

No.	분류.	점검항목.	위험도.	비고.
1.	입력 값 검증.	SQL Injection.	H.	
2.		Command Injection.	H.	
3.		외부 참조.	M.	
4.		시스템 권한 상승.	H.	
5.		XSS(Cross Site Script).	M.	
6.		CSRF(Cross Site Request Forgery).	M.	
7.		파일 업로드.	H.	
8.		파일 다운로드.	H.	
9.		매개변수 변조.	H.	
10.		검증되지 않은 Redirect와 Forward.	H.	
11.	접근 제어.	관리자 페이지 접근 통제.	H.	
12.	정보 노출.	중요 정보 노출.	M.	
13.		디폴트 페이지 노출.	M.	
14.	보안 구성.	디렉토리 인덱싱.	M.	
15.		에러 처리 미흡.	M.	
16.		불필요한 Method 허용.	H.	
17.		서버/커머셜/오픈소스 취약점.	L.	
18.	인증 및	취약한 인증 처리.	H.	
19.	세션 관리.	계정 관리 미흡.	L.	
20.	네트워크.	통신구간 평문 전송.	L.	
21.	기타.	기타 취약점.	-	

### 3. 결과 상세

#### 3.1. XSS(Cross Site Script)

##### 가) 취약점 현황 및 문제점

공지사항 내 악성 코드를 이용하여 타인에게 피해를 줄 가능성이 존재한다..

##### 나) 위협 요소

스크립트가 실행되어 사용자 쿠키를 가로채거나 특정 사이트로 강제 이동시키는 등 의도하지 않은 행위를 하거나, 특히 탈취된 쿠키에 인증 정보가 포함되어 있는 경우 권한 도용이 발생 할 가능성이 존재한다..

##### 다) 상세 내역

##### 공지사항 내 악성 코드를 이용하여 타인에게 피해를 줄 가능성이 존재

13

취약점 발생 메뉴	공지사항
URI	http://10.10.35.178:8085/Notice/NoticeWrite.aspx


14

단계1) 공지사항 게시글 작성

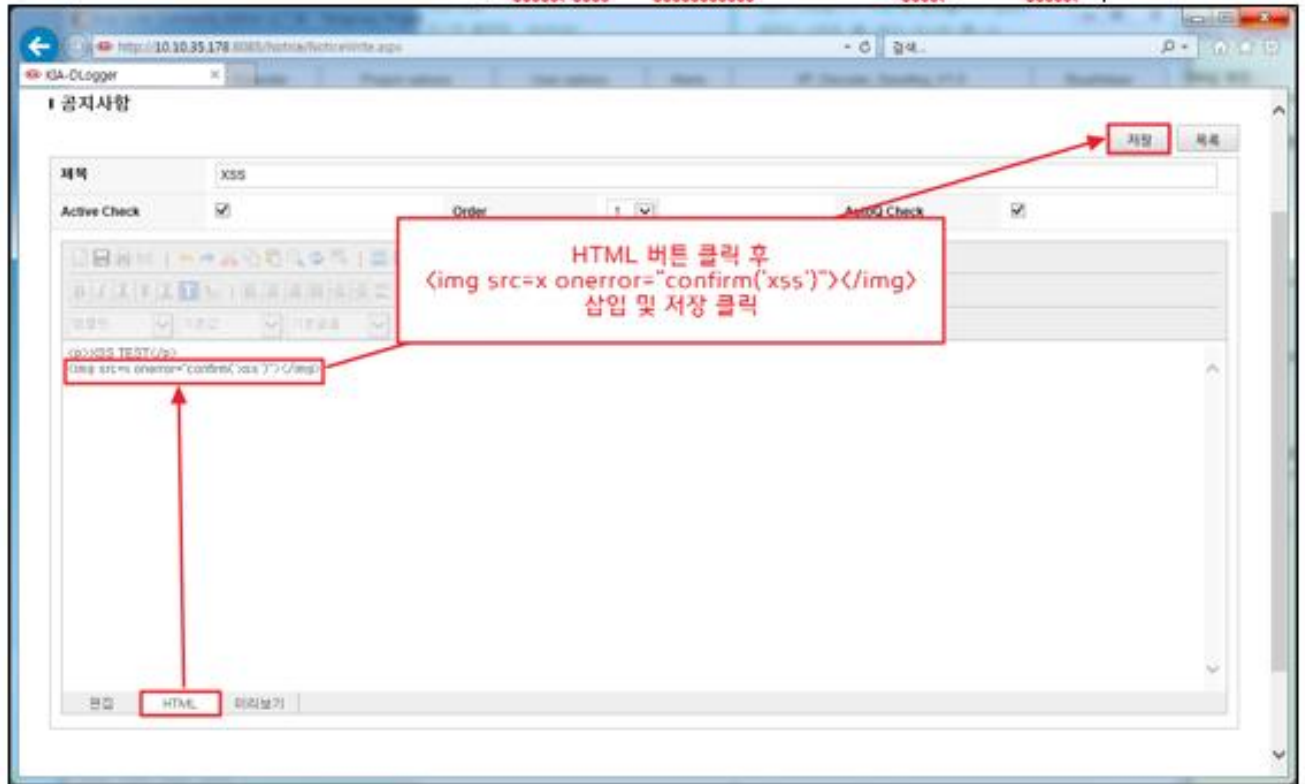


15

16


	<b>WEB 모의해킹 결과보고서</b> <b>EMS 자동분석 (AI 고장진단) 시스템 개발 프</b> <b>로젝트-디로거 시스템 (기아)</b>	버전	0.9.0
		일자	2019.09.20

단계2) HTML 수정 후 XSS 구문 삽입 [<img src=x onerror="confirm('xss')"></img>]



단계3) XSS 게시물 클릭



	<b>WEB 모의해킹 결과보고서</b> <b>EMS 자동분석 (AI 고장진단) 시스템 개발 프로젝트-디로거 시스템 (기아)</b>	버전.	0.9.0.
		일자.	2019.09.20.


#### 단계4) XSS 실행 확인.



#### ■ 라) 대응방안

사용자의 입력 값에 대한 필터링 로직 구현 시 서버 측에서 구현되어야 하고, XSS가 가능한 특수문자 (ex html태그, onload와 같은 이벤트핸들러 등)에 대한 필터링을 최신회 해야 한다.

※ HKMC 애플리케이션 보안가이드 Web Application\_v2.6 – 1.5 XSS(Cross Site Script) 참고.

	<b>WEB 모의해킹 결과보고서</b> <b>EMS 자동분석 (AI 고장진단) 시스템 개발 프</b> <b>로젝트-디로거 시스템 (기아)</b>	버전.	0.9.0.
		일자.	2019.09.20.

## 3.2. 파일 업로드

### 가) 취약점 현황 및 문제점

악성 해킹도구 업로드가 가능하여 이를 이용하여 서버침투가 가능하다.

### 나) 위협 요소

웹 애플리케이션 서버 침투 및 주요 민감정보 탈취, 장애발생 등의 가능성이 존재한다.

### 다) 상세 내역

#### 악성 해킹도구 업로드

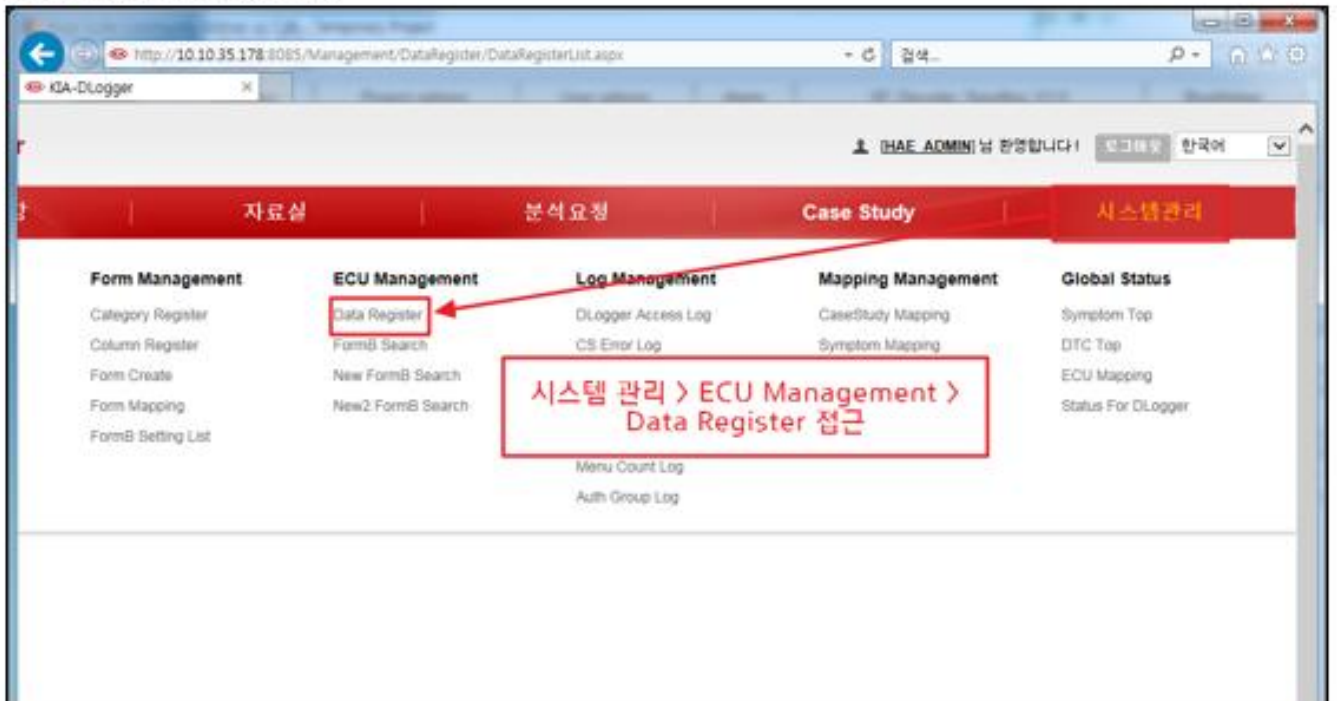
취약점 발생 메뉴.	시스템 관리 > ECM Management > Data Register.
URI.	http://10.10.35.178:8085/Management/DataRegister/DataRegisterHandler.ashx.

단계1) 관리자 계정으로 로그인 시도.

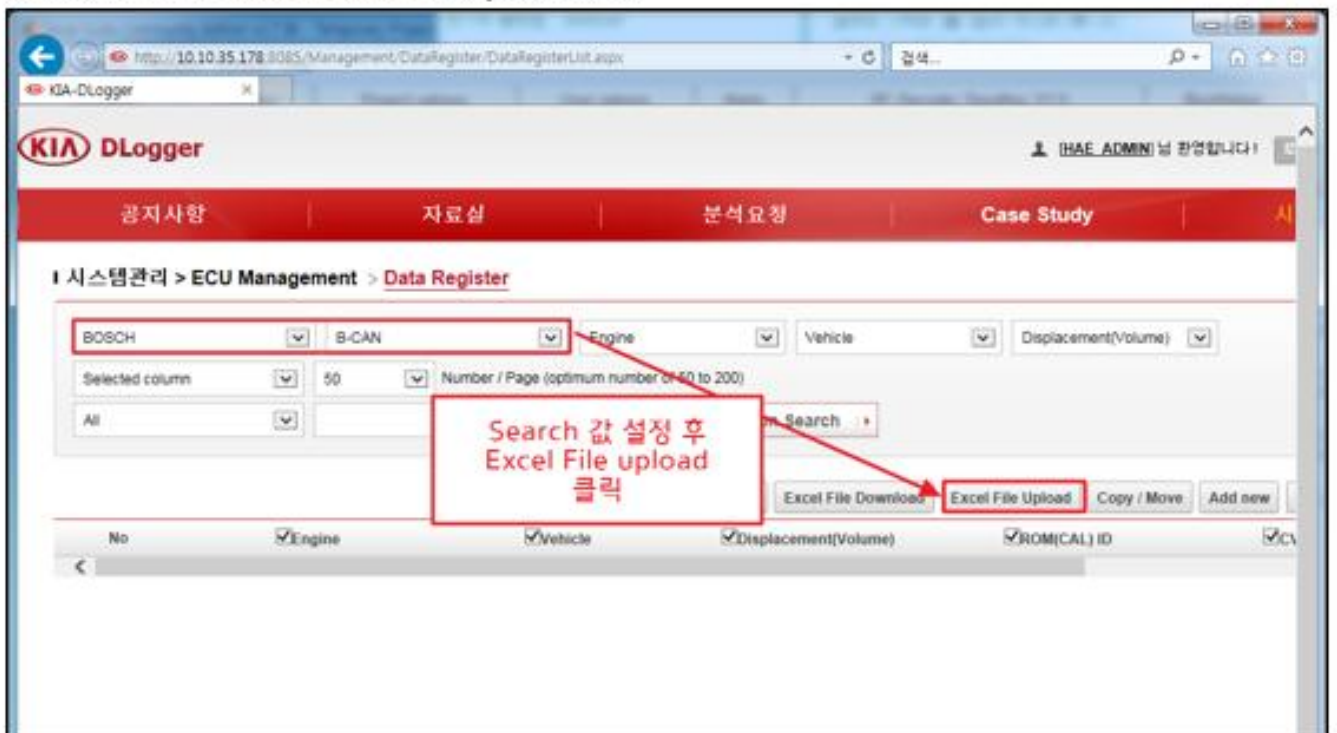





단계2) Data Register 접근.

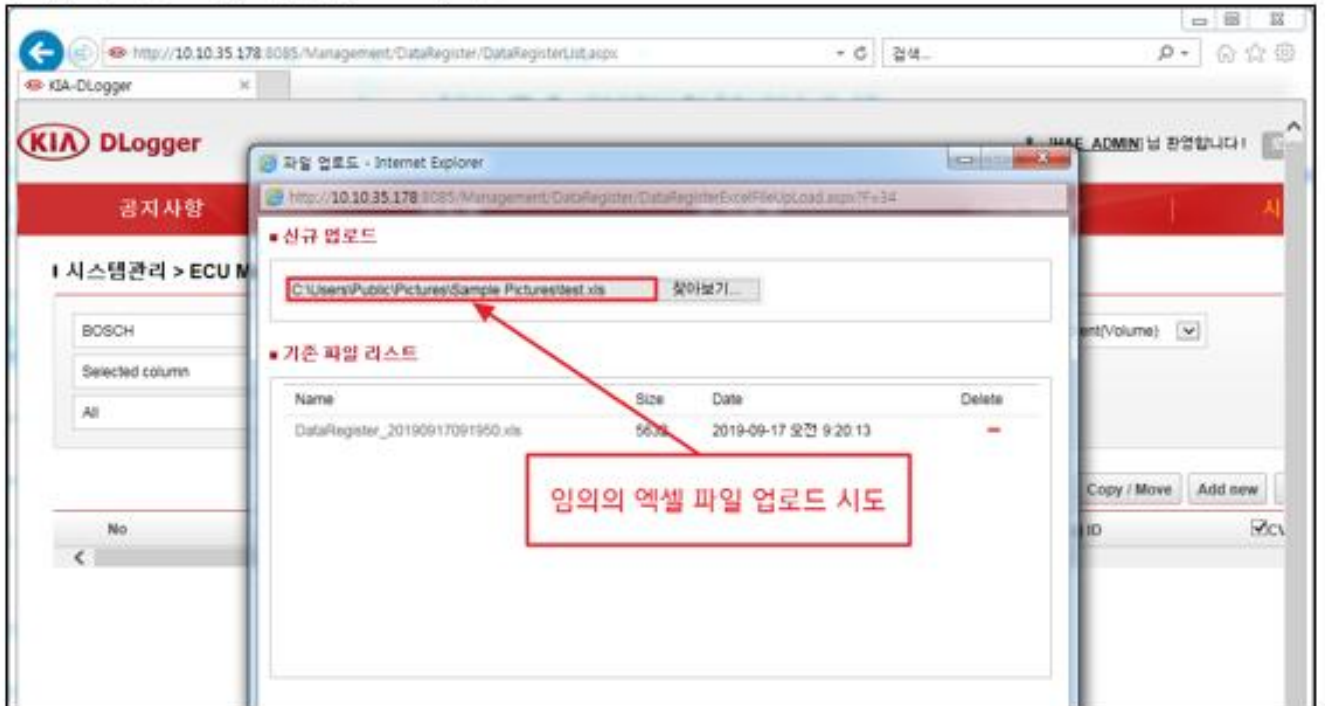


단계3) Search 값 설정 후 Excel File Upload 클릭.

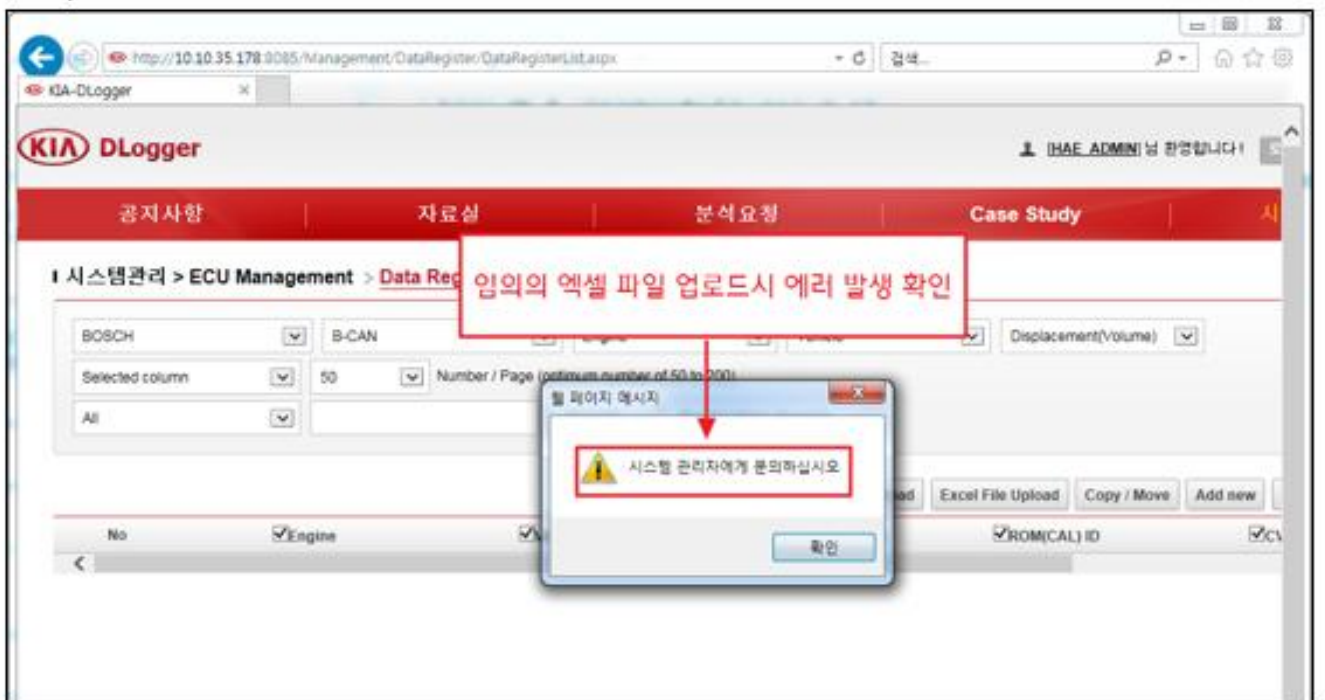



	<b>WEB 모의해킹 결과보고서</b> <b>EMS 자동분석 (AI 고장진단) 시스템 개발 프</b> <b>로젝트-디로거 시스템 (기아)</b>	버전	0.9.0
		일자	2019.09.20

단계4) 임의의 엑셀 파일 업로드 시도

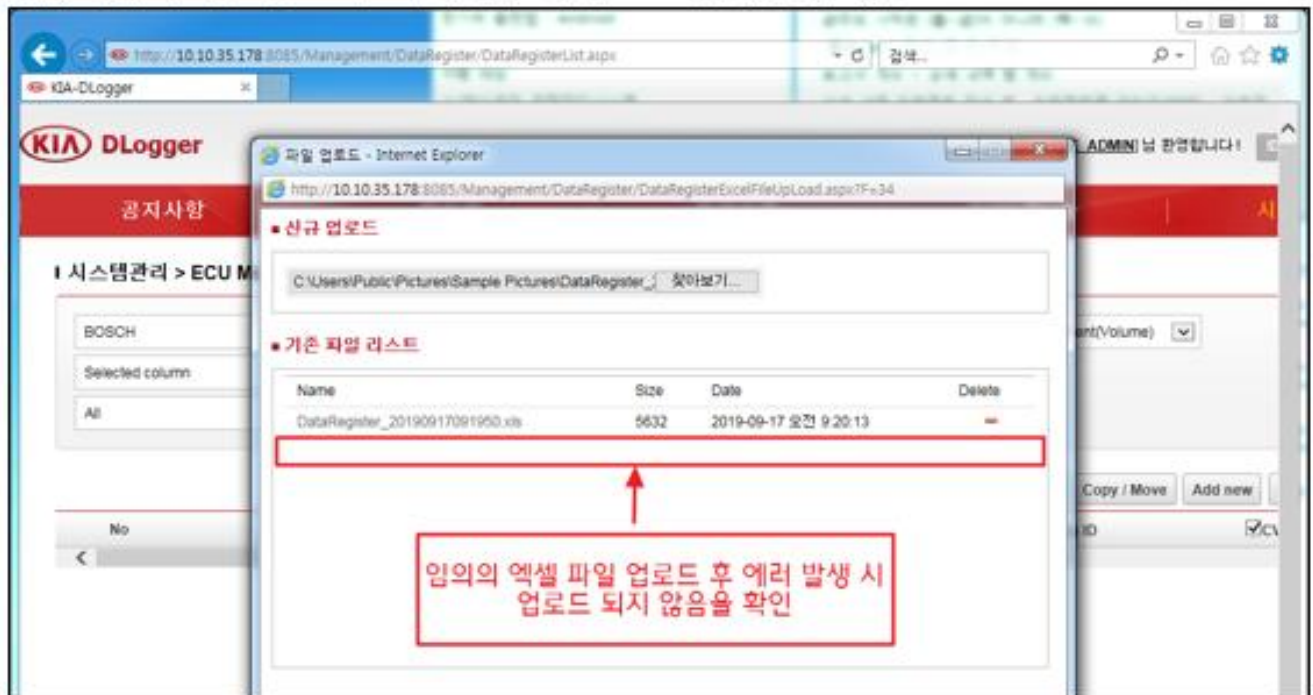


단계5) 임의의 엑셀 파일 업로드 시 에러 발생

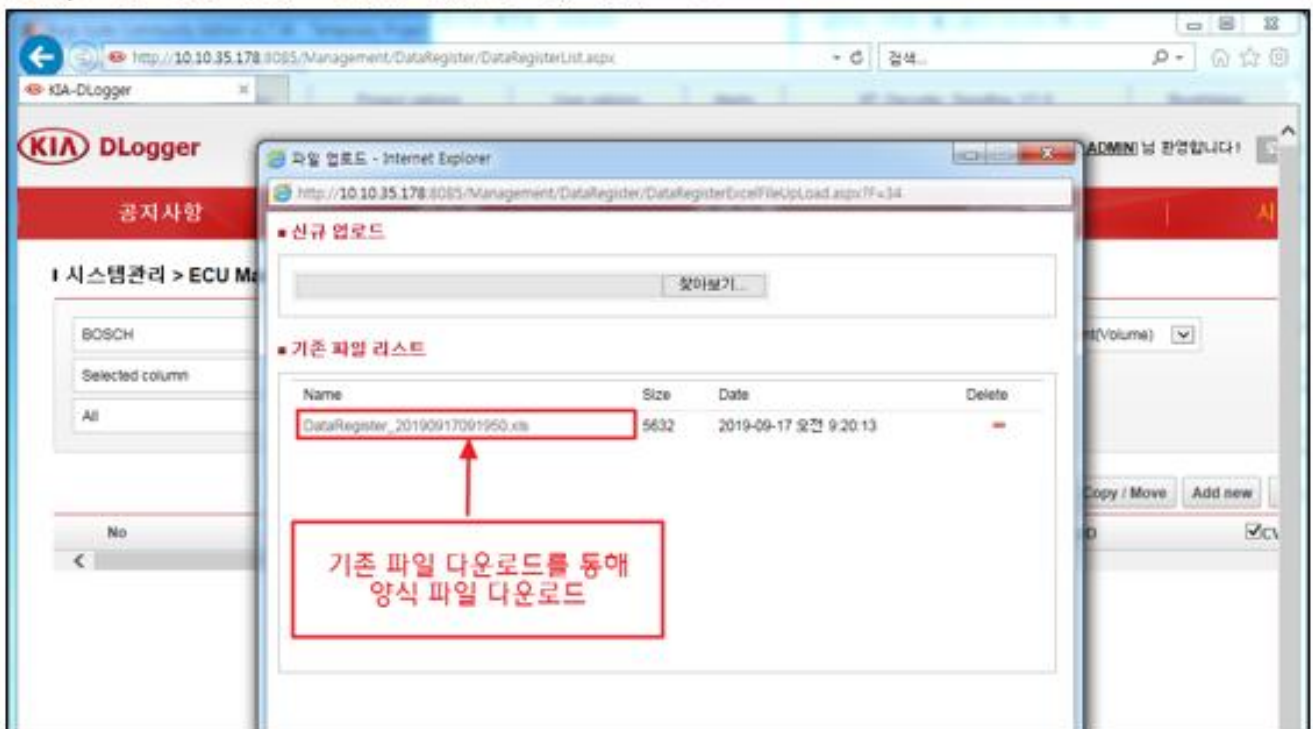


	<b>WEB 모의해킹 결과보고서</b> <b>EMS 자동분석 (AI 고장진단) 시스템 개발 프</b> <b>로젝트-디로거 시스템 (기아)</b>	버전	0.9.0.
		일자	2019.09.20.


단계6) 임의의 엑셀 업로드 후 에러 발생 시 업로드 되지 않음을 확인.



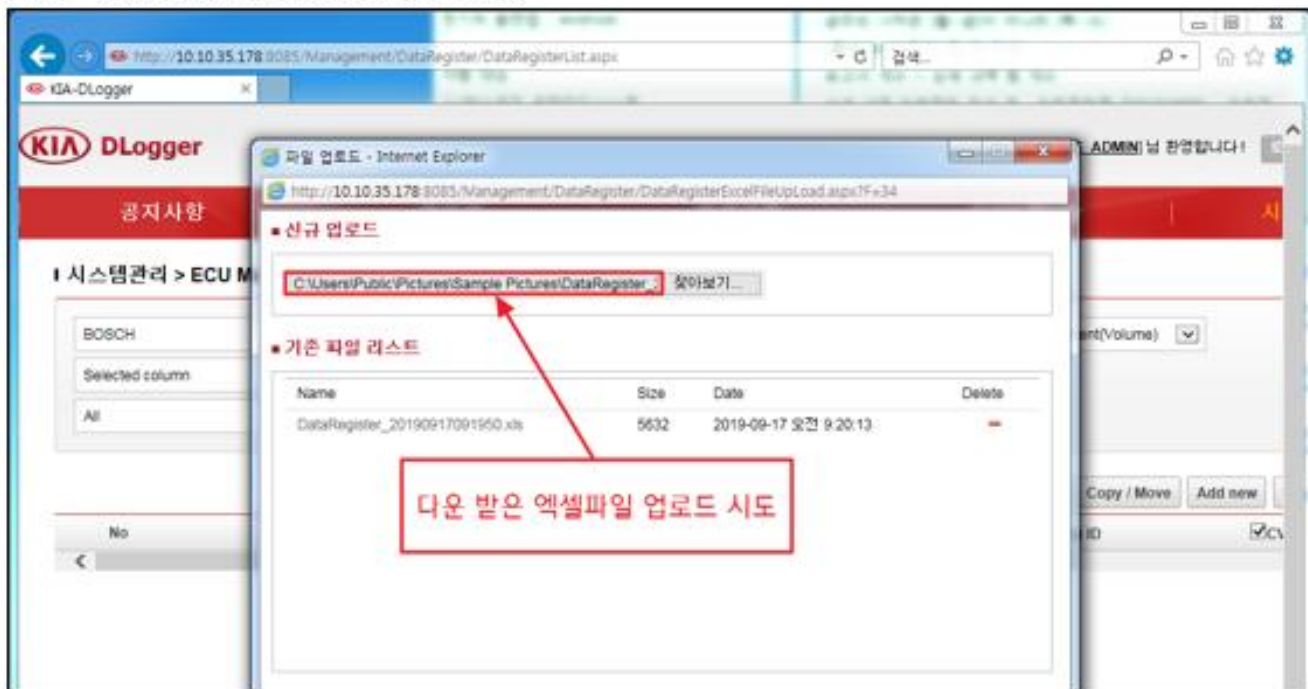
단계7) 기존 파일 다운로드를 통해 양식 파일 다운로드.






	<b>WEB 모의해킹 결과보고서</b> <b>EMS 자동분석 (AI 고장진단) 시스템 개발 프</b> <b>로젝트-디로거 시스템 (기아)</b>	버전.	0.9.0.
		일자.	2019.09.20.

단계8) 다운 받은 엑셀파일 업로드 시도.

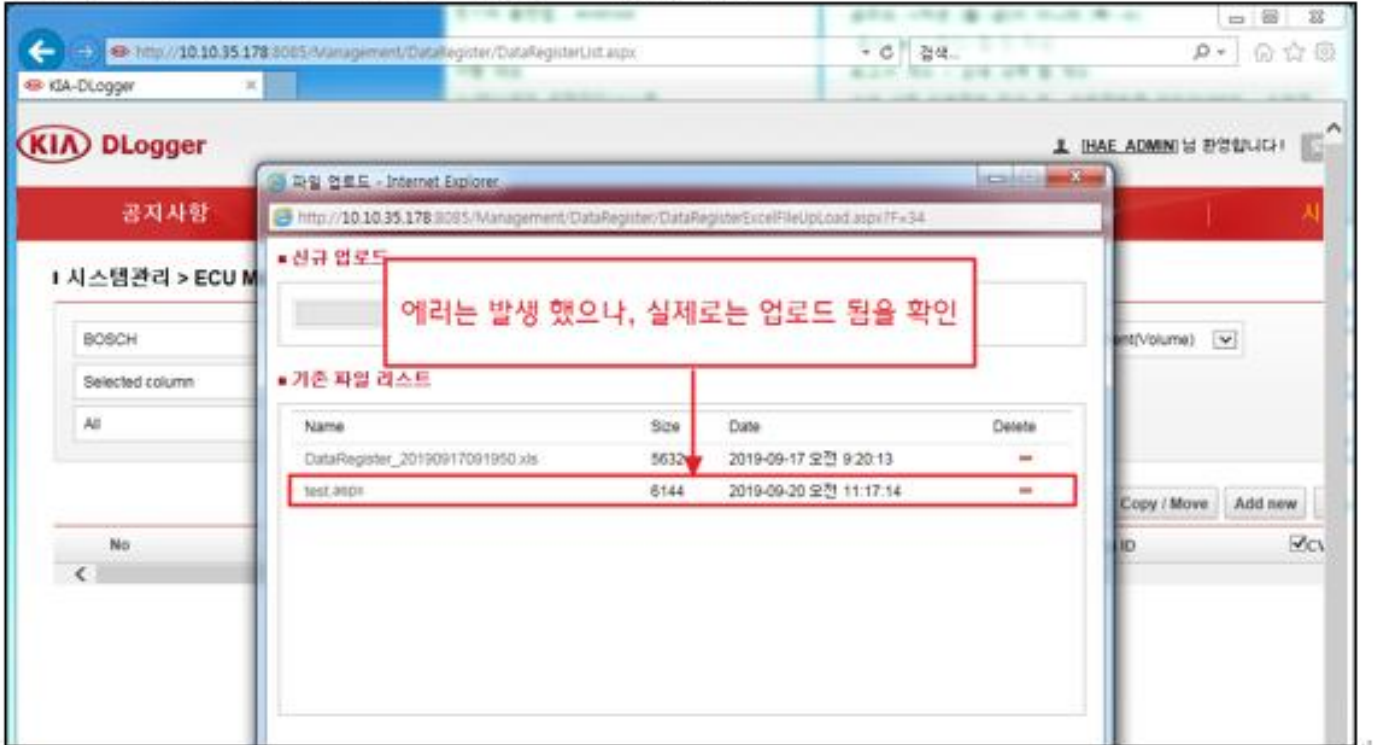


단계9) 엑셀 업로드 시 파일명 변경 후 업로드.

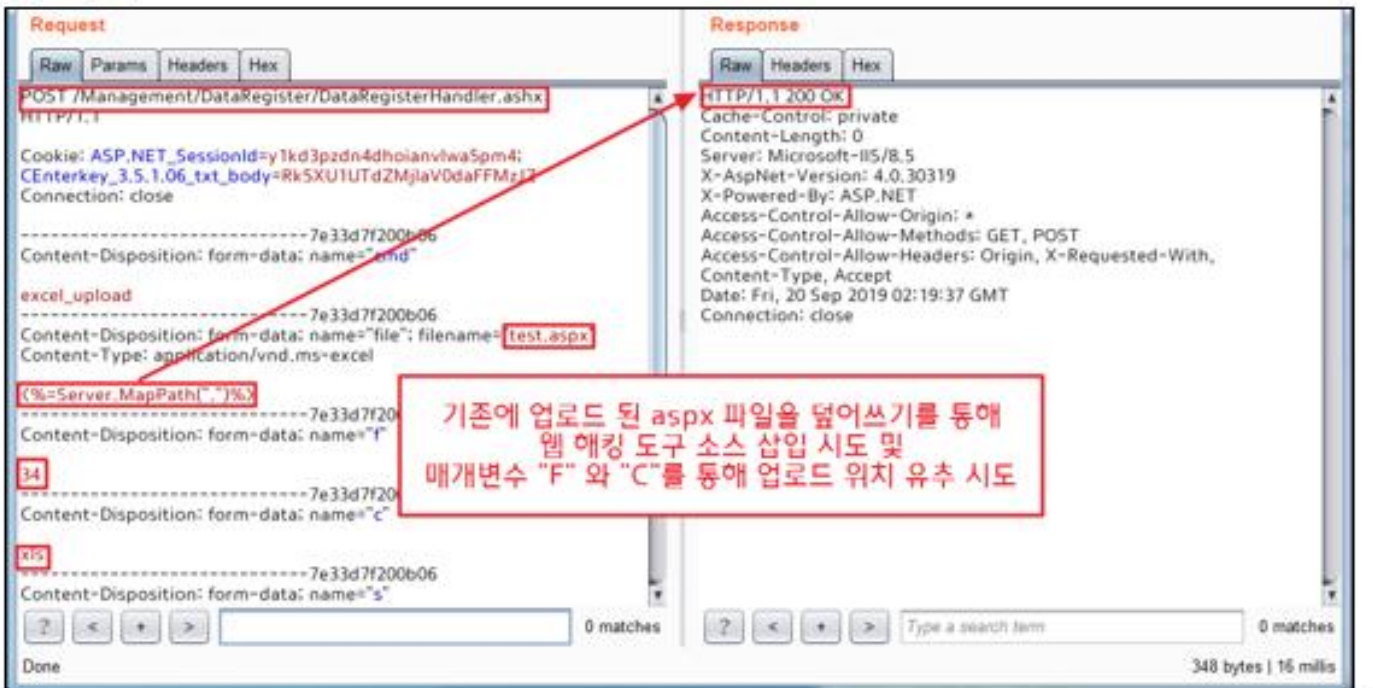



	<b>WEB 모의해킹 결과보고서</b> <b>EMS 자동분석 (AI 고장진단) 시스템 개발 프</b> <b>로젝트-디로거 시스템 (기아)</b>	버전,	0.9.0.
		일자,	2019.09.20.

단계10) 에러는 발생 했으나 실제로는 업로드 됨을 확인.

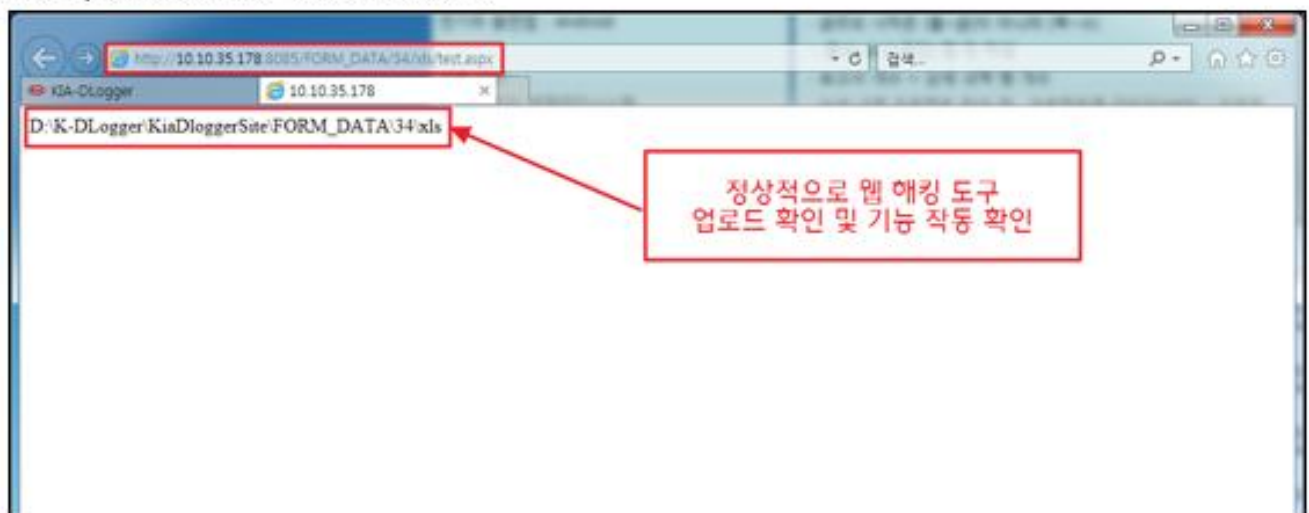


단계11) 기존에 업로드 된 aspx 파일 덮어쓰기를 통해 웹 해킹 도구 소스 삽입 시도 및 업로드 위치 유추 시도.



	<b>WEB 모의해킹 결과보고서</b> <b>EMS 자동분석 (AI 고장진단) 시스템 개발 프</b> <b>로젝트-디로거 시스템 (기아)</b>	버전.	0.9.0.
		일자.	2019.09.20.

단계12) 웹 해킹 도구 기능 작동 확인.



단계13) 웹 해킹 도구를 이용하여 현재 서버 정보 획득 가능.

