|  |  |
| --- | --- |
|  |  |

고객사 CI

|  |  |  |
| --- | --- | --- |
|  |  |  |

**JM Collection**

**모듈프로젝트 1**

**[모듈프로젝트 조 이름]**

**2024-00-00**

**제∙개정 이력표**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **개정번호** | **일자** | **제∙개정 내용** | **작성자** | **버전** |
| 1 | 2024.00.00 | 모듈프로젝트 결과 보고서 최초 작성 | XXX | v1.0 |

**목 차**

[1. 클라우드 아키텍쳐 개요 4](#_Toc134718658)

[1.1. 클라우드 아키텍쳐 구성 4](#_Toc134718659)

[1.2. 클라우드 용어 정리 4](#_Toc134718660)

[2. 취약점 진단 개요 5](#_Toc134718661)

[2.1. 목적 5](#_Toc134718662)

[2.2. 점검 대상 5](#_Toc134718663)

[2.3. 점검 일정 5](#_Toc134718664)

[2.4. 점검 인력 6](#_Toc134718665)

[2.4.1. 수행방안 6](#_Toc134718666)

[2.4.2. 진단방법 6](#_Toc134718667)

[2.4.3. 진단도구 6](#_Toc134718668)

[2.4.4. 진단항목 6](#_Toc134718669)

[3. 점검 결과 8](#_Toc134718670)

[3.1. 결과 요약 8](#_Toc134718671)

[4. 사이트별 취약점 현황 9](#_Toc134718672)

[4.1. 도메인1 (WWW.XXX.COM) 9](#_Toc134718673)

[5. 세부 수행내역 10](#_Toc134718674)

[5.1. 홈페이지 1 10](#_Toc134718675)

[5.1.1. XXS. 크로스사이트스크립팅 10](#_Toc134718676)

1. 클라우드 아키텍쳐 개요
   1. 클라우드 아키텍쳐 구성

텍스트, 스크린샷, 번호, 도표이(가) 표시된 사진

자동 생성된 설명

1. WEB Server Subnet (Public Subnet)

* 서로 다른 가용 영역 0개의 각 퍼블릭 서브넷에 인스턴스 생성

1. Web Application Server Subnet (Private Subnet)
2. 00 Server Subnet (0000)
3. 0000
4. 0000
5. 0000
6. 0000
7. 0000
   1. 클라우드 용어 정리

|  |  |
| --- | --- |
| **용어** | **설명** |
| EC2 |  |
| S3 |  |

1. 취약점 진단 개요
   1. 목적

본 프로젝트의 취약점 진단은 대상 시스템에 존재하는 주요 취약점을 분석하여 해당 취약점을 식별⬝제거하여 안전한 서비스의 기반을 마련하는데 목적이 있음.

* 1. 점검 대상

|  |  |  |
| --- | --- | --- |
| **번호** | **대상** | **서버 URL** |
| 1 | 도메인1 | www.xxx.co.kr |

* 1. 점검 일정

**대상선정**

**및**

**시스템현황 파악**

**취약점**

**진단 진행**

**결과 분석**

**대응방안**

**및**

**보고서**

* 2023년 00월 00일 ~ 2023년 00월 00일

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **단계** | **일정** | | | | |
| **00/00** | **00/00** | **00/00** | **00/00** | **00/00** |
| 대상선정 및 시스템 현황 파악 |  |  |  |  |  |
| 취약점 진단 진행 |  |  |  |  |  |
| 결과분석 |  |  |  |  |  |
| 대응방안 및 보고서 작성 |  |  |  |  |  |

* 1. 점검 인력

|  |  |  |
| --- | --- | --- |
| **번호** | **이름** | **이메일** |
| 1 | XXX | XXX@oooo.com |

* + 1. 수행방안
    2. 진단방법
* BurpSuite 외 점검도구를 이용하여 발견된 취약점을 통해 정보 시스템으로의 침투 가능성을 진단함.
* 운영 서비스에 장애를 발생시키지 않는 범위 내에서 실제 공격과 동일한 방법으로 진단함.
  + 1. 진단도구

|  |  |
| --- | --- |
| **점검 도구** | **내용** |
| BurpSuite | 로컬 프록시 서버 |
| WireShark | 패킷 캡처 도구 |

* + 1. 진단항목

진단 기준은 2023 OWASP TOP 10를 참고하여 10개 진단 항목을 선정함.

|  |  |  |  |
| --- | --- | --- | --- |
| **번호** | **코드** | **항목** | **위험도** |
| 1 | BA | 손상된 액세스 제어 | 상 |
| 2 | CF | 암호화 실패 | 상 |
| 3 | IJ | 인젝션 | 상 |
| 4 | ID | 안전하지 않은 디자인 | 상 |
| 5 | SM | 보안 구성 오류 | 상 |
| 6 | VO | 취약하고 오래된 요소 | 상 |
| 7 | IA | 식별 및 인증 오류 | 상 |
| 8 | SD | 소프트웨어 및 데이터 무결성 오류 | 상 |
| 9 | SF | 보안 로깅 및 모니터링 오류 | 상 |
| 10 | SS | SSRF | 상 |

1. 점검 결과
   1. 결과 요약

* 도메인 1 등 -개 사이트에 대한 웹 취약점 점검 결과, 취약점 -개 발견
* (도메인1) 자료실의 게시글 작성 기능에 사용자 입력 값 검증 절차가 없어 악성 스크립트 구문 삽입 가능하여 세션 하이재킹 및 악성 사이트 리다이렉션 가능

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **번호** | **대상** | **취약항목** | **공격영향** | **취약점 개수** |
| 1 | **도메인1** | 크로스사이트 스크립팅 | 세션 하이재킹 및  악성 사이트 리다이렉션 | 2개 |

1. 세부 수행내역
   1. 홈페이지 1
      1. XXS. 크로스사이트스크립팅

**취약점 개요**

* 자유게시판에서 사용자의 입력 데이터를 출력할 때 특수문자를 이스케이프 처리하지 않아 공격자가 등록한 악성 스크립트가 게시물을 열람하는 다른 사용자의 웹브라우저에서 실행 가능

*(발견된 취약점에 대한 간단한 설명 3-4줄 정도 권고)*

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

**취약점 설명**

|  |  |
| --- | --- |
| **Case 1** | 게시판 작성 (Case가 2개 이상일때만 작성) |

Step 1) 게시판 > 글쓰기 페이지 접근

|  |
| --- |
|  |

Step 2) 프록시 도구를 이용하여 악성스크립트 삽입

|  |
| --- |
| 스크립트 구문 <script>alert(document.cookie)</script> |
|  |

Step 3) 악성스크립트 동작 확인

|  |
| --- |
|  |

*스크린샷 너비 : 14 (권장 스크린샷 설정 너비: 1024 / 높이: 700, 14 x 9.57 / 그림테두리 색상-Black 두께-3/4pt )*

1. CloudWatch 실습
   1. 대시보드 생성 (\*개별 작성\*)\_

|  |  |
| --- | --- |
| 텍스트, 소프트웨어, 컴퓨터 아이콘, 웹 페이지이(가) 표시된 사진  자동 생성된 설명 | |
| **이름** | 홍길동 |
| **Logs Insights Query** | fields @timestamp, @message  | stats count(status) by path, status  | sort @timestamp desc |
| **설명** | 로그 그룹에서 path, status에 대한 status 이벤트 수를 보여줌 |

https://docs.aws.amazon.com/ko\_kr/AmazonCloudWatch/latest/logs/CWL\_AnalyzeLogData-discoverable-fields.html