인천광역시교육청
INCHEON METROPOLITAN CITY OFFICE OF EDUCATION

인천광역시교육청 웹 서비스 점검

웹 취약점 점검 결과보고서

2023. 10. 08.

IGRUS
Inha Group of Research for Unix Security

개 정 이 력

버전	제/개정 일자	제/개정 페이지 및 내용	작성자	검토자
1.0	2023.10.08	최초 작성	이창현	이 삭
1.2	2023.10.08	총평 및 목차 수정	이창현	이 삭

목 차

1. 개요

1.1. 목적

본 취약점 진단은 인천광역시교육청 웹 서비스를 대상으로 주어진 시나리오를 바탕으로 모의해킹을 수행하고, 도출된 취약점에 대한 적절한 보안 가이드를 제시하여 잠재적인 해킹위협을 제거함으로써 인천광역시교육청의 안정성 확보에 기여하고자 합니다.

1.2. 수행 일정

웹 취약점 진단 수행 세부 일정은 아래와 같습니다.

- 수행 일정: 2023년 09월 11일 월요일 ~ 2023년 10월 08일 일요일 (총 27일)

구분	수행일정	비고
대상 선정 및 계획수립	2023.09.06	-
취약점 진단	2023.09.11 ~ 2023.10.07	-
결과 분석 및 보고서 작성	2023.10.07 ~ 2023.10.08	-
결과보고서 제출	2023.10.09	-

1.3. 수행 인력

웹 취약점 진단 수행 인력은 아래와 같습니다.

No	소속	수행업무	성명
1	인하대학교	PM / 웹 취약점 진단	이창현
2	인하대학교	PL / 기술 자문	이 삭
3	인하대학교	웹 취약점 진단	이고원
4	인하대학교	웹 취약점 진단	서민찬
5	인하대학교	웹 취약점 진단	안형빈
6	인하대학교	웹 취약점 진단	한희수
7	인하대학교	암호화 통신/알고리즘 진단	유재균

2. 수행 대상 및 내용

2.1. 수행 대상

웹 취약점 진단 대상은 사전에 제시 받은 자산목록을 기준으로 프로젝트 범위를 선정하였으며, 운영 서비스 자산 32 개를 대상으로 취약점 진단을 수행합니다.

No	홈페이지	URL
1	인천광역시교육청	https://www.ice.go.kr/main.do?s=ice
2	인천사이버진로교육원	https://cyberjinro.ice.go.kr/
3	기초학력보정시스템	https://basic.ice.go.kr/pt/index.do
4	남부교육지원청	https://nambu.ice.go.kr/Main.do
5	북부교육지원청	https://bukbu.ice.go.kr/index.do
6	동부교육지원청	https://dongbu.ice.go.kr/
7	서부교육지원청	https://seobu.ice.go.kr/main
8	강화교육지원청	https://ganghwa.ice.go.kr/main/main.asp
9	인천교수학습지원플랫폼	https://edu-i.ice.go.kr/index.do?sso=ok
10	인천 SW 교육지원센터	https://softcon.ice.go.kr/index.do?sso=ok
11	인천학생과학관	https://science.ice.go.kr/index.do?sso=ok
12	인천광역시교육청교육연수원	https://www.ieti.or.kr/
13	학생교육문화회관	https://www.iecs.go.kr/index.do
14	학생교육원	https://www.isec.go.kr/
15	교직원수련원	https://isptc.ice.go.kr/
16	평생학습관	https://www.ilec.go.kr/
17	도서관통합홈페이지	https://lib.ice.go.kr/
18	독서교육종합지원	http://book.ice.go.kr/
19	유아교육진흥원	http://child.ice.go.kr/
20	동아시아국제교육원	http://iegi.go.kr/
21	다문화교육지원센터	https://kr.allim2.kr/
22	인천학교체육지원	https://issc.edukor.org:446/
23	미래교육위원회	http://www.futureedu.or.kr/
24	법무도우미	http://law.ice.go.kr/ice/index.jsp
25	고입포털	https://isatp.ice.go.kr/
26	교육정보화지원	http://support.ice.go.kr/

27	교원연수시스템	http://edu-t.ice.go.kr/
28	인천교육 e-book	http://edubook.ice.go.kr
29	교육과학정보원	http://ienet.ice.go.kr/
30	마을공유지도 찾다	https://maeulngdo.ice.go.kr/
31	안전스쿨관리자	https://meta-safety.ice.go.kr/
32	지역연계꿈이음대학	https://www.ice.go.kr/main.do?s=ice
합계		32

2.2. 진단 항목

진단 항목은 인천광역시교육청에서 제시한 시나리오와 그 외 추가적인 항목으로 구성하였습니다. 상세 항목은 아래 "**5. 별첨**"을 참고하시기 바랍니다.

3. 수행 방안 및 내용

3.1. 수행 방안

3.1.1. 웹 취약점 진단 세부사항

웹 취약점 진단의 세부사항은 아래와 같습니다.

구분	설명
계획수립	- 진단 범위 및 취약점 분석·평가 기준 선정 - 웹 취약점 진단 수행 계획 수립
취약점 진단	- 제시 받은 시나리오와 몇 가지 추가 항목을 바탕으로 취약점 진단 수행
보호대책 수립	- 도출된 취약점에 대한 보안대책 가이드

3.1.2. 수행 도구

웹 취약점 진단 시 아래와 같은 수행 도구를 사용하여 수행합니다.

구분	도구	상세 설명
프록시	BurpSuite	- 웹 파라미터 삽입, 변조 - 데이터 인코딩 및 디코딩 등
트래픽 분석	WireShark	- 유/무선 네트워크 패킷 캡처 - 트래픽 패킷 분석
포트 스캔	Nmap	- 포트 및 SSL 암호화 알고리즘 스캔
쿠키 변조	EditThisCookie	- 웹 쿠키 변조 도구

※ 기타 웹 서비스 수행 도구 사용 시 담당자와 협의를 통하여 진행함

4. 웹 취약점 진단 결과

4.1. 총평

- 인천광역시교육청 웹 어플리케이션을 점검한 결과 **총 25개의 취약점** 항목이 도출되었음

- 총 32개의 서비스를 대상으로 점검을 수행한 결과 **경로 추적**, **파일 다운로드**, **크로스 사이트 스크립팅** 등 다수의 취약점이 발견되었습니다. **경로 추적 취약점**의 경우 파일 업로드 시 공격자가 임의의 경로에 파일 업로드를 수행할 수 있었으며 이를 통해 기존에 있던 파일들을 덮어 씌울 수 있는 가능성이 있으므로 보완이 필요합니다. 또한 일부 **파일 다운로드 취약점**의 경우 해당 서비스의 시스템 파일 내용에 접근할 수 있었으며 **크로스 사이트 스크립팅 취약점**의 경우 임의의 자바스크립트 구문을 이용하여 해당 페이지에 접근한 사용자가 자신도 모르게 공격자가 의도한 악의적인 작업을 수행할 수 있기 때문에 이 또한 보완이 필요합니다. 그 밖에 웹 서버 설정 미흡/누락으로 인한 취약점들이 도출되었습니다.

4.2. 점검 결과 요약

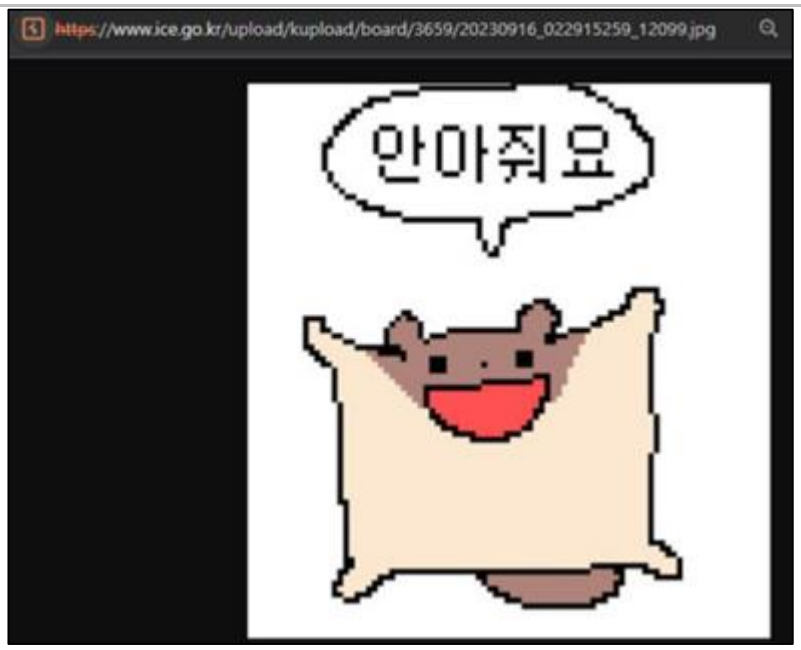
No	진단항목	점검내용	건수
1	파일 업로드	게시판에서 게시글 업로드 시 허가되지 않은 파일이 업로드 가능하고 접근까지 가능한지 점검	1
2	파일 다운로드	권한이 없는 게시글의 파일을 임의로 다운로드 할 수 있는지 점검	3
3	파라미터 변조	수동으로 요청에 포함된 파라미터 값을 조작해 허용되지 않은 권한이나 정보를 획득할 수 있는 취약점	3
4	크로스사이트 스크립팅	게시글과 같이 사용자의 입력을 처리하는 부분을 통해 임의의 스크립트를 실행할 수 있는지 점검	7
5	정보 노출	개발과정의 코멘트나 오류 메시지 등에서 중요 정보가 노출되어 있는지 점검	2
6	불충분한 인가	중요 기능이나 데이터에 권한없이 접근 가능한지 점검	5
7	관리자 페이지 노출	단순한 페이지 이름으로 관리자 메뉴에 직접 접근할 수 있는지 점검	3
8	경로 추적	../를 통해 웹 루트 디렉토리 외부에 저장된 파일 및 디렉토리에 접근할 수 있는지 점검	1
합계			25

4.3. 점검 결과 상세

4.3.1. 인천광역시교육청

4.3.1.1. 불충분한 인가

홈페이지명	인천광역시교육청 대표 홈페이지		
메뉴명	전자민원 > 민원안내 > 재증명발급 예약우편신청		
URL	https://www.ice.go.kr/boardCnts/list.do?boardID=3659&m=010207&s=ice		
점검자	서민찬	점검일시	2023.09.16. 02:29
취약점 개요	비밀글에 이미지가 타임스탬프 형식으로 되어 알아낼 수 있음		
취약점 상세 내용	Step1) 비밀 글에 있는 이미지가 타임 스탬프 형식이라 대략적인 시간과 브루트 포싱으로 비밀글에 있는 사진 위치를 알아내 사진을 볼 수 있음 		

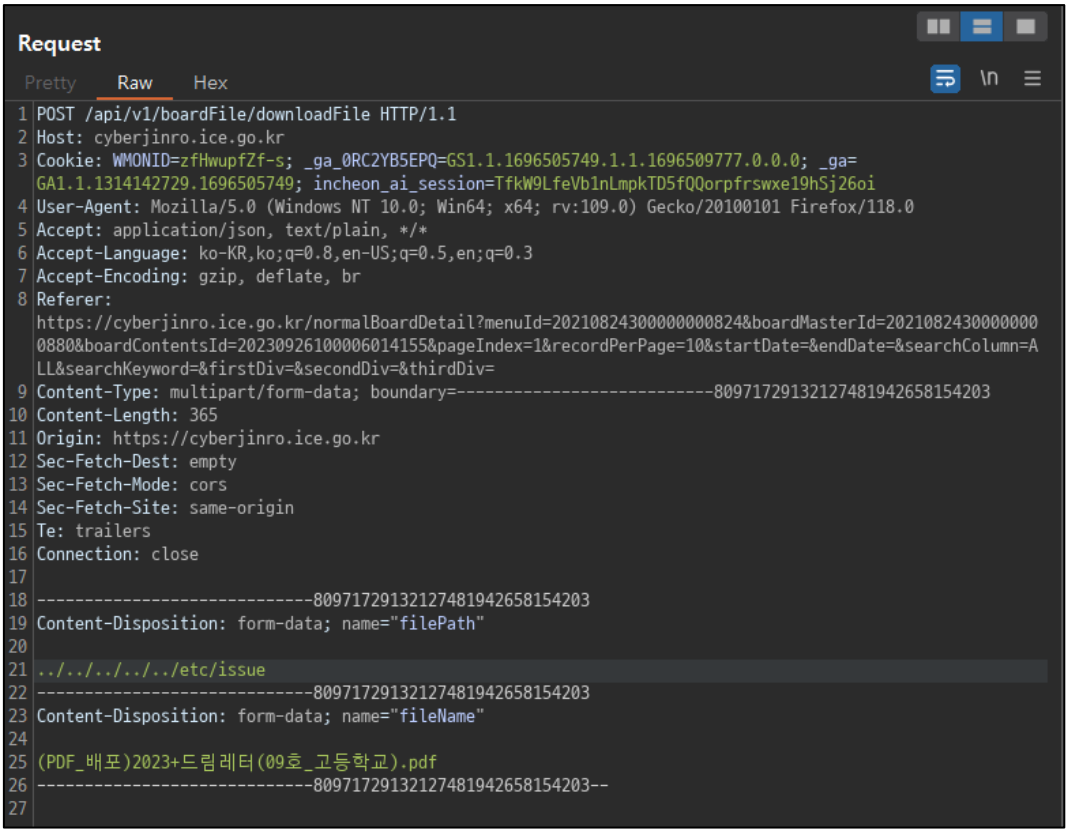

https://www.ice.go.kr/upload/kupload/board/3659/20230916_022915259_12099.jpg
안아줘요

4.3.1.2. 크로스사이트 스크립팅

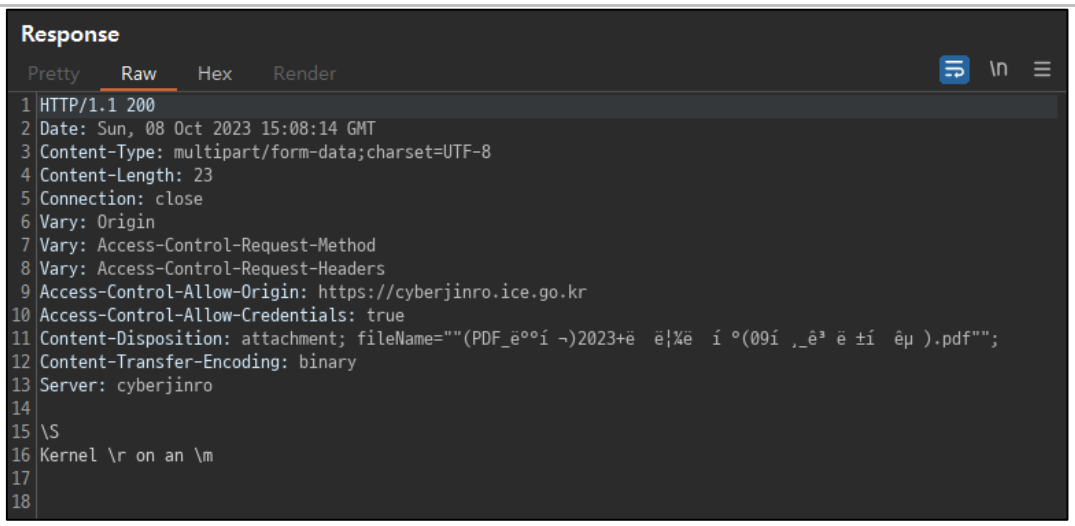
홈페이지명	인천광역시교육청 대표 홈페이지		
메뉴명	전자민원 > 민원안내 > 재증명발급 예약우편신청 전자민원 > 민원안내 > 민원기동대		
URL	https://www.ice.go.kr/boardCnts/list.do?boardID=3659&m=010207&s=ice https://www.ice.go.kr/boardCnts/list.do?searchStr=&boardID=3785&m=010207&s=ice https://www.ice.go.kr/boardCnts/list.do?boardID=3897&m=010211&s=ice		
점검자	서민찬	점검일시	2023.09.14. 12:01
취약점 개요	재증명발급 예약우편신청에서 stored xss 가 발생함		
취약점 상세 내용	Step1) Burp Suite 를 이용하여 cntslCnts 부분에 <img src='' onerror='alert(1)' alt=""> 를 넣는다.   Step2) stored XSS 로 인해 alert 창이 뜸  [참고] 찾은 게시판들 외에도 raon editor 를 이용해 글을 작성하는 게시판들은 동일한 취약점이 발견될 것으로 보임		

4.3.2. 인천사이버진로교육원

4.3.2.1. 파일 다운로드

<table>
<tr><td>홈페이지명</td><td colspan="3">인천사이버진로교육원</td></tr>
<tr><td>메뉴명</td><td colspan="3">진로/진학정보 - 진로/직업정보 - 진로정보자료</td></tr>
<tr><td>URL</td><td colspan="3">https://cyberjinro.ice.go.kr/normalBoardList?menuId=
20210824300000000824&boardMasterId=20210824300000000880</td></tr>
<tr><td>점검자</td><td>이고원</td><td>점검일시</td><td>2023.10.08. 19:30</td></tr>
<tr><td>취약점 개요</td><td colspan="3">파일 다운로드 취약점</td></tr>
<tr><td>취약점 상세 내용</td><td colspan="3">Step1) 게시물 내 첨부파일 다운로드 시 아래와 같은 요청이 발생하는데, 이때 filePath 를 조작하여 전송
 

Step2) 입력된 경로에 대한 필터링이 존재하지 않기 때문에 서버 시스템 파일 다운로드 가능</td></tr>
</table>



파일 다운로드 기능이 존재하는 게시판의 경우, 사용하는 API 의 경로가 다르지만 동일한 방법으로 취약점이 발생하는 것을 확인함

[동일 취약점 발생 API]

진로·진학정보 - 진로·직업정보 - 진로정보자료 (/api/v1/boardFile/downloadFile)

신청·접수 - 온라인상담신청 - 게시판상담 (/api/v1/onlineConsultFile/downloadFile)

열린공간 - 이벤트 (/api/v1/eventFile/downloadFile)

4.3.3. 기초학력정보시스템

4.3.3.1. 불충분한 인가

홈페이지명	기초학력보정시스템		
메뉴명	알림마당 > 문의하기		
URL	https://basic.ice.go.kr/pt/board/listBoard.do?mboardIdx=43&page=1&schTp=&schTxt=&categoryGroupCd=		
점검자	서민찬	점검일시	2023.10.05. 11:30
취약점 개요	비밀 글에 있는 사진을 검증없이 다운 받을 수 있다.		
취약점 상세 내용	Step1) burp suite 로 다운로드 페이지를 잡는다. Pretty Raw Hex 1 GET /pt/board/downloadBoard.do?mboardIdx=43&fileIdx=4837 HTTP/1.1 2 Host: basic.ice.go.kr 3 Cookie: JSESSIONID=RX7goOEcUfCL1HSzicmkZKUQOtgxPvXF4la1lQOl9GVUuPg7nHLpMJJ11spcPaAQ.basic-was_servlet_engine1 4 Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8" 5 Sec-Ch-Ua-Mobile: ?0 6 Sec-Ch-Ua-Platform: "Windows" 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document Step2) 비밀 글에 있는 첨부파일의 idx 를 예측해 집어넣으면 밑처럼 비밀 글을 올린 사람이라는 검증 없이도 다운 받을 수 있다. Pretty Raw Hex 1 GET /pt/board/downloadBoard.do?mboardIdx=43&fileIdx=4837 HTTP/1.1 2 Host: basic.ice.go.kr 3 Cookie: 4 Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8" 5 Sec-Ch-Ua-Mobile: ?0 6 Sec-Ch-Ua-Platform: "Windows" 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Accept-Encoding: gzip, deflate, br Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Content-Type: application/x-msdownload;charset=EUC-KR 3 Connection: close 4 Date: Thu, 05 Oct 2023 14:14:31 GMT 5 Pragma: no-cache 6 Content-Language: ko-KR 7 X-XSS-Protection: 1; mode=block 8 Content-Disposition: attachment; filename=20231005231 9 Cache-Control: no-cache, no-store, must-revalidate 10 Set-Cookie: JSESSIONID= 3UZOfafeTsGUIHWjiQF1Pz4UIkIZJrAF4juocYn1lOgRGZaJnzLD asic-was_servlet_engine1;Path=/;HttpOnly 11 Content-Length: 17099 12 13 □□□□□ExifMM*JR(□iZHH□0210□0100□□□□□□□□ 3.08BIM8BIM%□□□□ □□□B~□□(ICC_PROFILEapplmnt □acspAPPLAPPL□□□-appl□□□□8□G□m□□0z□/ 14 desc□Ocprt,Pwtpt|rXYZ□gXYZ□bXYZ□rTRC□ chad□,bTP mlucenUSDisplay P3mlucenUS4Copyright Apple Inc., 2023		

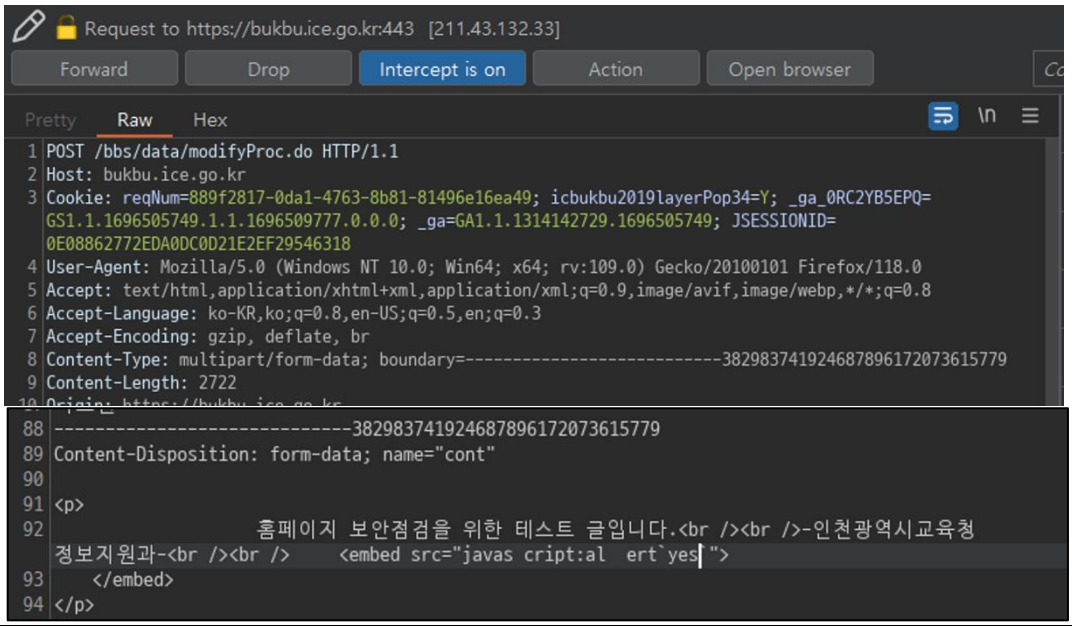
중요	고객만족센터 운영 안내	인천교육청	1240	2014-11-18
331	게시판 점검용 테스트 글입니다.	서**	0	2023-10-05

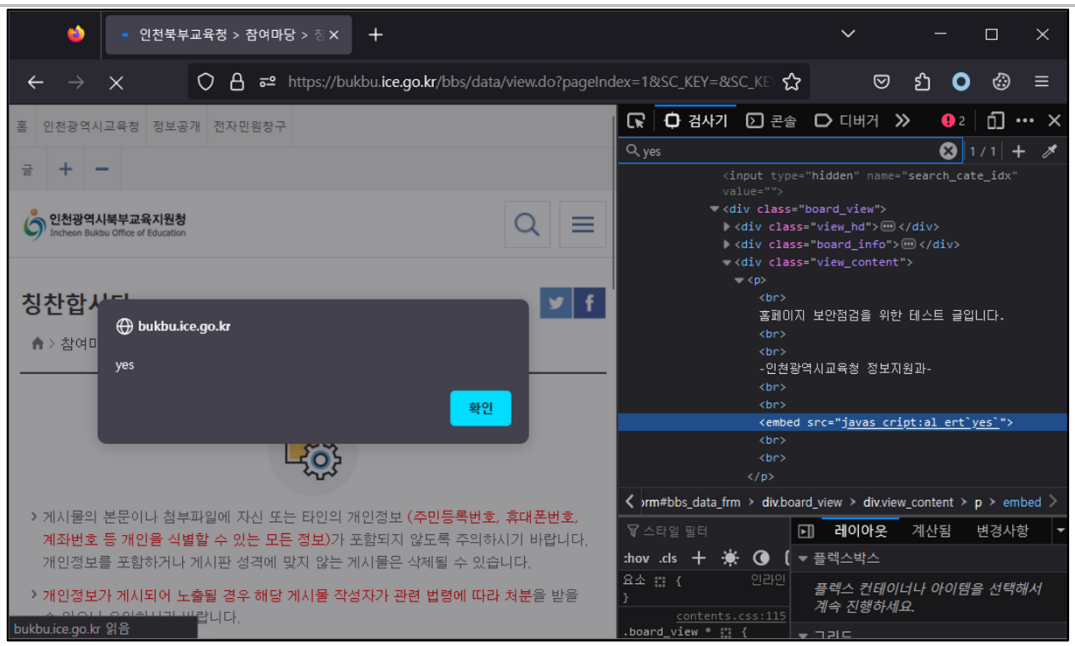
4.3.4. 남부교육지원청

발견된 취약점 없음

4.3.5. 북부교육지원청

4.3.5.1. 크로스사이트 스크립팅

<table>
<tr><td>홈페이지명</td><td colspan="3">북부교육지원청</td></tr>
<tr><td>메뉴명</td><td colspan="3">참여마당 - 칭찬합시다</td></tr>
<tr><td>URL</td><td colspan="3">https://bukbu.ice.go.kr/bbs/data/list.do?menu_idx=84</td></tr>
<tr><td>점검자</td><td>이고원</td><td>점검일시</td><td>2023.09.12. 22:20</td></tr>
<tr><td>취약점 개요</td><td colspan="3">게시글 본문 Stored XSS</td></tr>
<tr><td>취약점 상세 내용</td><td colspan="3">Step1) 스크립트 키워드 필터링을 우회하여 Stored XSS 가능
 
</td></tr>
</table>



이와 더불어 같은 기능을 사용하는 게시판의 경우, 동일한 방법으로 취약점 발생

[동일 취약점 발생 URL]

교육정보 - 북부 수업모아
(https://bukbu.ice.go.kr/bbs/data/list.do?per_menu_idx=310&tabCnt=2)

행정정보 - 청렴나눔방 - 청렴체크리스트
(https://bukbu.ice.go.kr/bbs/data/list.do?menu_idx=172)

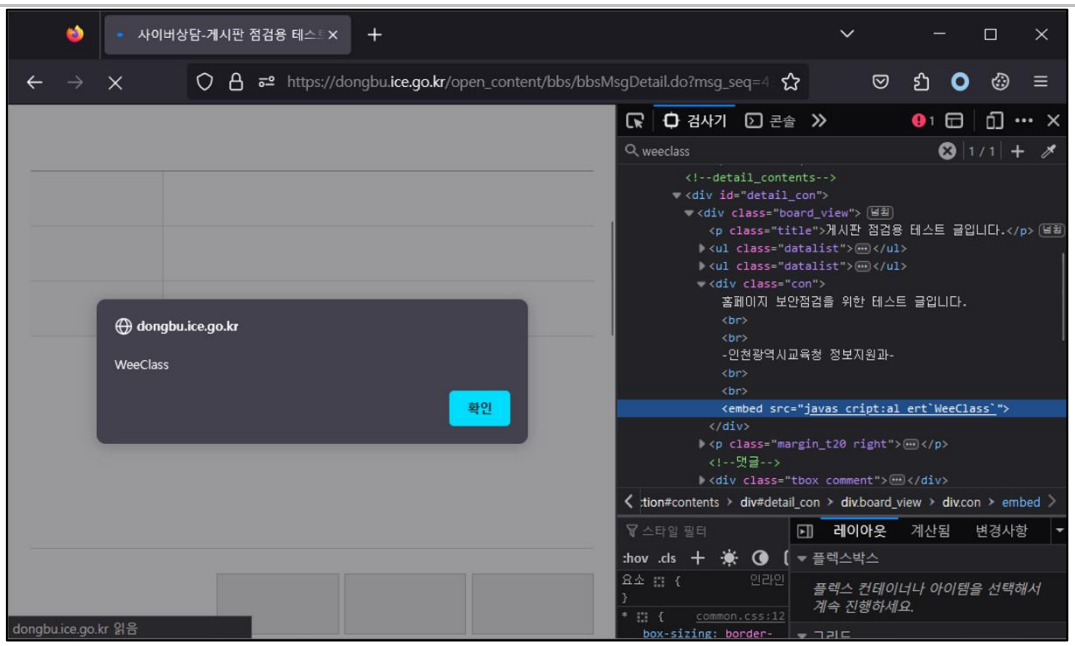
행정정보 - 교육재정 - 사립유치원 예결산서
(https://bukbu.ice.go.kr/bbs/data/list.do?menu_idx=320)

알림마당 - 학교소식 (https://bukbu.ice.go.kr/bbs/data/list.do?menu_idx=237)

4.3.6. 동부교육지원청

4.3.6.1. 크로스사이트 스크립팅

<table>
<tr><td>홈페이지명</td><td colspan="3">동부교육지원청</td></tr>
<tr><td>메뉴명</td><td colspan="3">교육 - Wee 센터 - 사이버상담</td></tr>
<tr><td>URL</td><td colspan="3">https://dongbu.ice.go.kr/scholarship/wee/counsel.jsp</td></tr>
<tr><td>점검자</td><td>이고원</td><td>점검일시</td><td>2023.10.05. 21:25</td></tr>
<tr><td>취약점 개요</td><td colspan="3">게시글 본문 Stored XSS</td></tr>
<tr><td>취약점 상세 내용</td><td colspan="3">Step1) 스크립트 키워드 필터링을 우회하여 Stored XSS 가능
 
</td></tr>
</table>



이와 더불어 같은 기능을 사용하는 게시판의 경우, 동일한 방법으로 취약점 발생

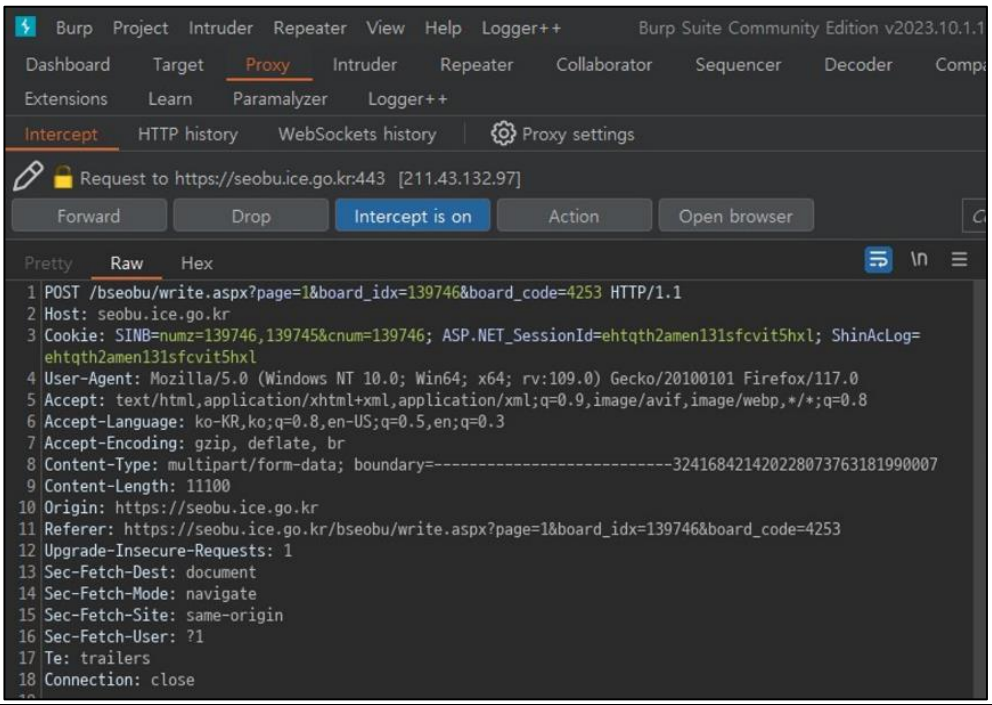
[동일 취약점 발생 URL]

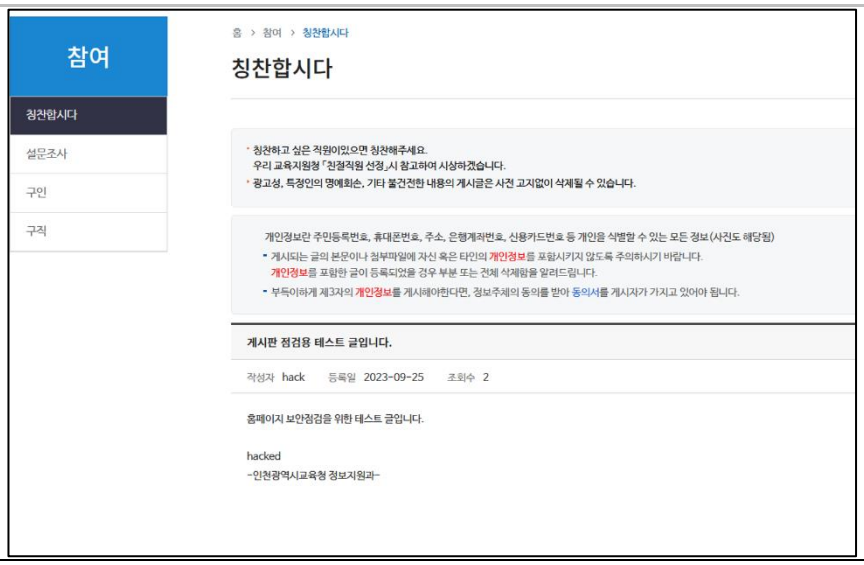
행정 - 청렴나눔방 - 청렴체크리스트
(https://dongbu.ice.go.kr/administration/checklist.jsp)
행정 – 교육행정지원
(https://dongbu.ice.go.kr/administration/support.jsp)
참여 – 구직
(https://dongbu.ice.go.kr/participation/job_search.jsp)
참여 – 칭찬합시다
(https://dongbu.ice.go.kr/participation/compliment.jsp)

4.3.7. 서부교육지원청

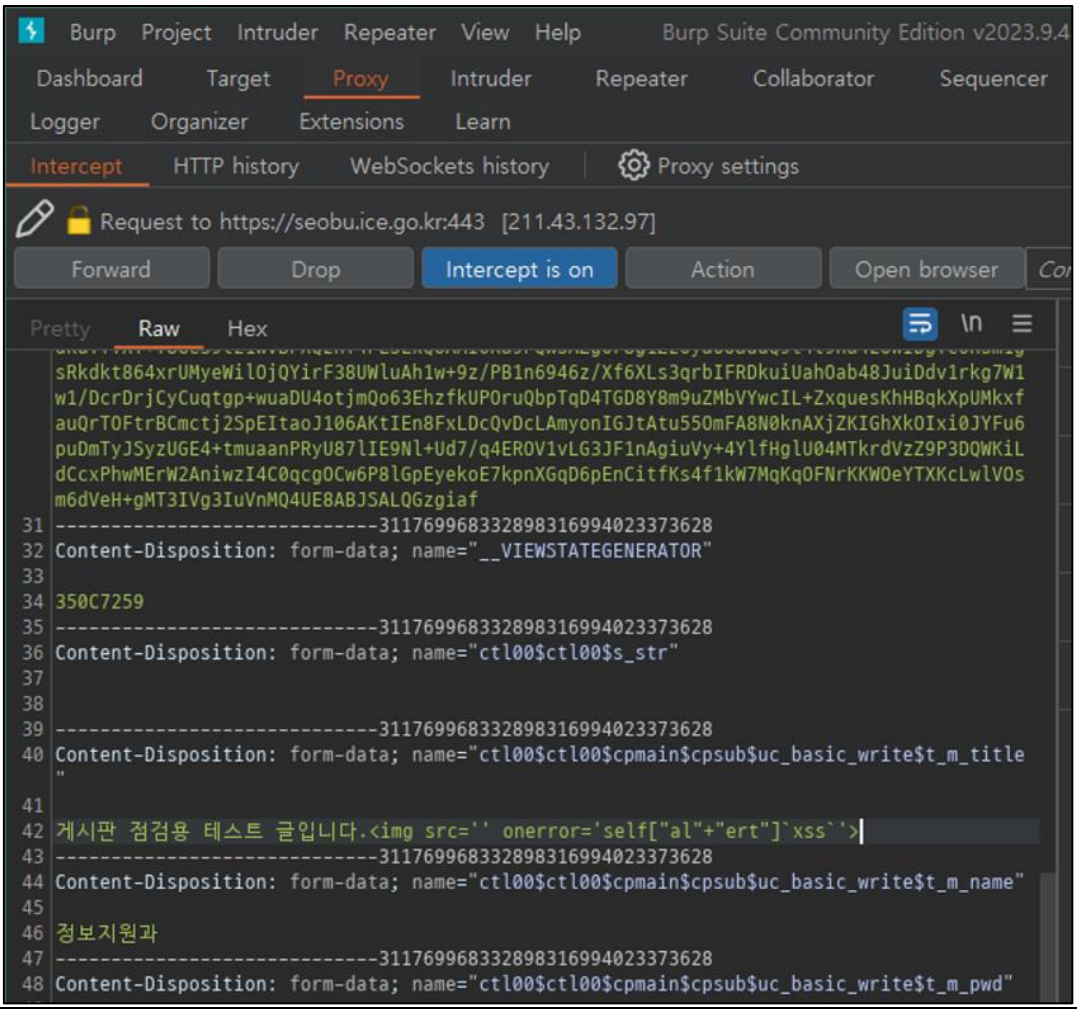
4.3.7.1. 불충분한 인가

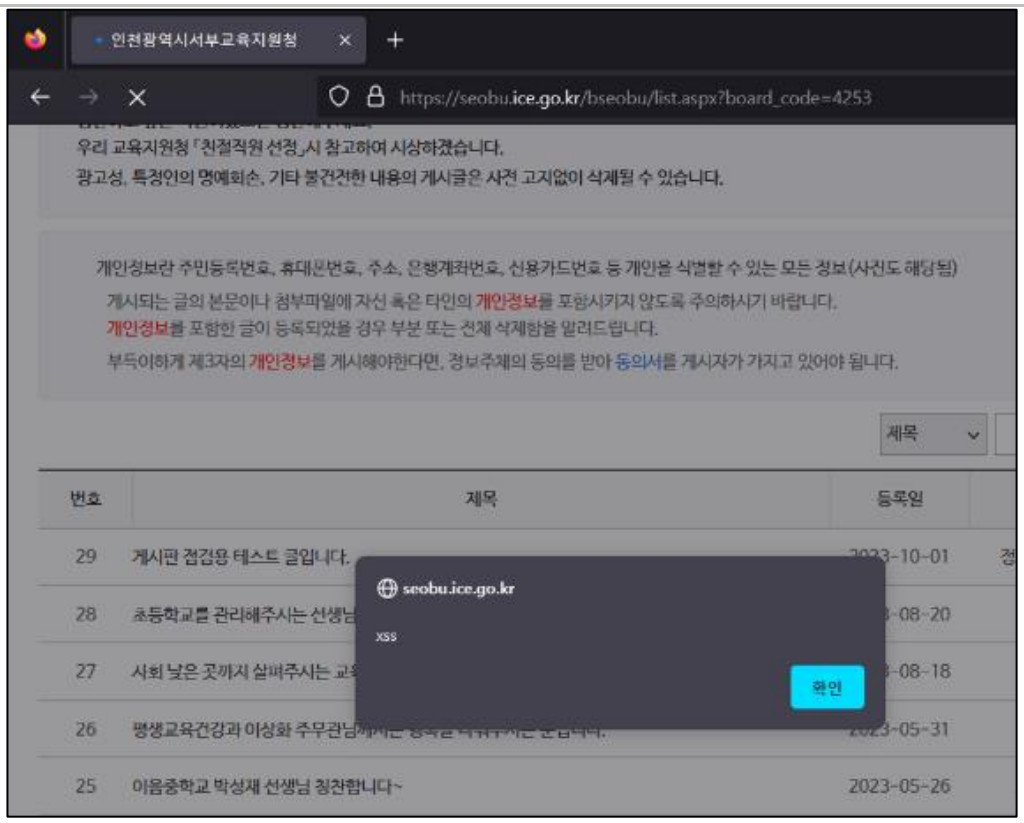
홈페이지명	서부교육지원청		
메뉴명	참여 – 칭찬합시다		
URL	https://seobu.ice.go.kr/bseobu/list.aspx?board_code=4253		
점검자	이고원	점검일시	2023.09.25. 23:00
취약점 개요	타인 게시물 수정		
취약점 상세 내용	Step1) 자신이 작성한 게시물을 경유하여 타인의 게시물 수정 가능 비밀글도 열람 가능하도록 수정이 가능하지만, 기존 내용을 확인할 수는 없음		



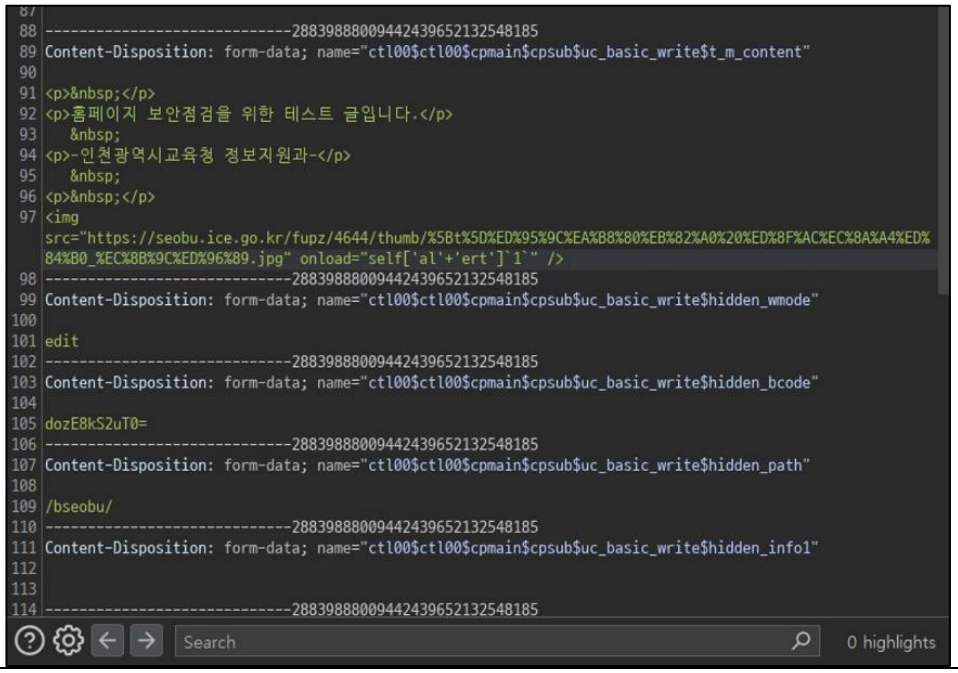

참여
칭찬합시다
설문조사
구인
구직
홈 > 참여 > 칭찬합시다
칭찬합시다
칭찬하고 싶은 직원이있으면 칭찬해주세요.
우리 교육지원청「친절직원 선정」시 참고하여 시상하겠습니다.
광고성, 특정인의 명예회손, 기타 불건전한 내용의 게시글은 사전 고지없이 삭제될 수 있습니다.
개인정보란 주민등록번호, 휴대폰번호, 주소, 은행계좌번호, 신용카드번호 등 개인을 식별할 수 있는 모든 정보(사진도 해당됨)
게시되는 글의 본문이나 첨부파일에 자신 혹은 타인의 개인정보를 포함시키지 않도록 주의하시기 바랍니다.
개인정보를 포함한 글이 등록되었을 경우 부분 또는 전체 삭제함을 알려드립니다.
부득이하게 제3자의 개인정보를 게시해야한다면, 정보주체의 동의를 받아 동의서를 게시자가 가지고 있어야 됩니다.
게시판 점검용 테스트 글입니다.
작성자 hack 등록일 2023-09-25 조회수 2
홈페이지 보안점검을 위한 테스트 글입니다.
hacked
-인천광역시교육청 정보지원과-

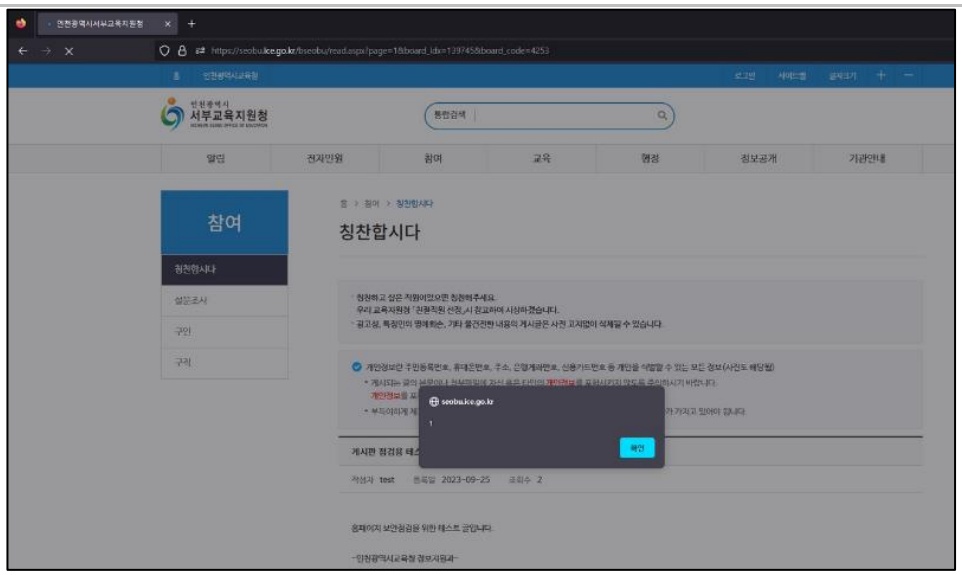
4.3.7.2. 크로스사이트 스크립팅

홈페이지명	서부교육지원청		
메뉴명	참여 - 칭찬합시다		
URL	https://seobu.ice.go.kr/bseobu/list.aspx?board_code=4253		
점검자	이고원	점검일시	2023.10.01. 15:30
취약점 개요	게시글 Stored XSS		
취약점 상세 내용	Step1) 제목 입력값 필터링 우회를 통해 게시물 목록에서 Stored XSS 발생 		

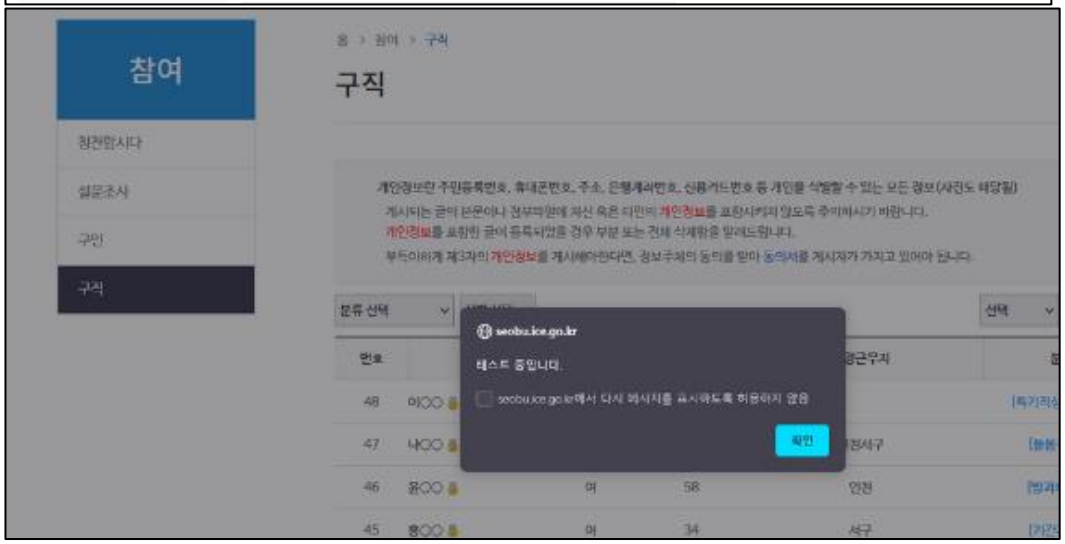


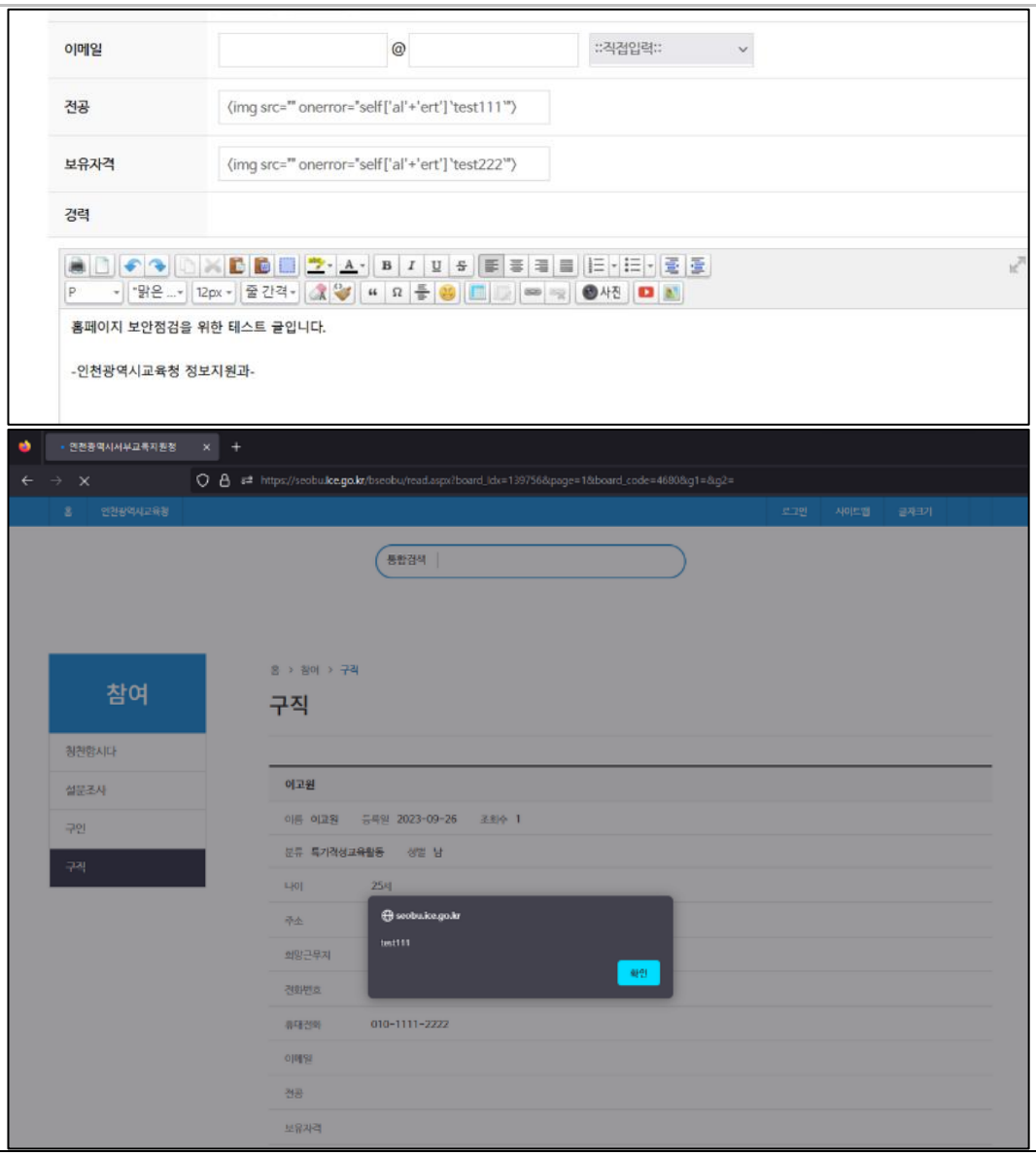
Step2) 키워드 필터링 우회를 통해 게시글 본문에서 Stored XSS 가능




서부교육지원청
참여
청찬합시다
seobu.ice.go.kr
1
확인

4.3.7.3. 크로스사이트 스크립팅

홈페이지명	서부교육지원청		
메뉴명	참여 – 구직		
URL	https://seobu.ice.go.kr/bseobu/list.aspx?board_code=4680		
점검자	이고원	점검일시	2023.09.26. 18:30
취약점 개요	게시판 Stored XSS		
취약점 상세 내용	Step1) 희망근무지에 스크립트 구문을 삽입하여 게시물 목록 출력 및 게시물 열람 시 XSS 발생   Step2) 전공과 보유자격에 입력하는 내용 필터링 우회를 통한 Stored XSS 발생 가능 (경력과 자기소개는 다른 페이지에서 사용되는 에디터와 동일하여 XSS 테스트 생략)		


이메일
@
::직접입력::
전공
<img src="" onerror="self['al'+'ert']`test111`">
보유자격
<img src="" onerror="self['al'+'ert']`test222`">
경력
홈페이지 보안점검을 위한 테스트 글입니다.
-인천광역시교육청 정보지원과-
통합검색
참여
참석합시다
설문조사
구인
구직
구직
이교원
seobu.ice.go.kr
test111
확인
010-1111-2222

4.3.8. 강화교육지원청

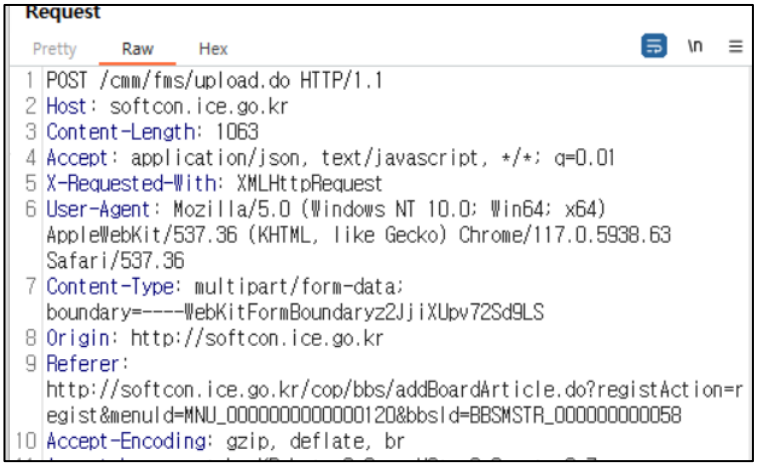
발견된 취약점 없음

4.3.9. 인천교수학습지원플랫폼

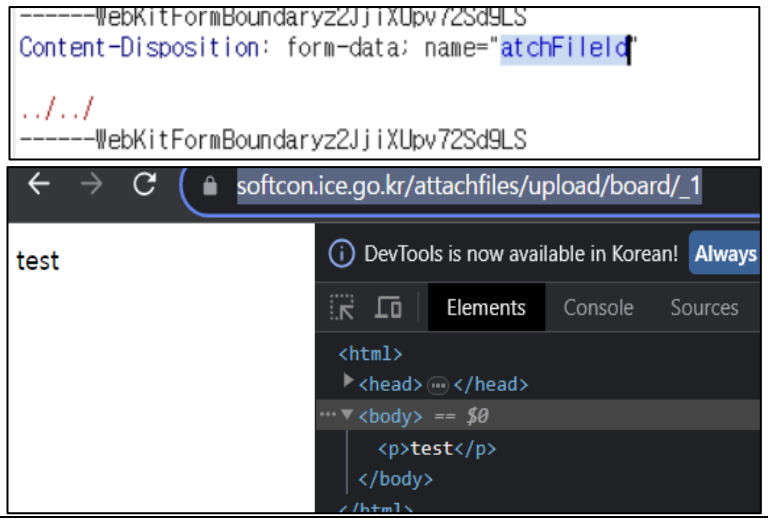
발견된 취약점 없음

4.3.10. 인천 SW 교육지원센터

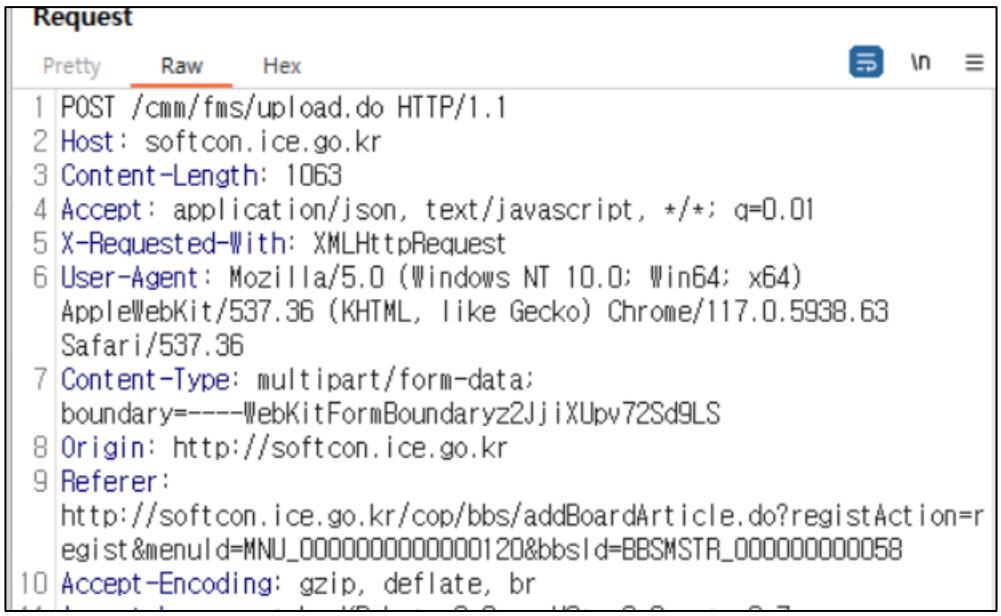
4.3.10.1. 경로 추적

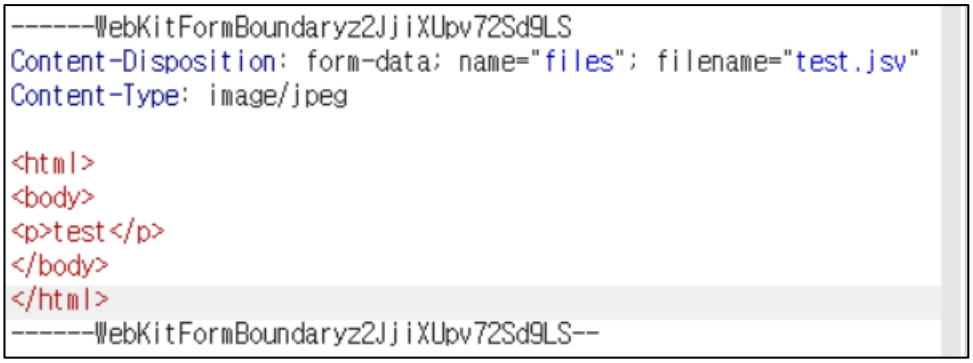
<table>
<tr><td>홈페이지명</td><td colspan="3">인천 SW 교육지원센터</td></tr>
<tr><td>메뉴명</td><td colspan="3">알림마당 > 공지사항</td></tr>
<tr><td>URL</td><td colspan="3">http://softcon.ice.go.kr/cop/bbs/addBoardArticle.do?registAction=regist&menuId=MNU_0000000000000120&bbsId=BBSMSTR_000000000058</td></tr>
<tr><td>점검자</td><td>서민찬</td><td>점검일시</td><td>2023.09.22. 02:58</td></tr>
<tr><td>취약점 개요</td><td colspan="3">파일 업로드를 할 때 path traversal 발생</td></tr>
<tr><td>취약점 상세 내용</td><td colspan="3">Step1) Burp Suite 로 공지사항 글쓰기부분에서 파일 업로드하는 부분을 잡는다.
 
</td></tr>
</table>

Step2) atchFileId 부분에 "../"를 이어붙인다.



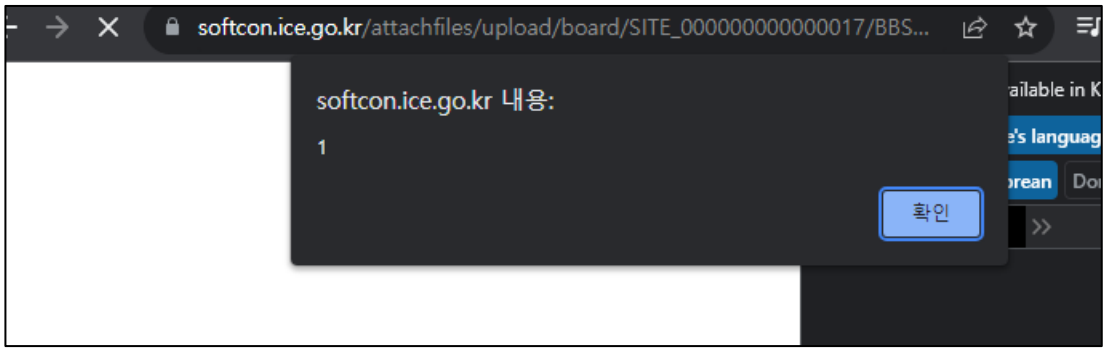
4.3.10.2. 파일 업로드

<table>
<tr><td>홈페이지명</td><td colspan="3">인천 SW 교육지원센터</td></tr>
<tr><td>메뉴명</td><td colspan="3">알림마당 > 공지사항</td></tr>
<tr><td>URL</td><td colspan="3">http://softcon.ice.go.kr/cop/bbs/addBoardArticle.do?registAction=regist&menuId=MNU_0000000000000120&bbsId=BBSMSTR_000000000058</td></tr>
<tr><td>점검자</td><td>서민찬</td><td>점검일시</td><td>2023.09.20. 01:03</td></tr>
<tr><td>취약점 개요</td><td colspan="3">파일 내용에 html 내용을 쓰면 html 로 인식</td></tr>
<tr><td>취약점 상세 내용</td><td colspan="3">Step1) Burp Suite 로 공지사항 글쓰기부분에서 파일 업로드하는 부분을 잡는다.
 

Step2) 이후 파일 내용을 html 내용으로 바꾼다.
 
</td></tr>
</table>

Step3) 파일 부분으로 가면 html 내용이 보인다.

Step4) 밑은 이를 이용해서 띄운 alert 창이다.



4.3.11. 인천학생과학관

발견된 취약점 없음

4.3.12. 인천광역시교육청교육연수원

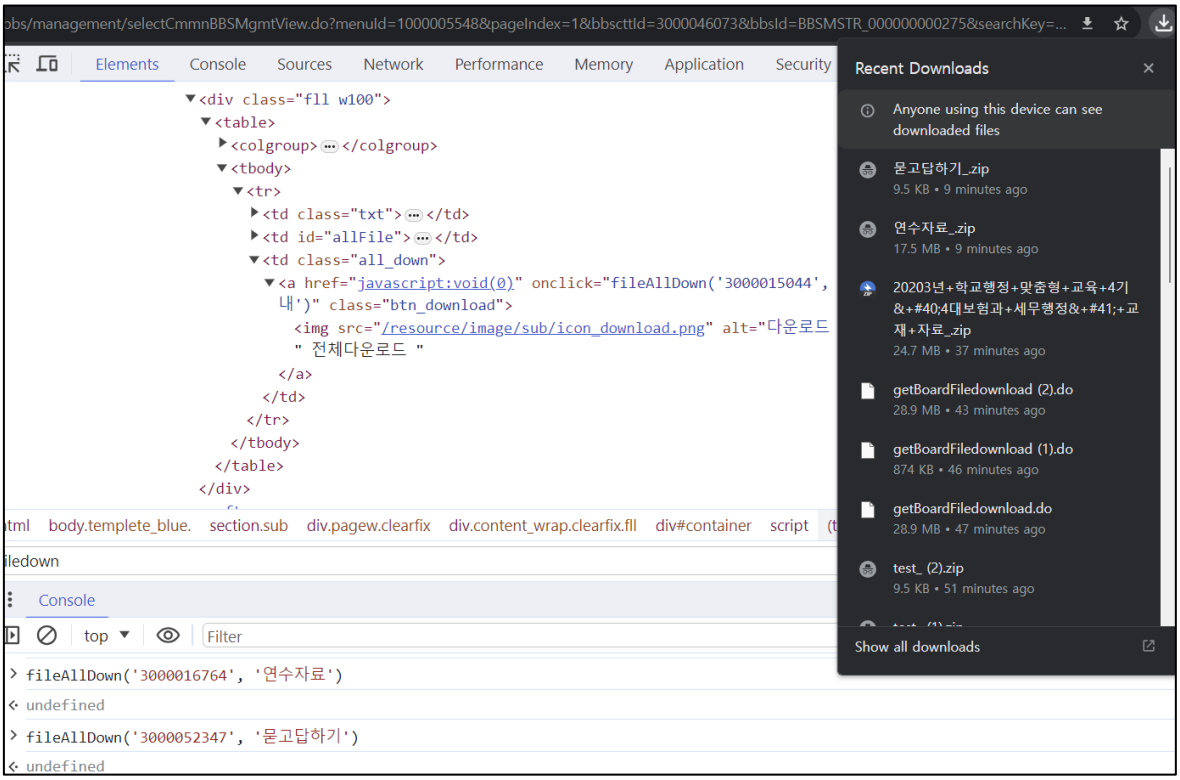
4.3.12.1. 파일 다운로드

홈페이지명	인천광역시교육청교육연수원		
메뉴명	연수도우미 > 공지사항 연수도우미 > 연수자료 연수도우미 > 묻고답하기		
URL	https://www.ieti.or.kr/common/bbs/management/selectCmmnBBSMgmtView.do?menuId=1000005548&pageIndex=1&bbscttId=3000046073&bbsId=BBSMSTR_000000000275&searchKey=&searchWord=&etc=&searchKeyTxt=1&searchWordTxt=&perPage=10		
점검자	한희수	점검일시	2023.09.15. 02:50
취약점 개요	권한 없는 사용자가 열람할 수 없는 게시글의 첨부파일 다운로드 가능		

취약점 상세 내용

Step1) 크롬의 개발자도구를 이용하여 파일 다운로드 요청을 보내는 함수의 fileId 파라미터를 조작하여 콘솔에 입력하면, 로그인 하지 않은 상태로 임의의 파일을 다운로드 할 수 있음

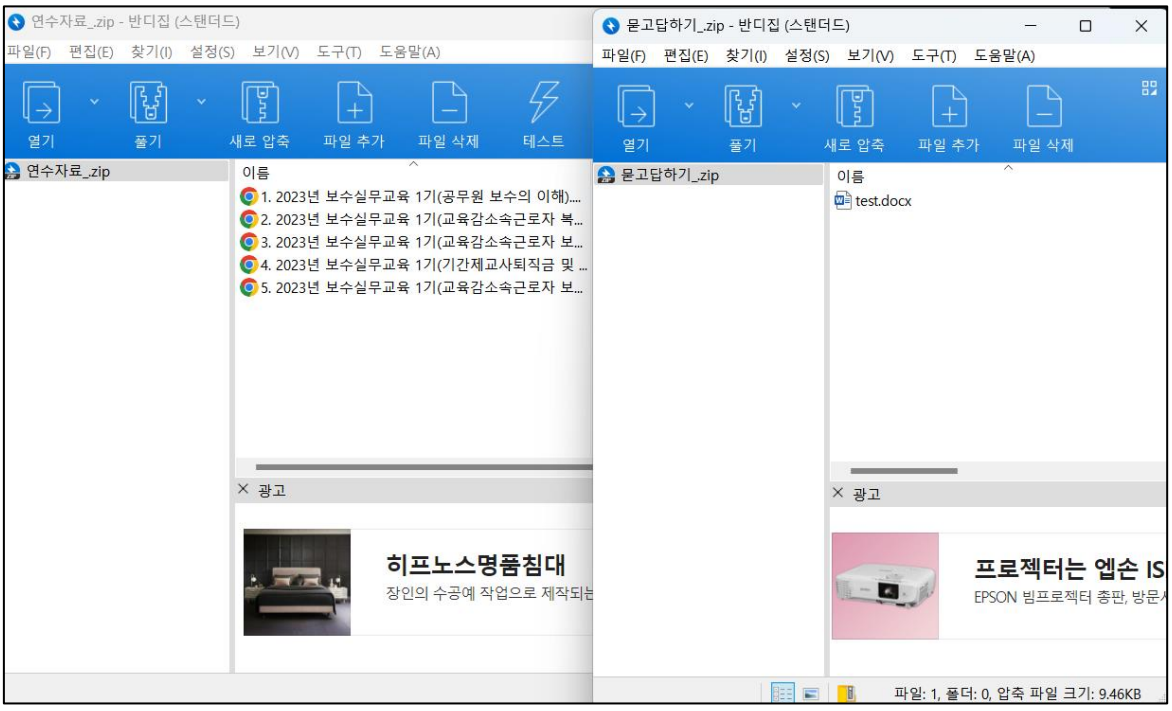
fileAllDown(fildId, cttNm)



Step2) 로그인 해야 열람 가능한 연수자료 게시글의 첨부파일을 비로그인 상태로 다운로드 가능함

Step3) 게시글 작성자만 열람 가능한 묻고답하기 게시글의 첨부파일을 비로그인 상태로 다운로드 가능함

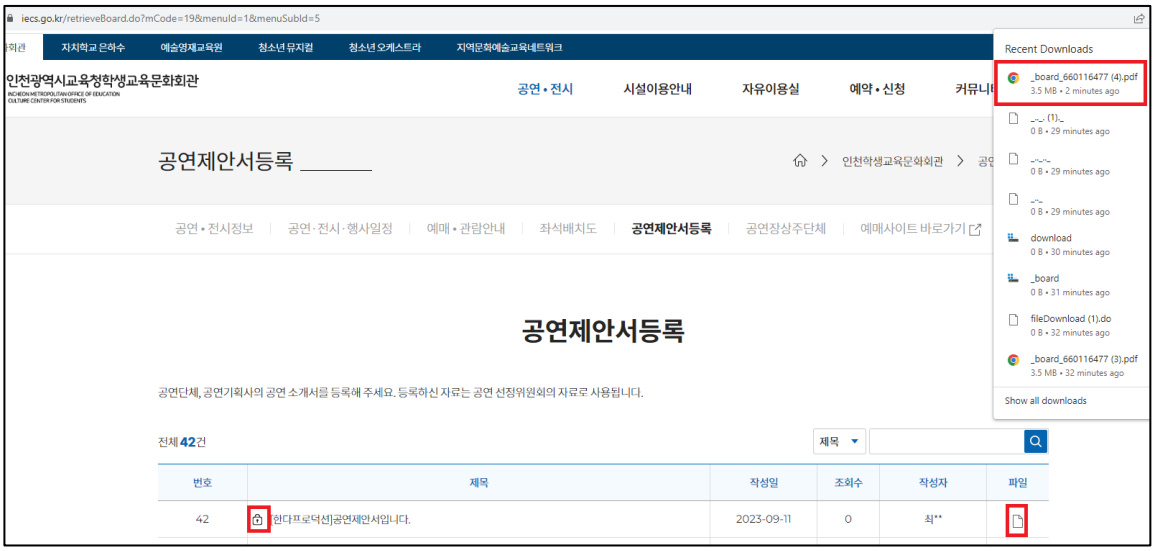
Step4) 다운로드 확인



단, 실제 공격자는 권한이 없는 게시글의 첨부파일의 fildId 를 정확히 알 수 없으므로, 다른 게시글을 통해 fileId 를 유추해야 함
혹은 Brute force 하여 임의의 첨부파일을 다운로드 시도할 수 있음

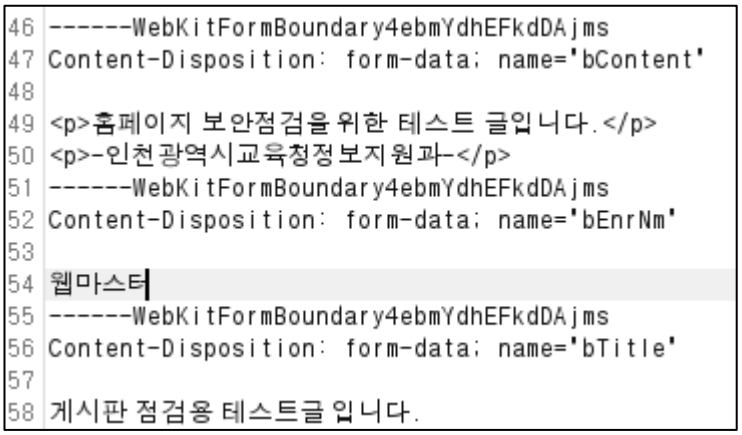
4.3.13. 학생교육문화회관

4.3.13.1. 파일 다운로드

홈페이지명	인천광역시교육청학생교육문화회관		
메뉴명	인천학생교육문화회관 > 공연,전시 > 공연제안서등록		
URL	https://www.iecs.go.kr/retrieveBoard.do?mCode=19&menuId=1&menuSubId=5		
점검자	한희수	점검일시	2023.09.16. 22:50
취약점 개요	우회나 변조 없이 비밀글의 첨부파일 다운로드 가능		
취약점 상세 내용	Step1) 권한 없는 사용자가 비밀글을 열람할 수는 없으나, 우측의 첨부파일을 클릭하면 아무런 권한 검증없이 파일이 다운로드 됨 		

4.3.13.2. 파라미터 변조

<table>
<tr><td>홈페이지명</td><td colspan="3">인천광역시교육청학생교육문화회관</td></tr>
<tr><td>메뉴명</td><td colspan="3">인천학생교육문화회관 > 커뮤니티 > 묻고답하기
지역문화예술교육네트워크 > 네트워크 커뮤니티 > 자유게시판</td></tr>
<tr><td>URL</td><td colspan="3">https://www.iecs.go.kr/retrieveBoardWrite.do?mCode=48&menuId=5&menuSubId=4
https://www.iecs.go.kr/retrieveBoardWrite.do?mCode=92&menuId=2&menuSubId=2</td></tr>
<tr><td>점검자</td><td>한희수</td><td>점검일시</td><td>2023.09.30. 05:19</td></tr>
<tr><td>취약점 개요</td><td colspan="3">게시글 작성 시, 작성자의 성명을 변조할 수 있음</td></tr>
<tr><td>취약점 상세 내용</td><td colspan="3">Step1) 게시글 작성 시, 일반적으로 성명은 현재 로그인 되어있는 계정의 이름이며, 변경할 수 없음
 

Step2) 하지만 Burp Suite 를 이용하여 작성자의 성명을 변경할 수 있음

</td></tr>
</table>

Step3) 변조 확인

자유게시판

전체 5건

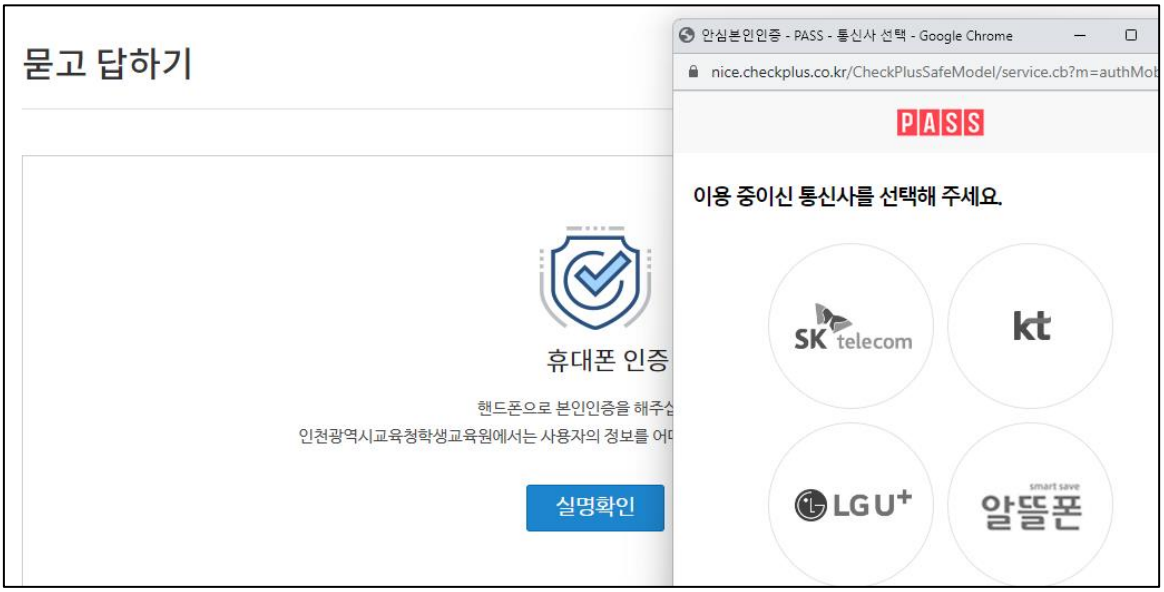
제목

번호	제목	작성일	조회수	작성자
5	게시판 점검용 테스트글 입니다. NEW	2023-09-30	0	웹**
4	게시판 점검용 테스트글 입니다. NEW	2023-09-30	0	한**
3	퓨전국악단구름 - 단소대금 어렵지않아요!(수행평가대비)교육 컨텐츠입니다.	2021-06-03	54	웹**
2	퓨전국악단구름 - 학교에서 새로운 꿈을 즐기자! 퓨전예술 교육 컨텐츠입니다.	2021-06-03	45	웹**
1	자유롭게 소통하는 장이 되었으면 합니다.	2021-05-18	66	웹**

이를 통해 관리자를 사칭할 수 있음

4.3.14. 학생교육원

4.3.14.1. 파라미터 변조

<table>
<tr><td>홈페이지명</td><td colspan="3">인천광역시교육청학생교육원</td></tr>
<tr><td>메뉴명</td><td colspan="3">참여마당 > 묻고 답하기</td></tr>
<tr><td>URL</td><td colspan="3">https://www.isec.go.kr/board/list.aspx?board_code=4018</td></tr>
<tr><td>점검자</td><td>한희수</td><td>점검일시</td><td>2023.09.30. 06:00</td></tr>
<tr><td>취약점 개요</td><td colspan="3">게시글 작성 시, 작성자의 이름을 변조할 수 있음</td></tr>
<tr><td>취약점 상세 내용</td><td colspan="3">Step1) 묻고 답하기 게시판에 글을 작성하려면 휴대폰 인증을 해야 함
 

Step2) 인증 후 글을 작성할 때, 작성자 이름을 변경할 수 없게 되어있음
하지만 Burp Suite 를 이용하여 작성자의 이름을 변경할 수 있음
<pre>
42 ------WebKitFormBoundaryaxjT6212UAn6CWBa
43 Content-Disposition: form-data; name="ctl00$ctl00$cpmain$cpsub$uc_basic_write$t_m_title"
44
45 게시판 점검용 테스트 글입니다.
46 ------WebKitFormBoundaryaxjT6212UAn6CWBa
47 Content-Disposition: form-data; name="ctl00$ctl00$cpmain$cpsub$uc_basic_write$t_m_name"
48
49 테스트
50 ------WebKitFormBoundaryaxjT6212UAn6CWBa
51 Content-Disposition: form-data; name="ctl00$ctl00$cpmain$cpsub$uc_basic_write$t_m_pwd"
52
53 testtest12
</pre></td></tr>
</table>

Step3) 생년월일은 페이지에 표시되는 정보는 아니지만, 변조 가능함

```
86 Content-Disposition: form-data; name='ctl00$ctl00$cpmain$cpsub$uc_basic_write$hidden_info2'
87
88 19991212
```

Step4) 변조 확인

번호	제목	등록일	작성자
2	게시판 점검용 테스트 글입니다. NEW	2023-09-30	테*트
1	23년 가족 캠핑	2023-07-03	김*미

4.3.15. 교직원수련원

발견된 취약점 없음

4.3.16. 평생학습관

발견된 취약점 없음

4.3.17. 도서관통합홈페이지

4.3.17.1. 불충분한 인가

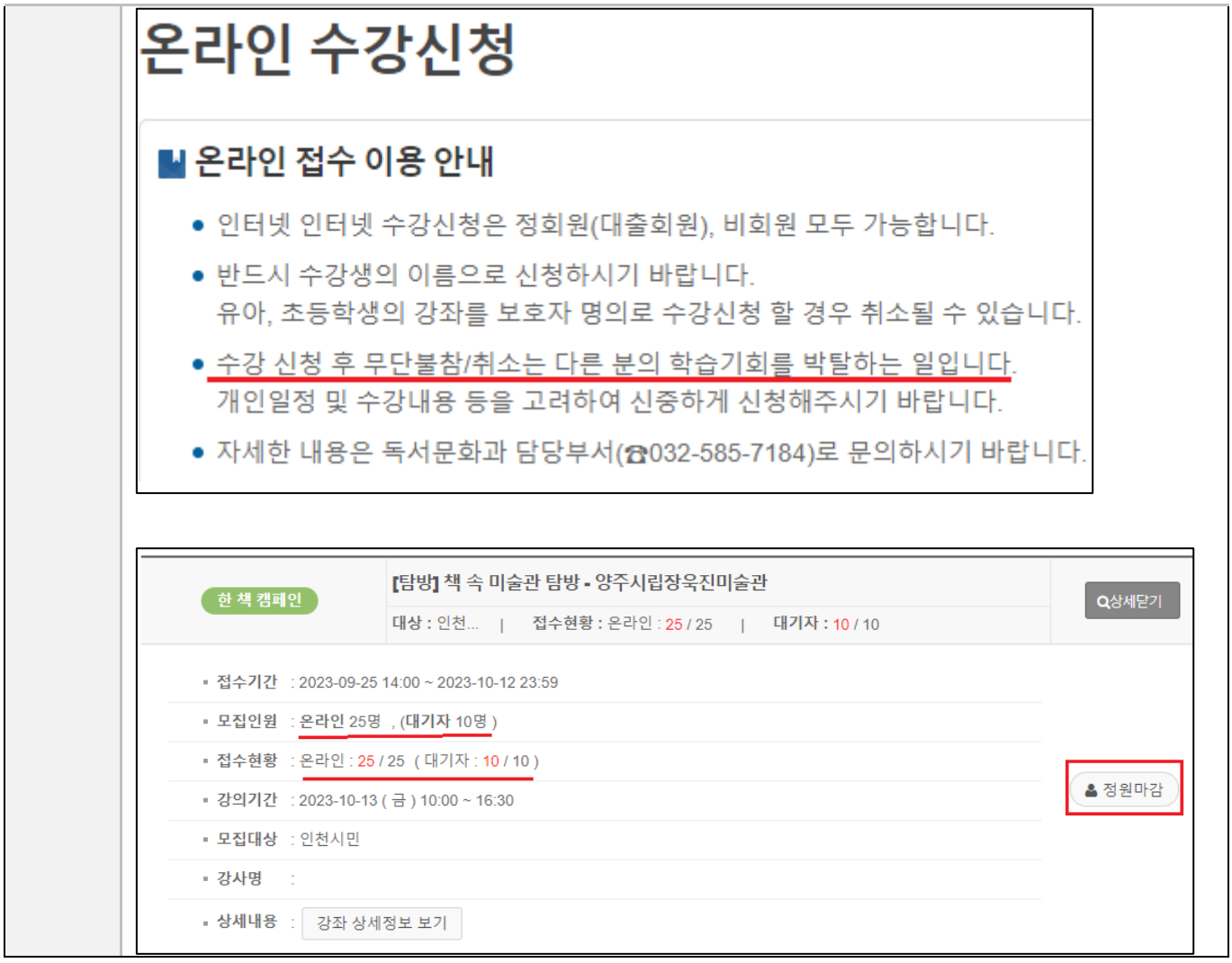
홈페이지명	인천광역시교육청통합공공도서관		
메뉴명	도서관서비스 > 독서문화행사 > 수강신청		
URL	https://lib.ice.go.kr/seogu/module/teach/student/edit.do?editMode=ADD&homepage_id=h6&group_idx=22&category_idx=0&teach_idx=6118&apply_status=1&menu_idx=85		
점검자	한희수	점검일시	2023.10.06. 04:20
취약점 개요	수강신청시 본인인증 절차가 없음		
취약점 상세 내용	Step1) 독서문화행사의 수강신청시, 본인인증 절차 없이 입력한 정보 그대로 수강신청이 됨		


신청자정보
신청자 - 성명(*)
김환
신청자 - 생년월일(*)
2000-01-01
신청자 - 성별(*)
남 여
신청자 - 우편번호
우편번호 찾기
신청자 - 주소
신청자 - 휴대전화번호(*)
010 - 1234 - 5678
신청하기
뒤로가기

순번	이름	전화번호	등록일시	신청상태	비고
1	권 * 정	010- **** - ** 80	2023-10-05 10:00:13	참여	
2	신 * 미	010- **** - ** 73	2023-10-05 10:00:46	참여	
3	이 * 미	010- **** - ** 23	2023-10-05 10:14:13	참여	
4	이 * 은	010- **** - ** 68	2023-10-05 10:42:40	참여	
5	김 * 숙	010- **** - ** 05	2023-10-05 10:48:26	참여	
6	배 * 준	010- **** - ** 27	2023-10-05 10:52:54	참여	
7	최 * 수	010- **** - ** 40	2023-10-05 11:18:12	참여	
8	이 * 연	010- **** - ** 10	2023-10-05 15:58:05	참여	
9	권 * 희	010- **** - ** 75	2023-10-05 20:55:10	참여	
10	조 * 아	010- **** - ** 36	2023-10-05 21:27:52	참여	
11	정 *** 과	010- **** - ** 78	2023-10-06 04:06:00	참여	
12	김	010- **** - ** 78	2023-10-06 04:12:57	참여	
13	권 * 희	010- **** - ** 75	2023-10-05 19:27:09	취소	
14	권 * 희	010- **** - ** 75	2023-10-05 20:50:29	취소	

이를 이용하여 타인의 개인정보를 이용해 수강신청 할 수 있음

또는 임의의 이름으로 수강신청 하여 모집 인원을 채워 정원 마감되게 하여 타인의 수강신청을 차단하고, 강의를 실제로 수강하는 인원이 적거나 없도록 하여 강의 진행에 문제를 일으킬 수 있음

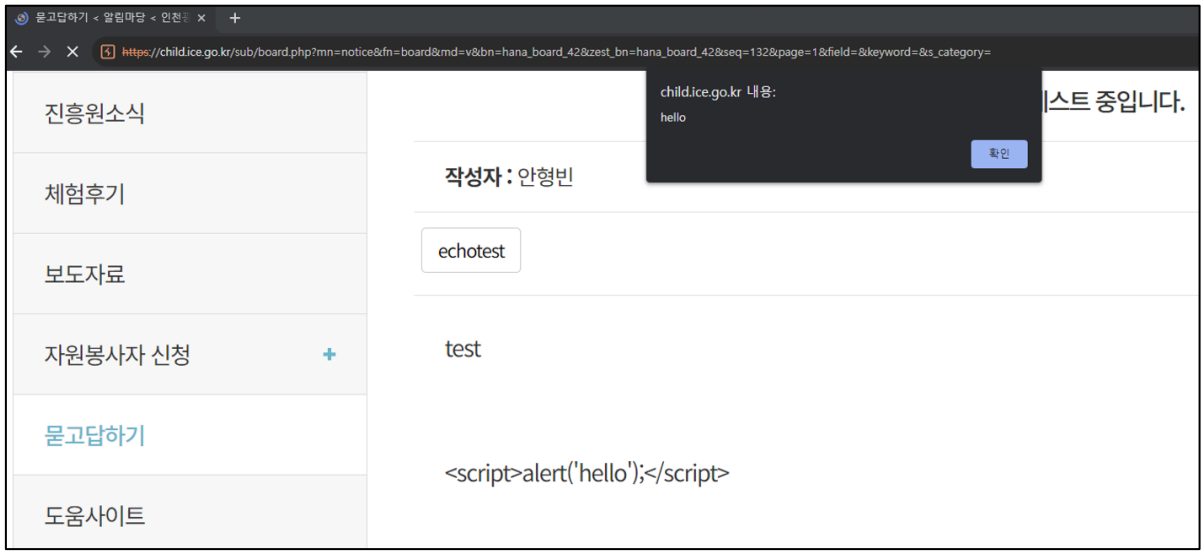

온라인 수강신청
온라인 접수 이용 안내
인터넷 인터넷 수강신청은 정회원(대출회원), 비회원 모두 가능합니다.
반드시 수강생의 이름으로 신청하시기 바랍니다.
유아, 초등학생의 강좌를 보호자 명의로 수강신청 할 경우 취소될 수 있습니다.
수강 신청 후 무단불참/취소는 다른 분의 학습기회를 박탈하는 일입니다.
개인일정 및 수강내용 등을 고려하여 신중하게 신청해주시기 바랍니다.
자세한 내용은 독서문화과 담당부서(☎032-585-7184)로 문의하시기 바랍니다.
한 책 캠페인
[탐방] 책 속 미술관 탐방 - 양주시립장욱진미술관
대상 : 인천...
접수현황 : 온라인 : 25 / 25
대기자 : 10 / 10
상세닫기
접수기간 : 2023-09-25 14:00 ~ 2023-10-12 23:59
모집인원 : 온라인 25명 , (대기자 10명)
접수현황 : 온라인 : 25 / 25 (대기자 : 10 / 10)
강의기간 : 2023-10-13 (금) 10:00 ~ 16:30
모집대상 : 인천시민
강사명 :
상세내용 : 강좌 상세정보 보기
정원마감

4.3.18. 독서교육종합지원

발견된 취약점 없음

4.3.19. 유아교육진흥원

4.3.19.1. 크로스사이트 스크립팅

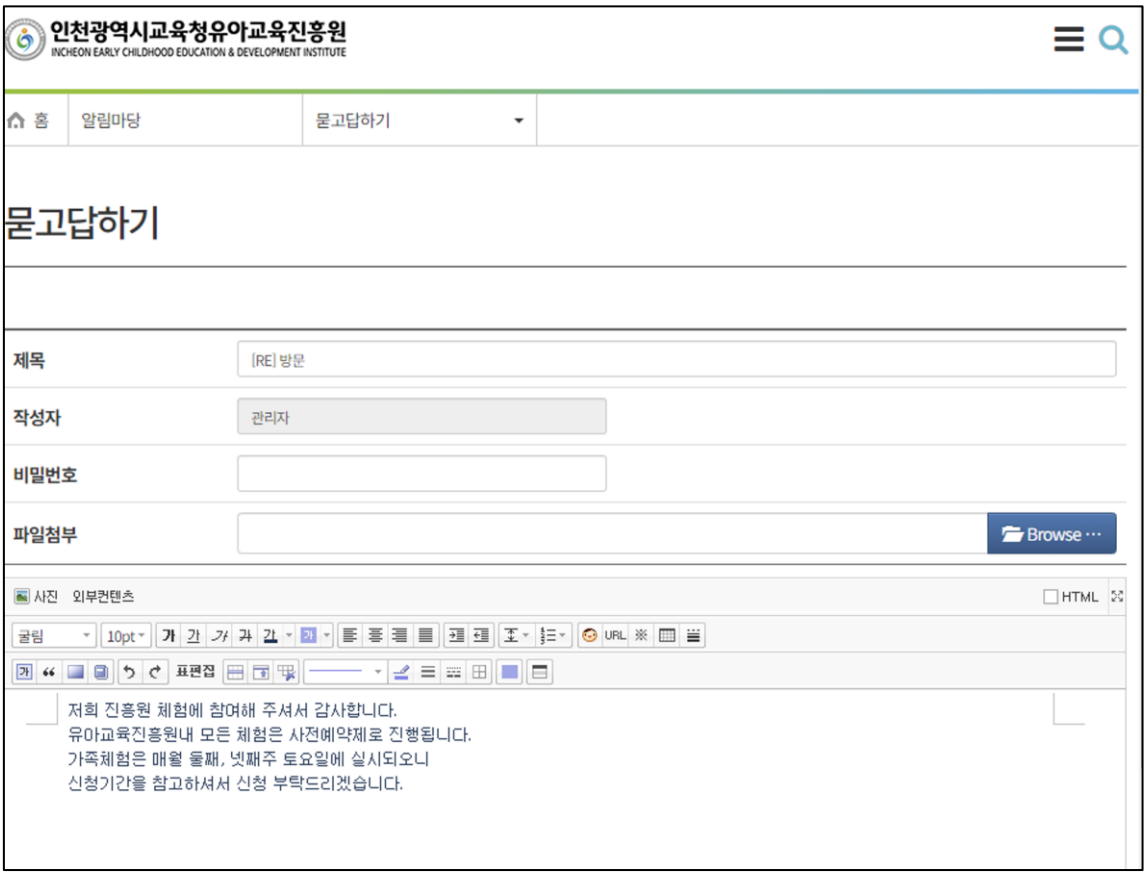
홈페이지명	인천광역시교육청유아교육진흥원		
메뉴명	홈 > 알림마당 > 체험후기 홈 > 알림마당 > 묻고답하기		
URL	https://child.ice.go.kr/sub/board.php?mn=notice&fn=board&zest_bn=hana_board_42&bn=hana_board_42&md=l&field=&keyword=&page=1&s_category=		
점검자	안형빈	점검일시	2023.09.28. 23:00
취약점 개요	글 작성 시, Stored XSS 취약점이 존재		
취약점 상세 내용	Step1) 게시물 작성 시, 아래의 payload 를 본문에 넣어두면 Stored XSS 가 발생합니다. test <img src="https://child.ice.go.kr/movie/picker_img/1695049068.bmp" class="txc-image" width="1200" onclick="javascript:alert('hello');" onload="javascript:alert('hello');" style="" ''=""> <script>alert('hello');</script>  		

4.3.19.2. 파라미터 변조

홈페이지명	인천광역시교육청유아교육진흥원		
메뉴명	홈 > 알림마당 > 체험후기 홈 > 알림마당 > 묻고답하기		
URL	https://child.ice.go.kr/sub/board.php?mn=notice&fn=board&md=v&zest_bn=hana_board_42&bn=hana_board_42&seq=126&page=1&field=&keyword=&s_category=		
점검자	안형빈	점검일시	2023.09.28. 23:00
취약점 개요	비밀 글을 패스워드 입력 없이 접근하여 열람이 가능		
취약점 상세 내용	Step1) 비밀 글 접근 시 비밀번호를 입력해야 하지만, 비밀글이 아닌 글에서 얻은 URL 로 `seq=`값을 해당 비밀글로 설정 시 비밀번호 입력 없이 접근이 가능합니다. 		

Step2) 비밀글을 볼 수 있는 트릭은 아래와 같습니다. URL 변수에서 `md=` 값을 `v`로 설정.

Step3) md=v 로 설정 시 수정도 할 수 있음.

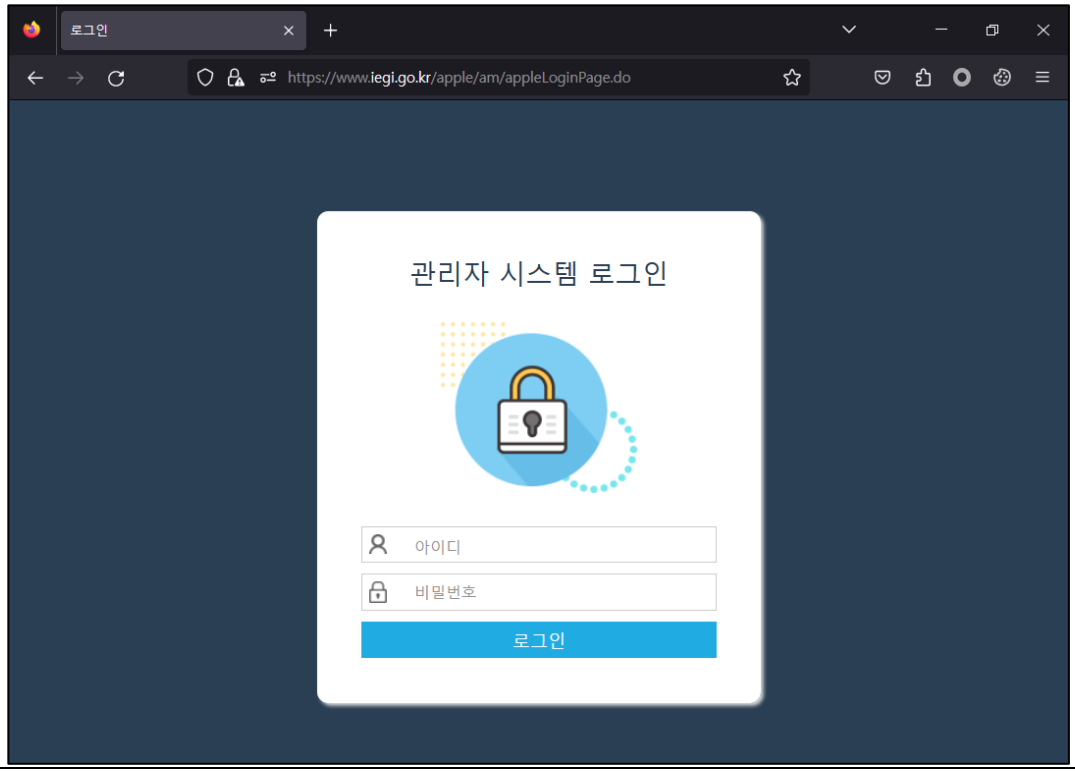


4.3.20. 동아시아국제교육원

4.3.20.1. 정보 노출

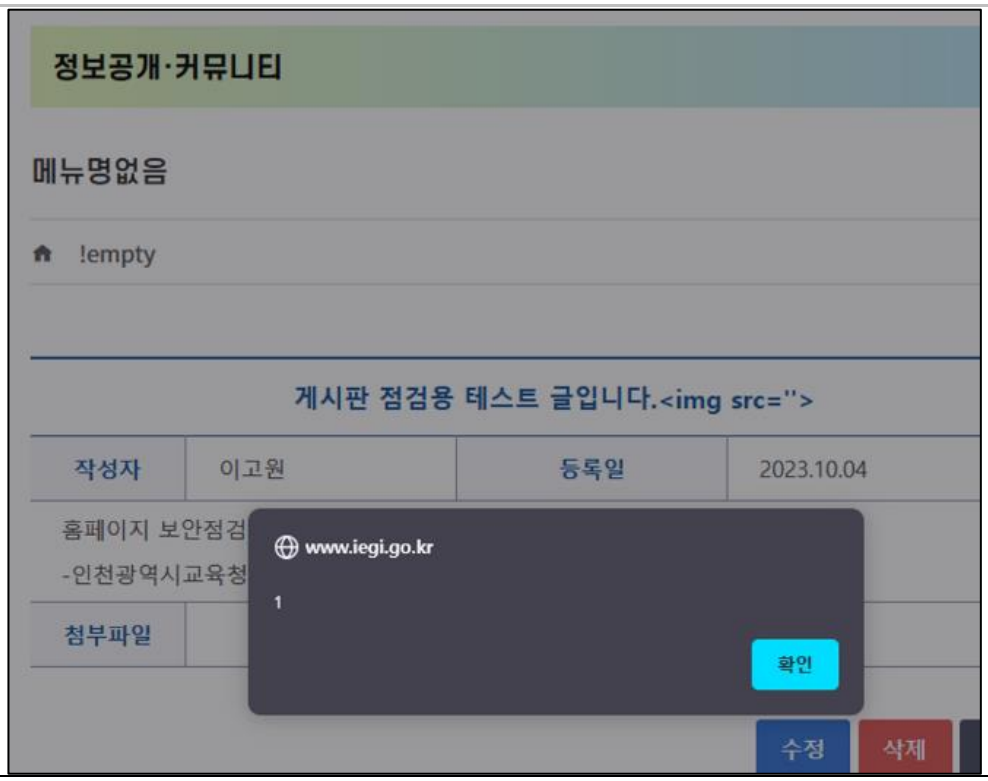
홈페이지명	동아시아국제교육원		
메뉴명	도움말 기능? - common.js 파일에서 URL 확인		
URL	https://www.iegi.go.kr/common/hc/hpcm/selectHpcm.do		
점검자	이고원	점검일시	2023.10.01. 18:30
취약점 개요	에러 페이지 출력		
취약점 상세 내용	Step1) 출력된 에러 페이지에서 톰캣 버전 노출(Apache Tomcat 8.5.73) 해당 버전에 여러 취약점이 존재하여 패치된 것으로 보임 		

4.3.20.2. 관리자 페이지 노출

홈페이지명	동아시아국제교육원		
메뉴명	관리자 페이지		
URL	https://www.iegi.go.kr/apple/am/appleLoginPage.do		
점검자	이고원	점검일시	2023.10.01. 16:00
취약점 개요	관리자 시스템 로그인 페이지 노출		
취약점 상세 내용	Step1) /js/common.js 파일 내 도움말기능 중 관리자 관련 기능 비동기 호출에 사용되는 URL 접속 시 접근 가능 		

4.3.20.3. 크로스사이트 스크립팅

홈페이지명	동아시아국제교육원		
메뉴명	정보공개/커뮤니티 - 동영상게시판 test		
URL	https://www.iegi.go.kr/iegi/na/ntt/selectNttList.do?mi=1121&bbsId=1041		
점검자	이고원	점검일시	2023.10.04. 23:00
취약점 개요	게시글 본문 Stored XSS		
취약점 상세 내용	Step1) 에디터 소스 편집을 통해 스크립트 삽입이 가능하여 Stored XSS 발생 사용자의 조작이 개입되어야 할 것으로 보임  		

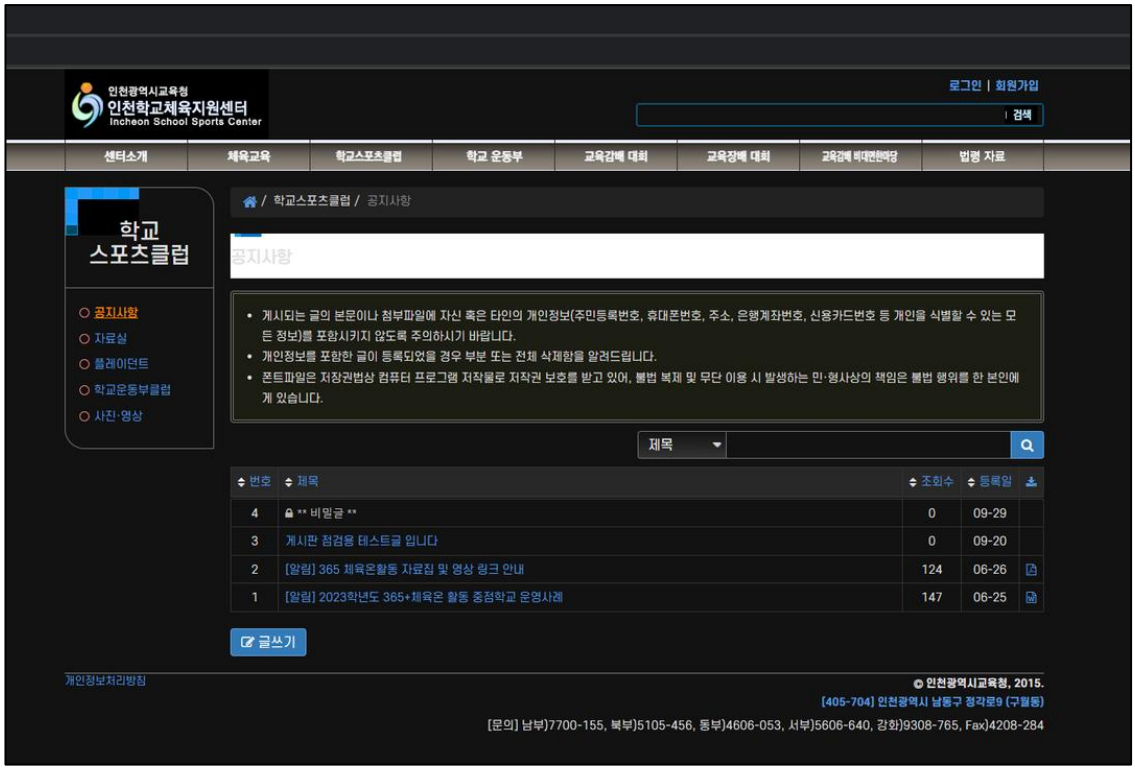

정보공개·커뮤니티
메뉴명없음
!empty
게시판 점검용 테스트 글입니다.<img src=''>
작성자
이고원
등록일
2023.10.04
홈페이지 보안점검
-인천광역시교육청
첨부파일
www.iegi.go.kr
1
확인
수정
삭제

4.3.21. 다문화교육지원센터

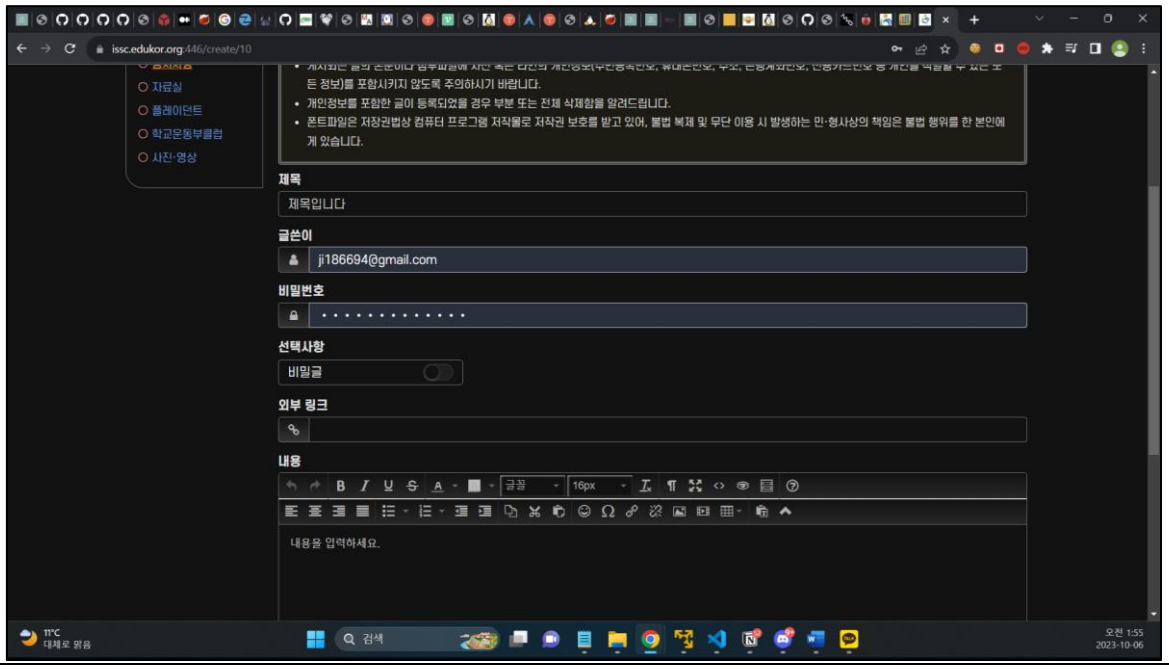
발견된 취약점 없음

4.3.22. 인천학교체육지원

4.3.22.1. 불충분한 인가

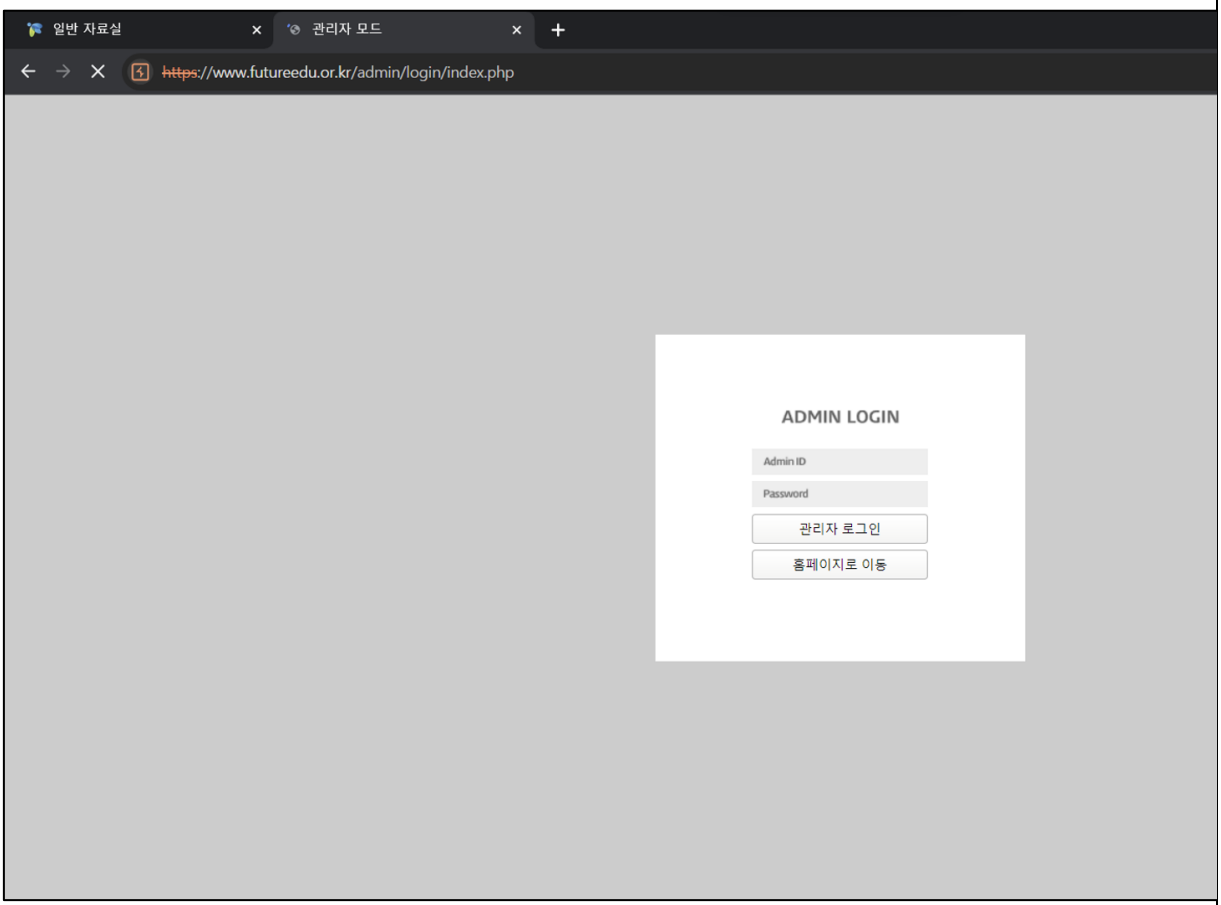
홈페이지명	인천학교체육지원센터		
메뉴명	학교스포츠클럽/공지사항		
URL	https://issc.edukor.org:446/create/10		
점검자	이창현	점검일시	2023.09.20. 01:50
취약점 개요	로그인없이 글쓰기가 가능함		
취약점 상세 내용	Step1) 로그인없이 글쓰기가 가능함. 일반 사용자들은 로그인 기능이 없음.  		

Step2) 글쓴이와 비밀번호 또한 임의로 입력할 수 있게 되어 다른 사람을 사칭하여 글을 쓸 수 있음



4.3.23. 미래교육위원회

4.3.23.1. 관리자 페이지 노출

홈페이지명	미래교육위원회		
메뉴명	관리자페이지		
URL	https://www.futureedu.or.kr/admin/login/index.php		
점검자	이창현	점검일시	2023.09.20 14:05
취약점 개요	관리자 페이지를 간단한 url 로 접속할 수 있음		
취약점 상세 내용	main 페이지의 url 에 /admin 을 추가하여 접속하면 아래와 같은 관리자 페이지로 redirect 하는 것을 확인할 수 있음. 		

4.3.24. 법무도우미

발견된 취약점 없음

4.3.25. 고입포털

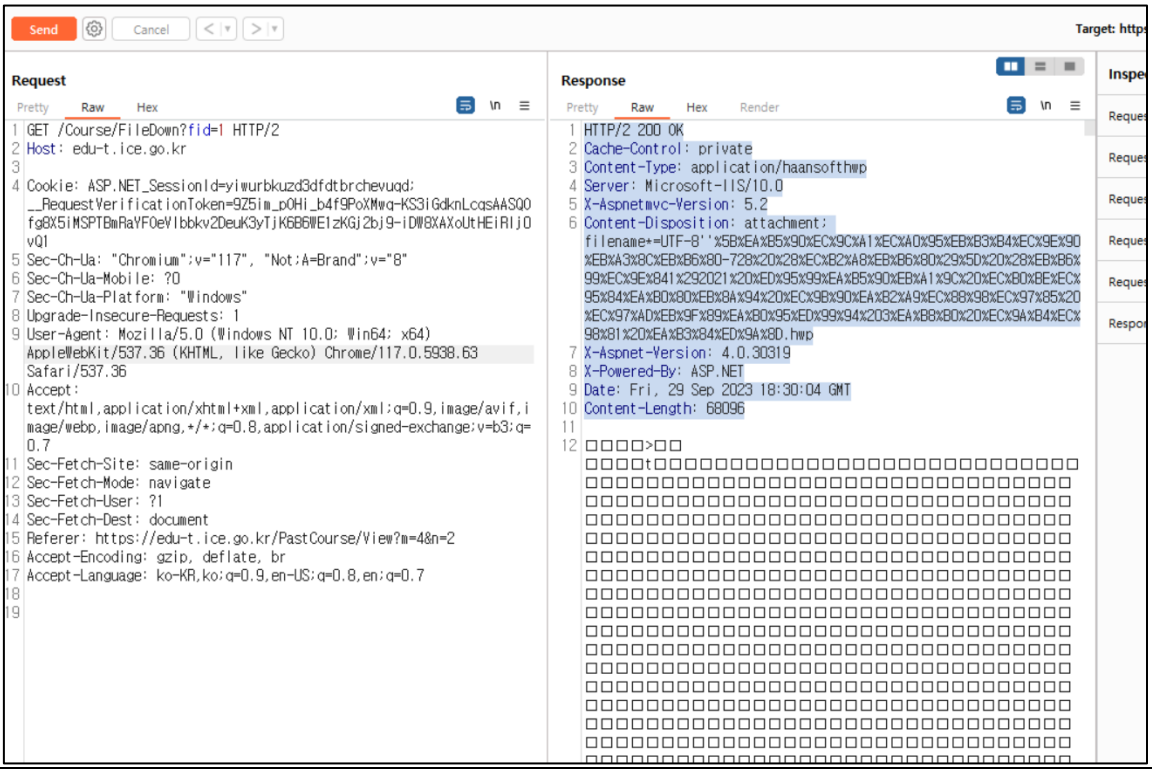
발견된 취약점 없음

4.3.26. 교육정보화지원

발견된 취약점 없음

4.3.27. 교원연수시스템

4.3.27.1. 정보 노출

홈페이지명	교원연수시스템		
메뉴명	전체		
URL	http://edu-t.ice.go.kr/		
점검자	서민찬	점검일시	2023.09.29. 18:30
취약점 개요	Response 데이터에서 버전 정보가 노출됨		
취약점 상세 내용	Step1) Request 메시지를 보내면 Response 에서 버전 정보를 알 수 있음 		

4.3.28. 인천교육 e-book

발견된 취약점 없음

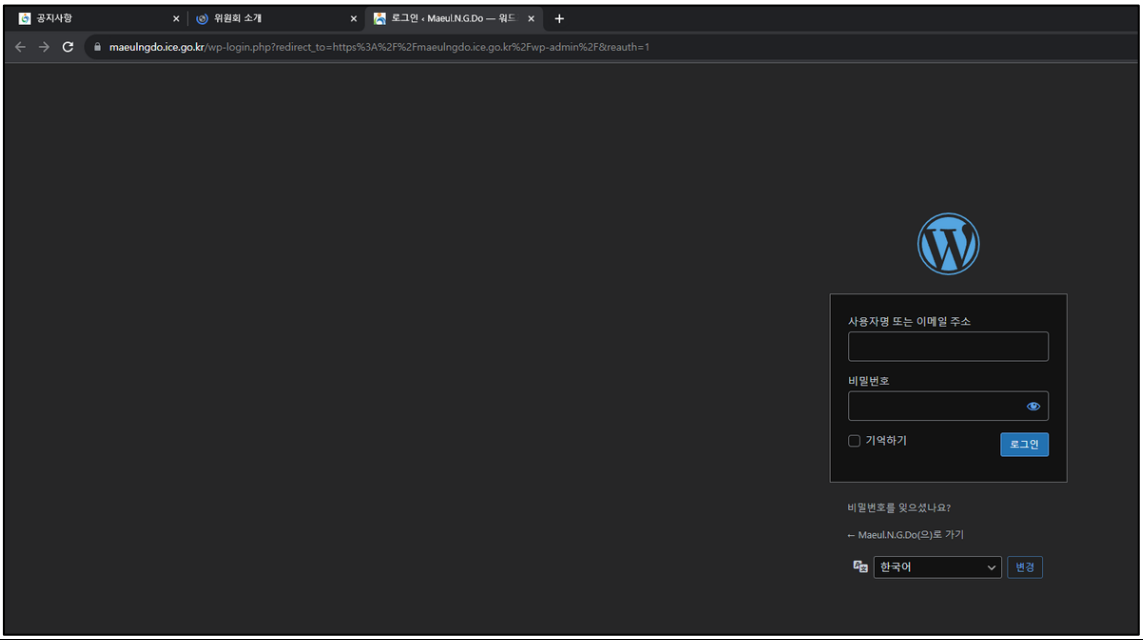
4.3.29. 교육과학정보원

발견된 취약점 없음

4.3.30. 마을공유지도 찾다

발견된 취약점 없음

4.3.30.1. 관리자 페이지 노출

홈페이지명	마을공유지도 찾다		
메뉴명	관리자페이지		
URL	https://maeulngdo.ice.go.kr/admin		
점검자	이창현	점검일시	2023.09.19 20:10
취약점 개요	관리자 페이지를 간단한 url 로 접속할 수 있음		
취약점 상세 내용	Step1) main 페이지의 url 에 /admin 을 추가하여 접속하면 아래와 같은 관리자 페이지로 redirect 하는 것을 확인할 수 있음. 		

4.3.31. 안전스쿨관리자

발견된 취약점 없음

4.3.32. 교육지역연계꿈이음대학

발견된 취약점 없음

4.4. 취약한 암호화 알고리즘

32 개 사이트를 대상으로 ssllabs.com 으로 점검한 결과 6 개의 사이트가 보안 등급이 F 로 나왔으며, 취약한 SSL 을 사용하는 것으로 확인되었습니다.

홈페이지	URL	보안 등급
인천광역시교육청	https://www.ice.go.kr/main.do?s=ice	F
남부교육지원청	https://nambu.ice.go.kr/Main.do	F
북부교육지원청	https://bukbu.ice.go.kr/index.do	F
학생교육문화회관	https://www.iecs.go.kr/index.do	F
평생학습관	https://www.ilec.go.kr/	F
고입포털	https://isatp.ice.go.kr/	F
합계		6

4.4.1. 인천광역시교육청

SSL 3.0 사용 지양 → POODLE 공격에 취약

Cipher suites 중 anonymous suite 사용 지양 → Middel Attack(중간자공격)에 취약

4.4.2. 남부교육지원청

SSL 3.0 사용 지양 → POODLE 공격에 취약

Cipher suites 중 anonymous suite 사용 지양 → Middel Attack(중간자공격)에 취약

4.4.3. 북부교육지원청

SSL 3.0 사용 지양 → POODLE 공격에 취약

Cipher suites 중 anonymous suite 사용 지양 → Middel Attack(중간자공격)에 취약

4.4.4. 학생교육문화회관

SSL 3.0 사용 지양 → POODLE 공격에 취약

Cipher suites 중 anonymous suite 사용 지양 → Middel Attack(중간자공격)에 취약

4.4.5. 평생학습관

SSL 3.0 사용 지양 → POODLE 공격에 취약

Cipher suites 중 anonymous suite 사용 지양 → Middel Attack(중간자공격)에 취약

4.4.6. 고입포털

SSL 3.0 사용 지양 → POODLE 공격에 취약

또한 가급적 TLS 1.0 과 TLS 1.1 도 지양 → ROBOT 공격에 취약

5. 별첨

5.1. 진단 항목

No	분류	항목코드	진단항목	비고
1	세션 예측	SE	단순히 숫자가 증가하는 방법 등의 취약한 특정 세션의 식별자(ID)를 예측하여 세션을 가로챌 수 있는 취약점	
2	불충분한 인가	IN	민감한 데이터 또는 기능에 대한 접근권한 제한을 두지 않은 취약점	
3	불충분한 세션 만료	SC	세션의 만료 기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하게 되는 취약점	
4	세션 고정	SF	세션 값을 고정하여 명확한 세션 식별자(ID) 값으로 사용자가 로그인하여 정의된 세션 식별자(ID)가 사용 가능하게 되는 취약점	
5	파일 업로드	FU	파일을 업로드 할 수 있는 기능을 이용하여 시스템 명령어를 실행할 수 있는 웹 프로그램을 업로드 할 수 있는 취약점	
6	파일 다운로드	FD	파일 다운로드 스크립트를 이용하여 첨부된 주요 파일을 다운로드 할 수 있는 취약점	
7	관리자 페이지 노출	AE	단순한 관리자 페이지 이름(admin, manager 등)이나 설정, 프로그램 설계 상의 오류로 인해 관리자 메뉴에 직접 접근하고 실행할 수 있는 취약점	
8	경로 추적	PT	공격자에게 외부에서 디렉터리에 접근할 수 있는 것이 허가되는 문제점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하고 실행할 수 있는 취약점	
9	위치 공개	PL	예측 가능한 디렉터리나 파일명을 사용하여 해당 위치가 쉽게 노출되어 공격자가 이를 악용하여 대상에 대한 정보와 민감한 정보가 담긴 데이터에 접근이 가능하게 되는 취약점	
10	쿠키 변조	CC	적절히 보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등이 가능한 취약점	
11	SQL 인젝션	SI	SQL 문으로 해석될 수 있는 입력을 시도하여 데이터베이스에 접근할 수 있는 취약점	
12	정보 누출	IL	웹 사이트 데이터가 노출되는 것으로 개발과정의 코멘트나 오류 메시지 등에서 중요한 정보가 노출되어 공격자에게 2 차 공격을 하기 위한 중요 정보를 제공할 수 있는 취약점	

No	분류	항목코드	진단항목	비고
13	크로스사이트 스크립팅	XS	웹 어플리케이션을 사용해서 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점	
14	취약한 암호화 알고리즘 사용	VC	HTTPS 통신시 취약한 암호화 알고리즘을 사용하여 추가적인 피해가 발생할 수 있는 취약점	추가항목
15	경로 추적	PT	파일 업로드/다운로드시 지정된 경로를 벗어나 파일을 업로드하거나 파일에 접근할 수 있는 취약점	추가항목
16	URL/파라미터 변조	UP	수동으로 요청에 포함된 파라미터 값을 조작해 허용되지 않은 권한이나 정보를 획득할 수 있는 취약점	추가항목