|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S/W 신규 취약점 신고서** | | | | | | |
| **성 명** | 김x성 | | **소 속** | | 인하대학교 | |
| **이메일** | lpott95@gmail.com | | **전화번호** | | x | |
| **주 소** | x | | | | | |
| **명예의 전당** | **KrCERT&보호나라 홈페이지 실명 게시** **동의여부 동의**  o 해당 내용은 보호나라&KrCERT 홈페이지의 “명예의 전당” 페이지에 게시됩니다.  ※ 아래 닉네임과 웹사이트 주소를 작성해 주실 경우, 실명과 함께 게시됩니다.  ※ 게시 대상은 포상금을 수령한 신고자에 한하여 게시됩니다. | | | | | |
| **닉네임** | gd | | **웹사이트 주소** | | 개인 서버 비공개 |
| **o 본 취약점을 KISA 신고 전에 공개, 다른 기관 신고, 해당업체 통보 등 여부**  **예 ( 대상 및 일자 : 서버담당자 김x환 2020. 1 .31 )** | | | | | | |
| **o 본 취약점이 정부 지원 사업\*을 통해 발굴된 취약점인지에 대한 여부 아니요**  \* 정부 예산이 투입된 연구과제 또는 프로젝트 | | | | | | |
| **<취약점 정보 활용 및 비밀유지>**  o 신고된 취약점은 포상 관련 평가, 취약점을 보완한 제품 개발(보안 업데이트 개발)을 위해 활용됩니다.  o 포상은 비공개된 취약점을 대상으로 하며(공개된 취약점은 포상 대상에서 제외), 신고 후에도 아래와 같이 그 어떠한 목적으로도 KISA를 제외한 제3자(제조사 포함)에게 공개할 수 없습니다.  - KISA 포상 취약점: 제조사가 보안패치 한 날로부터 120일(4개월) 이전에 외부 공개 불가  - 공동운영사 포상 취약점: 영구 공개 불가  o 신고서에 작성한 내용이 사실과 다르게 작성되거나, KISA를 제외한 제3자에게 취약점을 공개한 경우, 비밀유지 의무 등을 위반한 사실이 밝혀진 경우 다음과 같은 불이익을 당할 수 있습니다.  - 밝혀진 날로부터 1년 동안 평가 및 포상 대상에서 제외  - 해당 취약점으로 이미 포상 받은 경우 포상 취소 및 지급 포상금 전액 환수  **▷취약점 정보 활용 및 비밀유지 동의여부 동의** | | | | | | |
| **<정보통신망 이용촉진 및 정보보호에 관한 법률 위반행위 관련 안내>**  o 실제 서비스 중인 웹사이트나 시스템(서버, 네트워크, 보안장비 등)에 특정 데이터를 전송하여 영향을 줄 우려가 있는 서비스 취약점은 평가 및 포상 대상에서 제외됨은 물론, 법에 의해 처벌 받을 수 있습니다.   |  | | --- | | ｢정보통신망 이용촉진 및 정보보호에 관한 법률｣ 제71조 제10호 및 제48조 제3항에 따라 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하였다면 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. | | | | | | | |
| **<개인정보 수집·이용 동의>**  o 개인정보 수집 이용 목적 : 신규 취약점 신고포상제 운영 및 포상금 지급, 신고포상제 명예의 전당 게시  o 수집하는 개인정보 항목 : 성명, 소속, 이메일, 연락처, 주소, 닉네임, 웹사이트 주소  o 보유 및 이용기간 : 소득세법 등 관련법령에 따른 보유기간 또는 3년 / (명예의 전당) 사업 종료 시 파기  o 개인정보의 수집·이용을 거부할 수 있으며, 이 경우 기념품 또는 포상금 지급, 명예의 전당 게시 및 상위 신고자 선정 시, 불이익이 발생할 수 있음을 알려드립니다.  **▷개인정보 수집·이용 동의여부 동의** | | | | | | |

|  |
| --- |
| **취약점 상세 설명 작성 시 준수 사항** |
| **o 취약점 신고자는 다음 작성 방법을 준수하여 각 항목을 작성해야 하며, 내용이 불충분할 경우 재작성을 요청드릴 수 있습니다.**  - 취약점을 증명/검증할 수 있는 개념증명코드(Proof Of Concept Code)는 별도 파일로 제출(필수) 바랍니다.  - 취약점을 신고한 소프트웨어는 별도 파일로 제출 바랍니다.  ※ 상용 소프트웨어의 경우 해당 제조사 URL 기술해 주시기 바랍니다.  - 신고 문서 내용이 사실과 불일치할 경우 문서완성도 평가 시 감점될 수 있습니다.  - 취약점을 이용한 공격(계산기 팝업 등)이 포함된 공격코드(Exploit Code) 별도 제출 시, 기술 가산점을 부여합니다.  - 실장비가 아닌 가상환경에서 발생하는 IoT 취약점일 경우, 특정 평가항목에서 감점될 수 있습니다. (보호기법 적용 환경 등 고려)  ※ 취약점 상세 설명과 PoC 또는 공격코드에 신고자 정보가 노출되지 않도록 주의 부탁 드립니다. |
| **1. 취약점 발견 방법**  - 취약점을 어떻게 발견하였는지에 대한 기술 설명(크래시 발생, 퍼징 도구 활용, 코드 진단 등)  **2. 취약점 발생 원인**  - 취약점 발생 입력 데이터 설명(문자열, 이미지 등의 파일)  - 취약점 발생 위치 설명(함수, 어셈블리코드, 프로그램 주소 위치 등)  - 취약점 발생 원인 설명(소스코드 분석, 리버싱 결과 등으로 취약점 발생 원인을 파악한 내용 기술)  **3. 취약점 증명/검증**  - 취약점에 대한 상세 분석 결과 기술  **※** 취약점 분석 결과 스크린샷 및 설명, POC 디버깅 과정 설명 , 보호 기법 우회 기술, 취약점 발생 동영상 첨부 등  **4. 취약점 악용 시나리오**  - 취약점이 악용될 수 있는 공격 시나리오와 관련 서비스(또는 시스템)에 미칠 수 있는 영향  **5. 조치 방안**  - 취약점을 해결할 수 있는 효과적인 방법 제시  **6. 기타**  - 취약점 관련하여 참고할 수 있는 자료(웹사이트 주소 등)  - 발견한 취약점을 악용하고 있는 사례가 있다면 이에 대한 설명  - 첨부한 각 파일에 대한 설명(파일명 : 파일에 대한 설명) |

**<취약점 개요>**

|  |  |
| --- | --- |
| **취약점 제목** | o 게시글 내 xss, 게시글 제목 xss, 로그인 sqli |
| **취약점 요약** | o XSS, Time Based SQL injection |
| **취약한 S/W의 버전** | o php |
| **취약점 발생환경** | o Apple LLVM version 10.0.1 (clang-1001.0.46.4)  Target: x86\_64-apple-darwin18.6.0 |

**<취약점 상세 설명>**

**1. 취약점 발견 방법**

o <script>alert(1);</script> 명령어를 기반으로 한 여러 우회 xss 공격시도

o 구글 크롬 웹브라우저 개발자 도구

o sqli 공격문 입력 시도

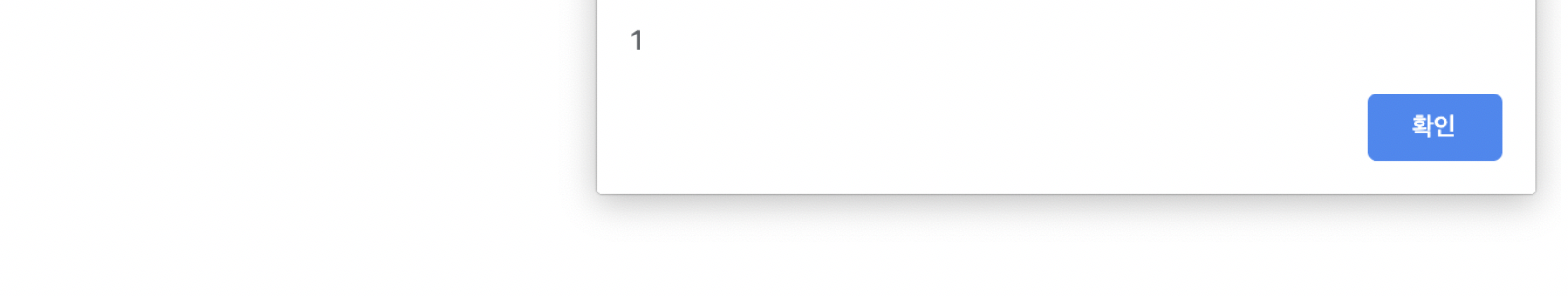
**2. 취약점 발생원인**

o 제목 , 게시글 내용에 대한 입력 값 검증 및 필터링 조건 부재

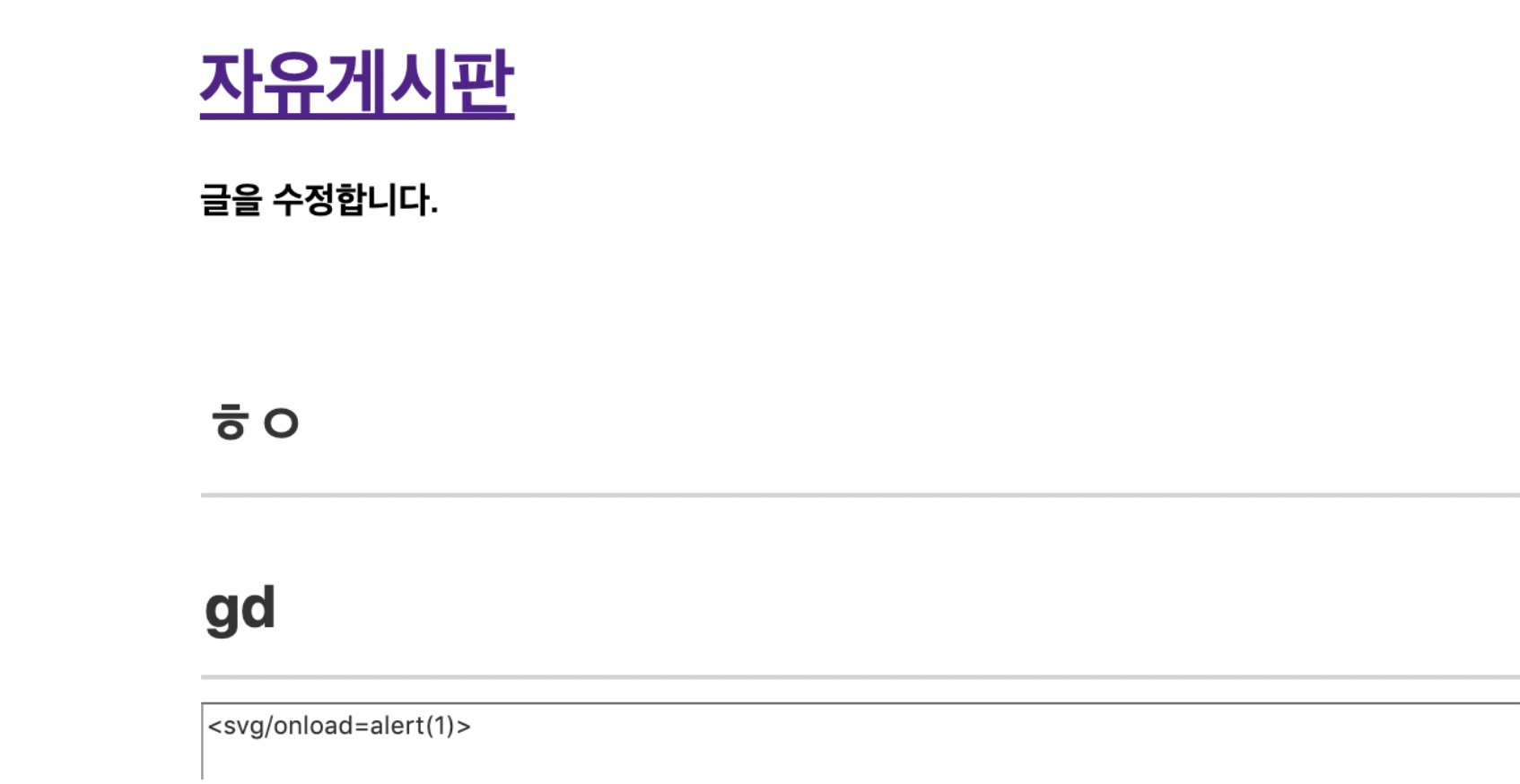
o 로그인 시 문자열에 대한 필터링 부재

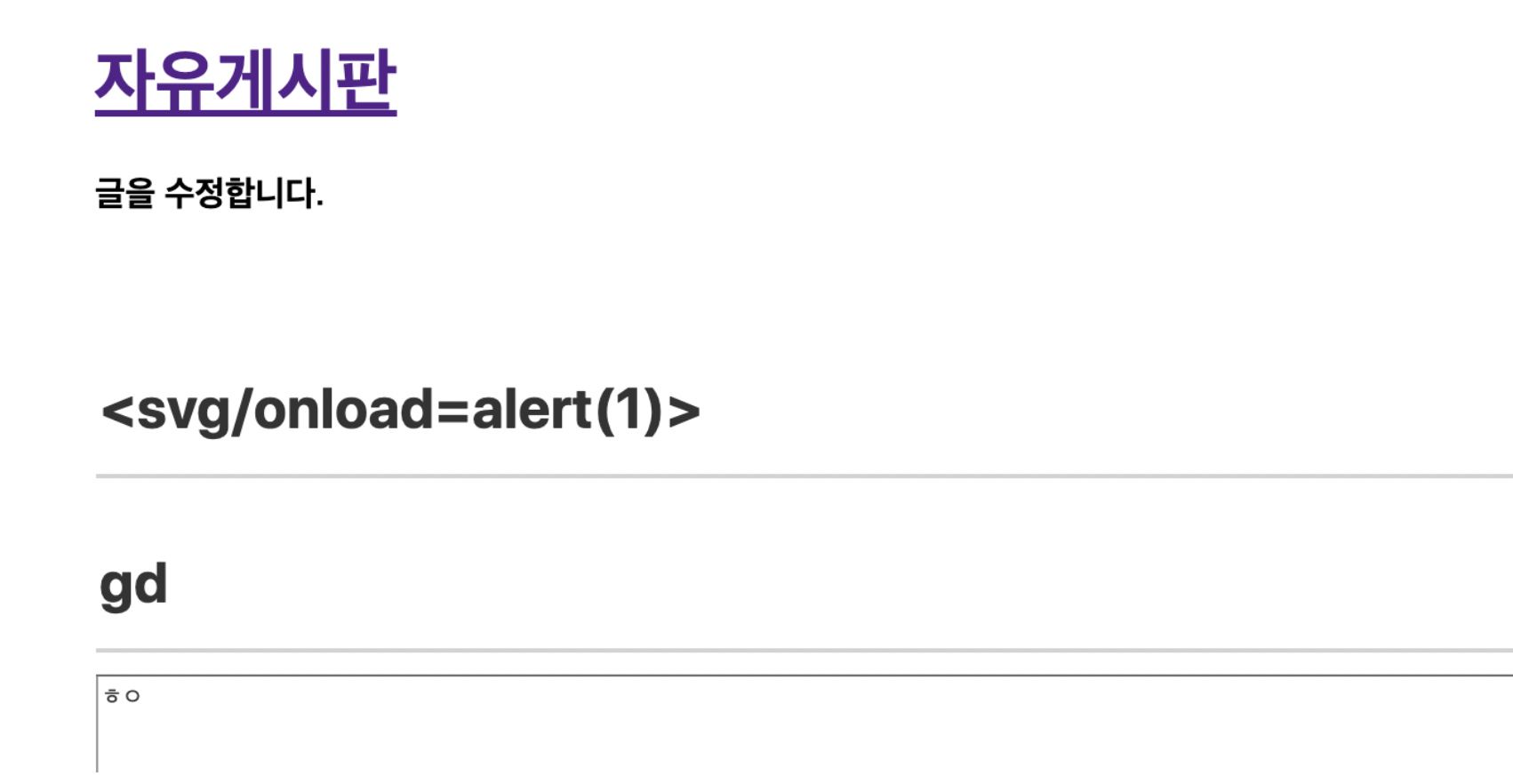
**3. 취약점 증명 / 검증**

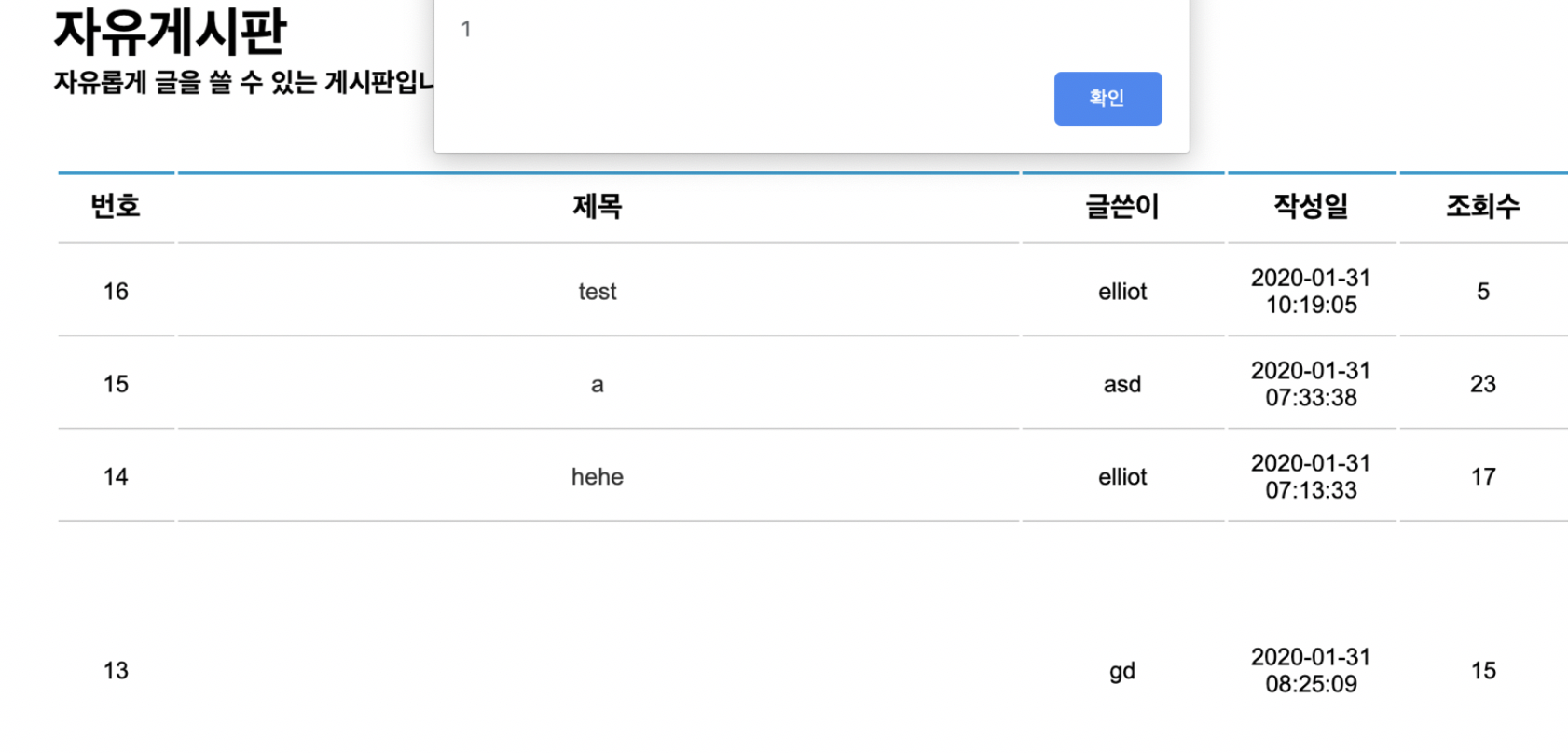
o <svg/onload=alert(1)> 명령어를 게시글 내용에 작성



o <svg/onload=alert(1)> 명령어를 게시글 제목에 작성







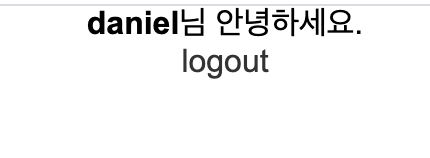
o Time Based Blind SQL injection

다음과 같은 회원 정보를 획득

사용자의 아이디는 게시판에 등록된 게시글을 통해 얻은 후 비밀번호를 따로 injection을 통해 획득

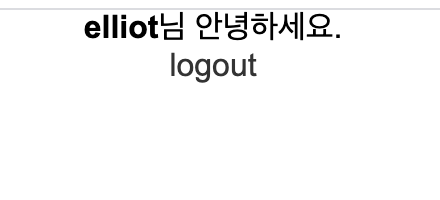
Id : daniel(서버 담당자)

Pw: 1234

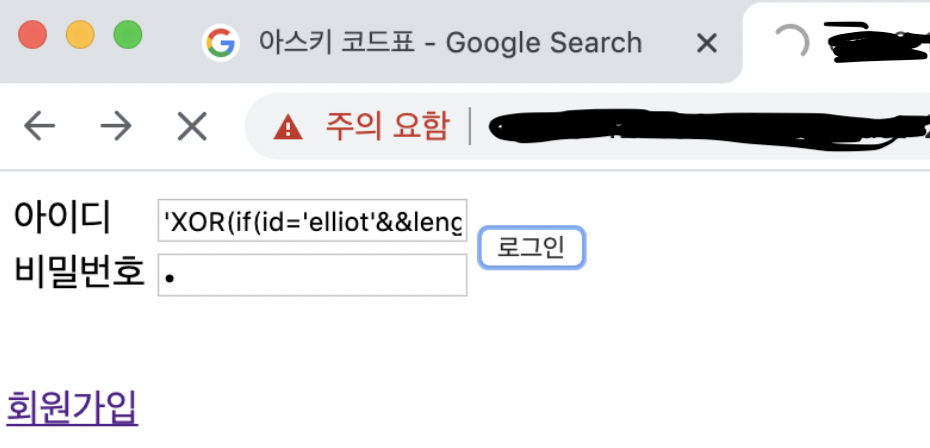


Id: elliot(웹사이트 사용자)

Pw: robot







공격문 예시 if 조건 TRUE 시 5초간 sleep

'XOR(if(id='elliot'&&length(pw)<10,sleep(5),0))OR'

'XOR(if(id='elliot'&&ascii(pw,1,1)<120,sleep(5),0))OR'

**4. 취약점 악용 시나리오**

o 게시글을 클릭하였을 때 원하지 않는 악성코드 다운로드 또는 리다이렉트, fake 사이트로 이동 후 정보 피싱

o 본 취약점 분석에서는 파이썬을 통한 Brute-Force 방법을 이용하지 않았지만, 이용한다면 게시판에 공개된 아이디외에 데이터베이스 상에 있는 다른 아이디 및 비밀번호등 개인 정보를 얻을 수 있게 된다. 또한, 정보 취득외에 다른 공격과 연계될 수 있다.

**5. 조치 방안**

o 입력된 값 검증 , <>, script 문자열에 대한 필터링을 통해 방지

o 로그인 시 입력 값에 대한 필터링 조건 추가

**6. 기타**

o 고생하셨습니다.