



# 웹 애플리케이션 보고서

이 보고서는 웹 애플리케이션에 대한 중요 보안 정보를 포함하고 있습니다.

## 보안 보고서

이 보고서는 HCL AppScan Standard에서 작성하였습니다. 10.0.3  
스캔 시작: 2021-02-25 오전 9:24:27

# 목차

## 소개

- 일반 정보
- 로그인 설정

## 요약

- 문제 유형
- 취약한 URL
- 수정 권장 사항
- 보안 위험
- 원인
- WASC 위험 분류

## 문제 유형으로 정렬된 문제

- XSS(Cross-Site Scripting) ⑤
- 프레임을 통한 피싱 ⑤
- SRI(Subresource Integrity) 지원 검사 ①
- SSL 요청의 조회 매개변수 ⑧
- 누락되었거나 안전하지 않은 "Content-Security-Policy" 헤더 ②
- 누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더 ②
- 누락되었거나 안전하지 않은 "X-XSS-Protection" 헤더 ②
- 누락되었거나 안전하지 않은 HTTP Strict-Transport-Security 헤더 ①
- 본문 매개변수가 조회에서 허용됨 ③
- 비밀번호 필드에 대해 자동 완료 HTML 속성이 비활성화되지 않았습니다. ①
- 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키 ②
- 안전하지 않은 서드파티 링크(target="\_blank") ①
- 암호화 강제 실행되지 않음 ①
- 캐시화 가능한 SSL 페이지 발견 ⑤
- 누락된 "Content-Security-Policy" 헤더 ②
- 이메일 주소 패턴 발견 ①
- 클라이언트측(JavaScript) 쿠키 참조 ①

# 소개

이 보고서에는 HCL AppScan Standard가 수행한 웹 애플리케이션 보안 스캔의 결과가 포함되어 있습니다.

높은 심각도 문제: 5  
중간 심각도 문제: 5  
낮은 심각도 문제: 29  
정보용 심각도 문제: 4  
이 보고서에 포함된 총 보안 문제: 43  
이 스캔에서 발견된 총 보안 문제: 43

## 일반 정보

스캔 파일 이름: [사소01] 교육과학연구원 교수학습지원센터  
스캔 시작: 2021-02-25 오전 9:24:27  
테스트 정책: Default  
테스트 최적화 레벨: 고속

호스트: edu-i.ice.go.kr  
포트: 80  
운영 체제: 알 수 없음  
웹 서버: 알 수 없음  
애플리케이션 서버: JavaAppServer

호스트: edu-i.ice.go.kr  
포트: 443  
운영 체제: 알 수 없음  
웹 서버: 알 수 없음  
애플리케이션 서버: 모든

## 로그인 설정

로그인 메소드: 없음

# 요약

## 문제 유형 17

TOC

| 문제 유형 |  | 문제 수 |                        |
|-------|--|------|------------------------|
| 상     | XSS(Cross-Site Scripting)                        | 5    | <div><div></div></div> |
| 중     | 프레임을 통한 피싱                                       | 5    | <div><div></div></div> |
| 하     | SRI(Subresource Integrity) 지원 검사                 | 1    | <div><div></div></div> |
| 하     | SSL 요청의 조회 매개변수                                  | 8    | <div><div></div></div> |
| 하     | 누락되었거나 안전하지 않은 "Content-Security-Policy" 헤더      | 2    | <div><div></div></div> |
| 하     | 누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더       | 2    | <div><div></div></div> |
| 하     | 누락되었거나 안전하지 않은 "X-XSS-Protection" 헤더             | 2    | <div><div></div></div> |
| 하     | 누락되었거나 안전하지 않은 HTTP Strict-Transport-Security 헤더 | 1    | <div><div></div></div> |
| 하     | 본문 매개변수가 조회에서 허용됨                                | 3    | <div><div></div></div> |
| 하     | 비밀번호 필드에 대해 자동 완료 HTML 속성이 비활성화되지 않았습니다.         | 1    | <div><div></div></div> |
| 하     | 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키         | 2    | <div><div></div></div> |
| 하     | 안전하지 않은 세드파티 링크(target="_blank")                 | 1    | <div><div></div></div> |
| 하     | 암호화 강제 실행되지 않음                                   | 1    | <div><div></div></div> |
| 하     | 캐시화 가능한 SSL 페이지 발견                               | 5    | <div><div></div></div> |
| 정     | 누락된 "Content-Security-Policy" 헤더                 | 2    | <div><div></div></div> |
| 정     | 이메일 주소 패턴 발견                                     | 1    | <div><div></div></div> |
| 정     | 클라이언트측(JavaScript) 쿠키 참조                         | 1    | <div><div></div></div> |

## 취약한 URL 16

TOC

| URL |  | 문제 수 |                        |
|-----|--|------|------------------------|
| 상   | http://edu-i.ice.go.kr/rsv/rsv/list.do                     | 4    | <div><div></div></div> |
| 상   | http://edu-i.ice.go.kr/sw/popup/swPop.do                   | 3    | <div><div></div></div> |
| 상   | https://edu-i.ice.go.kr/rsv/rsv/list.do                    | 9    | <div><div></div></div> |
| 하   | http://edu-i.ice.go.kr/msi/cntntsService.do                | 1    | <div><div></div></div> |
| 하   | https://edu-i.ice.go.kr/template/common/js/common.js       | 2    | <div><div></div></div> |
| 하   | https://edu-i.ice.go.kr/template/member/js/script.js       | 2    | <div><div></div></div> |
| 하   | https://edu-i.ice.go.kr/uat/uia/egovLoginUsr.do            | 3    | <div><div></div></div> |
| 하   | https://edu-i.ice.go.kr/uss/umt/cmm/EgovUserConfirmView.do | 1    | <div><div></div></div> |

|   |  |   |                        |
|---|--|---|------------------------|
| 하 | http://edu-i.ice.go.kr/  | 6 | <div><div></div></div> |
| 하 | https://edu-i.ice.go.kr/   | 6 | <div><div></div></div> |
| 하 | http://edu-i.ice.go.kr/sw/swMain.do  | 1 | <div><div></div></div> |
| 하 | https://edu-i.ice.go.kr/rsv/rsv/list.json  | 1 | <div><div></div></div> |
| 하 | http://edu-i.ice.go.kr/cop/bbs/selectBoardArticle.do   | 1 | <div><div></div></div> |
| 하 | https://edu-i.ice.go.kr/str/cre/lyt/tmplat/sit/LYTTMP_0000000000002/font/NotoSansKR-Regular.ottf | 1 | <div><div></div></div> |
| 정 | http://edu-i.ice.go.kr/template/common/js/plyr/hls.js  | 1 | <div><div></div></div> |
| 정 | http://edu-i.ice.go.kr/template/common/js/common.js  | 1 | <div><div></div></div> |

## 수정 권장사항 15

TOC

| 조치방안 태스크 |   | 문제 수 |                        |
|----------|---|------|------------------------|
| 상        | 위험한 문자 인젝션에서 사용 가능한 솔루션 검토  | 10   | <div><div></div></div> |
| 하        | "Cache-Control: no-store" 및 "Pragma: no-cache" 헤더를 해당 응답에 추가하여 SSL 페이지의 캐싱을 방지하십시오. | 5    | <div><div></div></div> |
| 하        | "nosniff" 값으로 "X-Content-Type-Options" 헤더를 사용하도록 서버를 구성하십시오.                        | 2    | <div><div></div></div> |
| 하        | "자동 완료" 속성을 "Off"로 올바르게 설정하십시오.   | 1    | <div><div></div></div> |
| 하        | rel = "noopener noreferrer" 속성을 target = "_blank"가 있는 각 링크 요소에 추가                   | 1    | <div><div></div></div> |
| 하        | SameSite 쿠키 속성을 권장 값으로 구성하기 위한 가능한 솔루션을 검토하십시오                                      | 2    | <div><div></div></div> |
| 하        | SRI(Subresource Integrity)에 대한 각 썬드파티 스크립트/링크 요소 지원에 추가하십시오.                        | 1    | <div><div></div></div> |
| 하        | 값 '1'(사용 가능)로 "X-XSS-Protection" 헤더를 사용하도록 서버를 구성하십시오.                              | 2    | <div><div></div></div> |
| 하        | 긴 "max-age"로 HTTP Strict-Transport-Security 정책을 구현하십시오.                             | 1    | <div><div></div></div> |
| 하        | 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용  | 8    | <div><div></div></div> |
| 하        | 보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.                         | 4    | <div><div></div></div> |
| 하        | 웹 사이트에서 이메일 주소를 제거하십시오.   | 1    | <div><div></div></div> |
| 하        | 조회 문자열로 전송되는 본문 매개변수를 허용하지 마십시오.  | 3    | <div><div></div></div> |
| 하        | 중요 정보 송신 시 HTTPS를 사용 하십시오.  | 1    | <div><div></div></div> |
| 하        | 클라이언트 측으로부터 비즈니스와 보안 로직을 제거하십시오.  | 1    | <div><div></div></div> |

## 보안 위험 8

TOC

| 위험 | 문제 수  |    |  |
|----|---|----|--|
| 상  | 합법적인 사용자로 위장하는 데 사용될 수 있는 고객 세션 및 쿠키를 빼내거나 조작하는 것이 가능하여 해커가 사용자 레코드를 보거나 변경할 수 있으며 해당 사용자처럼 트랜잭션을 수행할 수 있습니다. | 5  | <div><div></div></div>                       |
| 중  | 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.                                 | 18 | <div><div></div><div></div><div></div></div> |
| 하  | 써드파티 서버가 손상되는 경우, 사이트의 콘텐츠/동작이 변경됩니다.   | 1  | <div><div></div></div>                       |
| 하  | 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.   | 9  | <div><div></div></div>                       |

|   |  |    |                        |
|---|--|----|------------------------|
| 하 | 사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.  | 18 | <div><div></div></div> |
| 하 | 웹 애플리케이션의 인증 메커니즘을 무시(bypass)하는 것이 가능할 것입니다.   | 1  | <div><div></div></div> |
| 하 | 쿠키를 자사 또는 <b>Same Site</b> 컨텍스트로 제한하여 쿠키 정보 유출을 방지하십시오. <b>CSRF</b> 방지 토큰과 같은 추가적인 보호가 적용되지 않을 경우 공격이 <b>CSRF(Cross-Site-Request-Forgery)</b> 공격으로 이어질 수 있습니다. | 2  | <div><div></div></div> |
| 정 | 이러한 공격에 대한 최악의 시나리오는 컨텍스트와 클라이언트측에서 작성된 쿠키의 역할에 달려있습니다.  | 1  | <div><div></div></div> |

## 원인 11

TOC

| 원인   | 문제 수                     |
|--|--------------------------|
| 상 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.                              | 5 <div><div></div></div> |
| 중 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.                              | 5 <div><div></div></div> |
| 하 하부 자원 무결성에 대해 지원하지 않습니다.   | 1 <div><div></div></div> |
| 하 조회 매개변수가 <b>SSL</b> 을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.    | 8 <div><div></div></div> |
| 하 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.                              | 7 <div><div></div></div> |
| 하 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.                              | 7 <div><div></div></div> |
| 하 올바르게 않거나 안전하지 않거나 누락된 <b>SameSite</b> 속성을 갖는 민감한 쿠키              | 2 <div><div></div></div> |
| 하 링크 요소의 <b>rel</b> 속성은 " <b>noopener noreferrer</b> "로 설정되지 않습니다. | 1 <div><div></div></div> |
| 하 사용자 이름, 비밀번호, 신용카드 번호와 같은 민감한 입력 필드가 암호화되지 않은 상태로 전송합니다.         | 1 <div><div></div></div> |
| 하 민감한 정보가 브라우저에 의해 캐시화되었을 수 있습니다.                                  | 5 <div><div></div></div> |
| 정 클라이언트 측에 쿠키가 작성됩니다.  | 1 <div><div></div></div> |

## WASC 위협 분류

TOC

| 위협                        | 문제 수                      |
|---------------------------|---------------------------|
| XSS(Cross-site scripting) | 5 <div><div></div></div>  |
| 기능 악용                     | 1 <div><div></div></div>  |
| 올바르지 않은 서버 구성             | 2 <div><div></div></div>  |
| 원격 파일 포함                  | 1 <div><div></div></div>  |
| 정보 유출                     | 29 <div><div></div></div> |
| 콘텐츠 위조                    | 5 <div><div></div></div>  |

# 문제 유형으로 정렬된 문제

상 XSS(Cross-Site Scripting) 5

TOC

문제 1 / 5

TOC

## XSS(Cross-Site Scripting)

심각도: 상

CVSS 점수: 7.5

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: searchResveType (Parameter)

**위험:** 합법적인 사용자로 위장하는 데 사용될 수 있는 고객 세션 및 쿠키를 빼내거나 조작하는 것이 가능하여 해커가 사용자 레코드를 보거나 변경할 수 있으며 해당 사용자처럼 트랜잭션을 수행할 수 있습니다.

**원인:** 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.

**수정사항:** 위험한 문자 인젝션에서 사용 가능한 솔루션 검토

**이유:** 사용자의 브라우저에 페이지가 로드될 때 실행되는 스크립트를 Appscan이 응답에 임베드했으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

**원시 테스트 응답:**

```
...
document.location.href = '/rsv/rsv/view.do?
menuId=MNU_0000000000000458&resveSeCode=EDU_RSV_01&searchResveType=TY02</script><script>
[window['location']='\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3a\x61\x6c\x65\x72\x74\x281733\x29']</script>&resveId=' +
event.resveId + '&searchBeginDt=' + event.useBeginDt + "&adiIem01=BBSC TG_00000000000680";
}
},
eventAfterAllRender: function(view) {
/* $('#calenBody .fc-day-number').each(function(idx, ele) {
var txt = $(ele).text();
$(ele).empty().append('<a href="#" class="customNumber">' + txt + '</a>');
}); */
lblChange();
}
...

```

문제 2 / 5

TOC

## XSS(Cross-Site Scripting)

심각도: **상**

CVSS 점수: 7.5

URL: <http://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: searchResveType (Parameter)

**위험:** 합법적인 사용자로 위장하는 데 사용될 수 있는 고객 세션 및 쿠키를 빼내거나 조작하는 것이 가능하여 해커가 사용자 레코드를 보거나 변경할 수 있으며 해당 사용자처럼 트랜잭션을 수행할 수 있습니다.

**원인:** 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.

**수정사항:** 위험한 문자 인젝션에서 사용 가능한 솔루션 검토

**이유:** 사용자의 브라우저에 페이지가 로드될 때 실행되는 스크립트를 Appscan이 응답에 임베드했으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

**원시 테스트 응답:**

```
...
document.location.href = '/rsv/rsv/view.do?
menuId=MNU_0000000000000458&resveSeCode=EDU_RSV_01&searchResveType=TY02</script><script>
[window['location']='\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3a\x61\x6c\x65\x72\x74\x281229\x29']</script>&resveId=' +
event.resveId + '&searchBeginDt=' + event.useBeginDt + "&adiIem01=BBSTG_00000000000680";
}
},
eventAfterAllRender: function(view) {
/* $('#calenBody .fc-day-number').each(function(idx, ele) {
var txt = $(ele).text();
$(ele).empty().append('<a href="#" class="customNumber">' + txt + '</a>');
}); */
lblChange();
}
}
...
```

문제 3 / 5

TOC

## XSS(Cross-Site Scripting)

심각도: **상**

CVSS 점수: 7.5

URL: <http://edu-i.ice.go.kr/sw/popup/swPop.do>

엔티티: videoPath (Parameter)

**위험:** 합법적인 사용자로 위장하는 데 사용될 수 있는 고객 세션 및 쿠키를 빼내거나 조작하는 것이 가능하여 해커가 사용자 레코드를 보거나 변경할 수 있으며 해당 사용자처럼 트랜잭션을 수행할 수 있습니다.

**원인:** 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.

**수정사항:** 위험한 문자 인젝션에서 사용 가능한 솔루션 검토

**이유:** 사용자의 브라우저에 페이지가 로드될 때 실행되는 스크립트를 Appscan이 응답에 임베드했으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

**테스트 응답**





#### 원시 테스트 응답:

```
...

<script src="/template/common/js/plyr/plyr.js"></script>
<script src="/template/common/js/plyr/hls.js"></script>
<script>
(function () {
  var video = document.querySelector('#player');

  if (Hls.isSupported()) {
    var hls = new Hls();

    hls.loadSource('http://middle.vod.cdn.cloudn.co.kr/sgm_nfs/_definst_/mp4:middle/streaming//data/origin_img/sw/382/01.mp4'+
[window['location']='\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3a\x61\x6c\x65\x72\x74\x281172\x29']+
'/playlist.m3u8');
    hls.attachMedia(video);
    hls.on(Hls.Events.MANIFEST_PARSED,function() {
      video.play();
    });
  }

  plyr.setup(video);
})();
</script>

...
```

| XSS(Cross-Site Scripting) |   |
|---------------------------|---|
| 심각도:                      | 상   |
| CVSS 점수:                  | 7.5   |
| URL:                      | <a href="http://edu-i.ice.go.kr/rsv/rsv/list.do">http://edu-i.ice.go.kr/rsv/rsv/list.do</a>                   |
| 엔티티:                      | adilem01 (Parameter)  |
| 위험:                       | 합법적인 사용자로 위장하는 데 사용될 수 있는 고객 세션 및 쿠키를 빼내거나 조작하는 것이 가능하여 해커가 사용자 레코드를 보거나 변경할 수 있으며 해당 사용자처럼 트랜잭션을 수행할 수 있습니다. |
| 원인:                       | 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.   |
| 수정사항:                     | 위험한 문자 인젝션에서 사용 가능한 솔루션 검토  |

**이유:** 사용자의 브라우저에 페이지가 로드될 때 실행되는 스크립트를 Appscan이 응답에 임베드했으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

**원시 테스트 응답:**

```
...
document.location.href = '/rsv/rsv/view.do?
menuId=MNU_0000000000000369&resveSeCode=EDU_RSV_01&searchResveType=&resveId=' + event.resveId + '&searchBeginDt=' +
event.useBeginDt + "&adiIem01=BBSTG_000000000000635</script ><script>
[window['location']='\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3a\x61\x6c\x65\x72\x74\x281205\x29']</script>";
}
},
eventAfterAllRender: function(view) {
/* $('#calenBody .fc-day-number').each(function(idx, ele) {
var txt = $(ele).text();
$(ele).empty().append('<a href="#" class="customNumber">' + txt + '</a>');
}); */
lblChange();
}
}
...
```

| XSS(Cross-Site Scripting) |   |
|---------------------------|---|
| 심각도:                      | 상   |
| CVSS 점수:                  | 7.5   |
| URL:                      | <a href="https://edu-i.ice.go.kr/rsv/rsv/list.do">https://edu-i.ice.go.kr/rsv/rsv/list.do</a>                 |
| 엔티티:                      | adilem01 (Parameter)  |
| 위험:                       | 합법적인 사용자로 위장하는 데 사용될 수 있는 고객 세션 및 쿠키를 빼내거나 조작하는 것이 가능하여 해커가 사용자 레코드를 보거나 변경할 수 있으며 해당 사용자처럼 트랜잭션을 수행할 수 있습니다. |
| 원인:                       | 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.   |
| 수정사항:                     | 위험한 문자 인젝션에서 사용 가능한 솔루션 검토  |

**이유:** 사용자의 브라우저에 페이지가 로드될 때 실행되는 스크립트를 Appscan이 응답에 임베드했으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

## 원시 테스트 응답:

```
...
    document.location.href = '/rsv/rsv/view.do?
menuId=MNU_0000000000000458&resvSeCode=EDU_RSV_01&searchResvType=TY02&resvId=' + event.resvId + '&searchBeginDt=' +
event.useBeginDt + "&adiItem01=BBSC TG_00000000000680</script><script>
[window['location']='\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3a\x61\x6c\x65\x72\x74\x281703\x29']</script>";
    }
    },
    eventAfterAllRender: function(view) {
        /* $('#calenBody .fc-day-number').each(function(idx, ele) {
        var txt = $(ele).text();
        $(ele).empty().append('<a href="#" class="customNumber">' + txt + '</a>');
        }); */
        lblChange();
    }
}
...
```

## 문제 1 / 5

TOC

## 프레임을 통한 피싱

심각도: 중

CVSS 점수: 6.4

URL: <http://edu-i.ice.go.kr/sw/popup/swPop.do>

엔티티: videoPath (Parameter)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.

**원인:** 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.

**수정사항:** 위험한 문자 인젝션에서 사용 가능한 솔루션 검토

**이유:** 테스트 응답에 "http://demo.testfire.net/phishing.html" URL의 frame/iframe이 포함되었으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

**테스트 응답**

**프레임을 통한 피싱**

|          |   |
|----------|---|
| 심각도:     | 중   |
| CVSS 점수: | 6.4   |
| URL:     | <a href="http://edu-i.ice.go.kr/rsv/rsv/list.do">http://edu-i.ice.go.kr/rsv/rsv/list.do</a> |
| 엔티티:     | searchResveType (Parameter)   |
| 위험:      | 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.               |
| 원인:      | 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.   |
| 수정사항:    | 위험한 문자 인젝션에서 사용 가능한 솔루션 검토  |

**이유:** 테스트 응답에 "http://demo.testfire.net/phishing.html" URL의 frame/iframe이 포함되었으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

## 프레임을 통한 피싱

심각도: 중

CVSS 점수: 6.4

URL: <http://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: adilem01 (Parameter)

위험: 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.

원인: 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.

수정사항: 위험한 문자 인젝션에서 사용 가능한 솔루션 검토

**이유:** 테스트 응답에 "http://demo.testfire.net/phishing.html" URL의 frame/iframe이 포함되었으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

## 프레임을 통한 피싱

심각도: 중

CVSS 점수: 6.4

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: adilem01 (Parameter)


위험: 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.

원인: 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.

수정사항: 위험한 문자 인젝션에서 사용 가능한 솔루션 검토

**이유:** 테스트 응답에 "http://demo.testfire.net/phishing.html" URL의 frame/iframe이 포함되었으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

## 프레임을 통한 피싱

심각도: 

CVSS 점수: 6.4

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: searchResveType (Parameter)

위험: 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.

원인: 사용자 입력값에서 위험한 문자가 올바르게 필터링되지 않았습니다.

수정사항: 위험한 문자 인젝션에서 사용 가능한 솔루션 검토

**이유:** 테스트 응답에 "http://demo.testfire.net/phishing.html" URL의 frame/iframe이 포함되었으므로 테스트 결과가 취약성을 표시하는 것으로 보입니다.

문제 1 / 1

TOC

## SRI(Subresource Integrity) 지원 검사

심각도: **하**

CVSS 점수: 5.0

URL: <http://edu-i.ice.go.kr/msi/cntntsService.do>

엔티티: cntntsService.do (Page)

위험: 써드파티 서버가 손상되는 경우, 사이트의 콘텐츠/동작이 변경됩니다.

원인: 하부 자원 무결성에 대해 지원하지 않습니다.

수정사항: SRI(Subresource Integrity)에 대한 각 써드파티 스크립트/링크 요소 지원에 추가하십시오.

**이유:** 써드파티 링크/스크립트에 브라우저가 이들이 손상되지 않았음을 확인하기 위한 무결성 속성이 없습니다.

**원시 테스트 응답:**

```
...
<!--
2. 설치 스크립트
* 지도 퍼가기 서비스를 2개 이상 넣을 경우, 설치 스크립트는 하나만 삽입합니다.
-->
<script charset="UTF-8" class="daum_roughmap_loader_script" src="http://dmaps.daum.net/map_js_init/roughmapLoader.js">
</script>
...
```

문제 1 / 8

TOC



## SSL 요청의 조회 매개변수

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/template/member/js/script.js>

엔티티: v (Parameter)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 조회 매개변수가 SSL을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.

수정사항: 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용

이유: AppScan이 SSL을 통해 송신된 HTTP 요청의 조회 부분에서 매개변수를 찾았습니다.

원본 요청

```
...
GET /template/member/js/script.js?v=5 HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://edu-i.ice.go.kr/uat/uia/egovLoginUsr.do?siteId=SITE_0000000000000002
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO5lySyTq9KHBeWyMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDctwkpaqQiv.YXBwX2RvbWFPbi9BUFAxLTE=
Connection: keep-alive
Sec-Fetch-Mode: no-cors
Host: edu-i.ice.go.kr
Accept: */*
Accept-Language: en-US
...
```

문제 2 / 8

TOC

## SSL 요청의 조회 매개변수

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/template/common/js/common.js>

엔티티: v (Parameter)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 조회 매개변수가 SSL을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.

수정사항: 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용

이유: AppScan이 SSL을 통해 송신된 HTTP 요청의 조회 부분에서 매개변수를 찾았습니다.

원본 요청

```
...
GET /template/common/js/common.js?v=17 HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://edu-i.ice.go.kr/rsv/rsv/list.do?resvSeCode=EDU_RSV_01&menuId=MNU_00000000000000341
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO5lySyTq9KHBeWyMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDctwkpaqQiv.YXBwX2RvbWFPbi9BUFAxLTE=
Connection: keep-alive
Sec-Fetch-Mode: no-cors
...
```

```
Host: edu-i.ice.go.kr
Accept: */*
Accept-Language: en-US
```

...

## 문제 3 / 8

TOC

### SSL 요청의 조회 매개변수

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/uat/uia/egovLoginUsr.do>

엔티티: siteld (Parameter)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 조회 매개변수가 SSL을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.

수정사항: 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용

**이유:** AppScan이 SSL을 통해 송신된 HTTP 요청의 조회 부분에서 매개변수를 찾았습니다.

**원본 요청**

```
...
GET /uat/uia/egovLoginUsr.do?siteId=SITE_0000000000000002 HTTP/1.1
Sec-Fetch-Site: cross-site
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://edu-i.ice.go.kr/msi/cntntsService.do?menuId=MNU_00000000000000152
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO5lySyTq9KHBeWyaMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDctwkpaqQiv.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: keep-alive
Sec-Fetch-Mode: navigate
Upgrade-Insecure-Requests: 1
Host: edu-i.ice.go.kr
Sec-Fetch-User: ?1
...
```

## 문제 4 / 8

TOC

## SSL 요청의 조회 매개변수

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: resveSeCode (Parameter)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 조회 매개변수가 SSL을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.

수정사항: 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용

이유: AppScan이 SSL을 통해 송신된 HTTP 요청의 조회 부분에서 매개변수를 찾았습니다.

원본 요청

```
...
GET /rsv/rsv/list.do?resveSeCode=EDU_RSV_01&menuId=MNU_0000000000000341 HTTP/1.1
Sec-Fetch-Site: cross-site
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://edu-i.ice.go.kr/msi/siteMap.do
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO51ySyTq9KHBwYAMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDctwkpaqQiV.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: keep-alive
Sec-Fetch-Mode: navigate
Upgrade-Insecure-Requests: 1
Host: edu-i.ice.go.kr
Sec-Fetch-User: ?1
...
```

문제 5 / 8

TOC

## SSL 요청의 조회 매개변수

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: menuId (Parameter)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 조회 매개변수가 SSL을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.

수정사항: 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용

이유: AppScan이 SSL을 통해 송신된 HTTP 요청의 조회 부분에서 매개변수를 찾았습니다.

원본 요청

```
...
GET /rsv/rsv/list.do?resveSeCode=EDU_RSV_01&menuId=MNU_0000000000000341 HTTP/1.1
Sec-Fetch-Site: cross-site
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://edu-i.ice.go.kr/msi/siteMap.do
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO51ySyTq9KHBwYAMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDctwkpaqQiV.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: keep-alive
Sec-Fetch-Mode: navigate
```

```
Upgrade-Insecure-Requests: 1
Host: edu-i.ice.go.kr
Sec-Fetch-User: ?1
```

...

## 문제 6 / 8

TOC

### SSL 요청의 조회 매개변수

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: adilem01 (Parameter)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 조회 매개변수가 SSL을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.

수정사항: 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용

**이유:** AppScan이 SSL을 통해 송신된 HTTP 요청의 조회 부분에서 매개변수를 찾았습니다.

**원본 요청**

```
...
GET /rsv/rsv/list.do?resvSeCode=EDU_RSV_01&adilem01=BBSTG_000000000000635&menuId=MNU_0000000000000369 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://edu-i.ice.go.kr/rsv/rsv/list.do?
resvSeCode=EDU_RSV_01&adilem01=BBSTG_000000000000635&menuId=MNU_0000000000000369
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO5lySyTq9KHBeWyaMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDctwkpaaqQiv.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: Keep-Alive
Host: edu-i.ice.go.kr
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

...

## 문제 7 / 8

TOC

## SSL 요청의 조회 매개변수

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: searchResveType (Parameter)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 조회 매개변수가 SSL을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.

수정사항: 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용

이유: AppScan이 SSL을 통해 송신된 HTTP 요청의 조회 부분에서 매개변수를 찾았습니다.

원본 요청

```
...
GET /rsv/rsv/list.do?resveSeCode=EDU_RSV_01&searchResveType=TY02&adiIem01=BBSTG_0000000000680&menuId=MNU_000000000000458
HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO5lySyTq9KHBeWyaMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDCtwkpaaqQiv.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: keep-alive
Sec-Fetch-Mode: navigate
Upgrade-Insecure-Requests: 1
Host: edu-i.ice.go.kr
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
...
```

## SSL 요청의 조회 매개변수

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/uss/umt/cmm/EgovUserConfirmView.do>

엔티티: trgtPge (Parameter)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 조회 매개변수가 SSL을 통해 전송되었습니다. 이 매개변수는 민감한 정보를 포함할 수 있습니다.

수정사항: 민감한 정보의 전송 시 항상 SSL 및 POST(본문) 매개변수 사용

이유: AppScan이 SSL을 통해 송신된 HTTP 요청의 조회 부분에서 매개변수를 찾았습니다.

원본 요청

```
...
GET /uss/umt/cmm/EgovUserConfirmView.do?trgtPge=update HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://edu-i.ice.go.kr/uss/umt/cmm/EgovUserConfirmView.do?trgtPge=update
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO5lySyTq9KHBeWyaMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDCtwkpaaqQiv.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: Keep-Alive
```

```
Host: edu-i.ice.go.kr
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

...

...
r:white;background-color:#525D76;} P {font-family:Courier,Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}</style-->
</head>
<body><h1>The document has been moved.</h1>
The document has been moved. <a href="https://edu-i.ice.go.kr/uat/uia/egovLoginUsr.do">here</a>.<p>
</body>

GET /uat/uia/egovLoginUsr.do HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://edu-i.ice.go.kr/uss/umt/cmm/EgovUserConfirmView.do?trgtPge=update
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=Wro051ySyTq9KHBewyMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDCTwkpaaqQiV.YXBwX2RvbWVpbi9BUFAxLTE=
Connection: Keep-Alive
Host: edu-i.ice.go.kr
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Transfer-Encoding: chunked

...
```

## 하 누락되었거나 안전하지 않은 "Content-Security-Policy" 헤더 2

TOC

## 문제 1 / 2

TOC

### 누락되었거나 안전하지 않은 "Content-Security-Policy" 헤더

|          |  |
|----------|--|
| 심각도:     | 하  |
| CVSS 점수: | 5.0  |
| URL:     | http://edu-i.ice.go.kr/  |
| 엔티티:     | edu-i.ice.go.kr (Page)   |
| 위험:      | 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.<br>사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다. |
| 원인:      | 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.  |
| 수정사항:    | 보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.  |

**이유:** AppScan에서 Content-Security-Policy 응답 헤더가 누락되었거나 안전하지 않은 정책을 포함하고 있음을 발견했습니다. 따라서 다양한 크로스 사이트 인젝션 공격에 더 많이 노출될 수 있습니다.

**원시 테스트 응답:**

...

```
Referer: http://edu-i.ice.go.kr/index.do?sso=ok
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO51ySyTq9KHBeWyaMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDCtwkpaqQiV.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: keep-alive
Host: edu-i.ice.go.kr
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 249
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8
```

...

### 누락되었거나 안전하지 않은 "Content-Security-Policy" 헤더

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/>

엔티티: edu-i.ice.go.kr (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** 보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.

**이유:** AppScan에서 Content-Security-Policy 응답 헤더가 누락되었거나 안전하지 않은 정책을 포함하고 있음을 발견했습니다. 따라서 다양한 크로스 사이트 인젝션 공격에 더 많이 노출될 수 있습니다.

**원시 테스트 응답:**

```
...

Sec-Fetch-Mode: navigate
Upgrade-Insecure-Requests: 1
Host: edu-i.ice.go.kr
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Dest: document
```

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Language: en-US
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8
```

...

## 문제 1 / 2

TOC

### 누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더

심각도: **하**

CVSS 점수: 5.0

URL: <http://edu-i.ice.go.kr/>

엔티티: edu-i.ice.go.kr (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** "nosniff" 값으로 "X-Content-Type-Options" 헤더를 사용하도록 서버를 구성하십시오.

**이유:** AppScan에서 "X-Content-Type-Options" 응답 헤더가 누락되었거나 안전하지 않은 값을 포함하고 있음을 발견했습니다. 따라서 드라이브 바이 다운로드 공격에 더 많이 노출될 수 있습니다.

**원시 테스트 응답:**

...

```
Referer: http://edu-i.ice.go.kr/index.do?sso=ok
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=Wro05lySyTq9KHBeWyaMBmzihDDDE2NUB6koBy1K3RnTAhPVJxApDCtwkpaaqQiV.YXBwX2RvbWVpbi9BUFAxLTE=
Connection: keep-alive
Host: edu-i.ice.go.kr
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 249
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8
```

...



## 누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/>

엔티티: edu-i.ice.go.kr (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** "nosniff" 값으로 "X-Content-Type-Options" 헤더를 사용하도록 서버를 구성하십시오.

**이유:** AppScan에서 "X-Content-Type-Options" 응답 헤더가 누락되었거나 안전하지 않은 값을 포함하고 있음을 발견했습니다. 따라서 드라이브 바이 다운로드 공격에 더 많이 노출될 수 있습니다.

**원시 테스트 응답:**

```
...

Sec-Fetch-Mode: navigate
Upgrade-Insecure-Requests: 1
Host: edu-i.ice.go.kr
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Dest: document

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Language: en-US
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8

...
```

하누락되었거나 안전하지 않은 "X-XSS-Protection" 헤더 2

TOC

## 누락되었거나 안전하지 않은 "X-XSS-Protection" 헤더

심각도: 하

CVSS 점수: 5.0

URL: <http://edu-i.ice.go.kr/>

엔티티: edu-i.ice.go.kr (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** 값 '1'(사용 가능)로 "X-XSS-Protection" 헤더를 사용하도록 서버를 구성하십시오.

**이유:** AppScan에서 X-XSS-Protection 응답 헤더가 누락되었거나 안전하지 않은 값을 포함하고 있음을 발견했습니다. 따라서 XSS(Cross-Site Scripting) 공격을 허용할 수 있습니다.

## 원시 테스트 응답:

```
...
Referer: http://edu-i.ice.go.kr/index.do?sso=ok
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=Wro051ySyTq9KHBewyMBmziHDDDE2NUB6koBy1K3RnTAhPVJxApDCtwkpaaqQiv.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: keep-alive
Host: edu-i.ice.go.kr
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US

HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 249
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8

...
```

## 누락되었거나 안전하지 않은 "X-XSS-Protection" 헤더

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/>

엔티티: edu-i.ice.go.kr (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** 값 '1'(사용 가능)로 "X-XSS-Protection" 헤더를 사용하도록 서버를 구성하십시오.

**이유:** AppScan에서 X-XSS-Protection 응답 헤더가 누락되었거나 안전하지 않은 값을 포함하고 있음을 발견했습니다. 따라서 XSS(Cross-Site Scripting) 공격을 허용할 수 있습니다.

**원시 테스트 응답:**

```
...  
Sec-Fetch-Mode: navigate  
Upgrade-Insecure-Requests: 1  
Host: edu-i.ice.go.kr  
Sec-Fetch-User: ?1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Accept-Language: en-US  
Sec-Fetch-Dest: document  
  
HTTP/1.1 200 OK  
Transfer-Encoding: chunked  
Connection: keep-alive  
Content-Language: en-US  
Date: Thu, 25 Feb 2021 00:35:28 GMT  
Content-Type: text/html; charset=utf-8  
  
...
```

## 누락되었거나 안전하지 않은 HTTP Strict-Transport-Security 헤더

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/>

엔티티: edu-i.ice.go.kr (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** 긴 "max-age"로 HTTP Strict-Transport-Security 정책을 구현하십시오.

**이유:** AppScan에서 HTTP Strict-Transport-Security 응답 헤더가 누락되었거나 "max-age"가 충분하지 않음을 발견했습니다.

**원시 테스트 응답:**

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Language: en-US
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8
```

...

**하** 본문 매개변수가 조회에서 허용됨 **3**

TOC

문제 1 / 3

TOC

## 본문 매개변수가 조회에서 허용됨

심각도: **하**

CVSS 점수: 5.0

URL: <http://edu-i.ice.go.kr/sw/swMain.do>

엔티티: swMain.do (Page)

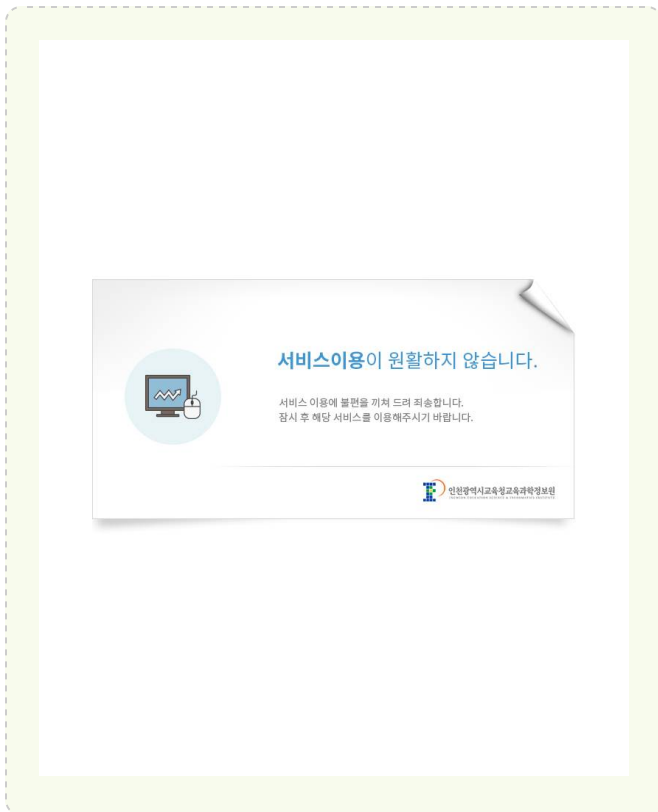
**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** 조회 문자열로 전송되는 본문 매개변수를 허용하지 마십시오.

**이유:** 테스트 응답이 원래 응답과 유사하며, 이는 애플리케이션이 조회에 제출된 본문 매개변수를 처리했음을 표시하므로 테스트 결과는 취약성을 표시하는 것으로 나타납니다.

### 원본 응답



### 테스트 응답



### 본문 매개변수가 조회에서 허용됨

심각도: 하

CVSS 점수: 5.0

URL: <http://edu-i.ice.go.kr/sw/popup/swPop.do>

엔티티: swPop.do (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** 조회 문자열로 전송되는 본문 매개변수를 허용하지 마십시오.

**이유:** 테스트 응답이 원래 응답과 유사하며, 이는 애플리케이션이 조회에 제출된 본문 매개변수를 처리했음을 표시하므로 테스트 결과는 취약성을 표시하는 것으로 나타납니다.

원본 응답



테스트 응답



문제 3 / 3

TOC

### 본문 매개변수가 조회에서 허용됨

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.json>

엔티티: list.json (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** 조회 문자열로 전송되는 본문 매개변수를 허용하지 마십시오.

**이유:** 테스트 응답이 원래 응답과 유사하며, 이는 애플리케이션이 조회에 제출된 본문 매개변수를 처리했음을 표시하므로 테스트 결과는 취약성을 표시하는 것으로 나타납니다.

하 비밀번호 필드에 대해 자동 완료 HTML 속성이 비활성화되지 않았습니다. ①

TOC

문제 1 / 1

TOC

### 비밀번호 필드에 대해 자동 완료 HTML 속성이 비활성화되지 않았습니다.

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/uat/uia/egovLoginUsr.do>

엔티티: egovLoginUsr.do (Page)

위험: 웹 애플리케이션의 인증 메커니즘을 무시(bypass)하는 것이 가능할 것입니다.

원인: 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

수정사항: "자동 완료" 속성을 "Off"로 올바르게 설정하십시오.

**이유:** AppScan이 비밀번호 필드가 자동 완료 기능 비활성화를 강제 실행하지 않음을 발견했습니다.

**원시 테스트 응답:**

```
...

<h4 class="login_txt">로그인</h4>
<section class="box_login">
  <form action="/uat/uia/actionLogin.do" id="frmGnrlLogin" name="frmGnrlLogin" method="post" onsubmit="return
checkGnrlLogin(this)">
    <input type="hidden" name="siteId" value="SITE_0000000000000002"/>
    <fieldset>
      <legend>로그인 폼</legend>
      <div class="box_inp">
        <label>아이디 <input type="text" id="id" name="id" value="" class="inp" title="아이디" /></label>
        <label>패스워드 <input type="password" id="pwd" name="password" value="" class="inp" title="패스워드" /></label>
      </div>
      <button id="btn_submit" type="submit">로그인</button>
      <p id="lblLogin">통합 로그인 페이지 입니다.</p>
      <a href="https://edu-p.ice.go.kr/uss/umt/cmm/EgovSelectMber.do" class="btn_join">회원가입</a>
      <nav>
        <a href="https://edu-p.ice.go.kr/uat/uia/egovIdSearchView.do">아이디 찾기</a>
        <a href="https://edu-p.ice.go.kr/uat/uia/egovPasswordSearchView.do">비밀번호 재발급</a>
      </nav>
    </fieldset>
  </form>
</section>

...
```

하 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키 ②

TOC

## 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키

심각도: 하

CVSS 점수: 4.1

URL: <http://edu-i.ice.go.kr/>

엔티티: WMONID (Cookie)

**위험:** 쿠키를 자사 또는 Same Site 컨텍스트로 제한하여 쿠키 정보 유출을 방지하십시오. CSRF 방지 토큰과 같은 추가적인 보호가 적용되지 않을 경우 공격이 CSRF(Cross-Site-Request-Forgery) 공격으로 이어질 수 있습니다.

**원인:** 올바르지 않거나 안전하지 않거나 누락된 SameSite 속성을 갖는 민감한 쿠키

**수정사항:** SameSite 쿠키 속성을 권장 값으로 구성하기 위한 가능한 솔루션을 검토하십시오

**이유:** 응답에 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 민감한 쿠키가 포함되어 있습니다. 이로 인해 쿠키 정보가 유출될 수 있으며, 추가적인 보호가 적용되지 않을 경우 CSRF(Cross-Site-Request-Forgery) 공격으로 이어질 수 있습니다.

## 원본 응답

...

```
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Language: en-US
Set-Cookie: WMONID=DWq4lVTUM15; Expires=Fri, 25-Feb-2022 09:46:02 GMT; Path=/
Set-Cookie: JSESSIONID=NH2Up5qO7Uvk4K1KIfDaQCWPqaSHtMFqB0YMia9VlwIgQM7MJrgz71nEUVzapCzy.YXBwX2RvbWVpbi9BUFAxLTE=; Path=/; HttpOnly
Date: Thu, 25 Feb 2021 00:46:02 GMT
Content-Type: text/html; charset=utf-8
```

...



## 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키

심각도: **하**

CVSS 점수: 4.1

URL: <http://edu-i.ice.go.kr/>

엔티티: JSESSIONID (Cookie)

**위험:** 쿠키를 자사 또는 Same Site 컨텍스트로 제한하여 쿠키 정보 유출을 방지하십시오. CSRF 방지 토큰과 같은 추가적인 보호가 적용되지 않을 경우 공격이 CSRF(Cross-Site-Request-Forgery) 공격으로 이어질 수 있습니다.

**원인:** 올바르지 않거나 안전하지 않거나 누락된 SameSite 속성을 갖는 민감한 쿠키

**수정사항:** SameSite 쿠키 속성을 권장 값으로 구성하기 위한 가능한 솔루션을 검토하십시오

**이유:** 응답에 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 민감한 쿠키가 포함되어 있습니다. 이로 인해 쿠키 정보가 유출될 수 있으며, 추가적인 보호가 적용되지 않을 경우 CSRF(Cross-Site-Request-Forgery) 공격으로 이어질 수 있습니다.

### 원본 응답

...

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Language: en-US
Set-Cookie: WMONID=sSoKB3-8E7U; Expires=Fri, 25-Feb-2022 09:47:51 GMT; Path=/
Set-Cookie: JSESSIONID=AghawTHQnjLBMhDCI2Pw2r318EX1CMZDBZl2luxjZwdljYQ7J5p7utYuHHSTofPi.YXBwX2RvbWpbi9BUFAyLTE=; Path=/; HttpOnly
Date: Thu, 25 Feb 2021 00:47:51 GMT
Content-Type: text/html; charset=utf-8
```

...

**하** 안전하지 않은 써드파티 링크(target="\_blank") **1**

TOC

문제 1 / 1

TOC

## 안전하지 않은 써드파티 링크(target="\_blank")

심각도: **하**

CVSS 점수: 5.0

URL: <http://edu-i.ice.go.kr/cop/bbs/selectBoardArticle.do>

엔티티: selectBoardArticle.do (Page)

위험: 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.

원인: 링크 요소의 rel 속성은 "noopener noreferrer"로 설정되지 않습니다.

수정사항: rel = "noopener noreferrer" 속성을 target="\_blank"가 있는 각 링크 요소에 추가

**이유:** target="\_blank" 속성 및 no rel="noopener noreferrer" 속성이 있는 써드파티 링크가 링크 페이지 창 오브젝트에 대한 링크된 페이지 부분 액세스 허용

**원시 테스트 응답:**

```
...

<p>2019 인천e학습터 홍보영상입니다.</p>
<p>다운로드 하신 후 아래의 예시처럼 사용하시면 됩니다.</p>
<p>&nbsp;</p>
<p>&nbsp;<span style="background-color: #ffffff; color: #3366ff;"><strong><a style="background-color: #ffffff; color: #3366ff;"
title="교사용_다운로드" href="http://dw-middle.dl.cdn.cloudn.co.kr/incheon/2019_e_study_teacher.mp4" target="_blank"
rel="noopener">교사용_다운로드</a></strong></span></p>
<p>&nbsp;</p>
<p><span style="background-color: #ffffff; color: #3366ff;"><strong><a style="background-color: #ffffff; color: #3366ff;"
title="학생용_다운로드" href="http://dw-middle.dl.cdn.cloudn.co.kr/incheon/2019_e_study_student.mp4" target="_blank"
rel="noopener">학생용_다운로드</a></strong></span></p>
<p>&nbsp;</p>
<p><span style="background-color: #ffffff; color: #3366ff;"><strong><a style="background-color: #ffffff; color: #3366ff;"
title="학부모용_다운로드" href="http://dw-middle.dl.cdn.cloudn.co.kr/incheon/2019_e_study_parents.mp4" target="_blank"
rel="noopener">학부모용_다운로드</a></strong></span></p>
<p>&nbsp;</p>
<p>&nbsp;</p>

</div>
</td>
</tr>

...
```

**하** 암호화 강제 실행되지 않음 ①

TOC

## 암호화 강제 실행되지 않음

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/>

엔티티: edu-i.ice.go.kr (Page)

위험: 암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.

원인: 사용자 이름, 비밀번호, 신용카드 번호와 같은 민감한 입력 필드가 암호화되지 않은 상태로 전송합니다.

수정사항: 중요 정보 송신 시 HTTPS를 사용 하십시오.

**이유:** 테스트 응답이 원래 응답과 매우 유사합니다. 이것은 HTTPS 대신 HTTP를 사용하여 자원에 정상적으로 액세스했음을 표시합니다.

## 하 캐시화 가능한 SSL 페이지 발견 5

TOC

## 문제 1 / 5

TOC

## 캐시화 가능한 SSL 페이지 발견

심각도: **하**

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/uat/uia/egovLoginUsr.do>

엔티티: egovLoginUsr.do (Page)

위험: 사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

원인: 민감한 정보가 브라우저에 의해 캐시화되었을 수 있습니다.

수정사항: "Cache-Control: no-store" 및 "Pragma: no-cache" 헤더를 해당 응답에 추가하여 SSL 페이지의 캐싱을 방지하십시오.

**이유:** 애플리케이션에서 페이지를 캐시해야 한다고 응답했으나 캐시 컨트롤이 설정되지 않았습니다. ("Cache-Control: no-store", "Cache-Control: no-cache" 또는 "Pragma: no-cache"를 설정하여 캐싱을 방지할 수 있습니다.)

**원시 테스트 응답:**

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Language: en-US
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8
```

| 캐시화 가능한 SSL 페이지 발견 |   |
|--------------------|---|
| 심각도:               | 하   |
| CVSS 점수:           | 5.0   |
| URL:               | https://edu-i.ice.go.kr/template/common/js/common.js                                |
| 엔티티:               | common.js (Page)  |
| 위험:                | 사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.         |
| 원인:                | 민감한 정보가 브라우저에 의해 캐시화되었을 수 있습니다.   |
| 수정사항:              | "Cache-Control: no-store" 및 "Pragma: no-cache" 헤더를 해당 응답에 추가하여 SSL 페이지의 캐싱을 방지하십시오. |

**이유:** 애플리케이션에서 페이지를 캐시해야 한다고 응답했으나 캐시 컨트롤이 설정되지 않았습니다. ("Cache-Control: no-store", "Cache-Control: no-cache" 또는 "Pragma: no-cache"를 설정하여 캐싱을 방지할 수 있습니다.)

**원시 테스트 응답:**

```
HTTP/1.1 200 OK
Last-Modified: Wed, 03 Apr 2019 07:24:24 GMT
Connection: Keep-Alive
Accept-Ranges: bytes
Content-Length: 31307
Keep-Alive: timeout=60
ETag: "0-7a4b-5ca45fa8"
Date: Thu, 25 Feb 2021 00:35:26 GMT
Content-Type: application/x-javascript

function fnImageCheck(fileId) {
    var fileValue = $('#'+fileId).val();
    if(fileValue && fileValue != '') {
        if(fileValue.toUpperCase().indexOf('.PNG') == -1 && fileValue.toUpperCase().indexOf('.JPG') == -1
&& fileValue.toUpperCase().indexOf('.GIF') == -1 && fileValue.toUpperCase().indexOf('.BMP') == -1) {
            alert("이미지만 첨부 가능합니다.");
            $('#'+fileId).focus();
            return false;
        }
    }
}
```

## 캐시화 가능한 SSL 페이지 발견

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/template/member/js/script.js>

엔티티: script.js (Page)

위험: 사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

원인: 민감한 정보가 브라우저에 의해 캐시화되었을 수 있습니다.

수정사항: "Cache-Control: no-store" 및 "Pragma: no-cache" 헤더를 해당 응답에 추가하여 SSL 페이지의 캐싱을 방지하십시오.

**이유:** 애플리케이션에서 페이지를 캐시해야 한다고 응답했으나 캐시 컨트롤이 설정되지 않았습니다. ("Cache-Control: no-store", "Cache-Control: no-cache" 또는 "Pragma: no-cache"를 설정하여 캐싱을 방지할 수 있습니다.)

**원시 테스트 응답:**

```
HTTP/1.1 200 OK
Last-Modified: Tue, 15 Jan 2019 09:08:51 GMT
Connection: Keep-Alive
Accept-Ranges: bytes
Content-Length: 2005
Keep-Alive: timeout=60
ETag: "0-7d5-5c3da323"
Date: Thu, 25 Feb 2021 00:35:37 GMT
Content-Type: application/x-javascript

$(document).ready(function(){
    // 첨부파일
    $(".file_attach").change(function(){
        var data = $(this).val();
        $(".file_inp").val(data);
    });

    // 프로필 사진
    $(".btn_del_pic").click(function(){
        confirm("프로필 사진을 삭제하시겠습니까?");
    });
    ...
});
```

## 캐시화 가능한 SSL 페이지 발견

심각도: 하

CVSS 점수: 5.0

URL: <https://edu-i.ice.go.kr/rsv/rsv/list.do>

엔티티: list.do (Page)

위험: 사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

원인: 민감한 정보가 브라우저에 의해 캐시화되었을 수 있습니다.

수정사항: "Cache-Control: no-store" 및 "Pragma: no-cache" 헤더를 해당 응답에 추가하여 SSL 페이지의 캐싱을 방지하십시오.

**이유:** 애플리케이션에서 페이지를 캐시해야 한다고 응답했으나 캐시 컨트롤이 설정되지 않았습니다. ("Cache-Control: no-store", "Cache-Control: no-cache" 또는 "Pragma: no-cache"를 설정하여 캐싱을 방지할 수 있습니다.)

**원시 테스트 응답:**

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Language: en-US
Date: Thu, 25 Feb 2021 00:36:58 GMT
Content-Type: text/html; charset=utf-8
```

...

## 캐시화 가능한 SSL 페이지 발견

|          |   |
|----------|---|
| 심각도:     | 하   |
| CVSS 점수: | 5.0   |
| URL:     | <a href="https://edu-i.ice.go.kr/str/cre/lyt/tmplat/sit/LYTTMP_0000000000002/font/NotoSansKR-Regular.otf">https://edu-i.ice.go.kr/str/cre/lyt/tmplat/sit/LYTTMP_0000000000002/font/NotoSansKR-Regular.otf</a> |
| 엔티티:     | NotoSansKR-Regular.otf (Page)   |
| 위험:      | 사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.   |
| 원인:      | 민감한 정보가 브라우저에 의해 캐시화되었을 수 있습니다.   |
| 수정사항:    | "Cache-Control: no-store" 및 "Pragma: no-cache" 헤더를 해당 응답에 추가하여 SSL 페이지의 캐싱을 방지하십시오.   |

**이유:** 애플리케이션에서 페이지를 캐시해야 한다고 응답했으나 캐시 컨트롤이 설정되지 않았습니다. ("Cache-Control: no-store", "Cache-Control: no-cache" 또는 "Pragma: no-cache"를 설정하여 캐싱을 방지할 수 있습니다.)

## 문제 1 / 2

TOC

## 누락된 "Content-Security-Policy" 헤더

|          |  |
|----------|--|
| 심각도:     | 정보용  |
| CVSS 점수: | 0.0  |
| URL:     | <a href="http://edu-i.ice.go.kr/">http://edu-i.ice.go.kr/</a>  |
| 엔티티:     | edu-i.ice.go.kr (Page)   |
| 위험:      | 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.<br>사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다. |
| 원인:      | 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.  |
| 수정사항:    | 보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.  |

**이유:** AppScan에서 Content-Security-Policy 응답 헤더가 누락되었거나 안전하지 않은 정책을 포함하고 있음을 발견했습니다. 따라서 다양한 크로스 사이트 인젝션 공격에 더 많이 노출될 수 있습니다.

**원시 테스트 응답:**

```
...
Referer: http://edu-i.ice.go.kr/index.do?sso=ok
Cookie: WMONID=5c9Rpj2bomL;
JSESSIONID=WroO5lySyTq9KHBeWyaMBmzihDDDE2NUB6koBylK3RnTAhPVJxApDctwkpaqQiV.YXBwX2RvbWFpbi9BUFAxLTE=
Connection: keep-alive
Host: edu-i.ice.go.kr
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US

HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 249
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8

...
```

## 문제 2 / 2

TOC

## 누락된 "Content-Security-Policy" 헤더

심각도: **정보용**

CVSS 점수: 0.0

URL: <https://edu-i.ice.go.kr/>

엔티티: edu-i.ice.go.kr (Page)

**위험:** 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.  
사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

**원인:** 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

**수정사항:** 보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.

**이유:** AppScan에서 Content-Security-Policy 응답 헤더가 누락되었거나 안전하지 않은 정책을 포함하고 있음을 발견했습니다. 따라서 다양한 크로스 사이트 인젝션 공격에 더 많이 노출될 수 있습니다.

**원시 테스트 응답:**

```
...

Sec-Fetch-Mode: navigate
Upgrade-Insecure-Requests: 1
Host: edu-i.ice.go.kr
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Dest: document

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Language: en-US
Date: Thu, 25 Feb 2021 00:35:28 GMT
Content-Type: text/html; charset=utf-8

...
```



## 이메일 주소 패턴 발견

심각도: **정보용**

CVSS 점수: 0.0

URL: <http://edu-i.ice.go.kr/template/common/js/plyr/hls.js>

엔티티: hls.js (Page)

위험: 사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.

원인: 안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

수정사항: 웹 사이트에서 이메일 주소를 제거하십시오.

이유: 응답에는 개인용 이메일 주소가 포함되어 있습니다.

원시 테스트 응답:

```
...
// http://stackoverflow.com/questions/8936984/uint8array-to-string-in-javascript/22373197
// http://www.onicos.com/staff/iz/amuse/javascript/expert/utf.txt
/* utf.js - UTF-8 <=> UTF-16 conversion
 *
 * Copyright (C) 1999 Masanao Izumo <iz@onicos.co.jp>
 * Version: 1.0
 * LastModified: Dec 25 1999
 * This library is free. You can redistribute it and/or modify it.
 */
...
```

## 정 클라이언트측(JavaScript) 쿠키 참조 ①

TOC

## 문제 1 / 1

TOC

## 클라이언트측(JavaScript) 쿠키 참조

심각도: **정보용**

CVSS 점수: 0.0

URL: <http://edu-i.ice.go.kr/template/common/js/common.js>

엔티티: function fnImageCheck(fileId) { (Page)

위험: 이러한 공격에 대한 최악의 시나리오는 컨텍스트와 클라이언트측에서 작성된 쿠키의 역할에 달려있습니다.

원인: 클라이언트 측에 쿠키가 작성됩니다.

수정사항: 클라이언트 측으로부터 비즈니스와 보안 로직을 제거하십시오.

이유: AppScan이 Javascript에서 쿠키 참조를 찾았습니다.

원본 응답

```
...
```

```

else
    return null;
}

function fnSetCookieValue(name, value) {
    var expireDate = new Date();
    expireDate.setFullYear(expireDate.getFullYear() + 1);
    document.cookie = name + "=" + escape(value) + "; path=/; expires=" + expireDate.toGMTString() + ";";
}

function fnSetCookiePopup( name, value, expiredays ) {
    var todayDate = new Date();
    todayDate.setDate( todayDate.getDate() + expiredays );
    if(value != null) {
        document.cookie = name + "=" + escape( value ) + "; path=/; expires=" + todayDate.toGMTString() + ";";
    } else {
        document.cookie = name + "; path=/; expires=" + todayDate.toGMTString() + ";";
    }
}

function fn_egov_popupOpen_PopupManage (popupId, fileUrl, width, height, top, left, stopVewAt) {

    var url = "/uss/ion/pwm/openPopupManage.do?";
    url = url + "fileUrl=" + fileUrl;
    url = url + "&stopVewAt=" + stopVewAt;
    url = url + "&popupId=" + popupId;

```

...