**[SKdevsec]**

**2차 취약점진단 결과보고서**

**2021. 06. 13.**

**목 차**

[**1.**](#_gjdgxs)**개요**[**3**](#개요)

[**1.1.**](#_30j0zll) [**진단 목적 3**](#진단목적)

[**1.2.**](#_1fob9te) [**진단 대상 3**](#진단대상)

[**1.3.**](#_2et92p0) [**진단 일정 3**](#진단일정)

[**1.4.**](#_3dy6vkm) **[진단 인력 3](#진단인력)**

[**2.**](#_4d34og8) [**진단 항목 및 도구 6**](#진단항목및도구)

[**2.1.**](#_2s8eyo1) [**취약점 진단 도구 6**](#취약점진단도구)

[**2.2.**](#_3rdcrjn) [**진단 항목 6**](#진단항목)

[**3.**](#_1ksv4uv) [**취약점진단 결과요약 6**](#취약점진단결과요약)

[**3.1.**](#_44sinio) [**총평 6**](#총평)

[**3.2.**](#_2jxsxqh) [**대상 별 취약점 요약 6**](#대상별취약점요약)

[**4.**](#_3j2qqm3) **[취약점진단 상세결과 7](#취약점진단상세결과)**

[**4.1.**](#_2xcytpi) **메인 서비스(http://www.kilhyomin.com)** [**7**](#메인서비스)

[(1) 관리자 페이지 분리 여부 (중요) 7](#관리자페이지분리여부)

[**Ⅰ. 별첨 10**](#별첨)

[**1.**](#_3b2epr8) **취약점 진단 방법론** 10

1. **개요**
   1. **진단 목적**

본 취약점 진단은 “skdevsec”에서 운영중인 컴퓨터 쇼핑몰 서비스에 대하여 취약점 체크리스트를 기반으로 주요정보의 전자적 침해 행위에 대한 취약점을 분석ᆞ평가하고, 존재하는 위협 요소에 대해 정확한 분석을 통해 보안대책을 수립 및 취약점을 제거하여 보안 위협을 최소화함으로써 사고 예방 및 안전한 운영에 기여하고자 합니다.

* 1. **진단 대상**

|  |  |  |
| --- | --- | --- |
| **No** | **URL** | **서비스명** |
| 1 | http://www.kilhyomin.com/ | 컴퓨터 쇼핑몰 |

[표] 1. 진단대상

* 1. **진단 일정**

|  |  |
| --- | --- |
| **업무 수행 내역** | **일정** |
| 사전준비 및 대상 관련 자료 수령 | 2021.05.11 이전 |
| 취약점 점검 | 2021.06.03~ 2021.06.06 |
| 결과 분석 및 결과 보고서 작성 | 2021.06.09 |
| 보고서 최종 수정 및 완료 | 2021.06.11 |

[표] 2. 진단 일정

* 1. **진단 인력**

|  |  |  |  |
| --- | --- | --- | --- |
| **이름** | **수행업무** | **연락처** | **E-Mail** |
| 길효민 | 취약점진단 | 010-4794-0055 | bigjoy22@naver.com |
| 김경한 | 취약점진단 | 010-8419-1477 | jobapplication010@gmail.com |
| 이지호 | 취약점진단 | 010-7979-3287 | leejeeho6661@naver.com |
| 이지선 | 취약점진단 | 010-9555-2873 | wia\_hawm@naver.com |
| 박진환 | 취약점진단 | 010-6676-8229 | zkzlaptb@naver.com |

[표] 3. 진단 인력

1. **진단 항목 및 도구**
   1. **취약점진단 진단 도구**

취약점진단의 특성상 툴을 이용한 진단은 정확도가 떨어지며 상황 별 판단이 필요하므로 대부분 취약점진단 전문인력이 수동으로 진단합니다.

취약점진단을 수행하기 위해 사용되는 도구들을 정리하면 다음과 같습니다.

|  |  |
| --- | --- |
| **구분** | **진단 항목 설명** |
| Burp Suite | Proxy 기능을 이용한 웹 세션 조작 도구 |
| Wireshark | 네트워크 패킷 점검 도구  http://www.wireshark.com/ |
| 기타 | 진단자가 작성한 Exploit Code 및 Script, 기타 점검 도구 |

[표] 4. 진단 도구

* 1. **진단 항목**

진단에 사용될 항목은 OWASP[[1]](#footnote-1), NIST[[2]](#footnote-2), 행정안전부 등에서 권고하는 내용을 기반으로 본 프로젝트와 연관성이 있는 보안상의 문제점을 주축으로 총 8개 분류 27개 항목의 체크리스트로 수립한 항목입니다.

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | **취약점 번호** | **세부 진단 항목** | **준수기준** |
| 입/출력 값  검증 부재 | **1-1** | **XSS / CSRF 공격 가능성** | **중요** |
| **1-2** | **SQL / Command Injection 공격 가능성** | **중요** |
| **1-3** | **파라미터 값 및 히든(hidden) 필드 조작 가능성** | **중요** |
| **1-4** | **파라미터 값 위조/변조를 통한 서버 데이터 활용 가능성** | **중요** |
| 1-5 | 검증되지 않은 리다이렉트와 포워드 | 일반 |
| 취약한  파일처리 | **2-1** | **악성코드파일 업로드** | **중요** |
| 2-2 | 중요 정보 파일 다운로드 가능성 | 일반 |
| 취약한 접근  통제 관리 | 3-1 | 패스워드 정책 유무 및 반영 여부 | 일반 |
| 3-2 | 인증 실패 횟수 제한 | 일반 |
| 3-3 | 계정 정보 파악 가능성 | 일반 |
| **3-4** | **관리자 페이지 분리 여부** | **중요** |
| 3-5 | 검색엔진 정보 노출 가능성 | 일반 |
| 3-6 | 백업 파일 및 테스트 파일 존재 여부 | 일반 |
| 취약한 인증 및  세션 관리 | 4-1 | 쿠키 조작 가능성 | 일반 |
| 4-2 | 세션 재사용 가능성 및 타임아웃 설정 여부 | 일반 |
| 4-3 | 접근제어 우회 가능성 확인 | 일반 |
| **4-4** | **비인증 상태로 중요 page접근 가능성** | **중요** |
| **4-5** | **일반계정 권한 상승 가능성** | **중요** |
| 중요 정보 저장/전송 처리 미흡 | 5-1 | 소스코드 내 주요정보 노출 여부 | 일반 |
| **5-2** | **요청 및 응답 값 내 주요정보 포함여부 확인** | **중요** |
| 부적절한  오류 처리 | 6-1 | 오류페이지를 통한 정보 노출 여부 | 일반 |
| 6-2 | 일괄적인 오류 처리 페이지 존재 여부 | 일반 |
| 취약한  컴포넌트  구성요소 | 7-1 | Client Request Method | 일반 |
| 7-2 | 파일 목록화 가능성 | 일반 |
| 7-3 | 서버 헤더정보 노출 | 일반 |
| **7-4** | **취약한 보안설정** | **중요** |
| 기타 취약점 | 8-1 | 취약점 진단 항목에 정의되지 않은 취약점 | - |

[표] 5. 주요 진단 항목

1. **취약점진단 결과요약**
   1. **총평**

**“skdevsec”**의 총 1개의 도메인을 대상으로 웹 취약점진단을 진행한 결과 외부에 오픈된 1개 사이트에서 **“관리자 페이지 분리 여부”** 취약점이 1개 발견되었습니다.

자세한 사항은 아래 취약점진단 상세결과를 확인하시고 본 결과보고서와 함께 제공해드리는 보안 가이드라인을 참고하시어 적절한 보안 대책을 수립 후 조치하시길 권고 드립니다.

* 1. **대상 별 취약점 요약**

|  |  |  |  |
| --- | --- | --- | --- |
| **대상(도메인)** | **취약점**  **심각도** | **취약점 명칭** | **개수** |
| **컴퓨터 쇼핑몰(http://www.kilhyomin.com/)** | **중요** | **관리자 페이지 분리 여부** | 1 |

[표] 6. 대상 별 취약점 요약

※ 취약점 심각도

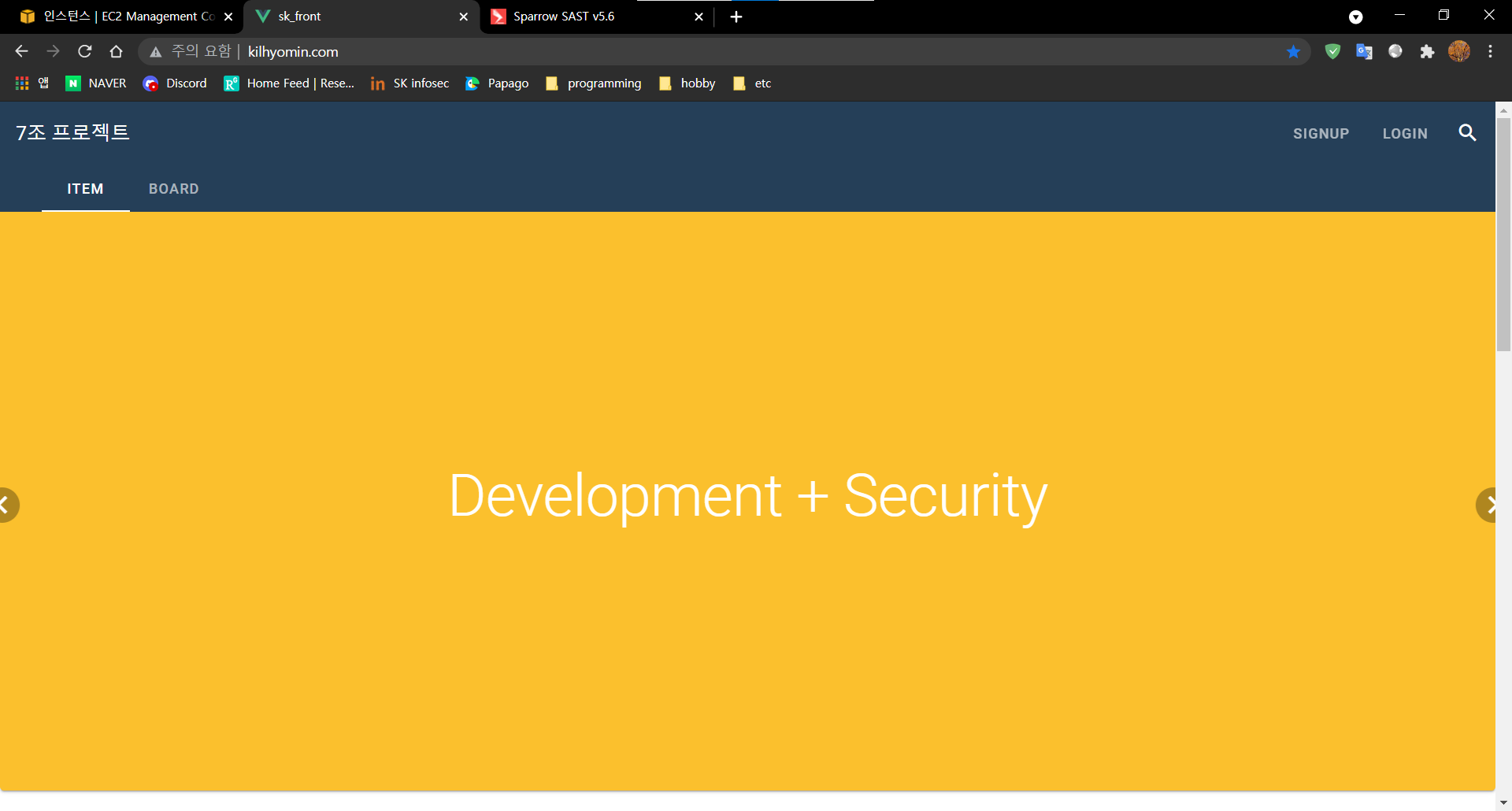
중요 : 시스템의 직접적인 접근 및 침입, DB 획득 등 서버 시스템 장악이 가능한 취약점

일반 : 시스템 직접 접근은 되지 않으나 취약한 체크리스트 항목

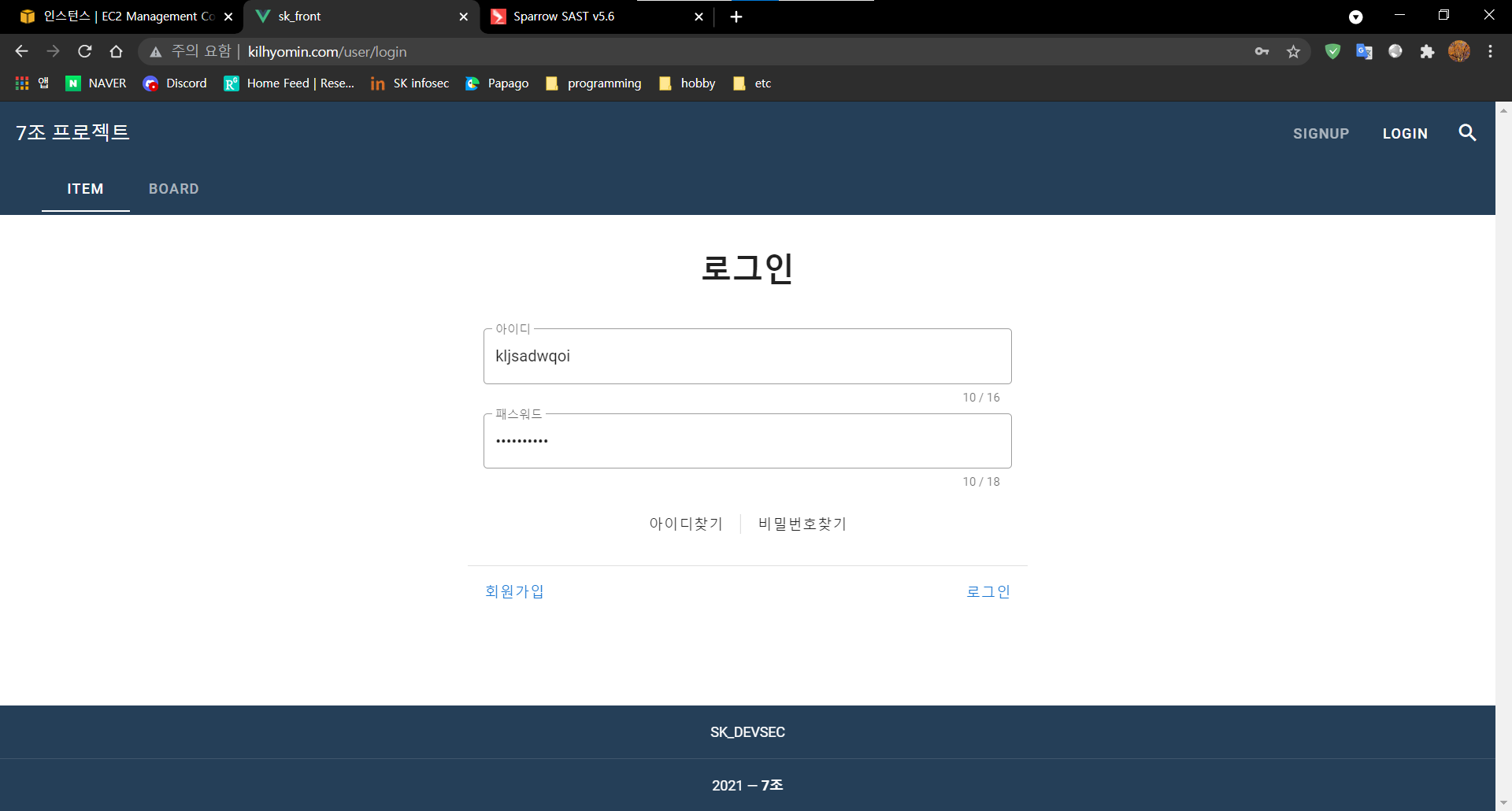
기타 : 그 외의 취약점

1. **취약점진단 상세결과**
   1. **메인 서비스 ( http://www.kilhyomin.com )**
      1. **관리자 페이지 분리 여부 (중요)**
         1. **문제점**

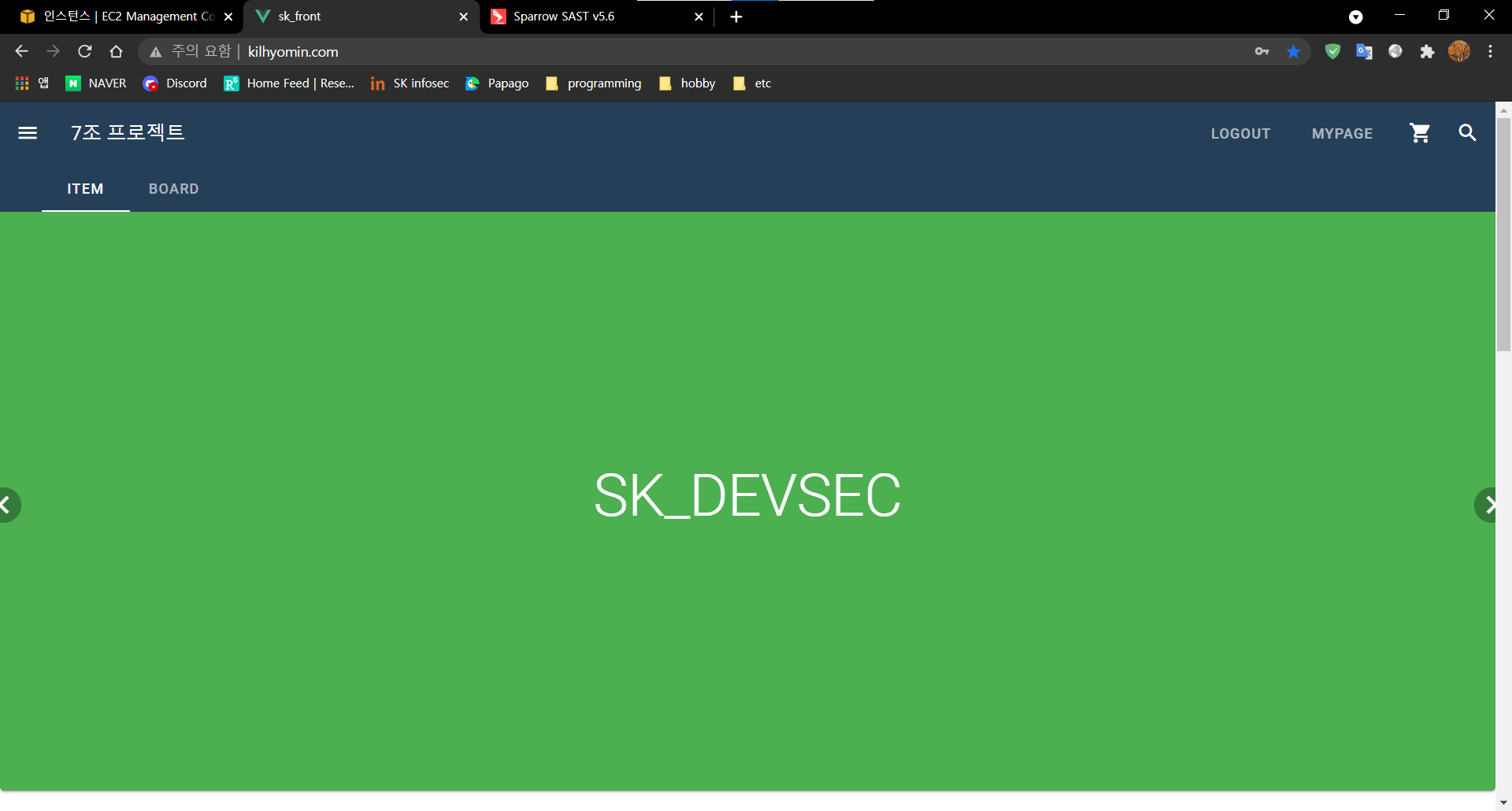
* 관리자 아이디로 접속할 경우 메인 페이지에 맨 왼쪽 상단에 목록 아이콘이 생기는 것을 확인
* 해당 아이콘을 클릭 시 해당 웹 사이트 데이터들에 대한 관리 페이지 목록이 나오게 된다.
* 관리자 페이지를 분리하지 않고, 공개/비공개로 아이콘 버튼으로 접근 제어를 하고 있다.



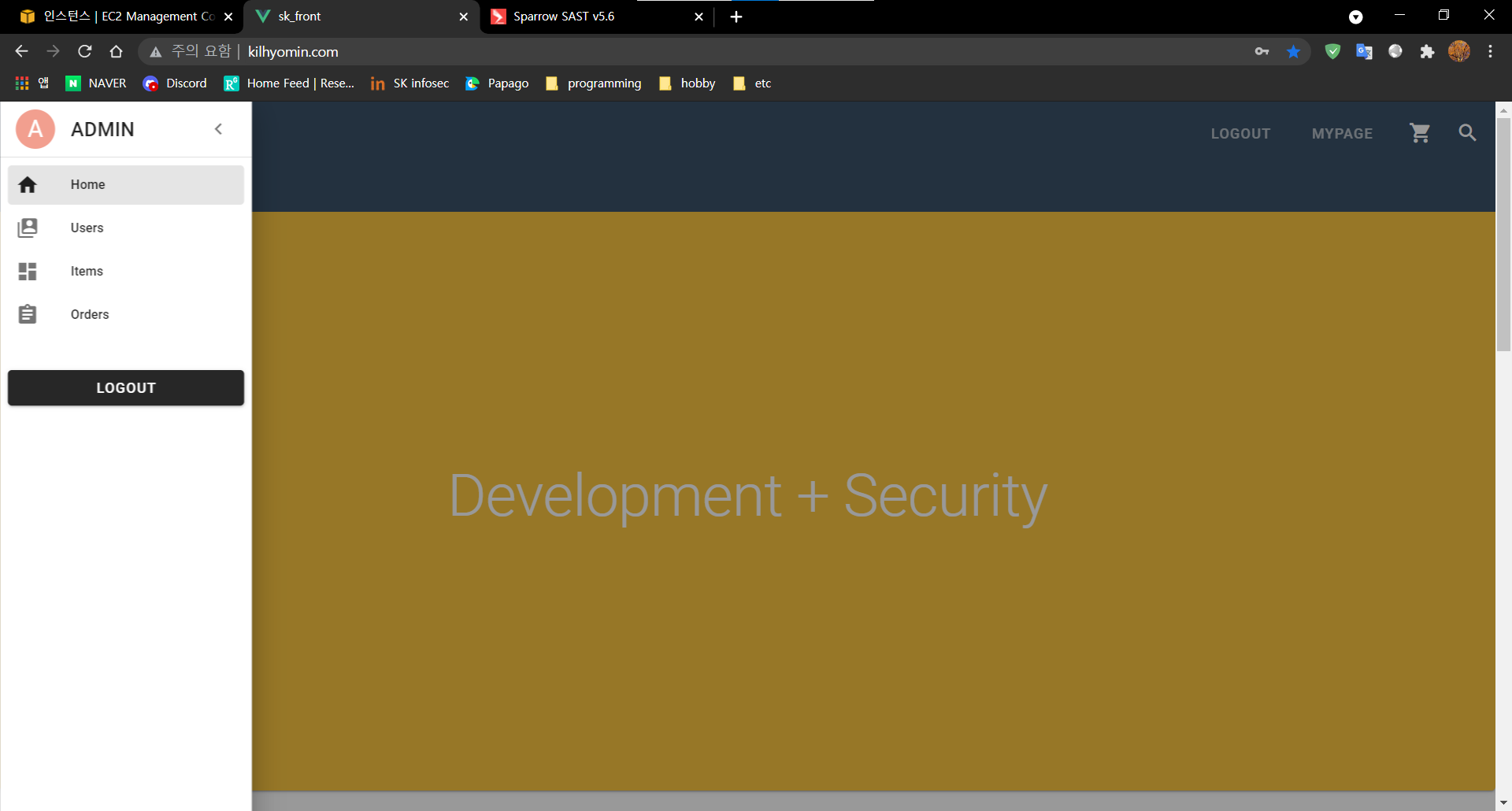
[그림] 1. 테스트 파일 확인 ①



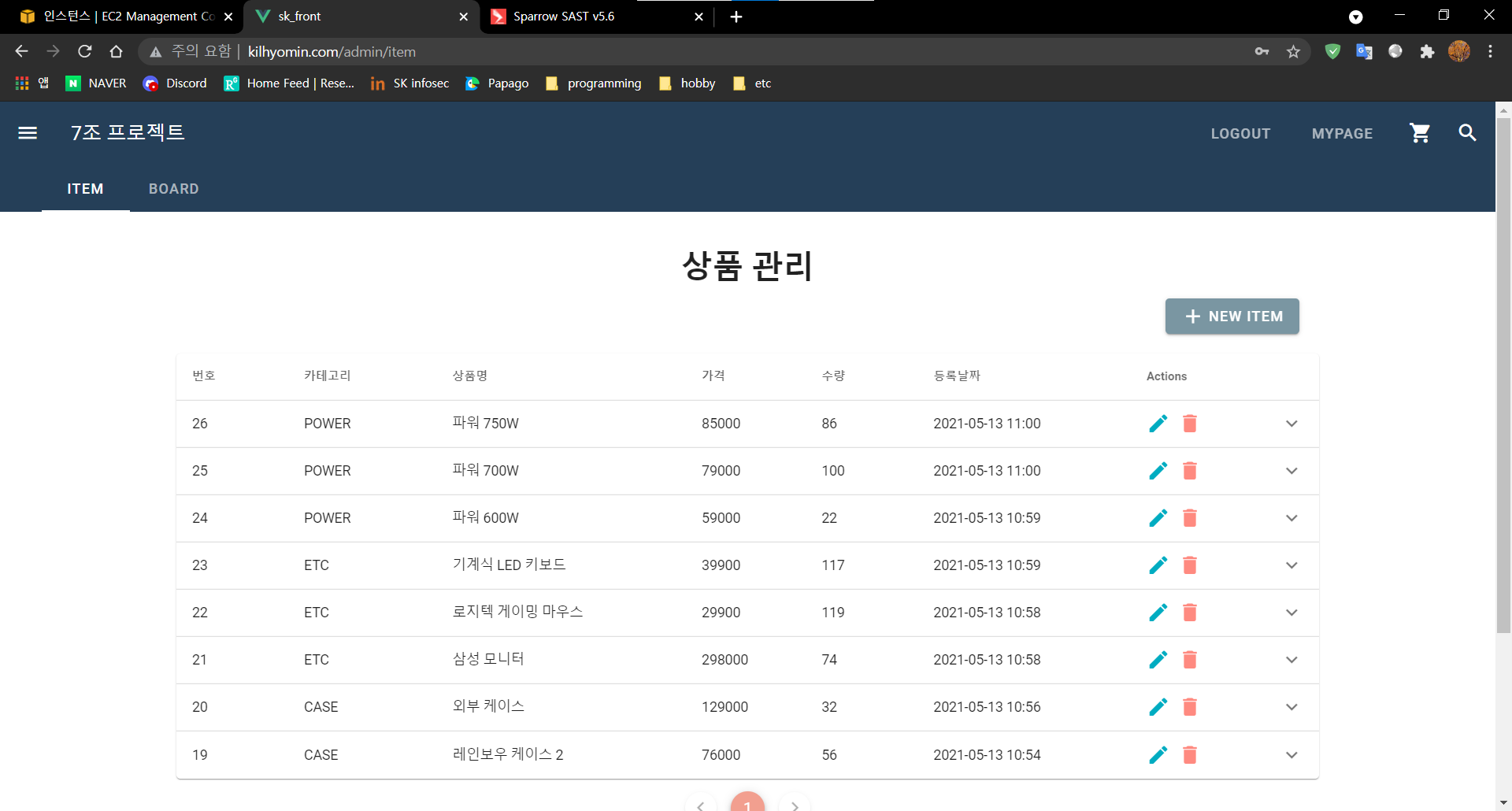
[그림] 2. 테스트 파일 확인 ②



[그림] 3. 테스트 파일 확인 ③



[그림] 4. 테스트 파일 확인 ④



[그림] 5. 테스트 파일 확인 ⑤

* + - 1. **관련 URL**

|  |  |  |
| --- | --- | --- |
| **번호** | **경로** | **URL** |
| 1 | 메인 페이지 | http://www.kilhyomin.com |

* + - 1. **해결방안**

※ 누구나 접근할 수 있는 메인 페이지에 관리자 페이지로 이동할 수 있는 아이콘 버튼을 만듦으로써

노출될 가능성이 매우 높아지며, 때문에 메인 페이지에 포함시키는 것이 아닌 접근이 힘든 다른 공간에 관리자 페이지를 연결시켜야 한다.

* 더 좋은 방법으로는 관리자 페이지를 해당 웹 사이트와 분리시켜 다른 url을 가지게 하는 것이 가장 좋은 방법이다.

Ⅰ. 별첨

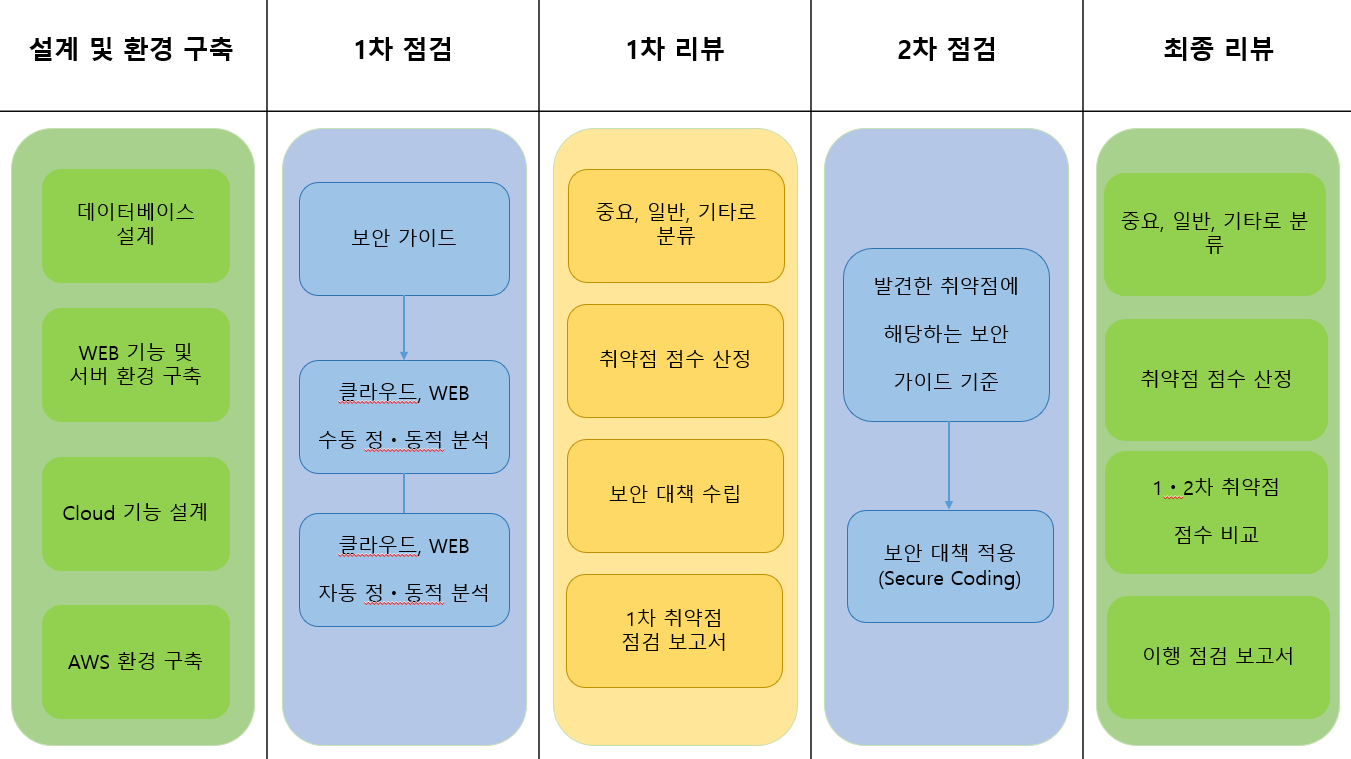
1. **취약점진단 방법론**
2. 취약점진단 개요

비 인가자로 인한 해킹의 위협을 테스트하기 위하여 고객사의 내ㆍ외부 서비스용 시스템을 대상으로 아래와 같은 환경에서 테스트를 실시합니다.

* 고객사 사이트의 취약점 진단 의뢰 가정(사이트 개발)
* 대상시스템의 IP Address 정보와 코드를 제공받아 취약점진단을 수행
* 고객사의 내ㆍ외부 서비스용 시스템을 대상으로 수행
* 가이드 라인을 바탕으로 취약점 진단 수행
* 자동화 툴과 병행하여 다양한 방법의 취약점 진단 수행

1. 취약점진단 수행 방법

아래 그림과 같이 기본적인 프로젝트 준비와 실제 구축을 진행하는 (1) 설계 및 환경 구축을 거쳐 수동 및 자동 점검을 실시하는 (2) 1차 점검을 진행합니다. 이 단계에서 수집된 정보를 바탕으로 하여 (3) 1차 리뷰를 진행하며 발생한 취약점을 보완하여 시큐어 코딩이 적용되는 (4) 2차 점검을 수행합니다. 마지막으로 개선전과 개선후의 비교를 통한 보고서 작성과 미흡한 부분에 대해서 검토하는 (5) 최종 리뷰를 수행합니다.



[그림] 6. 모의 해킹 수행 방법

1. 취약점진단 수행 방법 단계별 상세

**(1) 설계 및 환경 구축**

가정한 고객사의 웹페이지를 개발하는 단계입니다. 데이터 베이스 설계, 웹의 기능 및 서버 환경을 구축하고 프론트 엔드와 백 엔드의 서버를 위한 클라우드 기능 설계와 AWS환경 구축을 진행합니다.

**(2) 1차 점검**

보안 가이드를 바탕으로 정적 분석과 동적 분석을 진행합니다. 두가지 분석 모두 수동과 자동을 병행합니다. 수동 점검은 보안 가이드에 있는 XSS/CSRF 공격 가능성, SQL/Command Injection 공격 가능성 등 26항목을 주요항목과 일반항목으로 나누고, 시스템의 직접적인 접근 및 침입, DB 획득 등 서버 시스템 장악이 가능한 취약점을 주는 주요항목을 중점으로 공격을 진행합니다. 이와 더불어 자동화 툴을 이용하여 수동점검과 비교하여 미진한 부분을 보충하여 점검을 실시합니다.

**(3) 1차 리뷰**

1차 점검에서 나온 결과를 기반으로 하여 중요, 일반, 기타를 내부적으로 분류합니다. 주요항목과 일반항목의 개수를 종합하여 100점 만점을 기준으로 취약점 점수를 산정합니다. 이후 해당 고객사의 맞는 보안 대책을 수립하고, 취약점 점검 보고서를 작성합니다.

**(4) 2차 점검**

점검에서 포착된 보안상 취약한 부분을 보안 가이드를 기준으로 시큐어 코딩을 조사하고 적용합니다.

**(5) 최종 리뷰**

개선되지 못한부분에 대하여 중요, 일반, 기타를 재 분류 취약점 점수를 재 산정하여 개선의 정도를 비교합니다. 이후 적용한 보안대책에 대한 보고서를 작성합니다.

1. 주) OWASP : The Open Web Application Security Project [↑](#footnote-ref-1)
2. 주) NIST : National Institute of Standards and Technology [↑](#footnote-ref-2)