아야 한다.	0
9-08. 해제된 메모리 영역 사용하지 말아야 한다.	0
9-09.복사 연산자를 통해서, 복사되지 않는 멤버 변수가 존재하지 말아야 한다	0
9-10. C 코딩 방법으로 메모리를 할당 하면 안된다.	0
9-11. 순수 가상함수는 반드시 0으로 초기화 되어야 한다	0
9-12. 순수함수는 반드시 가상함수로 선언되어야 한다	0
9-13. virtual base 클래스의 포인터는 derived 클래스의 포인터로 cast 할 때에는 dynamic_cast만 사용해야 한다.	0
9-14. 생성자/소멸자 내에서 가상함수는 식별자 없이 호출하면 안된다.	0
9-15. 생성자/소멸자에 dynamic type을 사용하면 안된다.	0

● 소프트웨어 보안약점 진단가이드 2021

레퍼런스 항목 이름	이슈 수
DNS lookup에 의존한 보안 결정	0
HTTP 응답분할	0
LDAP 삽입	0
Null Pointer 역참조	0
Private 배열에 Public 데이터 할당	0
Public 메소드부터 반환된 Private 배열	0
SQL 삽입	0
XML 삽입	0
경로 조작 및 자원 삽입	0
경쟁조건: 검사시점과 사용시점(TOCTOU)	0
메모리 버퍼 오버플로우	0
무결성 검사없는 코드 다운로드	0
반복된 인증시도 제한 기능 부재	0
보안기능 결정에 사용되는 부적절한 입력값	0

부적절한 XML 외부개체 참조	0
부적절한 예외처리	0
부적절한 인가	0
부적절한 인증서 유효성 검증	0
부적절한 자원 해제	0
부적절한 전자서명 확인	0
사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출	0
서버사이드 요청 위조	0
솔트 없이 일방향 해쉬 함수 사용	0
신뢰되지 않는 URL 주소로 자동 접속 연결	0
신뢰할 수 없는 데이터의 역직렬화	0
암호화되지 않은 중요정보	0
오류 상황 대응 부재	0
오류메시지 정보 노출	0
운영체제 명령어 삽입	0
위험한 형식 파일 업로드	0
잘못된 세션에 의한 데이터 정보 노출	0
적절하지 않은 난수 값 사용	0
적절한 인증없는 중요기능 허용	0
정수형 오버플로우	0
제거되지 않고 남은 디버그 코드	0
종료되지 않는 반복문 또는 재귀 함수	0
주석문 안에 포함된 시스템 주요정보	0
중요한 자원에 대한 잘못된 권한 설정	0
초기화되지 않은 변수 사용	0
충분하지 않은 키 길이 사용	0
취약한 API 사용	0
취약한 비밀번호 허용	0
취약한 암호화 알고리즘 사용	0
코드 삽입	0
크로스사이트 스크립트	1
크로스사이트 요청 위조	0
포맷스트링 삽입	0
하드코드된 중요정보	0
해제된 자원 사용	0

● 주요정보통신기반시설 취약점 분석·평가 기준

레퍼런스 항목 이름	이슈 수
SQL 인젝션	0
XPath 인젝션	0
경로 추적	0
디렉토리 인덱싱	0
세션 고정	0
세션 예측	0
약한 문자열 강도	0
운영체제 명령 실행	0
위치 공개	0
크로스사이트 스크립팅	1
파일 다운로드	0

■ 이슈 상세 결과

● [규칙 이름] CSRF 토큰이 없는 폼 태그 (높음, common)

크로스 사이트 요청 위조(CSRF)는 임의 사용자의 권한으로 임의 주소에 HTTP 요청을 보낼 수 있는 취약점입니다. CSRF는 XSS와 같이 클라이언트를 대상으로 하여 웹 페이지에 스크립트를 삽입하는 방법으로 공격을 수행합니다. 공격자는 악성 스크립트가 포함된 페이지에 접근한 사용자의 권한으로 웹 서비스의 임의 기능을 실행할 수 있습니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

페이지 내부 특정 요소 중 CSRF를 방지하는 Anti-CSRF 토큰이 있는지 검사합니다.

분석 결과

검사 결과 CSRF를 발생시키는 페이지 요소는 다음과 같습니다.

```
<form action="/benchmark/BenchmarkTest01660" method="GET" id="
FormBenchmarkTest01660">
<div><label>Please enter your details:</label></div>
<br /><div><label>Username:</label></div><div><input type="text" id="
username" name="username" /></div><div><label>Password:</label><
/div><div><input type="text" id="password" name="password" value="" /><
/div><div> </div><div><label>Parameter: vector <br /></label>
<input type="text" id="vector" name="vector" value="SafeText" /></div><br
/><div><input type="submit" value="Login" /></div></form>
```

해결 방법

CSRF를 막기 위해 FORM 요소에 Anti-CSRF 토큰을 추가해야 합니다.

Anti-CSRF 토큰은 FORM 요소 내에 "CSRFToken", "anticsrf", "OWASP_CSRFTOKEN" 등의 Anti-CSRF 토큰을 HIDDEN 필드로 추가하여 사용합니다.

혹은 JavaSctipt에서 Anti-CSRF 토큰을 사용할 수 있습니다.

하지만 XSS가 발생하는 페이지라면 토큰 유무와 관계 없이 CSRF가 발생할 수도 있습니다.

● [규칙 이름] Slowloris HTTP DOS (보통, common)

Slowloris HTTP DOS 취약점은 다수의 미완성 헤더를 포함하는 HTTP GET 요청을 전송함으로써, 서버에서 사용 가능한 HTTP 연결을 강제로 점유하는 취약점입니다. 이 취약점은 HTTP 요청에 대한 최대 동시 접속 허용 수 혹은 연결 타임아웃 등 연결 제어를 설정하지 않은 경우 발생할 수 있습니다. 공격자는 공격을 수행하기 위해 HTTP GET 요청 헤더의 마지막 CRLF를 제거한 뒤, 일정 간격을 두고 해당 HTTP 요청을 반복적으로 서버에 전송할 수 있습니다. 공격이 성공한 경우, 공격자는 서버의 가용 HTTP 연결을 모두 소진시킴으로써 서버가 일반 사용자의 요청을 처리하지 못하거나 응답을 거부하도록 할 수 있습니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

서버에 전송할 HTTP 요청을 다음과 같이 구성했습니다.

HTTP 요청에 대하여 헤더 정보의 끝을 의미하는 마지막 개행 문자(" ")를 생략했습니다.

다음과 같은 HTTP 요청을 서버로 전송했습니다.

```
GET /benchmark/BenchmarkTest01660.html HTTP/1.1\r\n
Host: 125.141.219.118:39251\r\n
User-Agent: Mozilla/5.0 (Windows NT x.y; Win64; x64; rv:10.0) Gecko/20100101
Firefox/10.0\r\n
Connection: keep-alive\r\n
```

5000ms 동안 대기한 뒤, 전송하지 않았던 개행 문자를 이어서 전송했습니다.

분석 결과

서버로 전송한 HTTP 요청에 대한 HTTP 응답은 다음과 같습니다.

```
HTTP/1.1 200
Accept-Ranges: bytes
ETag: W/"1070-1709185617269"
Last-Modified: Thu, 29 Feb 2024 05:46:57 GMT
Content-Type: text/html
Content-Length: 1070
Date: Wed, 05 Feb 2025 14:00:05 GMT
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.
org/TR/html4/loose.dtd">
<html>
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<meta name="insight-app-sec-validation" content="5d884ba7-805f-4bee-a23e-
228ae4174950">
<script src="js/jq
```

서버로부터 수신한 HTTP 응답은 정상적인 HTTP 응답에 해당합니다.

분석 결과, 헤더 정보의 마지막 개행 문자가 없는 HTTP 요청에 대하여 해당 요청이 완결될 때까지 대기함을 발견했습니다.

따라서 해당 HTTP 요청이 최소 5000ms 동안 서버의 네트워크 리소스를 점유할 수 있습니다.

해결 방법

각 HTTP 요청에 대한 제한시간 값을 적정한 수준으로 조정하여, 단일 HTTP 요청이 지나치게 긴 시간 동안 세션을 점유하지 않도록 합니다.

제한시간을 설정하기 어려운 경우 웹 캐시 소프트웨어를 통해 트래픽 장애 방지가 가능합니다.

● [규칙 이름] Tomcat 예제 (높음, common)

Apahce Tomcat 예제 취약점은 크로스 사이트 스크립팅 취약점을 가지고 있는 Apache Tomcat의 JSP 예제 페이지가 노출되는 취약점입니다. 공격자는 Apache Tomcat 예제가 위치한 /examples/에 접근하려고 시도합니다. 공격자는 취약점을 이용해 Apahce Tomcat 예제 페이지에 접근할 수 있습니다. 그 결과 공격자는 Apache 예제 페이지가 가지고 있는 크로스 사이트 스크립팅 등의 치명적인 취약점을 공격할 수 있습니다. 이 취약점을 해결하기 위해서는 Apahce Tomcat 기본 페이지에 대한 접근을 차단해야 합니다. 접근이 필요한 경우 접근 허용 권한을 가지고 있는 사용자만 접근할 수 있게 해야 합니다.

- OWASP 2017
  - A5-Broken Access Control

URL http://125.141.219.118:39251/examples/servlets/servlet/SessionExample

분석 방법

Apache Tomcat 예제 취약점은 크로스 사이트 스크립팅 취약점을 가지고 있는 Apache Tomcat의 JSP 예제들이 노출되는 취약점입니다.

Apache Tomcat의 /examples/ 아래에는 다양한 예제 코드들과 실행 환경이 제공되어 있습니다.

하지만 이러한 예제들은 보안을 고려하지 않을 상태로 구현되어 있기 때문에 공격자가 이러한 예제들을 통해 크로스 사이트 스크립팅 등의 공격을 수행할 수 있습니다.

이와 같이 보안에 취약한 Apache Tomcat 예제에 접근이 가능한지 확인하기 위해 다음과 같은 HTTP 요청을 보냈습니다.

```
GET http://125.141.219.118:39251/examples/servlets/servlet/SessionExample HTTP
/1.1
Accept-Language: en-US
```

```
Empty String
```

분석 결과

Apache Tomcat 예제 접근을 위한 HTTP 요청에 대해 다음과 같은 HTTP 응답이 왔습니다.

```
HTTP/1.1 200
Content-Length: 1289
Content-Type: text/html;charset=UTF-8
Date: Wed, 05 Feb 2025 13:57:45 GMT
Set-Cookie: JSESSIONID=109DE10BF2EE1E4D77490D421A9E4134;path=/examples;
HttpOnly
<!DOCTYPE html><html>
<head>
<meta charset="UTF-8" />
<title>Sessions Example</title>
</head>
<body bgcolor="white">
<a href="../sessions.html">
<img src="../images/code.gif" height=24 width=24 align=right border=0 alt="
view code"></a>
<a href="../index.html">
<img src="../images/return.gif" height=24 width=24 align=right border=0 alt="
return"></a>
<h3>Sessions Example</h3>
Session ID: 109DE10BF2EE1E4D77490D421A9E4134
<br>
Created:
```

```
Wed Feb 05 22:57:46 KST 2025<br>
Last Accessed:
Wed Feb 05 22:57:46 KST 2025
<P>
The following data is in your session:<br>
<P>
<form action="SessionExample;jsessionid=109DE10BF2EE1E4D77490D421A9E4134"
method=POST>
Name of Session Attribute:
<input type=text size=20 name=dataname>
<br>
Value of Session Attribute:
<input type=text size=20 name=datavalue>
<br>
<input type=submit>
</form>
<P>GET based form:<br>
<form action="SessionExample;jsessionid=109DE10BF2EE1E4D77490D421A9E4134"
method=GET>
Name of Session Attribute:
<input type=text size=20 name=dataname>
<br>
Value of Session Attribute:
<input type=text size=20 name=datavalue>
<br>
<input type=submit>
</form>
<p><a href="SessionExample;jsessionid=109DE10BF2EE1E4D77490D421A9E4134?
dataname=foo&amp;datavalue=bar" >URL encoded </a>
</body>
</html>
```

위의 HTTP 응답 메시지를 통해 취약한 Apache Tomcat 예제 중에 하나인 세션 예제에 접근 가능함을 확인할 수 있습니다.

해결 방법

Apache Tomcat 예제 취약점을 막기 위해서는 기본적으로 Apache Tomcat 기본 페이지에 대한 접근을 차단해야 합니다.

● [규칙 이름] 기본 언어 표시 누락 (매우 낮음, common)

기본 언어 표시 누락 체커는 주로 사용하는 기본 언어를 명시하지 않은 페이지를 검출합니다. 페이지에서 주로 사용하는 기본 언어를 명시하지 않은 경우, 화면 낭독 프로그램이 언어를 인식하여 자동으로 음성을 변환하거나, 해당 언어에 적합한 발음을 제공하지 못하도록 할 수 있습니다. 이를 해결하기 위해 페이지에서 주로 사용하는 기본 언어를 명시해야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

다음과 같은 HTTP 요청을 전송했습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

HTTP 응답을 수신했습니다.

HTTP 응답 본문이 HTML 문서인지를 검사했습니다.

HTTP 응답 본문에서 <html> 요소를 탐색했습니다.

탐색한 요소의 lang 속성을 탐색했습니다.

분석 결과

HTTP 응답 본문이 HTML 문서에 해당합니다.

HTTP 응답 본문에 <html> 요소가 존재합니다. 해당 요소의 XPath는 다음과 같습니다.

/HTML[1]

해당 요소의 lang 속성이 존재하지 않습니다. 해당 속성이 없으므로 HTML 문서의 기본 언어가 누락되었습니다.

해결 방법

<html> 요소의 lang 속성을 추가하세요.

● [규칙 이름] 누락된 Content-Security-Policy (CSP) 헤더 (낮음, common)

누락된 Content-Security-Policiy (CSP) 헤더는 HTTP 응답 메시지에 CSP 헤더가 없는 취약점입니다. CSP는 Same-Origin-Policy(SOP) 에 근간을 둔 콘텐츠 보안 정책입니다. CSP는 신뢰할 수 있는 콘텐츠 소스의 허용 목록을 생성하고, 브라우저가 이런 소스에서 받은 리소스만을 실행하거나 렌더링하도록 합니다. 공격자는 이 취약점을 이용하여 사용자의 브라우저에서 악의적인 클라이언트 스크립트 실행을 시도할 수 있습니다. 이를 통해 공격자는 사용자의 중요 정보 또는 권한을 탈취할 수 있으며, 사용자가 의도치 않은 행동을 하도록 유도할 수 있습니다. 이를 해결하기 위해서는 Content-Security-Policy 헤더를 추가하여 신뢰할 수 없는 소스에서 리소스를 받지 못하게 막아야 합니다.

- OWASP 2017
  - A6-Security Misconfiguration

- OWASP 2021
  - A05 Security Misconfiguration

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

누락된 Content-Security-Policy(CSP) 헤더 취약점은 HTTP 응답에 Content-Security-Policy 헤더가 없는 취약점입니다.

이를 검출하기 위해서 다음과 같은 HTTP 요청을 보냈습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660?
username=sparrow8dast2text4&password=sparrow8dast2text4&vector=SafeText HTTP
/1.1
Upgrade-Insecure-Requests: 1
Referer: http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) HeadlessChrome/103.0.5060.134 Safari/537.36
```

```
Empty String
```

분석 결과

HTTP 요청에 대한 HTTP 응답 헤더는 다음과 같습니다.

```
HTTP/1.1 200
Content-Length: 8
Content-Type: text/html;charset=ISO-8859-1
Date: Wed, 05 Feb 2025 13:57:40 GMT
```

위의 HTTP 응답 헤더에 Content-Security-Policy 헤더나 Content-Security-Policy-Report-Only 헤더가 없음을 확인할 수 있습니다.

Content-Security-Policy 헤더가 없기 때문에 신뢰할 수 없는 도메인의 리소스가 브라우저에서 실행되거나 렌더링 되는 것을 막을 수 없습니다.

해결 방법

누락된 Content-Security-Policy 헤더 취약점을 해결하기 위해서는 웹 애플리케이션 서버에서 Content-Security-Policy 헤더를 추가해야 합니다.

모든 웹 사이트 내의 콘텐츠를 서브 도메인을 제외한 같은 도메인에서만 제공 받으려면 다음과 같이 사용합니다.

```
Content-Security-Policy: default-src 'self'
```

서브 도메인을 포함시키려면 다음과 같이 사용합니다.

```
Content-Security-Policy: default-src 'self'*.125.141.219.118
```

이외에도 신뢰할 수 있는 도메인의 리소스를 특정 웹 페이지 요소에서만 사용하도록 설정할 수도 있습니다.

또한, 신뢰할 수 없는 도메인의 리소스가 사용되지는 것을 막지 않고 사용되었다는 정보만을 제공받으려면 다음과 같이 사용합니다.

```
Content-Security-Policy-Report-Only: policy
```

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

누락된 Content-Security-Policy(CSP) 헤더 취약점은 HTTP 응답에 Content-Security-Policy 헤더가 없는 취약점입니다.

이를 검출하기 위해서 다음과 같은 HTTP 요청을 보냈습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

분석 결과

HTTP 요청에 대한 HTTP 응답 헤더는 다음과 같습니다.

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Length: 1070
Content-Type: text/html
Date: Wed, 05 Feb 2025 13:57:34 GMT
ETag: W/"1070-1709185617269"
Last-Modified: Thu, 29 Feb 2024 05:46:57 GMT
```

위의 HTTP 응답 헤더에 Content-Security-Policy 헤더나 Content-Security-Policy-Report-Only 헤더가 없음을 확인할 수 있습니다.

Content-Security-Policy 헤더가 없기 때문에 신뢰할 수 없는 도메인의 리소스가 브라우저에서 실행되거나 렌더링 되는 것을 막을 수 없습니다.

해결 방법

누락된 Content-Security-Policy 헤더 취약점을 해결하기 위해서는 웹 애플리케이션 서버에서 Content-Security-Policy 헤더를 추가해야 합니다.

모든 웹 사이트 내의 콘텐츠를 서브 도메인을 제외한 같은 도메인에서만 제공 받으려면 다음과 같이 사용합니다.

```
Content-Security-Policy: default-src 'self'
```

서브 도메인을 포함시키려면 다음과 같이 사용합니다.

```
Content-Security-Policy: default-src 'self'*.125.141.219.118
```

이외에도 신뢰할 수 있는 도메인의 리소스를 특정 웹 페이지 요소에서만 사용하도록 설정할 수도 있습니다.

또한, 신뢰할 수 없는 도메인의 리소스가 사용되지는 것을 막지 않고 사용되었다는 정보만을 제공받으려면 다음과 같이 사용합니다.

```
Content-Security-Policy-Report-Only: policy
```

● [규칙 이름] 누락된 X 콘텐츠 타입 옵션 (보통, common)

누락된 X 콘텐츠 타입 옵션 취약점은 HTTP 응답 메시지에 nosniff 플래그가 설정된 X-Content-Type-Options 헤더가 포함되지 않는 경우에 발생하는 취약점입니다. 여기서 nosniff 플래그는 MIME 타입 스니핑을 방지하는 역할을 수행합니다. MIME 타입 스니핑이란 MIME 타입이 없거나 잘못 설정되었다고 판단한 경우, 브라우저가 리소스를 훑어보고 정확한 MIME 타입을 추측하여 판단하는 기능을 의미합니다. 공격자는 MIME 타입 스니핑을 이용하여 악의적인 코드가 포함되어 있는 비실행 MIME 타입을 실행 MIME 타입인 것처럼 속여서 웹 애플리케이션에서 악의적인 코드를 실행하게 합니다. 이를 통해 공격자는 악의적인 코드를 웹 애플리케이션에 업로드하여 해당 코드를 웹 애플리케이션이 반복적으로 실행하도록 합니다. 이 취약점을 해결하기 위해서는 HTTP 응답 메시지에 값이 nosniff인 X-Content-Type-Options 헤더를 포함시켜야 합니다.

- OWASP 2017
  - A6-Security Misconfiguration

- OWASP 2021
  - A05 Security Misconfiguration

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

누락된 X 콘텐츠 타입 옵션은 HTTP 응답에 X-Content-Type-Options 헤더가 존재하지 않거나 값이 잘못된 취약점입니다.

HTTP 응답메시지에 X-Content-Type-Options가 있고, 그 값이 nosniff이면 MIME 타입 스니핑을 막습니다.

MIME 타입 스니핑이란 MIME 타입이 없거나 클라이언트 타입이 잘못 설정됐다고 판단될 경우, 브라우저가 리소스를 훑어보고 정확한 MIME 타입을 추측해내는 것입니다.

만약 MIME 타입 스니핑을 허용한다면 공격자는 비실행 MIME 타입을 실행 MIME 타입으로 전달할 수 있습니다.

예를 들어, 크로스 사이트 스크립팅이 포함된 HTML을 MIME 타입 스니핑을 통해 이미지 파일인 것처럼 업로드할 수 있습니다.

X-Content-Type-Options의 값을 nosniff로 설정하면 유효한 Content-Type인 경우에만 서버에 업로드 됩니다.

유효한 Content-Type의 매칭은 다음과 같습니다.

```
text/css
image/*
application/javascript
application/x-javascript
application/ecmascript
application/json
text/ecmascript
text/javascript
text/json
```

분석 결과

X-Content-Type-Options 헤더가 HTTP 응답에 없습니다.

HTTP 응답의 헤더는 다음과 같습니다.

```
HTTP/1.1 200
Content-Length: 8
Content-Type: text/html;charset=ISO-8859-1
Date: Wed, 05 Feb 2025 13:57:40 GMT
```

해결 방법

MIME 타입 스니핑으로 인한 취약점을 막기 위해서는 웹 애플리케이션 서버가 HTTP 응답에 값이 nosniff인 X-Content-Type-Options 헤더를 포함하도록 해야 합니다.

또는, 사용자가 웹 애플리케이션에 파일을 업로드하지 못하도록 막아야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

누락된 X 콘텐츠 타입 옵션은 HTTP 응답에 X-Content-Type-Options 헤더가 존재하지 않거나 값이 잘못된 취약점입니다.

HTTP 응답메시지에 X-Content-Type-Options가 있고, 그 값이 nosniff이면 MIME 타입 스니핑을 막습니다.

MIME 타입 스니핑이란 MIME 타입이 없거나 클라이언트 타입이 잘못 설정됐다고 판단될 경우, 브라우저가 리소스를 훑어보고 정확한 MIME 타입을 추측해내는 것입니다.

만약 MIME 타입 스니핑을 허용한다면 공격자는 비실행 MIME 타입을 실행 MIME 타입으로 전달할 수 있습니다.

예를 들어, 크로스 사이트 스크립팅이 포함된 HTML을 MIME 타입 스니핑을 통해 이미지 파일인 것처럼 업로드할 수 있습니다.

X-Content-Type-Options의 값을 nosniff로 설정하면 유효한 Content-Type인 경우에만 서버에 업로드 됩니다.

유효한 Content-Type의 매칭은 다음과 같습니다.

```
text/css
image/*
application/javascript
application/x-javascript
application/ecmascript
application/json
text/ecmascript
text/javascript
text/json
```

분석 결과

X-Content-Type-Options 헤더가 HTTP 응답에 없습니다.

HTTP 응답의 헤더는 다음과 같습니다.

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Length: 1070
Content-Type: text/html
Date: Wed, 05 Feb 2025 13:57:34 GMT
ETag: W/"1070-1709185617269"
Last-Modified: Thu, 29 Feb 2024 05:46:57 GMT
```

해결 방법

MIME 타입 스니핑으로 인한 취약점을 막기 위해서는 웹 애플리케이션 서버가 HTTP 응답에 값이 nosniff인 X-Content-Type-Options 헤더를 포함하도록 해야 합니다.

또는, 사용자가 웹 애플리케이션에 파일을 업로드하지 못하도록 막아야 합니다.

● [규칙 이름] 누락된 X 프레임 옵션 (높음, common)

누락된 X 프레임 옵션 취약점은 X-Frame-Options 헤더가 HTTP 응답에 포함되지 않거나 헤더가 올바른 값이 아닌 경우에 발생하는 취약점입니다. X-Frame-Options 헤더는 HTTP 응답의 헤더로써 브라우저가 <frame>, <iframe>, <object> 태그 안의 페이지를 랜더링하도록 설정합니다. 공격자는 악의적인 사이트를 <frame>, <iframe>, <object> 태그 안에 렌더링하여 클릭잭킹을 시도할 수 있습니다. 클릭잭킹이란 사용자가 자신이 클릭하고 있다고 인지하는 것과 다른 것을 클릭하도록 속이는 공격 방식입니다. 이를 통해 공격자는 사용자의 정보를 유출하거나 사용자의 컴퓨터를 제어할 수 있습니다. 이 취약점을 해결하기 위해서는 HTTP 응답 메시지에 올바른 값을 가진 X-Frame-Options 헤더를 포함시켜야 합니다.

- OWASP 2017
  - A6-Security Misconfiguration

- OWASP 2021
  - A05 Security Misconfiguration

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

누락된 X 프레임 옵션 취약점은 X-Frame-Options 헤더가 HTTP 응답에 포함되지 않는 취약점입니다.

X-Frame-Options 헤더는 브라우저가 <frame>, <iframe>, 또는 <object> 태그 안의 페이지를 브라우저가 랜더링할지 여부를 설정하는 HTTP 응답의 헤더입니다.

X-Frame-Options 헤더를 통해 클릭잭킹을 막을 수 있습니다.

클릭잭킹이란 사용자의 인식 없이 실행될 수 있는 임베디드 코드나 스크립트의 형태를 갖추어, 사용자가 자신이 클릭하고 있다고 인지하는 것과 다른 것을 클릭하게 속이는 공격 방식입니다.

이를 통해 공격자는 사용자의 정보를 유출하거나 사용자의 컴퓨터를 제어할 수 있습니다.

분석 결과

HTTP 응답에 X-Frame-Options 헤더가 존재하지 않습니다.

HTTP 응답의 헤더는 다음과 같습니다.

```
HTTP/1.1 200
Content-Length: 8
Content-Type: text/html;charset=ISO-8859-1
Date: Wed, 05 Feb 2025 13:57:40 GMT
```

해결 방법

웹 애플리케이션의 서버가 HTTP 응답에 올바른 값을 가진 X-Frame-Options 헤더를 넣어야 합니다.

X-Frame-Options 헤더의 올바른 값은 다음과 같습니다.

```
DENY : The page cannot be displayed in a frame, regardless of the site
attempting to do so.
SAMEORIGIN : The page can only be displayed in a frame on the same origin as
the page itself.
ALLOW-FROM uri : The page can only be displayed in a frame on the specified
origin.
```

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

누락된 X 프레임 옵션 취약점은 X-Frame-Options 헤더가 HTTP 응답에 포함되지 않는 취약점입니다.

X-Frame-Options 헤더는 브라우저가 <frame>, <iframe>, 또는 <object> 태그 안의 페이지를 브라우저가 랜더링할지 여부를 설정하는 HTTP 응답의 헤더입니다.

X-Frame-Options 헤더를 통해 클릭잭킹을 막을 수 있습니다.

클릭잭킹이란 사용자의 인식 없이 실행될 수 있는 임베디드 코드나 스크립트의 형태를 갖추어, 사용자가 자신이 클릭하고 있다고 인지하는 것과 다른 것을 클릭하게 속이는 공격 방식입니다.

이를 통해 공격자는 사용자의 정보를 유출하거나 사용자의 컴퓨터를 제어할 수 있습니다.

분석 결과

HTTP 응답에 X-Frame-Options 헤더가 존재하지 않습니다.

HTTP 응답의 헤더는 다음과 같습니다.

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Length: 1070
Content-Type: text/html
Date: Wed, 05 Feb 2025 13:57:34 GMT
ETag: W/"1070-1709185617269"
Last-Modified: Thu, 29 Feb 2024 05:46:57 GMT
```

해결 방법

웹 애플리케이션의 서버가 HTTP 응답에 올바른 값을 가진 X-Frame-Options 헤더를 넣어야 합니다.

X-Frame-Options 헤더의 올바른 값은 다음과 같습니다.

```
DENY : The page cannot be displayed in a frame, regardless of the site
attempting to do so.
SAMEORIGIN : The page can only be displayed in a frame on the same origin as
the page itself.
ALLOW-FROM uri : The page can only be displayed in a frame on the specified
origin.
```

● [규칙 이름] 누락된 XSS 보호 헤더 (보통, common)

누락된 XSS 보호 헤더 취약점은 HTTP 응답 메시지의 X-XSS-Protection 헤더가 없거나 제대로 설정되어 있지 않은 취약점입니다. X-XSS-Protection 헤더는 비 지속적 크로스 사이트 스크립팅 감지 시, 페이지 로딩을 중단합니다. 공격자는 이 취약점을 확인하여 비 지속적 크로스 사이트 스크립팅 공격을 시도할 수 있습니다. 그 결과 공격자는 사용자의 정보를 탈취하거나, 서버로 하여금 의도하지 않은 동작을 수행하도록 강제할 수 있습니다. 이를 해결하기 위해서는 웹 애플리케이션의 설정을 변경하여 X-XSS-Protection 헤더를 추가하고 그 값을 0으로 설정해야 합니다.

- OWASP 2017
  - A6-Security Misconfiguration

- OWASP 2021
  - A05 Security Misconfiguration

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

누락된 XSS 보호 헤더 취약점은 HTTP 응답에 XSS 보호 헤더가 없는 취약점입니다.

HTTP 응답의 X-XSS-Protection 헤더는 인터넷 익스플로러, 크롬, 사파리 브라우저에서 페이지 로딩 중 비지속적 크로스 사이트 스크립팅 공격이 감지된 경우, 페이지 로딩을 중단하는 기능의 상태를 나타냅니다.

X-XSS-Protection 헤더의 값이 0이면 크로스 사이트 스크립팅 필터가 사용되지 않음을 나타냅니다.

분석 결과

HTTP 응답에 X-XSS-Protection 헤더가 존재하지 않습니다.

HTTP 응답은 다음과 같습니다.

```
HTTP/1.1 200
Content-Length: 8
Content-Type: text/html;charset=ISO-8859-1
Date: Wed, 05 Feb 2025 13:57:40 GMT
```

해결 방법

웹 애플리케이션의 서버에서 X-XSS-Protection 헤더를 동작시키는 방법은 다음과 같습니다.

Apache(.htaccess) :

```
<IfModule mod_headers.c>
Header set X-XSS-Protection "1; mode=block"
</IfModule>
```

PHP :

```
header("X-XSS-Protection: 1; mode=block");
```

Spring Framework :

```
<http>
<!-- ... -->
<headers>
<xss-protection block="true"/>
</headers>
</http>
```

Node js :

```
app.use(function(req, res, next) {
res.header('X-XSS-Protection', 0);
next();
});
```

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

누락된 XSS 보호 헤더 취약점은 HTTP 응답에 XSS 보호 헤더가 없는 취약점입니다.

HTTP 응답의 X-XSS-Protection 헤더는 인터넷 익스플로러, 크롬, 사파리 브라우저에서 페이지 로딩 중 비지속적 크로스 사이트 스크립팅 공격이 감지된 경우, 페이지 로딩을 중단하는 기능의 상태를 나타냅니다.

X-XSS-Protection 헤더의 값이 0이면 크로스 사이트 스크립팅 필터가 사용되지 않음을 나타냅니다.

분석 결과

HTTP 응답에 X-XSS-Protection 헤더가 존재하지 않습니다.

HTTP 응답은 다음과 같습니다.

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Length: 1070
Content-Type: text/html
Date: Wed, 05 Feb 2025 13:57:34 GMT
ETag: W/"1070-1709185617269"
Last-Modified: Thu, 29 Feb 2024 05:46:57 GMT
```

해결 방법

웹 애플리케이션의 서버에서 X-XSS-Protection 헤더를 동작시키는 방법은 다음과 같습니다.

Apache(.htaccess) :

```
<IfModule mod_headers.c>
Header set X-XSS-Protection "1; mode=block"
</IfModule>
```

PHP :

```
header("X-XSS-Protection: 1; mode=block");
```

Spring Framework :

```
<http>
<!-- ... -->
<headers>
<xss-protection block="true"/>
</headers>
</http>
```

Node js :

```
app.use(function(req, res, next) {
res.header('X-XSS-Protection', 0);
next();
});
```

● [규칙 이름] 레이블 누락 (매우 낮음, common)

레이블 누락 체커는 입력 서식에서 레이블이 누락되었는지 여부를 검출합니다. 레이블을 누락하는 경우 장애가 있는 사용자가 서식에 자료를 입력하는 데 불편을 겪을 수 있습니다. 이를 해결하기 위해 입력 서식에 대응하는 레이블을 제공해야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

다음과 같은 HTTP 요청을 전송했습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

HTTP 응답을 수신했습니다.

HTTP 응답 본문이 HTML 문서인지를 검사했습니다.

HTTP 응답 본문에서 레이블이 필요한 요소를 탐색했습니다.

탐색한 요소의 id 속성을 탐색했습니다.

탐색한 요소의 부모 요소 중 <label> 요소를 탐색했습니다.

분석 결과

HTTP 응답 본문이 HTML 문서에 해당합니다.

HTTP 응답 본문에 레이블이 필요한 요소에 해당하는 <input> 요소가 존재합니다. 해당 요소의 XPath는 다음과 같습니다.

```
/HTML[1]/BODY[1]/FORM[1]/DIV[3]/INPUT[1]
```

해당 요소의 id 속성 값은 다음과 같습니다.

```
username
```

해당 요소의 부모 요소 중, <label> 요소가 존재하지 않습니다.

HTTP 응답 본문에서 for 속성의 값이 다음과 같은 <label> 요소가 존재하지 않습니다.

```
username
```

따라서 레이블이 필요한 요소에 레이블이 누락되었습니다.

해결 방법

<input> 요소의 부모 요소로서 <label> 요소를 추가하세요. 또는 <label> 요소를 추가하고, 해당 요소의 for 속성 값을 <input> 요소의 id 속성 값으로 설정하세요.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

다음과 같은 HTTP 요청을 전송했습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

HTTP 응답을 수신했습니다.

HTTP 응답 본문이 HTML 문서인지를 검사했습니다.

HTTP 응답 본문에서 레이블이 필요한 요소를 탐색했습니다.

탐색한 요소의 id 속성을 탐색했습니다.

탐색한 요소의 부모 요소 중 <label> 요소를 탐색했습니다.

분석 결과

HTTP 응답 본문이 HTML 문서에 해당합니다.

HTTP 응답 본문에 레이블이 필요한 요소에 해당하는 <input> 요소가 존재합니다. 해당 요소의 XPath는 다음과 같습니다.

```
/HTML[1]/BODY[1]/FORM[1]/DIV[5]/INPUT[1]
```

해당 요소의 id 속성 값은 다음과 같습니다.

```
password
```

해당 요소의 부모 요소 중, <label> 요소가 존재하지 않습니다.

HTTP 응답 본문에서 for 속성의 값이 다음과 같은 <label> 요소가 존재하지 않습니다.

```
password
```

따라서 레이블이 필요한 요소에 레이블이 누락되었습니다.

해결 방법

<input> 요소의 부모 요소로서 <label> 요소를 추가하세요. 또는 <label> 요소를 추가하고, 해당 요소의 for 속성 값을 <input> 요소의 id 속성 값으로 설정하세요.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

다음과 같은 HTTP 요청을 전송했습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
```

```
Accept-Language: en-US
```

```
Empty String
```

HTTP 응답을 수신했습니다.

HTTP 응답 본문이 HTML 문서인지를 검사했습니다.

HTTP 응답 본문에서 레이블이 필요한 요소를 탐색했습니다.

탐색한 요소의 id 속성을 탐색했습니다.

탐색한 요소의 부모 요소 중 <label> 요소를 탐색했습니다.

분석 결과

HTTP 응답 본문이 HTML 문서에 해당합니다.

HTTP 응답 본문에 레이블이 필요한 요소에 해당하는 <input> 요소가 존재합니다. 해당 요소의 XPath는 다음과 같습니다.

```
/HTML[1]/BODY[1]/FORM[1]/DIV[7]/INPUT[1]
```

해당 요소의 id 속성 값은 다음과 같습니다.

```
vector
```

해당 요소의 부모 요소 중, <label> 요소가 존재하지 않습니다.

HTTP 응답 본문에서 for 속성의 값이 다음과 같은 <label> 요소가 존재하지 않습니다.

```
vector
```

따라서 레이블이 필요한 요소에 레이블이 누락되었습니다.

해결 방법

<input> 요소의 부모 요소로서 <label> 요소를 추가하세요. 또는 <label> 요소를 추가하고, 해당 요소의 for 속성 값을 <input> 요소의 id 속성 값으로 설정하세요.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

다음과 같은 HTTP 요청을 전송했습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

HTTP 응답을 수신했습니다.

HTTP 응답 본문이 HTML 문서인지를 검사했습니다.

HTTP 응답 본문에서 레이블이 필요한 요소를 탐색했습니다.

탐색한 요소의 id 속성을 탐색했습니다.

탐색한 요소의 부모 요소 중 <label> 요소를 탐색했습니다.

분석 결과

HTTP 응답 본문이 HTML 문서에 해당합니다.

HTTP 응답 본문에 레이블이 필요한 요소에 해당하는 <input> 요소가 존재합니다. 해당 요소의 XPath는 다음과 같습니다.

```
/HTML[1]/BODY[1]/FORM[1]/DIV[8]/INPUT[1]
```

해당 요소의 id 속성 값이 존재하지 않습니다.

해당 요소의 부모 요소 중, <label> 요소가 존재하지 않습니다. 따라서 레이블이 필요한 요소에 레이블이 누락되었습니다.

해결 방법

<input> 요소의 부모 요소로서 <label> 요소를 추가하세요. 또는 <label> 요소를 추가하고, 해당 요소의 for 속성 값을 <input> 요소의 id 속성 값으로 설정하세요.

● [규칙 이름] 비인가된 OPTIONS HTTP 메소드 사용 (보통, common)

OPTIONS 메소드는 현재 웹 서버에서 지원하는 HTTP 메소드의 종류를 확인할 때 사용할 수 있는 메소드입니다. OPTIONS 메소드 요청을 허용하는 경우 공격자가 웹 서버를 보다 효과적으로 공격할 수 있게 됩니다. 공격자는 OPTIONS 메소드에 해당하는 임의의 요청을 서버로 전송합니다. 그 결과, 공격자는 서버로부터 OPTIONS 메소드 요청에 대한 정상 응답을 수신하여 해당 웹 서버에서 허용하는 메소드 목록에 대한 정보를 탈취할 수 있습니다. 그리고 추가적인 공격을 위한 자료로 활용할 수 있습니다. 이 취약점을 해결하기 위해서는 불필요한 OPTIONS 메소드 요청을 허용하지 않도록 조치가 필요합니다.

- OWASP 2017
  - A3-Sensitive Data Exposure

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

OPTIONS 메소드 허용 취약점은 웹 서버가 허용되지 않는 사용자에게 OPTIONS 메소드의 결과를 돌려주는 취약점입니다.

OPTIONS 메소드는 현재 웹 서버에서 지원하는 메소드의 종류를 확인할 때 사용할 수 있는 메소드입니다.

이러한 OPTIONS 메소드의 허용은 웹 서버의 민감한 정보를 노출할 수 있으며, 2차적 공격으로 이어질 수 있습니다.

비인가된 OPTIONS 메소드를 검출하기 위해 OPTIONS 메소드를 설정한 다음의 HTTP 요청을 보냈습니다.

```
OPTIONS http://125.141.219.118:39251/benchmark/BenchmarkTest01660?
username=sparrow8dast2text4&password=sparrow8dast2text4&vector=SafeText HTTP
/1.1
Upgrade-Insecure-Requests: 1
Referer: http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) HeadlessChrome/103.0.5060.134 Safari/537.36
```

```
Empty String
```

분석 결과

HTTP 요청에 따른 HTTP 응답은 다음과 같습니다.

```
HTTP/1.1 200
Allow: GET, HEAD, POST, TRACE, OPTIONS
Content-Length: 0
Date: Wed, 05 Feb 2025 13:57:46 GMT
```

OPTIONS 메소드 HTTP 요청에 대하여 다음의 허용된 HTTP 메소드 목록이 포함되었음을 확인할 수 있습니다.

```
GET, HEAD, POST, TRACE, OPTIONS
```

해결 방법

임의의 사용자에 의한 OPTIONS 메소드 HTTP 요청은 허용하지 않도록 권장합니다.

이를 위하여 적절한 서버 설정이 필요합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

OPTIONS 메소드 허용 취약점은 웹 서버가 허용되지 않는 사용자에게 OPTIONS 메소드의 결과를 돌려주는 취약점입니다.

OPTIONS 메소드는 현재 웹 서버에서 지원하는 메소드의 종류를 확인할 때 사용할 수 있는 메소드입니다.

이러한 OPTIONS 메소드의 허용은 웹 서버의 민감한 정보를 노출할 수 있으며, 2차적 공격으로 이어질 수 있습니다.

비인가된 OPTIONS 메소드를 검출하기 위해 OPTIONS 메소드를 설정한 다음의 HTTP 요청을 보냈습니다.

```

```

```
OPTIONS http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.
1
Accept-Language: en-US
```

```
Empty String
```

분석 결과

HTTP 요청에 따른 HTTP 응답은 다음과 같습니다.

```
HTTP/1.1 200
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
Content-Length: 0
Date: Wed, 05 Feb 2025 13:57:45 GMT
```

OPTIONS 메소드 HTTP 요청에 대하여 다음의 허용된 HTTP 메소드 목록이 포함되었음을 확인할 수 있습니다.

```
GET, HEAD, POST, PUT, DELETE, OPTIONS
```

해결 방법

임의의 사용자에 의한 OPTIONS 메소드 HTTP 요청은 허용하지 않도록 권장합니다.

이를 위하여 적절한 서버 설정이 필요합니다.

● [규칙 이름] 입력 누락에 대한 반응 없음 (매우 낮음, common)

입력 누락에 대한 반응 없음 체커는 사용자가 누락한 입력에 대해 적절한 반응이 없는 경우를 검출합니다. 사용자가 누락한 입력에 대해 적절한 반응이 없는 경우, 사용자 스스로가 잘못 입력했는지 여부를 파악하기가 어려울 수 있습니다. 이를 해결하기 위해 사용자가 누락한 입력에 대한 적절한 반응을 제공해야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

분석 대상 페이지에 접근했습니다. 접근 과정은 다음과 같습니다.

```
URL: http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html
```

분석 대상 페이지가 HTML 문서인지를 검사했습니다.

분석 대상 페이지에서 <form> 요소를 탐색했습니다.

탐색한 <form> 요소의 자식 요소 중 입력 가능한 요소를 탐색했습니다.

탐색한 <form> 요소의 값을 빈 문자열로 설정했습니다.

탐색한 <form> 요소의 자식 요소 중 <input type='submit'> 요소를 탐색했습니다.

탐색한 <form> 요소에 대하여 <input type='submit'> 이벤트가 발생했습니다.

해당 이벤트를 수행한 후에 서버의 반응을 확인했습니다.

분석 결과

분석 대상 페이지가 HTML 문서에 해당합니다.

분석 대상 페이지에 <form> 요소가 존재합니다. 해당 요소의 XPath는 다음과 같습니다.

```
/HTML[1]/BODY[1]/FORM[1]
```

<form> 요소의 자식 요소 중 3개의 입력 가능한 요소가 존재합니다.

<form> 요소의 자식 요소 중 <input type='submit'> 요소가 존재합니다. 해당 요소의 XPath는 다음과 같습니다.

```
/HTML[1]/BODY[1]/FORM[1]
```

<input type='submit'> 요소에 대하여 <form> 이벤트를 발생시킨 결과, 해당 이벤트 이전과 DOM이 동일하고 메시지 창이 팝업되지 않습니다.

따라서 입력이 누락된 경우 서버가 응답하지 않았습니다.

해결 방법

<form> 요소에 빈 문자열을 입력한 경우, DOM을 변경하거나 메시지 창을 팝업하도록 수정하세요.

● [규칙 이름] 잘못된 HTML (매우 낮음, common)

잘못된 HTML 체커는 페이지 내용 중 표준 (X)HTML 문법을 준수하지 않은 부분이 존재하는지 여부를 검사합니다. 페이지를 작성할 때 표준 (X)HTML 문법을 준수하지 않는 경우 해당 페이지의 처리 방식이 브라우저마다 다르기 때문에 사용자에게 전달하는 정보에 차이가 발생할 수 있습니다. 이를 해결하기 위해 페이지를 작성할 때 표준 (X)HTML 문법을 준수해야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

다음과 같은 HTTP 요청 메시지를 전송했습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

HTTP 응답을 수신했습니다.

HTTP 응답 본문이 (X)HTML 문서인지를 검사했습니다.

HTTP 응답 본문에 대하여 W3C 마크업 검사기 분석을 수행했습니다.

분석 결과

HTTP 응답 본문이 (X)HTML 문서에 해당합니다.

W3C 마크업 검사기 분석 결과, 다음과 같은 ''오류'' 항목이 발생했습니다.

```
Almost standards mode doctype. Expected <!DOCTYPE html>.
```

해결 방법

W3C 마크업 검사기 분석 결과를 참고하여 HTTP 응답 본문에 해당하는 (X)HTML 문서를 수정하세요.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

다음과 같은 HTTP 요청 메시지를 전송했습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

HTTP 응답을 수신했습니다.

HTTP 응답 본문이 (X)HTML 문서인지를 검사했습니다.

HTTP 응답 본문에 대하여 W3C 마크업 검사기 분석을 수행했습니다.

분석 결과

HTTP 응답 본문이 (X)HTML 문서에 해당합니다.

W3C 마크업 검사기 분석 결과, 다음과 같은 ''경고'' 항목이 발생했습니다.

```
The type attribute is unnecessary for JavaScript resources.
```

해결 방법

W3C 마크업 검사기 분석 결과를 참고하여 HTTP 응답 본문에 해당하는 (X)HTML 문서를 수정하세요.

● [규칙 이름] 쿠키 속성 검사(HttpOnly) (낮음, common)

웹 쿠키는 악의적인 사용자의 주요 공격 벡터인 경우가 많으므로 애플리케이션은 쿠키를 보호하기 위한 보안 속성을 사용해야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

쿠키 속성 검사(HttpOnly)는 HTTP 응답에 Set-Cookie를 확인하여 HttpOnly 속성이 있는지 확인하는 체커입니다.

이를 검출하기 위해 다음과 같은 HTTP 요청을 보냈습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660?
username=sparrow8dast2text4&password=sparrow8dast2text4&vector=SafeText HTTP
/1.1
Upgrade-Insecure-Requests: 1
Referer: http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) HeadlessChrome/103.0.5060.134 Safari/537.36
```

```
Empty String
```

분석 결과

HTTP 요청에 대한 응답에 Set-Cookie 정보가 존재하지 않습니다.

해결 방법

쿠키 속성은 서버에서 HTTP 응답에 Set-Cookie 헤더를 포함하거나 JavaScript를 통해 설정할 수 있습니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

쿠키 속성 검사(HttpOnly)는 HTTP 응답에 Set-Cookie를 확인하여 HttpOnly 속성이 있는지 확인하는 체커입니다.

이를 검출하기 위해 다음과 같은 HTTP 요청을 보냈습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

분석 결과

HTTP 요청에 대한 응답에 Set-Cookie 정보가 존재하지 않습니다.

해결 방법

쿠키 속성은 서버에서 HTTP 응답에 Set-Cookie 헤더를 포함하거나 JavaScript를 통해 설정할 수 있습니다.

● [규칙 이름] 쿠키 속성 검사(SameSite) (보통, common)

웹 쿠키는 악의적인 사용자의 주요 공격 벡터인 경우가 많으므로 애플리케이션은 쿠키를 보호하기 위한 보안 속성을 사용해야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

쿠키 속성 검사(SameSite)는 HTTP 응답에 Set-Cookie를 확인하여 SameSite 속성이 있는지 확인하는 체커입니다.

이를 검출하기 위해 다음과 같은 HTTP 요청을 보냈습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660?
username=sparrow8dast2text4&password=sparrow8dast2text4&vector=SafeText HTTP
/1.1
Upgrade-Insecure-Requests: 1
Referer: http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) HeadlessChrome/103.0.5060.134 Safari/537.36
```

```
Empty String
```

분석 결과

HTTP 요청에 대한 응답에 Set-Cookie 정보가 존재하지 않습니다.

해결 방법

사이트 간 요청 위조(CSRF)를 막기 위해 SameSite 속성을 Lax나 Strict로 설정하는 것이 좋습니다.

구글 크롬도 80 버전으로 업데이트되면서 SameSite 속성의 기본값을 None에서 Lax로 강화했습니다.

만약 None으로 사용해야 한다면 반드시 Secure 속성과 함께 사용해야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

쿠키 속성 검사(SameSite)는 HTTP 응답에 Set-Cookie를 확인하여 SameSite 속성이 있는지 확인하는 체커입니다.

이를 검출하기 위해 다음과 같은 HTTP 요청을 보냈습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

분석 결과

HTTP 요청에 대한 응답에 Set-Cookie 정보가 존재하지 않습니다.

해결 방법

사이트 간 요청 위조(CSRF)를 막기 위해 SameSite 속성을 Lax나 Strict로 설정하는 것이 좋습니다.

구글 크롬도 80 버전으로 업데이트되면서 SameSite 속성의 기본값을 None에서 Lax로 강화했습니다.

만약 None으로 사용해야 한다면 반드시 Secure 속성과 함께 사용해야 합니다.

● [규칙 이름] 쿠키 속성 검사(Secure) (보통, common)

웹 쿠키는 악의적인 사용자의 주요 공격 벡터인 경우가 많으므로 애플리케이션은 쿠키를 보호하기 위한 보안 속성을 사용해야 합니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

쿠키 속성 검사(Secure)는 HTTP 응답에 Set-Cookie를 확인하여 Secure 속성이 있는지 확인하는 체커입니다.

이를 검출하기 위해 다음과 같은 HTTP 요청을 보냈습니다.

```
```

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660?
username=sparrow8dast2text4&password=sparrow8dast2text4&vector=SafeText HTTP
/1.1
Upgrade-Insecure-Requests: 1
Referer: http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) HeadlessChrome/103.0.5060.134 Safari/537.36
```

```
Empty String
```

분석 결과

HTTP 요청에 대한 응답에 Set-Cookie 정보가 존재하지 않습니다.

해결 방법

Secure 속성은 HTTP에서 동작하지 않으므로 HTTPS로 변경해야 합니다.

쿠키 속성은 서버에서 HTTP 응답에 Set-Cookie 헤더를 포함하거나 JavaScript를 통해 설정할 수 있습니다.

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html

분석 방법

쿠키 속성 검사(Secure)는 HTTP 응답에 Set-Cookie를 확인하여 Secure 속성이 있는지 확인하는 체커입니다.

이를 검출하기 위해 다음과 같은 HTTP 요청을 보냈습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html HTTP/1.1
Accept-Language: en-US
```

```
Empty String
```

분석 결과

HTTP 요청에 대한 응답에 Set-Cookie 정보가 존재하지 않습니다.

해결 방법

Secure 속성은 HTTP에서 동작하지 않으므로 HTTPS로 변경해야 합니다.

쿠키 속성은 서버에서 HTTP 응답에 Set-Cookie 헤더를 포함하거나 JavaScript를 통해 설정할 수 있습니다.

● [규칙 이름] 크로스 사이트 스크립팅 (매우 높음, common)

크로스 사이트 스크립팅 취약점은 웹 사이트에 악성 스크립트를 삽입할 수 있는 취약점입니다. 공격자는 폼 내부에 있는 텍스트 입력과 같은 웹 요소를 통해 악성 스크립트를 서버로 전송합니다. 서버가 해당 데이터를 검증하지 않고 그대로 응답에 포함하는 경우, 악성 스크립트가 브라우저에서 실행됩니다. 그 결과, 공격자는 세션, 쿠키와 같은 사용자의 정보를 탈취하거나 서버에서 의도하지 않은 동작을 실행하도록 강제할 수 있습니다. 이 취약점을 해결하기 위해서는 웹 애플리케이션이 사용자로부터 입력 받은 값을 검증 및 필터링해야 합니다. 즉, 태그의 이름, 속성, <script> 태그 내부, <style> 태그 내부, HTML 주석 내부 등에 사용자 입력 데이터를 되도록 사용하지 않고 사용자 입력 데이터를 사용해야만 하는 경우 ''<'', ''>'' 와 같은 기호를 변환하거나 인코딩하도록 합니다.

- 소프트웨어 보안약점 진단가이드 2021
  - 크로스사이트 스크립트

- 주요정보통신기반시설 취약점 분석·평가 기준
  - 크로스사이트 스크립팅

URL http://125.141.219.118:39251/benchmark/BenchmarkTest01660

분석 방법

크로스 사이트 스크립팅(xss) 취약점은 웹 사이트에 대하여 악성 스크립트를 삽입할 수 있는 취약점입니다.

웹 애플리케이션 서버가 외부에서 입력되는 값을 검증 없이 사용하면, 공격자가 악의적인 스크립트를 입력하여 웹 애플리케이션 사용자의 정보를 탈취하거나 웹 애플리케이션이 의도치 않은 동작을 하도록 만들 수 있습니다.

비지속적 크로스사이트 스크립팅은 공격자가 입력한 악의적인 스크립트가 별도의 검증 없이 즉시 웹 페이지에 표시되는 취약점입니다.

이러한 비지속적 크로스 사이트 스크립팅 취약점을 검출하기 위해 vector 파라미터에 135abc<script>alert(1);</script>efg246 공격 문자열을 포함한 HTTP 요청을 다음과 같이 보냈습니다.

```
GET http://125.141.219.118:39251/benchmark/BenchmarkTest01660?
username=sparrow8dast2text4&vector=135abc%3Cscript%3Ealert(1);%3C/script%
3Efg246&password=sparrow8dast2text4 HTTP/1.1
Upgrade-Insecure-Requests: 1
Referer: http://125.141.219.118:39251/benchmark/BenchmarkTest01660.html
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) HeadlessChrome/103.0.5060.134 Safari/537.36
```

```
Empty String
```

분석 결과

비지속적 크로스 사이트 스크립팅은 에러 메시지, 검색 결과, 기타 입력 데이터를 포함한 HTTP 응답 메시지 등으로 서버에 입력한 스크립트가 돌아옵니다.

HTTP 요청에 대한 HTTP 응답 메시지는 다음과 같습니다.

```
HTTP/1.1 200
Content-Length: 38
Content-Type: text/html;charset=ISO-8859-1
Date: Wed, 05 Feb 2025 13:57:46 GMT
135abc<script>alert(1);</script>efg246
```

위 HTTP 응답 메시지에서 <script>alert(1);</script> 공격 문자열이 포함되어 있는 것을 확인할 수 있습니다.

해결 방법

해결 방법은 다음과 같습니다.

비 지속적 크로스 사이트 스크립팅 취약점을 제거하려면 사용자로부터 입력 받은 외부 데이터를 검증 및 필터링해야 합니다.

기본적으로 태그의 이름이나 태그 속성의 이름, <script> 태그 사이, <style> 태그 사이 및 HTML 주석 사이와 허용되지 않은 위치에 사용자로부터 입력 받은 외부 데이터를 사용하지 않아야 합니다.

또는, 사용자로부터 입력 받은 외부 데이터를 사용해야 하는 경우에는 다음과 같이 데이터를 인코딩하여 사용하여야 합니다.

웹 페이지 요소 사용자로부터 입력 받은 외부 데이터를 사용할 때의 인코딩

```
& --> &amp;
< --> &lt;
> --> &gt;
" --> &quot;
' --> &#x27;
/ --> &#x2F;
```

이외에도 사용자로부터 입력 받은 외부 데이터를 HTML 속성값이나 URL 매개변수, JavaScript, CSS 값 등에 사용할 때에도 인코딩이 필요합니다.

Java :

```
String userInput = request.getParameter("input");
// ## # ## # ###
if (isValidInput(userInput)) {
// ### ##
} else {
// ## ##
}
boolean isValidInput(String input) {
// ## ## ## ### #### ### #### ## ### ##
return !input.matches(".*[<>&\"].*");
}
```

JSP :

```
<%
String userInput = request.getParameter("input");
// ## # ## # ###
if (isValidInput(userInput)) {
// ### ##
} else {
// ## ##
```

```
}
%>
<%
boolean isValidInput(String input) {
// ## ## ## ### #### ### #### ## ### ##
return !input.matches(".*[<>&\"].*");
}
%>
```

PHP :

```
<?php
$userInput = $_POST['input'];
// ## # ## # ###
if (isValidInput($userInput)) {
// ### ##
} else {
// ## ##
}
function isValidInput($input) {
// ## ## ## ### #### ### #### ## ### ##
return !preg_match("/[<>&\"]/", $input);
}
?>
```

제외된 이슈 정보

제외된 이슈가 없습니다.

■ 이슈 검출 규칙 정보

유형	위험도	언어	이름
웹취약점	보통	common	AJP 서비스 노출
웹취약점	매우 높음	common	CRLF 삽입
웹취약점	높음	common	CSRF 토큰이 없는 폼 태그
웹취약점	보통	common	Host 헤더
웹취약점	매우 낮음	common	HTML5에서 사용되지 않는 구성 요소
웹취약점	보통	common	HTTP 메소드 위조
웹취약점	높음	common	HTTP 응답 헤더에 포함된 서버 정보
웹취약점	보통	common	JMX/RMI 서비스 노출
웹취약점	낮음	common	Meta 태그 안에 포함된 민감한 정보
웹취약점	매우 높음	common	PHF CGI 원격 명령 실행
웹취약점	보통	common	Slow HTTP Post Attack
웹취약점	보통	common	Slowloris HTTP DOS
웹취약점	낮음	common	Snoop 서블릿 정보 노출
웹취약점	매우 높음	common	SQL 삽입
웹취약점	높음	common	SQL 인젝션
웹취약점	매우 높음	common	SSI 삽입
웹취약점	높음	common	Tomcat 예제
웹취약점	높음	common	URL 내 세션 ID
웹취약점	높음	common	URL 접근 제한 실패
웹취약점	낮음	common	web.xml 노출
웹취약점	보통	common	X-XSS-나이트메어(XXN)
웹취약점	낮음	common	Xitami Web Server 정보 유출
웹취약점	매우 높음	common	XPath 삽입
웹취약점	높음	common	XPath 인젝션
웹취약점	보통	common	개별 주소 노출
웹취약점	매우 높음	common	검증되지 않은 리다이렉션
웹취약점	매우 높음	common	경로 조작
웹취약점	보통	common	관리자 페이지 노출
웹취약점	매우 낮음	common	기본 언어 표시 누락
웹취약점	매우 낮음	common	끊어진 건너뛰기 링크
웹취약점	낮음	common	누락된 Content-Security-Policy (CSP) 헤더
웹취약점	보통	common	누락된 X 콘텐츠 타입 옵션

웹취약점	높음	common	누락된 X 프레임 옵션
웹취약점	보통	common	누락된 XSS 보호 헤더
웹취약점	보통	common	누락된 콘텐츠 타입
웹취약점	보통	common	누락된 쿠키 HttpOnly 플래그
웹취약점	보통	common	누락된 쿠키 보안 플래그
웹취약점	매우 낮음	common	대체 텍스트 누락
웹취약점	보통	common	디렉터리 인덱싱
웹취약점	매우 높음	common	디렉토리 목록화
웹취약점	매우 낮음	common	레이블 누락
웹취약점	매우 높음	common	로컬 파일 포함
웹취약점	높음	common	버퍼 오버플로우
웹취약점	매우 낮음	common	부적절한 제목
웹취약점	매우 높음	common	불충분한 세션 종료
웹취약점	매우 높음	common	블라인드 LDAP 삽입
웹취약점	매우 높음	common	블라인드 SQL 삽입
웹취약점	매우 높음	common	블라인드 XPath 삽입
웹취약점	보통	common	비밀번호 오류 제한 부재
웹취약점	보통	common	비밀번호 자동 완성
웹취약점	보통	common	비인가된 OPTIONS HTTP 메소드 사용
웹취약점	매우 낮음	common	비표준 기술 사용
웹취약점	매우 높음	common	세션 고정
웹취약점	매우 높음	common	세션 재사용
웹취약점	보통	common	신용카드번호 노출
웹취약점	높음	common	애플리케이션 오류
웹취약점	보통	common	여권번호 노출
웹취약점	매우 높음	common	예측 가능한 세션
웹취약점	낮음	common	오류 페이지 내의 민감한 정보
웹취약점	매우 높음	common	운영체제 명령어 삽입
웹취약점	보통	common	운전면허번호 노출
웹취약점	매우 높음	common	원격 파일 포함
웹취약점	매우 낮음	common	이메일 주소 노출
웹취약점	보통	common	인증서 무결성 위반
웹취약점	보통	common	임시 파일 노출
웹취약점	매우 낮음	common	입력 누락에 대한 반응 없음
웹취약점	매우 낮음	common	잘못된 CSS
웹취약점	매우 낮음	common	잘못된 HTML

웹취약점	매우 낮음	common	잘못된 링크 텍스트
웹취약점	보통	common	잘못된 캐시 통제
웹취약점	높음	common	적절하지 않은 난수값 사용
웹취약점	보통	common	조작 가능한 참조
웹취약점	보통	common	조작 가능한 폼 액션
웹취약점	보통	common	주민등록번호 노출
웹취약점	높음	common	주석문 안에 포함된 시스템 주요정보
웹취약점	높음	common	중요정보 평문 전송
웹취약점	높음	common	충분하지 않은 키 길이 사용
웹취약점	매우 높음	common	취약한 비밀번호
웹취약점	매우 높음	common	코드 삽입
웹취약점	낮음	common	쿠키 속성 검사(HttpOnly)
웹취약점	보통	common	쿠키 속성 검사(SameSite)
웹취약점	보통	common	쿠키 속성 검사(Secure)
웹취약점	보통	common	크로스 도메인 스크립트 포함
웹취약점	매우 높음	common	크로스 사이트 스크립팅
웹취약점	보통	common	크로스 프레임 스크립팅
웹취약점	보통	common	클라이언트가 시작한 SSL 재협상 활성화
웹취약점	높음	common	파라미터 변조
웹취약점	낮음	common	파라미터 쿼리 변환
웹취약점	매우 낮음	common	파일 절대 경로 노출
웹취약점	보통	common	형식 문자열 삽입
웹취약점	매우 낮음	common	호환되지 않는 CSS
웹취약점	매우 낮음	common	호환되지 않는 HTML
웹취약점	매우 낮음	common	호환되지 않는 자바스크립트
웹취약점	보통	common	혼합된 콘텐츠