Sparrow 분석 보고서

[클라이드 검사]

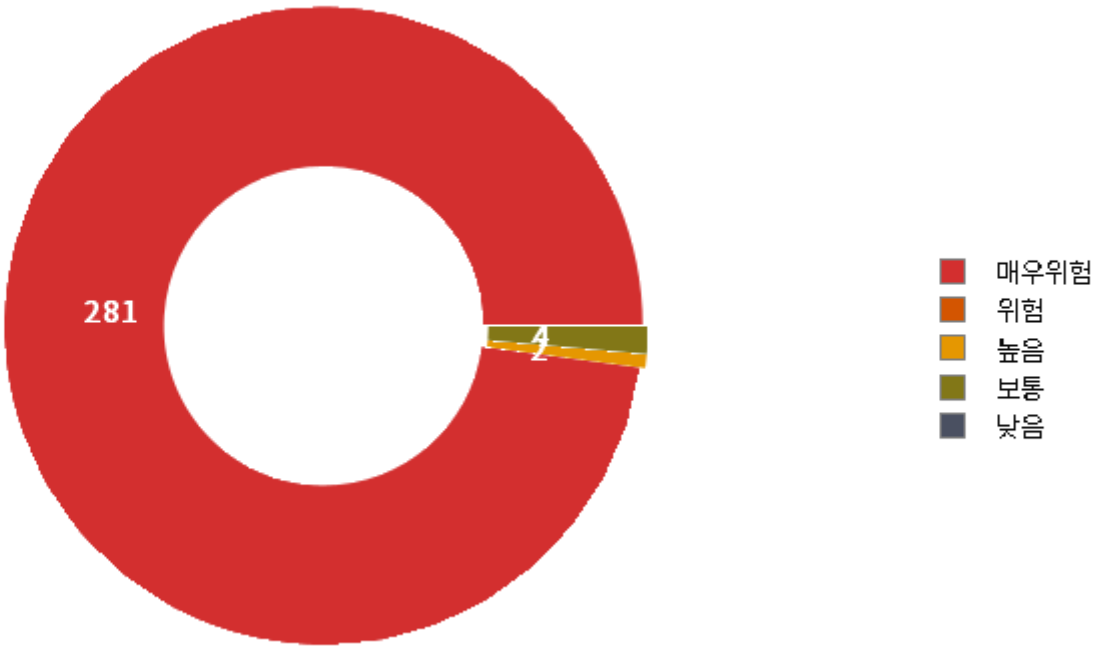
2021-03-09

1. 결과 요약

1.1 프로젝트 정보

상위 프로젝트	ROOT
프로젝트 명	클라이드 검사
프로젝트 키	admin_WEB_1605785552
분석ID	4117
분석 일시	2021-03-09 02:07:37 ~ 2021-03-09 02:08:11(00h 00m 34s)
분석자	UserName(admin)
체커 그룹	KT(423/873)
언어	PHP, ASP(.Net)/VBS
소스 파일	99
빌드라인	15529
총 이슈	287

1.2 위험도별 진단 결과



위험도	매우위험	위험	높음	보통	낮음	총계
개수	281	0	2	4	0	287

1.3 레퍼런스 별 진단 결과

레퍼런스	검출 결함	결과
CWE	862	부적합
OWASP	2229	부적합

1.3.1 CWE

중분류	소분류	결함수
#2011 CWE/SANS Top 25	Top 25 2011-01.SQL Injection	101
	Top 25 2011-04.Cross-site Scripting	145
	Top 25 2011-13.Path Traversal	12
	Top 25 2011-22.Open Redirect	19
001~099	CWE-22	12
	CWE-23	12
	CWE-36	12
	CWE-73	12
	CWE-79	145
	CWE-80	145
	CWE-89	101
	CWE-95	2
100~199	CWE-113	4
300~399	CWE-330	4
	CWE-338	4
400~499	CWE-426	12
500~599	CWE-564	101
600~699	CWE-601	19

1.3.2 OWASP

중분류	소분류	결함수
#Mobile Top 10 2014	Mobile Top 10 2014-M01-Weak Server Side Controls	246
	Mobile Top 10 2014-M07-Client Side Injection	246
#Mobile Top 10 2016	Mobile Top 10 2016-M07-Client Code Quality	145
#Top 10 2004	Top 10 2004-A01-Unvalidated Input	16
	Top 10 2004-A04-Cross Site Scripting	145
	Top 10 2004-A06-Injection Flaws	103
#Top 10 2007	Top 10 2007-A01-Cross Site Scripting	145
	Top 10 2007-A02-Injection Flaws	107
	Top 10 2007-A04-Insecure Direct Object Reference	12
#Top 10 2010	Top 10 2010-A01-Injection	107
	Top 10 2010-A02-Cross-site Scripting(XSS)	145
	Top 10 2010-A04-Insecure Direct Object References	12
	Top 10 2010-A07-Insecure Cryptographic Storage	4
	Top 10 2010-A10-Unvalidated Redirects and Forwards	23
#Top 10 2013	Top 10 2013-A01-Injection	107
	Top 10 2013-A03-Cross-Site Scripting (XSS)	145

	Top 10 2013-A04-Insecure Direct Object References	12
	Top 10 2013-A10-Unvalidated Redirects and Forwards	23
#Top 10 2017	Top 10 2017-A01-Injection	107
	Top 10 2017-A05-Broken Access Control	12
	Top 10 2017-A07-Cross-Site Scripting (XSS)	145
E~H	Failure of true random number generator	4
	HTTP Response Splitting	4
M~P	Preventing SQL Injection in Java	101
Q~T	Relative Path Traversal	12
	SQL Injection	101

2. 상세 결과

2.1 FORBIDDEN.EVAL_FUNCTION : Javascript(2)

원격 코드 실행 체커는 eval 함수를 사용하는 경우를 검출합니다.
eval 함수를 사용하면, 호출할 때 동적으로 파서가 동작하여 실행되므로 속도가 매우 느려집니다.
eval() 함수를 사용하지 않습니다.

CWE
CWE-95

OWASP
Top 10 2004-A06-Injection Flaws
Top 10 2007-A02-Injection Flaws
Top 10 2010-A01-Injection
Top 10 2013-A01-Injection
Top 10 2017-A01-Injection

예시

```
/** example 1 */
JSONData = '{"color" : new Date()}';
document.writeln(eval('('+JSONData + ')').color);
 /** example 2*/
var dateFn = "Date(1971,3,8)";
var myDate;
eval("myDate = new " + dateFn + ";");
 /** example 3*/
var a = 1;
eval("var a = 2");
alert(a) // 2
```

라인 3: eval() 함수를 사용했습니다.

해결방법

```
/** example 1 */
JSONData = '{"color" : new Date()}';
testObject = JSONData.parseJSON();
document.writeln(testObject.color);
 /** example 2*/
var dateFn = "Date(1971,3,8)";
var myDate;
myDate = new dateFn;
 /** example 3*/
var a = 1;
```

```
(function() {
    eval("var a = 2");
}());
alert(a) // 1;
```

라인 3: JSON 데이터를 파싱할 때는 eval대신 parseJSON을 사용합니다.
라인 8: eval을 사용하지 않습니다.
라인 12: function closure를 사용하여 호출하여, 외부 변수에 영향이 없도록 호출합니다.

이슈ID	위험도
472907	높음
체커명	FORBIDDEN.EVAL_FUNCTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	92
의견	

이슈ID	위험도
472908	높음
체커명	FORBIDDEN.EVAL_FUNCTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	25
의견	

2.2 HEADER_MANIPULATION : VBS(4)

HTTP 헤더 조작 체커는 검증되지 않은 외부 입력이 HTTP 응답 헤더에 포함되는 경우를 검출합니다.
외부 입력을 헤더에 포함시킬 때는 충분한 필터를 거친 안전한 값만 전달합니다.

CWE

CWE-113

OWASP

Top 10 2004-A01-Unvalidated Input

Top 10 2007-A02-Injection Flaws

Top 10 2010-A01-Injection

Top 10 2010-A10-Unvalidated Redirects and Forwards

Top 10 2013-A01-Injection

Top 10 2013-A10-Unvalidated Redirects and Forwards

Top 10 2017-A01-Injection

HTTP Response Splitting

예시

```
user = Request.Form(USER_PARAM)
Response.Cookies("user") = user
```

라인 2: 검증되지 않은 외부값이 HTTP 응답 헤더에 사용되었습니다.

해결방법

```
user = Request.Form(USER_PARAM)
user = Filter(user)
Response.Cookies("user") = user
```

라인 2: 검증되지 않은 값은 필터링하여 사용해야 합니다.

이슈ID	위험도
472910	매우위험
체커명	HEADER_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok_pro.asp
위반라인	95
의견	이슈일괄변경

이슈ID	위험도
472911	매우위험
체커명	HEADER_MANIPULATION

파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok_pro.asp
위반라인	96
의견	이슈일괄변경

이슈ID	위험도
472952	매우위험
체커명	HEADER_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok.asp
위반라인	119
의견	이슈일괄변경

이슈ID	위험도
472953	매우위험
체커명	HEADER_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok.asp
위반라인	120
의견	이슈일괄변경

2.3 INSECURE_RANDOMNESS : VBS(4)

부적절한 난수 생성 체커는 예측 가능한 난수를 사용하는 코드를 검출합니다.
Rnd() 함수는 예측 가능합니다.
암호학적으로 충분히 안전한 방식을 사용하여 예측 불가능한 난수를 생성해야 합니다.

CWE

CWE-330
CWE-338

OWASP

Top 10 2010-A07-Insecure Cryptographic Storage
Failure of true random number generator

예시

```
Function genReceiptURL(baseURL)
   Dim randNum
   randNum = Rnd()
   genReceiptURL = baseURL & randNum & ".html"
End Function
```

라인 3: 예측 가능한 Rnd() 함수를 사용했습니다.

해결방법

```
Function genReceiptURL(baseURL)
   Dim randNum
   randNum = SecureRnd()
   genReceiptURL = baseURL & randNum & ".html"
End Function
```

라인 3: Rnd() 함수가 아닌 예측 불가능한 SecureRnd() 함수를 사용하도록 합니다.

이슈ID	위험도
472936	보통
체커명	INSECURE_RANDOMNESS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ij.asp
위반라인	251
의견	

이슈ID	위험도
472942	보통
체커명	INSECURE_RANDOMNESS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ne.asp
위반라인	212
의견	

이슈ID	위험도
472955	보통
체커명	INSECURE_RANDOMNESS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_nj.asp
위반라인	252
의견	

이슈ID	위험도
472981	보통
체커명	INSECURE_RANDOMNESS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ie.asp
위반라인	216
의견	

2.4 OPEN_REDIRECT : VBS(19)

신뢰할 수 없는 주소로 자동 연결 체커는 검증되지 않은 외부 입력값으로 생성된 URL 주소로 자동 연결하는 코드를 검출합니다.
자동 연결할 외부 사이트의 URL과 도메인은 화이트 리스트로 관리하고, 사용자 입력값을 자동 연결할 사이트 주소로 사용하는 경우에는 입력된 값이 화이트 리스트에 존재하는지 확인해야 합니다.

CWE

Top 25 2011-22.Open Redirect
CWE-601

OWASP

Top 10 2010-A10-Unvalidated Redirects and Forwards
Top 10 2013-A10-Unvalidated Redirects and Forwards

예시

```
strDest = Request.Form("dest")
HyperLink.NavigateTo strDest
```

라인 2: 검증되지 않은 외부값이 자동 연결 URL에 사용되었습니다.

해결방법

```
strDest = Request.Form("dest")
strDest = Filter(strDesc)
HyperLink.NavigateTo strDest
```

라인 2: 필터 함수를 통해 외부 입력을 검증하여 사용합니다.

이슈ID	위험도
472828	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	594
의견	

이슈ID	위험도
472855	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	184
의견	

이슈ID	위험도
472887	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	227
의견	

이슈ID	위험도
472963	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form_ok.asp
위반라인	261
의견	

265.

이슈ID	위험도
472964	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form_ok.asp
위반라인	263
의견	

이슈ID	위험도
472987	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_form_ok.asp
위반라인	303
의견	

이슈ID	위험도
473020	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/dext_img_name_ok.asp
위반라인	100
의견	

104.%>

이슈ID	위험도
473021	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	67
의견	

이슈ID	위험도
473023	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	69
의견	

이슈ID	위험도
473030	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/del_ok.asp
위반라인	33
의견	

이슈ID	위험도
473032	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	142
의견	

이슈ID	위험도
473033	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	144
의견	

이슈ID	위험도
473044	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	43
의견	

이슈ID	위험도
473046	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/view.asp
위반라인	36
의견	

이슈ID	위험도
473052	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/view.asp
위반라인	74
의견	

이슈ID	위험도
473054	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/view.asp
위반라인	76
의견	

```
78.else
79.if board_type=3 then
80.Response.Redirect "digital_diary_c.asp?tb="&tb&"&page="&page&"&num="&num
```

이슈ID	위험도
473056	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/view.asp
위반라인	80
의견	

이슈ID	위험도
473058	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/view.asp
위반라인	82
의견	

이슈ID	위험도
473066	매우위험
체커명	OPEN_REDIRECT
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/abc_img_name_ok.asp
위반라인	108
의견	

```
109.end if
110.
111.
112.%>
```

2.5 PATH_MANIPULATION : VBS(12)

경로 조작 체커는 검증되지 않은 외부 입력값으로 생성된 경로를 통해 파일 시스템에 접근하는 코드를 검출합니다.
외부 입력을 리소스(파일 등)의 식별자로 사용하기 위해 적절한 검증을 거치도록 합니다. 특히, 파일명을 외부 입력으로 사용하는 경우 경로 순회(Directory Traversal) 공격의 위험이 있는 문자('', /, \, .. 등)를 제거하는 필터를 사용합니다.

CWE

Top 25 2011-13.Path Traversal
CWE-22
CWE-23
CWE-36
CWE-73
CWE-426

OWASP

Top 10 2004-A01-Unvalidated Input
Top 10 2007-A04-Insecure Direct Object Reference
Top 10 2010-A04-Insecure Direct Object References
Top 10 2013-A04-Insecure Direct Object References
Top 10 2017-A05-Broken Access Control
Relative Path Traversal

예시

```
Set rName = Request.Form("reportName")
Set rFile = fso.GetFile("C:\reports\" & rName)
```

라인 2: 외부 입력이 검증되지 않은 채로 경로 생성에 사용되었습니다.

해결방법

```
Set rName = Request.Form("reportName")
Set rNameFiltered = Filter(rName)
Set rFile = fso.GetFile("C:\reports\" & rNameFiltered)
```

라인 2: 외부 입력값을 적절하게 필터링한 후에 사용하도록 합니다.

이슈ID	위험도
472831	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp

위반라인	104
의견	

이슈ID	**위험도**
472832	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	149
의견	

이슈ID	**위험도**
472833	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	178
의견	

이슈ID	**위험도**
472834	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp

위반라인	224
의견	

이슈ID	위험도
472835	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	253
의견	

이슈ID	위험도
472836	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	299
의견	

이슈ID	위험도
472837	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp

위반라인	328
의견	

이슈ID	**위험도**
472838	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	374
의견	

이슈ID	**위험도**
473016	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_down.asp
위반라인	90
의견	

이슈ID	**위험도**
473017	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/dext_img_name_ok.a

	sp
위반라인	94
의견	

이슈ID	위험도
473029	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	111
의견	

이슈ID	위험도
473060	매우위험
체커명	PATH_MANIPULATION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/abc_img_name_ok.asp
위반라인	102
의견	

2.6 SQL_INJECTION : VBS(101)

SQL 삽입 체커는 검증되지 않은 외부 입력값을 사용하는 SQL 쿼리를 검출합니다.
SQL 쿼리를 생성하기 전에 외부 입력값을 검증하거나 매개변수화합니다.

CWE

Top 25 2011-01.SQL Injection
CWE-89
CWE-564

OWASP

Mobile Top 10 2014-M01-Weak Server Side Controls
Mobile Top 10 2014-M07-Client Side Injection
Top 10 2004-A06-Injection Flaws
Top 10 2007-A02-Injection Flaws
Top 10 2010-A01-Injection
Top 10 2013-A01-Injection
Top 10 2017-A01-Injection
Preventing SQL Injection in Java
SQL Injection

예시

```
str = Request.Form("username")
strSQL = "SELECT * FROM items WHERE owner = "'& userName
rsAddForum.Open strSQL, oconn, adOpenDynamic, adLockPessimistic
```

라인 2: 외부 입력을 적절한 처리 없이 SQL 쿼리문으로 사용했습니다.

해결방법

```
str = Request.Form("username")
strSQL = "SELECT * FROM items WHERE owner = "'& userName
rsAddForum.Open filter(strSQL), oconn, adOpenDynamic, adLockPessimistic
```

라인 3: 필터링을 통해 안전한 SQL 쿼리 문자열만 사용하도록 합니다.

이슈ID	위험도
472812	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	26
의견	

```
28.if not(rs.BOF or rs.EOF) then Response.Redirect "../inc/error.asp?no=5"
29.
30.pin = request.form("pin")
```

이슈ID	위험도
472813	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	35
의견	

이슈ID	위험도
472814	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	51
의견	

이슈ID	위험도
472815	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	110
의견	

112.
113.rs_f.close
114.set rs_f=nothing

이슈ID	위험도
472816	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	253
의견	

이슈ID	위험도
472817	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	438
의견	

이슈ID	위험도
472819	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	449
의견	

```
451.if IsNULL(rs(0)) then
452.num = 100000001
453.else
```

이슈ID	위험도
472821	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	464
의견	

이슈ID	위험도
472822	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	479
의견	

이슈ID	위험도
472823	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	490
의견	

```
492.if IsNULL(rs(0)) then
493.num = 1
494.else
```

이슈ID	위험도
472824	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	532
의견	

이슈ID	위험도
472825	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	542
의견	

이슈ID	위험도
472826	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	552
의견	

```
553.
554.if not (rs.BOF or rs.EOF) then
555.reid= rs("reid")
556.    end if
```

이슈ID	위험도
472827	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	559
의견	

이슈ID	위험도
472830	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_form_ok.asp
위반라인	35
의견	

이슈ID	위험도
472839	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	106
의견	

```
107.
108.recordCount = Rs(0)
109.pagecount = int((recordCount-1)/pagesize) +1
110.id_num = recordCount - (Page -1) * PageSize
```

이슈ID	위험도
472840	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	125
의견	

이슈ID	위험도
472851	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/memo_ok.asp
위반라인	52
의견	

이슈ID	위험도
472852	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/memo_ok.asp
위반라인	61
의견	

```
61.    Set com_rs = db.Execute(com_SQL)
62.
63.if com_rs.EOF or com_rs.BOF then Response.Redirect "../inc/error.asp?no=2"
64.
65.if com_rs("com_mem_id") <> "" then
```

이슈ID	위험도
472853	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/memo_ok.asp
위반라인	78
의견	

이슈ID	위험도
472854	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	174
의견	

이슈ID	위험도
472856	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	386
의견	

```
382.
383.dim com_sql,com_rs,com_id,com_num,com_name,com_writeday,com_memo,com_pin,com_ip,com_mem_auth,com_mem_id
384.
385.com_SQL = "SELECT com_id,com_mem_id,com_name,com_writeday,com_memo,com_pin,com_ip,com_mem_auth FROM inno_comment wh
ere tb='"&tb&"' and com_num="&request("num")&" order by com_id asc"
386.Set com_rs = db.Execute(com_SQL)
387.
388.i=1
389.Do until com_rs.EOF
390.
```

이슈ID	위험도
472870	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/index_ok.asp
위반라인	75
의견	

이슈ID	위험도
472871	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/index_ok.asp
위반라인	78
의견	

이슈ID	위험도
472873	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	153

의견	

이슈ID	위험도
472874	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	175
의견	

이슈ID	위험도
472886	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	217
의견	

이슈ID	위험도
472888	매우위험

체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	507
의견	

이슈ID	위험도
472909	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok_pro.asp
위반라인	60
의견	

이슈ID	위험도
472912	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	47
의견	

이슈ID	위험도
472913	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	73
의견	

이슈ID	위험도
472914	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	83
의견	

이슈ID	위험도
472921	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/id_check.asp
위반라인	83
의견	

이슈ID	위험도
472926	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/abc_down.asp
위반라인	41
의견	

이슈ID	위험도
472927	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/abc_down.asp
위반라인	46
의견	

이슈ID	위험도
472928	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/abc_down.asp
위반라인	51
의견	

이슈ID	위험도
472929	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/abc_down.asp
위반라인	56
의견	

이슈ID	위험도
472930	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/abc_down.asp
위반라인	61
의견	

이슈ID	위험도
472931	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_form_1.asp
위반라인	38
의견	

이슈ID	위험도
472935	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ij.asp
위반라인	212
의견	

이슈ID	위험도
472940	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ij.asp
위반라인	274
의견	

이슈ID	위험도
472941	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ne.asp
위반라인	173
의견	

이슈ID	위험도
472945	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ne.asp
위반라인	233
의견	

이슈ID	위험도
472946	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok.asp
위반라인	41
의견	

이슈ID	위험도
472947	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok.asp
위반라인	46
의견	

이슈ID	위험도
472948	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok.asp
위반라인	60
의견	

이슈ID	위험도
472954	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_nj.asp
위반라인	213
의견	

이슈ID	위험도
472959	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_nj.asp
위반라인	275
의견	

이슈ID	위험도
472961	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form_ok.asp
위반라인	89
의견	

이슈ID	위험도
472962	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form_ok.asp
위반라인	199
의견	

이슈ID	위험도
472965	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_del_ok.asp
위반라인	26
의견	

이슈ID	위험도
472967	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/mailling_1.asp
위반라인	84
의견	

이슈ID	위험도
472968	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_del_ok.asp
위반라인	23
의견	

이슈ID	위험도
472969	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_del_ok.asp
위반라인	26
의견	

이슈ID	위험도
472970	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_del_ok.asp
위반라인	29
의견	

이슈ID	위험도
472980	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ie.asp
위반라인	177
의견	

이슈ID	위험도
472984	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ie.asp
위반라인	237
의견	

이슈ID	위험도
472985	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_form_ok.asp
위반라인	204
의견	

이슈ID	위험도
472986	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_form_ok.asp
위반라인	298
의견	

이슈ID	위험도
472993	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/inc/joint.asp
위반라인	499
의견	

이슈ID	위험도
472994	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	105
의견	

이슈ID	위험도
472995	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	122
의견	

이슈ID	위험도
473007	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok_pro.asp
위반라인	41
의견	

이슈ID	위험도
473008	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok_pro.asp
위반라인	46
의견	

이슈ID	위험도
473010	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/institute_ok.asp
위반라인	99
의견	

이슈ID	위험도
473011	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_down.asp
위반라인	41
의견	

이슈ID	위험도
473012	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_down.asp
위반라인	46
의견	

이슈ID	위험도
473013	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_down.asp
위반라인	51
의견	

이슈ID	위험도
473014	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_down.asp
위반라인	56
의견	

이슈ID	위험도
473015	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/dext_down.asp
위반라인	61
의견	

이슈ID	위험도
473018	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/dext_img_name_ok.asp
위반라인	98
의견	

이슈ID	위험도
473019	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	61
의견	

이슈ID	위험도
473022	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_view.asp
위반라인	54
의견	

이슈ID	위험도
473024	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_view.asp
위반라인	78
의견	

이슈ID	위험도
473025	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	96
의견	

이슈ID	위험도
473027	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	101
의견	

이슈ID	위험도
473028	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/del_ok.asp
위반라인	28
의견	

이슈ID	위험도
473034	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_view.asp
위반라인	27
의견	

```
30.  name=rs1("name")
31.  email=rs1("email")
```

이슈ID	위험도
473039	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/point_ok.asp
위반라인	49
의견	

이슈ID	위험도
473040	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_write_ok.asp
위반라인	55
의견	

이슈ID	위험도
473041	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_write_ok.asp
위반라인	70
의견	

```
73.<HTML>
74.<HEAD>
```

이슈ID	위험도
473042	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	35
의견	

이슈ID	위험도
473043	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	41
의견	

이슈ID	위험도
473047	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/view.asp
위반라인	39
의견	

42.
43.session("read") = rs(0)

이슈ID	위험도
473048	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/view.asp
위반라인	50
의견	

이슈ID	위험도
473050	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/view.asp
위반라인	53
의견	

이슈ID	위험도
473051	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_edit_ok.asp
위반라인	166
의견	

169.
170.db.Close

이슈ID	위험도
473053	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_edit.asp
위반라인	30
의견	

이슈ID	위험도
473059	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	60
의견	

이슈ID	위험도
473061	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	77
의견	

```
77.  Set Rs = db.Execute(SQL)
78.%>
79.
80.<html>
81.<head>
```

이슈ID	위험도
473065	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/abc_img_name_ok.asp
위반라인	106
의견	

이슈ID	위험도
473067	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	47
의견	

이슈ID	위험도
473068	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	55
의견	

```
54.SQL="SELECT id,pin FROM "&tb&" where num="&num
55.Set rs = db.Execute(SQL)
56.
57.if session("id") <> rs(0) and session("admin") <> admin_name then Response.Redirect "../inc/error.asp?no=4&h_url="&h_url
58.form_pin = rs(1)
59.else
```

이슈ID	위험도
473070	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	66
의견	

이슈ID	위험도
473072	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	151
의견	

이슈ID	위험도
473074	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	165
의견	

```
163.
164.SQL2 = "DELETE FROM " & tb & " where num ="&num
165.db.Execute SQL2
166.
167.end if
168.
169.
```

이슈ID	위험도
473076	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	182
의견	

이슈ID	위험도
473078	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	199
의견	

이슈ID	위험도
473080	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	208
의견	

```
206.
207.SQL2 = "SELECT com_mem_id FROM inno_comment where com_num=" & num &" and com_id="&j
208.Set rs2= db.Execute(sql2)
209.
210.if rs2(0) <> "" and po_comment > 0 then
211.SQL = "Update member set po_comment=po_comment-1,point=point-"&c_point&" where id="'&rs2(0)&"'"
212.db.execute SQL
```

이슈ID	위험도
473085	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/del_ok.asp
위반라인	219
의견	

이슈ID	위험도
473093	매우위험
체커명	SQL_INJECTION
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/zipcode_ok.asp
위반라인	71
의견	

2.7 XSS : VBS(145)

크로스 사이트 스크립트 체커는 검증되지 않은 외부 입력값을 HTML에 포함시키는 코드를 검출합니다.
외부 입력값에 스크립트가 삽입되지 못하도록 문자 변환 함수 또는 메소드를 사용하여 <, >, &, " 등을 <, >, &, " 로 대체합니다. HTML 태그를 사용하도록 허용하는 게시판에서는 허용되는 HTML 태그를 화이트 리스트로 작성하여 리스트에 포함된 태그만 지원하도록 합니다.

CWE

Top 25 2011-04.Cross-site Scripting

CWE-79

CWE-80

OWASP

Mobile Top 10 2014-M01-Weak Server Side Controls

Mobile Top 10 2014-M07-Client Side Injection

Mobile Top 10 2016-M07-Client Code Quality

Top 10 2004-A04-Cross Site Scripting

Top 10 2007-A01-Cross Site Scripting

Top 10 2010-A02-Cross-site Scripting(XSS)

Top 10 2013-A03-Cross-Site Scripting (XSS)

Top 10 2017-A07-Cross-Site Scripting (XSS)

예시

```
userid = Request.Form("userid")
Response.Write "User ID :" & userid
```

라인 2: 외부 입력값을 필터 없이 사용했습니다.

해결방법

```
userid = Request.Form("userid")
Response.Write "User ID :" & filter(userid)
```

라인 2: 필터링을 거쳐 페이지를 생성하는데 사용하도록 합니다.

이슈ID	위험도
472807	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	869
의견	

```
870.<td width="100"><span onMousedown="inno_layer('info_layer<%=id_num%>','visible')" style=cursor:hand><% if mem_auth = 0 then %><%=name%><% else %><b><%=name%></b><% end if %></span><script>show_layer('info_layer<%=id_num%>', '<%=name%>', '<%=email%>', '<%=url%>', '<%=tb%>', '<%=mem_auth%>', '<%=id%>', '<% if session("id")="admin" then %>1<% end if %>');</script></td>
871.<td width="100"><%=writeday%></td>
872.<td width="40"><%=visit%></td>
873.<% if use_reco = 1 and view_reco = 1 then %><td width="40"><%=reco%></td><% end if %>
```

이슈ID	위험도
472808	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	869
의견	

이슈ID	위험도
472809	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	869
의견	

<% if use_reco = 1 and view_reco = 1 then %><td width="40"><%=reco%></td><% end if %><% end if %></td>
870.<td width="100"><span onMousedown="inno_layer('info_layer<%=id_num%>','visible')" style=cursor:hand><% if mem_auth = 0 then %><%=name%><% else %><%=name%><% end if %><script>show_layer('info_layer<%=id_num%>', '<%=name%>', '<%=email%>', '<%=url%>', '<%=tb%>', '<%=mem_auth%>', '<%=id%>', '<% if session("id")="admin" then %>1<% end if %>');</script></td>
871.<td width="100"><%=writeday%></td>
872.<td width="40"><%=visit%></td>
873.<% if use_reco = 1 and view_reco = 1 then %><td width="40"><%=reco%></td><% end if %>

이슈ID	위험도
472810	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	869
의견	

이슈ID	위험도
472811	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	869
의견	

<>"" then %>&st=<%=st%>&sc=<%=sc%>&sn=<%=sn%>&sw=<%=sw%><% end if %>"><%=title%><% if com_record<>0 then %> <img src="../img/comment.gif" border="0">(<%=com_record%>)<% end if %></td>
870.<td width="100"><span onMousedown="inno_layer('info_layer<%=id_num%>','visible')" style=cursor:hand><% if mem_auth = 0 then %><%=name%><% else %><%=name%><% end if %><script>show_layer('info_layer<%=id_num%>', '<%=name%>', '<%=email%>', '<%=url%>', '<%=tb%>', '<%=mem_auth%>', '<%=id%>', '<% if session("id")="admin" then %>1<% end if %>');</script></td>
871.<td width="100"><%=writeday%></td>
872.<td width="40"><%=visit%></td>
873.<% if use_reco = 1 and view_reco = 1 then %><td width="40"><%=reco%></td><% end if %>

이슈ID	위험도
472818	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	265
의견	

이슈ID	위험도
472820	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	265
의견	

이슈ID	위험도
472829	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	604
의견	

```
601.<input type="hidden" name="st" value="<%=Request.QueryString("st")%>">
602.<input type="hidden" name="sc" value="<%=Request.QueryString("sc")%>">
603.<input type="hidden" name="sn" value="<%=Request.QueryString("sn")%>">
604.<input type="hidden" name="sw" value="<%=Request.QueryString("sw")%>">
605.<% if board_type > 0 and mode = "edit" then %>
606.<input type="hidden" name="oldfilename1" value="<%=filename1%>" ID="Hidden1">
607.<input type="hidden" name="oldfilesize1" value="<%=filesize1%>" ID="Hidden2">
608.<input type="hidden" name="oldfilename2" value="<%=filename2%>" ID="Hidden3">
```

이슈ID	위험도
472841	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	200
의견	

이슈ID	위험도
472842	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	200
의견	

이슈ID	위험도
472843	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	207

의견	

이슈ID	위험도
472844	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	207
의견	

이슈ID	위험도
472845	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	222
의견	

이슈ID	위험도
472846	매우위험
체커명	XSS

파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	222
의견	

이슈ID	위험도
472847	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	229
의견	

이슈ID	위험도
472848	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	229
의견	

이슈ID	위험도
472849	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	235
의견	

이슈ID	위험도
472850	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_0.asp
위반라인	235
의견	

이슈ID	위험도
472857	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	516
의견	

o.gif" border="0"> <% end if %><%if rw_level >= session("level") then%><% if (board_type < 2 and notice <> 1) or board_type < 2 then %><a href="form.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&num=<%=num%>&mode=reply<% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_reply.gif" border="0"> <% end if %><% end if %><% if w_level >= session("level") then %><a href="form.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>"><img src="../img/but_write.gif" border="0"> <% end if %>
517.<% if mem_auth = 0 or (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>form<% else %>pin<% end if %>.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&num=<%=num%>&mode=edit<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_edit.gif" border="0"> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>del_ok<% else %>pin<% end if %>.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&num=<%=num%>&mode=del<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_del.gif" border="0"> <% end if %><% if sw<>"" then %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&st=<%=st%>&sc=<%=sc%>&sn=<%=sn%>&sw=<%=sw%>"><img src="../img/but_search_list.gif" border="0"> <% end if %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>"><img src="../img/but_list.gif" border="0"></td>
518.<td align="right" style="word-break:break-all;padding:5px;">
519.<%
520.

이슈ID	위험도
472858	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	516
의견	

```
=<%=sw%>"><img src="../img/but_search_list.gif" border="0"></a> <% end if %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=
<%=e%>&page=<%=page%>"><img src="../img/but_list.gif" border="0"></a></td>
518.<td align="right" style="word-break:break-all;padding:5px;">
519.<%
520.
```

이슈ID	위험도
472859	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	517
의견	

이슈ID	위험도
472860	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	517
의견	

516.<td align="left" style="word-break:break-all;padding:5px;"><% if use_reco = 1 then %><a href="view.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&num=<%=num%>&mode=reco<% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_reco.gif" border="0"> <% end if %><%if rw_level >= session("level") then%><% if (board_type < 2 and notice <> 1) or board_type < 2 then %><a href="form.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&num=<%=num%>&mode=reply<% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_reply.gif" border="0"> <% end if %><% end if %><% if w_level >= session("level") then %><a href="form.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>"><img src="../img/but_write.gif" border="0"> <% end if %>

517.<% if mem_auth = 0 or (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>form<% else %>pin<% end if %>.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&num=<%=num%>&mode=edit<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_edit.gif" border="0"> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>del_ok<% else %>pin<% end if %>.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&num=<%=num%>&mode=del<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_del.gif" border="0"> <% end if %><% if sw<>"" then %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&st=<%=st%>&sc=<%=sc%>&sn=<%=sn%>&sw=<%=sw%>"><img src="../img/but_search_list.gif" border="0"> <% end if %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>"><img src="../img/but_list.gif" border="0"></td>

518.<td align="right" style="word-break:break-all;padding:5px;">

519.<%

520.

521.dim p_num,p_title,p_name,n_num,n_title,n_name

이슈ID	위험도
472861	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	517
의견	

ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_del.gif" border="0"> <% end if %><% if sw<>"" then %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&st=<%=st%>&sc=<%=sc%>&sn=<%=sn%>&sw=<%=sw%>"><img src="../img/but_search_list.gif" border="0"> <% end if %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>"><img src="../img/but_list.gif" border="0"></td>
518.<td align="right" style="word-break:break-all;padding:5px;">
519.<%
520.
521.dim p_num,p_title,p_name,n_num,n_title,n_name

이슈ID	위험도
472862	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	517
의견	

이슈ID	위험도
472863	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	517

의견	

이슈ID	위험도
472864	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	517
의견	

mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_edit.gif" border="0"> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>del_ok<% else %>pin<% end if %>.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&num=<%=num%>&mode=del<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_del.gif" border="0"> <% end if %><% if sw<>"" then %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>&st=<%=st%>&sc=<%=sc%>&sn=<%=sn%>&sw=<%=sw%>"><img src="../img/but_search_list.gif" border="0"> <% end if %><a href="list.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&page=<%=page%>"><img src="../img/but_list.gif" border="0"></td>

518.<td align="right" style="word-break:break-all;padding:5px;">

519.<%

520.

521.dim p_num,p_title,p_name,n_num,n_title,n_name

이슈ID	위험도
472865	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	525
의견	

이슈ID	위험도
472866	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	525
의견	

```
528.</tr>
529.</table>
```

이슈ID	위험도
472867	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	525
의견	

이슈ID	위험도
472868	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	525
의견	

이슈ID	위험도
472869	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/digital_diary_c.asp
위반라인	525
의견	

```
522.call pre_next(p_num,n_num,p_title,p_name,n_title,n_name)
523.
524.%>
525.<% If p_num <> 0 Then %><a href="view.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&num=<%=p_num%>&page=<%=page%>&sw=<%=sw%>&sn=<%=sn%>&st=<%=st%>&sc=<%=sc%>"><img src="../img/but_pre.gif" border="0"></a><% end if %> <% If n_num <> 0 Then %><a href="view.asp?tb=<%=tb%>&o=<%=o%>&t=<%=t%>&e=<%=e%>&num=<%=n_num%>&page=<%=page%>&sw=<%=sw%>&sn=<%=sn%>&st=<%=st%>&sc=<%=sc%>"><img src="../img/but_next.gif" border="0"></a><% end if %>
526.
527.</td>
528.</tr>
529.</table>
```

이슈ID	위험도
472872	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	122
의견	

이슈ID	위험도
472875	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	201
의견	

이슈ID	위험도
472876	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp

위반라인	240
의견	

이슈ID	위험도
472877	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	240
의견	

이슈ID	위험도
472878	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	247
의견	

이슈ID	위험도
472879	매우위험

체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	247
의견	

이슈ID	위험도
472880	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	262
의견	

이슈ID	위험도
472881	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	262
의견	

이슈ID	위험도
472882	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	269
의견	

이슈ID	위험도
472883	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	269
의견	

이슈ID	위험도
472884	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	275
의견	

```
278.End If
279.%></td>
```

이슈ID	위험도
472885	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_list.asp
위반라인	275
의견	

이슈ID	위험도
472889	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	659
의견	

```
661.</tr>
662.</table>
663.<%
```

이슈ID	위험도
472890	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	659
의견	

이슈ID	위험도
472891	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	660
의견	

<%if rw_level >= session("level") then%><% if (board_type < 2 and notice <> 1) or board_type < 2 then %><a href="form.asp?tb=<%=tb%>&page=<%=page%>&num=<%=num%>&mode=reply<% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_reply.gif" border="0"> <% end if %><% end if %><% if w_level >= session("level") then %><a href="form.asp?tb=<%=tb%>"><img src="../img/but_write.gif" border="0"> <% end if %>

660.<% if mem_auth = 0 or (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>form<% else %>pin<% end if %>.asp?tb=<%=tb%>&page=<%=page%>&num=<%=num%>&mode=edit<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_edit.gif" border="0"> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>del_ok<% else %>pin<% end if %>.asp?tb=<%=tb%>&num=<%=num%>&mode=del<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_del.gif" border="0"> <% end if %><% if sw<>"" then %><a href="list.asp?tb=<%=tb%>&page=<%=page%>&st=<%=st%>&sc=<%=sc%>&sn=<%=sn%>&sw=<%=sw%>"><img src="../img/but_search_list.gif" border="0"> <% end if %><a href="list.asp?tb=<%=tb%>&page=<%=page%>"><img src="../img/but_list.gif" border="0"></td>

661.</tr>

662.</table>

663.<%

664.if relation = 1 then

이슈ID	위험도
472892	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	660
의견	

```
661.</tr>
662.</table>
663.<%
664.if relation = 1 then
```

이슈ID	위험도
472893	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	660
의견	

이슈ID	위험도
472894	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	660
의견	

quest.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_reco.gif" border="0"> <% end if %> <%if rw_level >= session("level") then%><% if (board_type < 2 and notice <> 1) or board_type < 2 then %><a href="form.asp?tb=<%=tb%>&page=<%=page%>&num=<%=num%>&mode=reply<% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_reply.gif" border="0"> <% end if %><% end if %><% if w_level >= session("level") then %><a href="form.asp?tb=<%=tb%>"><img src="../img/but_write.gif" border="0"> <% end if %>

660.<% if mem_auth = 0 or (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>form<% else %>pin<% end if %>.asp?tb=<%=tb%>&page=<%=page%>&num=<%=num%>&mode=edit<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_edit.gif" border="0"> <a href="<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>del_ok<% else %>pin<% end if %>.asp?tb=<%=tb%>&num=<%=num%>&mode=del<% if (mem_auth = 1 and session("id") = id) or session("admin") = admin_name then %>&mem=ok<% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %>"><img src="../img/but_del.gif" border="0"> <% end if %><% if sw<>"" then %><a href="list.asp?tb=<%=tb%>&page=<%=page%>&st=<%=st%>&sc=<%=sc%>&sn=<%=sn%>&sw=<%=sw%>"><img src="../img/but_search_list.gif" border="0"> <% end if %><a href="list.asp?tb=<%=tb%>&page=<%=page%>"><img src="../img/but_list.gif" border="0"></td>

661.</tr>

662.</table>

663.<%

664.if relation = 1 then

이슈ID	위험도
472895	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	660
의견	

```
<%=page%>"><img src="../img/but_list.gif" border="0"></a></td>
661.</tr>
662.</table>
663.<%
664.if relation = 1 then
```

이슈ID	위험도
472896	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	660
의견	

이슈ID	위험도
472897	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	698
의견	

```
698.<td align="left" style="word-break:break-all;">   <a href="view.asp?tb=<%=tb%>&num=<%=p_num%>&page=<%=page%>&sw
=<%=sw%>&sn=<%=sn%>&st=<%=st%>&sc=<%=sc%>" onfocus="this.blur()"><%=p_title%></a></td>
699.</tr>
700.<tr>
701.<td colspan="2" height="1" bgcolor="#cccccc"></td>
702.</tr>
```

이슈ID	위험도
472898	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	698
의견	

이슈ID	위험도
472899	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	698
의견	

이슈ID	위험도
472900	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	698
의견	

```
695.<% If p_num <> 0 Then %>
696.<tr align="center" height="22">
697.<td width="100"><b style="font-size:8pt;">이전글</b></td>
698.<td align="left" style="word-break:break-all;">   <a href="view.asp?tb=<%=tb%>&num=<%=p_num%>&page=<%=page%>&sw
=<%=sw%>&sn=<%=sn%>&st=<%=st%>&sc=<%=sc%>" onfocus="this.blur()"><%=p_title%></a></td>
699.</tr>
700.<tr>
701.<td colspan="2" height="1" bgcolor="#cccccc"></td>
702.</tr>
```

이슈ID	위험도
472901	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	698
의견	

이슈ID	위험도
472902	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	708
의견	

이슈ID	위험도
472903	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp

위반라인	708
의견	

이슈ID	위험도
472904	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	708
의견	

이슈ID	위험도
472905	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	708
의견	

이슈ID	위험도
472906	매우위험

체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/content.asp
위반라인	708
의견	

이슈ID	위험도
472915	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	598
의견	

이슈ID	위험도
472916	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	599
의견	

이슈ID	위험도

472917	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	600
의견	

이슈ID	위험도
472918	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	601
의견	

이슈ID	위험도
472919	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ij.asp
위반라인	287
의견	

이슈ID	위험도

472920	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	602
의견	

이슈ID	**위험도**
472922	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/form.asp
위반라인	603
의견	

이슈ID	**위험도**
472923	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/id_check.asp
위반라인	88
의견	

이슈ID	**위험도**

472924	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/id_check.asp
위반라인	90
의견	

이슈ID	**위험도**
472925	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/id_check.asp
위반라인	104
의견	

이슈ID	**위험도**
472932	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_form_1.asp
위반라인	698
의견	

702.</table>

이슈ID	위험도
472933	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/tb_form_1.asp
위반라인	699
의견	

이슈ID	위험도
472934	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/progressbar.asp
위반라인	6
의견	

이슈ID	위험도
472937	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ij.asp
위반라인	258
의견	

261.
262.<Meta http-equiv="Refresh" content="0; url=javascript:ok()">

이슈ID	위험도
472938	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ij.asp
위반라인	259
의견	

이슈ID	위험도
472939	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ij.asp
위반라인	260
의견	

이슈ID	위험도
472943	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ne.asp
위반라인	219
의견	

```
222.<Meta http-equiv="Refresh" content="0; url=javascript:ok()">
223.<% else %>
```

이슈ID	위험도
472944	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ne.asp
위반라인	220
의견	

이슈ID	위험도
472949	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok.asp
위반라인	64
의견	

이슈ID	위험도
472950	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok.asp
위반라인	65
의견	

```
68.</form>
69.
```

이슈ID	위험도
472951	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/login_ok.asp
위반라인	66
의견	

이슈ID	위험도
472956	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_nj.asp
위반라인	259
의견	

이슈ID	위험도
472957	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_nj.asp
위반라인	260
의견	

```
263.<Meta http-equiv="Refresh" content="0; url=javascript:ok()">
264.</form>
```

이슈ID	위험도
472958	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_nj.asp
위반라인	261
의견	

이슈ID	위험도
472960	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_nj.asp
위반라인	288
의견	

이슈ID	위험도
472966	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/mailling_1.asp
위반라인	69
의견	

72.if request("mode") = "sel" then'선택된 회원만 일때 73.cart_num = Request.Form("cart").count

이슈ID	위험도
472971	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ok.asp
위반라인	1
의견	

이슈ID	위험도
472972	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ok.asp
위반라인	2
의견	

이슈ID	위험도
472973	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ok.asp
위반라인	3
의견	

이슈ID	위험도
472974	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ok.asp
위반라인	4
의견	

```
1.<%=request.Form("process")%>/<br>
2.<%=request.Form("pro_pin")%>/<br>
3.<%=request.Form("free_pin")%>/<br>
4.<%=request.Form("o_pin")%>/<br>
5.<%=request.Form("name")%>/<br>
6.<%=request.Form("jumin")%>/<br>
```

이슈ID	위험도
472975	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ok.asp
위반라인	5
의견	

이슈ID	위험도
472976	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ok.asp
위반라인	6
의견	

이슈ID	위험도
472977	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_write.asp
위반라인	62
의견	

이슈ID	위험도
472978	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_write.asp
위반라인	65
의견	

이슈ID	위험도
472979	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/open_img.asp
위반라인	23
의견	

이슈ID	위험도
472982	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ie.asp
위반라인	223
의견	

이슈ID	위험도

472983	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/find_center_ie.asp
위반라인	224
의견	

이슈ID	**위험도**
472988	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/email.asp
위반라인	112
의견	

이슈ID	**위험도**
472989	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/pin.asp
위반라인	85
의견	

```
88.<table width="100%" border="0" cellpadding="0" cellspacing="0">
89.<tr>
```

이슈ID	위험도
472990	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/pin.asp
위반라인	85
의견	

이슈ID	위험도
472991	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/pin.asp
위반라인	85
의견	

이슈ID	위험도
472992	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/pin.asp
위반라인	85
의견	

```
82.end if
83.%>
84.<table width="300" border="0" cellpadding="0" cellspacing="0">
85.<form name="inno" method="POST" action="<%=url%>tb=<%=Request.QueryString("tb")%>&page=<%=Request.QueryString("page")%>&mode=<%=mode%><% if request("mode1") <> "" then %>&mode1=<%=request("mode1")%><% end if %><% if sw<>"" then %>&st=<%=Request.QueryString("st")%>&sc=<%=Request.QueryString("sc")%>&sn=<%=Request.QueryString("sn")%>&sw=<%=Request.QueryString("sw")%><% end if %><% if mode="com_del" then %>&h_url=<%=h_url%><% end if %>" onsubmit = "return submit_ok();">
86.<tr>
87.<td>
88.<table width="100%" border="0" cellpadding="0" cellspacing="0">
89.<tr>
```

이슈ID	위험도
472996	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	200
의견	

이슈ID	위험도
472997	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	200
의견	

이슈ID	위험도
472998	매우위험
체커명	XSS

파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	207
의견	

이슈ID	위험도
472999	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	207
의견	

이슈ID	위험도
473000	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	222
의견	

이슈ID	위험도

473001	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	222
의견	

이슈ID	**위험도**
473002	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	229
의견	

이슈ID	**위험도**
473003	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	229
의견	

```
231.end if
232.
233.If Int(Page) <> PageCount Then
```

이슈ID	위험도
473004	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	235
의견	

이슈ID	위험도
473005	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/mem_list_1.asp
위반라인	235
의견	

이슈ID	위험도
473006	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/admin/mailling_ok_1.asp
위반라인	109
의견	

```
109.<td align="right" style="word-break:break-all;padding:5px;"><a href="<%=request.form("h_url")%>"><img src="../img/but_ok.gif" border="0
"></a></td>
110.</tr>
111.</table><br>
112.</div>
113.
```

이슈ID	위험도
473009	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/zipcode_ok.asp
위반라인	99
의견	

이슈ID	위험도
473026	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/message/m_view.asp
위반라인	139
의견	

이슈ID	위험도
473031	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_process.asp
위반라인	135
의견	

```
133.<script language=javascript>
134.alert("회원탈퇴가 되었습니다.");
135.window.opener.location = '../board/list.asp?tb=<%=Request.QueryString("tb")%>';
136.self.close();
137.</script>
138.<%
139.else
```

이슈ID	위험도
473035	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	271
의견	

이슈ID	위험도
473036	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	276
의견	

이슈ID	위험도
473037	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	276
의견	

```
274.<script language=javascript>
275.self.close();
276.window.opener.location = '../member/login_ok.asp?join_id=<%=id%>&join_pin=<%=pin%>&term=1&h_url=<%=Request.Form("h_url")%>';
277.</script>
278.
279.<% end if %>
280.<% end if %>
```

이슈ID	위험도
473038	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join_ok.asp
위반라인	276
의견	

이슈ID	위험도
473045	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/gallery_c.asp
위반라인	95
의견	

```
97.<tr>
98.<td height="1" bgcolor="#cccccc"></td>
99.</tr>
```

이슈ID	위험도
473049	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/board/email_ok.asp
위반라인	93
의견	

이슈ID	위험도
473055	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_edit.asp
위반라인	216
의견	

이슈ID	위험도
473057	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_edit.asp
위반라인	470
의견	

```
469.</form>
470.<form method="post" name="del_id" action="user_process.asp?mode=del&sel=1&style=del&tb=<%=request.QueryString("tb")%>">
471.<input type="hidden" name="id" value="<%=id%>">
472.</form>
473.</table>
474.</div>
```

이슈ID	위험도
473062	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	112
의견	

이슈ID	위험도
473063	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	112
의견	

이슈ID	위험도
473064	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	118
의견	

```
115.
116.function mem_del()
117.{
118.inno_check.action = "user_process.asp?mode=del&pagesize=<%=pagesize%><% if sw<>"" then %>&ss=<%=ss%>&sw=<%=sw%><% end if %>"
119.inno_check.submit();
120.}
121.
122.function mem_mail()
```

이슈ID	위험도
473069	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	118
의견	

이슈ID	위험도
473071	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	359
의견	

이슈ID	위험도
473073	매우위험
체커명	XSS

파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	359
의견	

이슈ID	위험도
473075	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	372
의견	

이슈ID	위험도
473077	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	372
의견	

이슈ID	위험도
473079	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	379
의견	

이슈ID	위험도
473081	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	379
의견	

이슈ID	위험도
473082	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	394
의견	

```
396.End If
397.Next
398.
```

이슈ID	위험도
473083	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	394
의견	

이슈ID	위험도
473084	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	401
의견	

이슈ID	위험도
473086	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join.asp
위반라인	433
의견	

```
433.<input type="hidden" name="tb" value="<%=Request.QueryString("tb")%>">
434.<input type="hidden" name="page" value="<%=Request.QueryString("page")%>">
435.<input type="hidden" name="num" value="<%=Request.QueryString("num")%>">
436.<input type="hidden" name="f_jumin" value="<%=f_jumin%>">
437.<input type="hidden" name="h_url" value="<%=h_url%>">
```

이슈ID	위험도
473087	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join.asp
위반라인	434
의견	

이슈ID	위험도
473088	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join.asp
위반라인	435
의견	

이슈ID	위험도
473089	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	401
의견	

```
401. .. [<a href="user_list.asp?page=<%=PageCount%>&pagesize=<%=pagesize%><% if sw<>"" then %>&ss=<%=ss%>&sw=<%=sw%><% end if %>" onfocus="this.blur()"><font color="000000" style="font-size:8pt;"><%=PageCount%></font></a>]
402.<%
403.end if
404.
405.If Int(Page) <> PageCount Then
```

이슈ID	위험도
473090	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/join.asp
위반라인	438
의견	

이슈ID	위험도
473091	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	407
의견	

이슈ID	위험도
473092	매우위험
체커명	XSS
파일	/SeedCrock/RPT/Sparrow/202402_3923/source_file/1615255622102/테스트 소스/테스트 소스/member/user_list_1.asp
위반라인	407
의견	

```
405.If Int(Page) <> PageCount Then
406.%>
407. <a href="user_list.asp?page=<%=page+1%>&pagesize=<%=pagesize%><% if sw<>"" then %>&ss=<%=ss%>&sw=<%=sw%><% end if %>" onfocus="this.blur()"><font color="#000000" style="font-size:8pt;">[next]</font></a>
408.<%
409.End If
410.End If
411.%>
```

3. 예외 정보

3.1 파일 (8)

제외내용
/usr/include/*
/inculde/*
*icrosoft*include*
*icrosoft*vc98*
*icrosoft*sdks*
*indows*kits*
\mingw
jquery.js

3.2 예외 함수 (0)

N/A

3.3 제외 처리건 목록 (0)

N/A

4. 분석 기준

4.1 분석 체커 목록 (423)

위험도	카테고리	언어	체커명
매우위험	보안	ASP(.NET)	CLEAR_TEXT_TRANSMISSION_OF_SENSITIVE_INFORMATION
매우위험	보안	ASP(.NET)	COMMAND_INJECTION
매우위험	보안	ASP(.NET)	HTTP_RESPONSE_SPLITTING
매우위험	보안	ASP(.NET)	LDAP_INJECTION
매우위험	보안	ASP(.NET)	OPEN_REDIRECT
매우위험	보안	ASP(.NET)	PATH_TRAVERSAL
매우위험	보안	ASP(.NET)	PERSISTENT_COOKIE
매우위험	보안	ASP(.NET)	RESOURCE_INJECTION
매우위험	보안	ASP(.NET)	SQL_INJECTION
매우위험	보안	ASP(.NET)	WEAK_PASSWORD_REQUIREMENTS
매우위험	보안	ASP(.NET)	XPATH_INJECTION
매우위험	보안	ASP(.NET)	XQUERY_INJECTION
매우위험	보안	ASP(.NET)	XSS
매우위험	보안	ASP(.NET)	XSS_ERROR_MESSAGE
매우위험	보안	C#	ACCESS_CONTROL.ANONYMOUS_LDAP_BINDING
매우위험	보안	C#	CROSS_SITE_REQUEST_FORGERY
매우위험	보안	C#	DISABLED_HEADER_CHECKING
매우위험	보안	C#	DISABLED_VIEW_STATE_MAC
매우위험	보안	C#	IMPROPER_AUTHORIZATION
매우위험	보안	C#	PRIVACY_VIOLATION_SHOULDER_SURFING
매우위험	품질	C#	RESOURCE_LEAK
매우위험	보안	C#	UNVERIFIABLE_NATIVE_INVOCATION
매우위험	품질	C/C++	DOUBLE_CLOSE
매우위험	품질	C/C++	DOUBLE_FREE
매우위험	보안	C/C++	INFORMATION_LEAK
매우위험	보안	C/C++	LDAP_INJECTION
매우위험	품질	C/C++	LEAK.MEMORY
매우위험	품질	C/C++	LEAK.RESOURCE
매우위험	품질	C/C++	OVERRUN.DYNAMIC
매우위험	보안	C/C++	OVERRUN.STATIC
매우위험	보안	C/C++	OVERRUN.STATIC.BAD_COND
매우위험	보안	C/C++	OVERRUN.STATIC.MEMSET
매우위험	보안	C/C++	RACE_CONDITION.EXT
매우위험	보안	C/C++	SQL_INJECTION
매우위험	품질	C/C++	UNINIT
매우위험	품질	C/C++	USE_AFTER_CLOSE.EXT

매우위험	품질	C/C++	USE_AFTER_FREE
매우위험	보안	Java/JSP	COMMAND_INJECTION
매우위험	보안	Java/JSP	CROSS_SITE_REQUEST_FORGERY
매우위험	보안	Java/JSP	HTTP_RESPONSE_SPLITTING
매우위험	보안	Java/JSP	IMPROPER_AUTHORIZATION
매우위험	보안	Java/JSP	LDAP_INJECTION
매우위험	보안	Java/JSP	OPEN_REDIRECT
매우위험	보안	Java/JSP	PATH_TRAVERSAL
매우위험	보안	Java/JSP	PERSISTENT_COOKIE
매우위험	보안	Java/JSP	RESOURCE_INJECTION
매우위험	품질	Java/JSP	RESOURCE_LEAK
매우위험	보안	Java/JSP	SECURITY.FILE.GLOBAL_ACCESS
매우위험	보안	Java/JSP	SQL_INJECTION
매우위험	보안	Java/JSP	SQL_INJECTION_HIBERNATE
매우위험	보안	Java/JSP	SQL_INJECTION_JDO
매우위험	보안	Java/JSP	SQL_INJECTION_PERSISTENCE
매우위험	보안	Java/JSP	WEAK_PASSWORD_REQUIREMENTS
매우위험	보안	Java/JSP	XPATH_INJECTION
매우위험	보안	Java/JSP	XQUERY_INJECTION
매우위험	보안	Java/JSP	XSS
매우위험	보안	Java/JSP	XSS_ERROR_MESSAGE
매우위험	보안	Javascript	COMMAND_INJECTION
매우위험	보안	Javascript	COMMAND_INJECTION.TOBE
매우위험	보안	Javascript	FORBIDDEN.WEAK_ALGORITHM
매우위험	보안	Javascript	HTTP_RESPONSE_SPLITTING
매우위험	보안	Javascript	INFORMATION_LEAK.TOBE
매우위험	보안	Javascript	OPEN_REDIRECT
매우위험	보안	Javascript	PATH_CONTAMINATION
매우위험	보안	Javascript	PATH_TRAVERSAL.TOBE
매우위험	보안	Javascript	RESOURCE_INJECTION
매우위험	보안	Javascript	SQL_INJECTION
매우위험	보안	Javascript	XSS.DOM
매우위험	보안	Objective-C	CLEAR_TEXT_TRANSMISSION_OF_SENSITIVE_INFORMATION
매우위험	보안	Objective-C	FORMAT_STRING
매우위험	보안	Objective-C	HTTP_RESPONSE_SPLITTING
매우위험	보안	Objective-C	LDAP_INJECTION
매우위험	품질	Objective-C	LEAK.MEMORY
매우위험	보안	Objective-C	OPEN_REDIRECT
매우위험	보안	Objective-C	OVERRUN.STATIC.STRCPY
매우위험	보안	Objective-C	PATH_MANIPULATION

매우위험	보안	Objective-C	RESOURCE_INJECTION
매우위험	보안	Objective-C	SQL_INJECTION
매우위험	보안	Objective-C	XPATH_INJECTION
매우위험	보안	Objective-C	XQUERY_INJECTION
매우위험	보안	Objective-C	XSS
매우위험	보안	PHP	COMMAND_INJECTION
매우위험	보안	PHP	CROSS_SITE_REQUEST_FORGERY
매우위험	보안	PHP	FILE_PERMISSION_MANIPULATION
매우위험	보안	PHP	HEADER_MANIPULATION
매우위험	보안	PHP	HTTP_RESPONSE_SPLITTING
매우위험	보안	PHP	IMPROPER_AUTHORIZATION
매우위험	보안	PHP	LDAP_INJECTION
매우위험	품질	PHP	LEAK.RESOURCE
매우위험	보안	PHP	OPEN_REDIRECT
매우위험	보안	PHP	PATH_MANIPULATION
매우위험	보안	PHP	SQL_INJECTION
매우위험	보안	PHP	UNRESTRICTED_UPLOAD.FILE
매우위험	품질	PHP	USE_AFTER_RELEASE.RESOURCE
매우위험	보안	PHP	WEAK_PASSWORD_REQUIREMENTS
매우위험	보안	PHP	XPATH_INJECTION
매우위험	보안	PHP	XQUERY_INJECTION
매우위험	보안	PHP	XSS
매우위험	보안	Python	COMMAND_INJECTION
매우위험	보안	Python	CROSS_SITE_REQUEST_FORGERY
매우위험	보안	Python	DJANGO_FILE_RESPONSE_MANIPULATION
매우위험	보안	Python	EXPOSURE_OF_SYSTEM_DATA
매우위험	보안	Python	HTTP_RESPONSE_SPLITTING
매우위험	보안	Python	IMPROPER_AUTHORIZATION
매우위험	보안	Python	LDAP_INJECTION
매우위험	품질	Python	LEAK.RESOURCE
매우위험	보안	Python	OPEN_REDIRECT
매우위험	보안	Python	PATH_MANIPULATION
매우위험	보안	Python	RESOURCE_INJECTION
매우위험	보안	Python	SETTING_MANIPULATION
매우위험	보안	Python	SQL_INJECTION
매우위험	보안	Python	UNRESTRICTED_UPLOAD_OF_FILE
매우위험	보안	Python	WEAK_PASSWORD_REQUIREMENTS
매우위험	보안	Python	XPATH_INJECTION
매우위험	보안	Python	XQUERY_INJECTION
매우위험	보안	Python	XSS
매우위험	보안	SQL	SQL_INJECTION.IBATIS

매우위험	보안	SQL	SQL_INJECTION.MYBATIS
매우위험	보안	Swift	LDAP_INJECTION
매우위험	보안	Swift	OPEN_REDIRECT
매우위험	보안	Swift	RESOURCE_INJECTION
매우위험	보안	Swift	SQL_INJECTION
매우위험	보안	Swift	XPATH_INJECTION
매우위험	보안	Swift	XSS
매우위험	보안	VB.Net	COMMAND_INJECTION
매우위험	보안	VB.Net	HTTP_RESPONSE_SPLITTING
매우위험	보안	VB.Net	LDAP_INJECTION
매우위험	보안	VB.Net	OPEN_REDIRECT
매우위험	보안	VB.Net	PATH_MANIPULATION
매우위험	보안	VB.Net	SQL_INJECTION
매우위험	보안	VB.Net	UNRESTRICTED_UPLOAD.FILE
매우위험	보안	VB.Net	WEAK_PASSWORD_REQUIREMENTS
매우위험	보안	VB.Net	XPATH_INJECTION
매우위험	보안	VB.Net	XQUERY_INJECTION
매우위험	보안	VB.Net	XSS
매우위험	보안	VBS	COMMAND_INJECTION
매우위험	보안	VBS	HEADER_MANIPULATION
매우위험	보안	VBS	OPEN_REDIRECT
매우위험	보안	VBS	PATH_MANIPULATION
매우위험	보안	VBS	RESOURCE_INJECTION.PORT
매우위험	보안	VBS	SETTING_MANIPULATION
매우위험	보안	VBS	SQL_INJECTION
매우위험	보안	VBS	XSS
위험	보안	ASP(.NET)	EXPOSURE_OF_SYSTEM_DATA
위험	보안	ASP(.NET)	PASSWORD_SAVED_WITHOUT_ENCRYPTION
위험	보안	ASP(.NET)	RELIANCE_ON_DNS_LOOKUPS_IN_A_SECURITY_DECISION
위험	보안	ASP(.NET)	UNRESTRICTED_UPLOAD_OF_FILE
위험	보안	C#	BAD_CALL.RANDOM_NEXT
위험	보안	C#	COOKIE.DISABLED_HTTP_ONLY
위험	보안	C#	COOKIE.OVERLY_BROAD_DOMAIN
위험	보안	C#	COOKIE.OVERLY_BROAD_PATH
위험	보안	C#	DATA_LEAK_BETWEEN_SESSIONS
위험	보안	C#	DOWNLOAD_OF_CODE_WITHOUT_INTEGRITY_CHECK
위험	보안	C#	HARDCODED_PASSWORD
위험	보안	C#	HARDCODED_PASSWORD_COMPARISON
위험	보안	C#	HARD_CODED_CRYPTOGRAPHIC_KEY
위험	보안	C#	HARD_CODED_USER_NAME_AND_PASSWORD

위험	보안	C#	INCORRECT_PERMISSION_ASSIGNMENT_FOR_CRITICAL_RESOURCE
위험	보안	C#	INTEGER_OVERFLOW
위험	보안	C#	MISSING_AUTHENTICATION.CRITICAL_FUNCTION
위험	보안	C#	MISSING_LOGIN_CONTROL
위험	보안	C#	PASSWORD_IN_COMMENT
위험	보안	C#	PRIVATE_COLLECTION
위험	보안	C#	PUBLIC_DATA_ASSIGNED_TO_PRIVATE_ARRAY
위험	보안	C#	TOCTOU_RACE_CONDITION
위험	보안	C#	USING_HASH_WITHOUT_SALT
위험	보안	C#	WEAK_CRYPTOGRAPHIC_HASH
위험	보안	C#	WEAK_ENCRYPTION.DES
위험	보안	C#	WEAK_ENCRYPTION.INSECURE_MODE_OF_OPERATION
위험	보안	C#	WEAK_ENCRYPTION.INSUFFICIENT_KEY_SIZE
위험	보안	C#	WEAK_SIGNATURE.INSUFFICIENT_KEY_SIZE
위험	보안	C/C++	DO_NOT_USE_DANGEROUS_FUNCTIONS
위험	보안	C/C++	DO_NOT_USE_HARD_CODING.PASSWORD
위험	보안	C/C++	EXECL_REVEALS_DATA
위험	보안	C/C++	IMPROPER_AUTHORIZATION
위험	보안	C/C++	IMPROPER_RANDOM_USAGE
위험	보안	C/C++	INCORRECT_PERMISSION
위험	품질	C/C++	INTEGER_OVERFLOW
위험	품질	C/C++	INTEGER_UNDERFLOW
위험	품질	C/C++	MISMATCH.MALLOC_TO_DELETE
위험	품질	C/C++	MISMATCH.MALLOC_TO_DELETE_ARRAY
위험	품질	C/C++	MISMATCH.NEW_ARRAY_TO_DELETE
위험	품질	C/C++	MISMATCH.NEW_ARRAY_TO_FREE
위험	품질	C/C++	MISMATCH.NEW_TO_DELETE_ARRAY
위험	품질	C/C++	MISMATCH.NEW_TO_FREE
위험	보안	C/C++	MISMATCH.RESOURCE
위험	보안	C/C++	OVERRUN.DYNAMIC.BAD_COND
위험	보안	C/C++	PATH_TRAVERSAL
위험	보안	C/C++	RESOURCE_INJECTION
위험	품질	C/C++	RETURN_FREE
위험	보안	C/C++	TYPE_OVERRUN.BAD_COND
위험	보안	C/C++	TYPE_OVERRUN.STATIC
위험	코드 규칙	C/C++	UNCONTROLLED_RECURSION
위험	보안	Java/JSP	CLEAR_TEXT_TRANSMISSION_OF_SENSITIVE_INFORMATION
위험	보안	Java/JSP	DATA_LEAK_BETWEEN_SESSIONS

위험	품질	Java/JSP	DIRECT_MANAGEMENT_OF_CONNECTIONS
위험	품질	Java/JSP	DIRECT_USE_OF_SOCKETS
위험	보안	Java/JSP	DOWNLOAD_OF_CODE_WITHOUT_INTEGRITY_CHECK
위험	보안	Java/JSP	EXPOSURE_OF_SYSTEM_DATA
위험	보안	Java/JSP	HARD_CODED_USER_NAME_AND_PASSWORD
위험	보안	Java/JSP	INCORRECT_PERMISSION_ASSIGNMENT_FOR_CRITICAL_RESOURCE
위험	코드 규칙	Java/JSP	INFINITE_RECURSIVE_CALL
위험	보안	Java/JSP	INTEGER_OVERFLOW
위험	보안	Java/JSP	MISSING_AUTHENTICATION_FOR_CRITICAL_FUNCTION
위험	품질	Java/JSP	OVERRIDE_HASHCODE_AND_EQUALS
위험	보안	Java/JSP	PASSWORD_IN_COMMENT
위험	보안	Java/JSP	PASSWORD_IN_SERVLET_COMMENT
위험	보안	Java/JSP	PASSWORD_MANAGEMENT_PASSWORD_IN_REDIRECT
위험	보안	Java/JSP	PASSWORD_SAVED_FILE_WITHOUT_ENCRYPTION
위험	보안	Java/JSP	PRIVATE_COLLECTION
위험	보안	Java/JSP	PUBLIC_DATA_ASSIGNED_TO_PRIVATE_ARRAY
위험	보안	Java/JSP	RELIANCE_ON_DNS_LOOKUPS_IN_A_SECURITY_DECISION
위험	보안	Java/JSP	RELIANCE_ON_UNTRUSTED_INPUTS_IN_A_SECURITY_DECISION
위험	보안	Java/JSP	SENSITIVE_COOKIE_IN_HTTPS_SESSION_WITHOUT_SECURE_ATTRIBUTE
위험	보안	Java/JSP	TOCTOU_RACE_CONDITION
위험	보안	Java/JSP	UNRESTRICTED_UPLOAD_OF_FILE
위험	보안	Java/JSP	USE_OF_HARDCODED_CRYPTOGRAPHIC_KEY
위험	보안	Java/JSP	USE_OF_INSUFFICIENT_RANDOM_VALUES
위험	보안	Java/JSP	USE_OF_INSUFFICIENT_RANDOM_VALUES_OWASP
위험	품질	Java/JSP	USE_OF_SOCKETS
위험	보안	Java/JSP	USING_HASH_WITHOUT_SALT
위험	품질	Java/JSP	USING_SYSTEM_EXIT
위험	보안	Java/JSP	USING_WEAK_CRYPTOGRAPHIC_ALGORITHM
위험	보안	Java/JSP	WEAK_ENCRYPTION_INADEQUATE_RSA_PADDING
위험	보안	Java/JSP	WEAK_ENCRYPTION_INSUFFICIENT_KEY_SIZE
위험	보안	Java/JSP	XSS_DOM
위험	보안	Javascript	ACCESS_CONTROL.DATABASE
위험	보안	Javascript	FORBIDDEN.WEAK_MIUPDATER.TOBE
위험	보안	Javascript	OPEN_REDIRECT.TOBE

위험	보안	Javascript	TRANSACTION.PLAIN.TOBE
위험	보안	Javascript	WEAK_ENCRYPTION.INSUFFICIENT_KEY_SIZE
위험	보안	Javascript	WEAK_PASSWORD.EMPTY_PASSWORD
위험	보안	Javascript	WEAK_PASSWORD.HARDCODED_PASSWORD
위험	보안	Javascript	XSS.LOCAL_STORAGE
위험	보안	Objective-C	BAD_PASSWORD.EMPTY
위험	보안	Objective-C	BAD_PASSWORD.HARDCODED
위험	보안	Objective-C	COOKIE.OVERLY_BROAD_DOMAIN
위험	보안	Objective-C	COOKIE.OVERLY_BROAD_PATH
위험	보안	Objective-C	COOKIE.PERSISTENT
위험	보안	Objective-C	DOWNLOAD_OF_CODE_WITHOUT_INTEGRITY_CHECK
위험	보안	Objective-C	DO_NOT_USE_DANGEROUS_FUNCTIONS
위험	보안	Objective-C	INTEGER_OVERFLOW
위험	품질	Objective-C	OVERRUN_STATIC
위험	보안	Objective-C	PLAIN_TEXT_STORING.SENSITIVE_INFORMATION
위험	보안	Objective-C	RELIANCE_ON_UNTRUSTED_ENV_INPUTS
위험	코드 규칙	Objective-C	UNCONTROLLED_RECURSION
위험	보안	Objective-C	USE_OF_INSUFFICIENT_RANDOM_VALUES
위험	보안	Objective-C	WEAK_ENCRYPTION.HASH
위험	보안	Objective-C	WEAK_ENCRYPTION.INSUFFICIENT_KEY_SIZE
위험	보안	Objective-C	WEAK_ENCRYPTION.RISKY_ALGORITHM
위험	보안	Objective-C	WEAK_ENCRYPTION_HASH.EMPTY_PBE_SALT
위험	보안	PHP	BAD_SECURITY_DECISION.DNS_LOOKUP
위험	보안	PHP	BAD_SECURITY_DECISION.UNTRUSTED_INPUT
위험	보안	PHP	HARD_CODED.CRYPTOGRAPHIC_KEY
위험	보안	PHP	HARD_CODED.PASSWORD
위험	보안	PHP	IMPROPER_RANDOM_USAGE
위험	품질	PHP	INFINITE_RECURSIVE_CALL
위험	보안	PHP	LEAK.ERROR_INFORMATION
위험	보안	PHP	MISSING_AUTHENTICATION.CRITICAL_FUNCTION
위험	품질	PHP	OVERLY_BROAD_CATCH
위험	보안	PHP	PASSWORD_IN_COMMENT
위험	보안	PHP	PLAIN_TEXT_STORING.SENSITIVE_INFORMATION
위험	보안	PHP	PLAIN_TEXT_TRANSMISSION.SENSITIVE_INFORMATION
위험	보안	PHP	REMOTE_CODE_EXECUTION
위험	보안	PHP	WEAK_ENCRYPTION.HASH
위험	보안	PHP	WEAK_ENCRYPTION.HASH.WITHOUT_SALT
위험	보안	PHP	WEAK_ENCRYPTION.INSUFFICIENT_KEY_SIZE
위험	보안	PHP	WEAK_ENCRYPTION.RISKY_ALGORITHM

위험	보안	Python	DOWNLOAD_OF_CODE_WITHOUT_INTEGRITY_CHECK
위험	보안	Python	EMPTY_SALT
위험	보안	Python	HARDCODED_PASSWORD
위험	보안	Python	HARD_CODED.CRYPTOGRAPHIC_KEY
위험	보안	Python	INCORRECT_PERMISSION_ASSIGNMENT_FOR_CRITICAL_RESOURCE
위험	보안	Python	INSECURE_RANDOM
위험	보안	Python	LEAK.ERROR_INFORMATION
위험	보안	Python	MISSING_AUTHENTICATION.CRITICAL_FUNCTION
위험	보안	Python	PASSWORD_IN_COMMENT
위험	보안	Python	PLAIN_TEXT_STORING.SENSITIVE_INFORMATION
위험	보안	Python	PLAIN_TEXT_TRANSMISSION.SENSITIVE_INFORMATION
위험	보안	Python	RELIANCE_ON_DNS_LOOKUPS_IN_A_SECURITY_DECISION
위험	보안	Python	RELIANCE_ON_UNTRUSTED_INPUTS_IN_A_SECURITY_DECISION
위험	보안	Python	TOCTOU_RACE_CONDITION
위험	보안	Python	WEAK_ENCRYPTION_ALGORITHM
위험	보안	Python	WEAK_ENCRYPTION_INSUFFICIENT_KEY_SIZE
위험	보안	Swift	BAD_PASSWORD.EMPTY
위험	보안	Swift	BAD_PASSWORD.HARDCODED
위험	보안	Swift	COOKIE.OVERLY_BROAD_DOMAIN
위험	보안	Swift	COOKIE.OVERLY_BROAD_PATH
위험	보안	Swift	COOKIE.PERSISTENT
위험	보안	Swift	PLAIN_TEXT_STORING.SENSITIVE_INFORMATION
위험	보안	Swift	WEAK_ENCRYPTION.INSUFFICIENT_KEY_SIZE
위험	보안	Swift	WEAK_ENCRYPTION_HASH.EMPTY_PBE_SALT
위험	보안	VB.Net	HARD_CODED_USER_NAME_AND_PASSWORD
위험	보안	VB.Net	USE_PARAMETERIZED_QUERY
위험	보안	VB.Net	WEAK_ENCRYPTION
위험	보안	VB.Net	WEAK_ENCRYPTION.INSUFFICIENT_KEY_SIZE
위험	보안	VBS	DYNAMIC_CODE_EVALUATION
위험	보안	VBS	LEAK.SYSTEM_INFORMATION
위험	보안	VBS	WEAK_ENCRYPTION.DES
위험	보안	VBS	WEAK_ENCRYPTION.HASH
위험	보안	VBS	WEAK_ENCRYPTION.INSUFFICIENT_KEY_SIZE
높음	보안	C	IGNORED_RETURN_VALUE
높음	품질	C#	EMPTY_CATCH_BLOCK
높음	품질	C#	FORBIDDEN.MONITOR_PULSE
높음	보안	C#	HASH.INSECURE_HASH_ITERATION_COUNT

높음	보안	C#	HASH.PREDICTABLE_SALT
높음	보안	C#	HTML_INPUT_HIDDEN
높음	보안	C#	INADEQUATE_RSA_PADDING
높음	보안	C#	KEY_MANAGEMENT.EMPTY_HMAC_KEY
높음	보안	C#	KEY_MANAGEMENT.HARDCODED_ENCRYPTION_KEY
높음	보안	C#	KEY_MANAGEMENT.HARDCODED_HMAC_KEY
높음	보안	C#	LEAK.SYSTEM_INFORMATION
높음	보안	C#	PASSWORD.EMPTY_PASSWORD
높음	보안	C#	PASSWORD.PBE_EMPTY_PASSWORD
높음	보안	C#	PASSWORD.PBE_HARDCODED_PASSWORD
높음	품질	C#	USING_APPLICATION_EXIT
높음	보안	C#	WEAK_ENCRYPTION.INSECURE_INITIALIZATION_VECTOR
높음	보안	C/C++	AUTHENTICATION_ATTEMPT_LIMIT
높음	보안	C/C++	AVOID_CROSS_SITE_SCRIPTING
높음	품질	C/C++	BAD_CALL.TYPE_MISMATCH.SPRINTF
높음	품질	C/C++	CAST_ALTERS_VALUE.EXT
높음	코드 규칙	C/C++	EMPTY_BRANCH
높음	보안	C/C++	ERROR_WITHOUT_ACTION
높음	보안	C/C++	MISSING_INTEGRITY_CHECK
높음	보안	C/C++	OS_COMMAND_INJECTION
높음	보안	C/C++	OVERRUN.DYNAMIC.IN_FUNC_CALL
높음	보안	C/C++	OVERRUN.DYNAMIC.IN_FUNC_CALL.BAD_COND
높음	보안	C/C++	OVERRUN.STATIC.IN_FUNC_CALL
높음	보안	C/C++	OVERRUN.STATIC.IN_FUNC_CALL.BAD_COND
높음	보안	C/C++	PLAINTEXT_PASSWORD
높음	보안	C/C++	RELIANCE_ON_UNTRUSTED_INPUTS
높음	보안	C/C++	SECURITY_DECISION_ON_DNS_LOOKUP
높음	보안	C/C++	TOC_TOU_ACCESS
높음	보안	C/C++	TYPE_OVERRUN.IN_FUNC_CALL
높음	보안	C/C++	TYPE_OVERRUN.IN_FUNC_CALL.BAD_COND
높음	보안	C/C++	UNSALTED_ONE_WAY_HASH
높음	보안	C/C++	USE_OF_HARDCODED_CRYPTOGRAPHIC_KEY
높음	보안	C/C++	WEAK_ENCRYPTION.HARDCODED_SALT
높음	보안	C/C++	WEAK_ENCRYPTION.INSUFFICIENT_KEY
높음	보안	C/C++	WEAK_ENCRYPTION.PASSWORD
높음	보안	C/C++	WEAK_ENCRYPTION.RISKY_ALGORITHM
높음	보안	C/C++	WEAK_ENCRYPTION.RSA_PADDING
높음	보안	C/C++	WEAK_PASSWORD_REQUIREMENTS
높음	보안	ETC	ANDROID_MANIFEST_AVOID_EXPORTED_ACCESS

높음	보안	ETC	ANDROID_MANIFEST_AVOID_USING_SHARED_USER_ID
높음	품질	Java/JSP	EMPTY_CATCH_BLOCK
높음	보안	Java/JSP	FORMAT_STRING
높음	보안	Java/JSP	SECURITY.INFINITE_LOOP
높음	보안	Java/JSP	XSS_ATTRIBUTE
높음	품질	Javascript	EMPTY_CATCH_BLOCK
높음	보안	Javascript	FORBIDDEN.EVAL_FUNCTION
높음	보안	Javascript	FORBIDDEN.INSECURE_RANDOM
높음	보안	Javascript	TRANSACTION.GET.TOBE
높음	보안	Objective-C	DO_NOT_USE_ANONYMOUS_LDAP_BIND
높음	보안	Objective-C	OS_COMMAND_INJECTION
높음	보안	Objective-C	SECURITY_DECISION_ON_DNS_LOOKUP
높음	보안	Objective-C	TOC_TOU_ACCESS
높음	보안	Objective-C	WEAK_ENCRYPTION.HARDCODED_KEY
높음	보안	Objective-C	WEAK_ENCRYPTION_HASH.NULL_PBE_SALT
높음	보안	PHP	BAD_COOKIE.NOT_SENT_OVER_SSL
높음	보안	PHP	BAD_COOKIE.PATH
높음	보안	PHP	BAD_INI.COOKIE_DOMAIN
높음	보안	PHP	BAD_INI.COOKIE_PATH
높음	보안	PHP	BAD_INI.LEAK.ERROR
높음	보안	PHP	BAD_INI.LEAK.VERSION
높음	보안	PHP	BAD_INI.PERSISTENT_COOKIE
높음	코드 규칙	PHP	EMPTY_CATCH_BLOCK
높음	보안	PHP	EXCESSIVE_SESSION_TIMEOUT.CAKEPHP
높음	보안	PHP	FORMAT_STRING
높음	보안	PHP	HTTP_TRANSPORT.GET
높음	보안	PHP	LEAK.DEBUG_INFORMATION.CAKEPHP
높음	보안	Python	BAD_ARGUMENTS.UMASK
높음	품질	Python	EMPTY_CATCH_BLOCK
높음	보안	Python	INSECURE_PERSISTENT_COOKIE
높음	보안	Swift	OS_COMMAND_INJECTION
높음	보안	Swift	WEAK_ENCRYPTION.HARDCODED_KEY
높음	보안	Swift	WEAK_ENCRYPTION_HASH
높음	보안	Swift	WEAK_ENCRYPTION_HASH.NIL_PBE_SALT
높음	보안	Swift	WEAK_ENCRYPTION_OPTION
높음	보안	VB.Net	EMPTY_CATCH_BLOCK
높음	보안	VB.Net	LEAK.SYSTEM_INFORMATION
보통	품질	C#	EMPTY_FINALLY_BLOCK
보통	보안	C#	OVERLY_BROAD_CATCH
보통	보안	C#	POOR_LOGGING_PRACTICE

보통	보안	C++	EMPTY_CATCH_BLOCK
보통	보안	C++	PRIVATE_COLLECTION
보통	보안	C++	PRIVATE_COLLECTION.ASSIGN
보통	보안	C/C++	DO_NOT_USE_PRINTF
보통	보안	C/C++	LEFTOVER_DEBUG_CODE
보통	보안	C/C++	PASSWORD_IN_COMMENT
보통	보안	Java/JSP	EXPOSURE_OF_DANGEROUS_METHOD
보통	보안	Java/JSP	LEFTOVER_DEBUG_CODE
보통	보안	Java/JSP	MISSING_LOGIN_CONTROL
보통	보안	Java/JSP	XSS.JSTL_COUT_ESCAPE_XML_FALSE
보통	보안	Javascript	LEFTOVER_DEBUG_CODE.TOBE
보통	보안	Objective-C	EMPTY_CATCH_BLOCK
보통	보안	Objective-C	PASSWORD_IN_COMMENT
보통	보안	PHP	FORBIDDEN.COOKIE
보통	보안	PHP	LEFTOVER_DEBUG_CODE
보통	보안	PHP	MISSING_LOGIN_CONTROL
보통	보안	Python	DJANGO_DEBUG_ENABLED
보통	보안	Python	LEFTOVER_DEBUG_CODE
보통	보안	Python	MISSING_LOGIN_CONTROL
보통	보안	Python	OVERLY_BROAD_CATCH
보통	보안	Swift	SYSTEM_INFORMATION_LEAK
보통	코드 규칙	VB.Net	ACTION_NOT_RESTRICTED_TO_POST
보통	코드 규칙	VB.Net	DISABLED_HEADER_CHECKING
보통	코드 규칙	VB.Net	DISABLED_VIEW_STATE_MAC
보통	코드 규칙	VB.Net	IMPERSONATION_CONTEXT
보통	코드 규칙	VB.Net	LEFTOVER_DEBUG_CODE
보통	코드 규칙	VB.Net	NON_SERIALIZABLE_OBJECT_IN_SESSION
보통	코드 규칙	VB.Net	OPTIONAL_SUBMODEL_REQUIRED
보통	보안	VB.Net	OVERLY_BROAD_CATCH
보통	코드 규칙	VB.Net	PERSISTENT_AUTHENTICATION
보통	보안	VBS	INSECURE_RANDOMNESS
낮음	보안	C/C++	MISSING_LOGIN_CONTROL
낮음	보안	C/C++	MISSING_PASSWORD_RECOVERY_CONTROL
낮음	품질	Java/JSP	BAD_CALL.FORBIDDEN
낮음	품질	Javascript	BAD_CALL.FORBIDDEN
낮음	품질	PHP	BAD_CALL.FORBIDDEN
낮음	품질	Python	BAD_CALL.FORBIDDEN
낮음	품질	VB.Net	BAD_CALL.FORBIDDEN
낮음	품질	VB.Net	EMPTY_BRANCH