INFO & DMS

2021

WSC

Web Security Consulting With DMS

Project Report

1. 웹 보안 컨설팅

1.1. 웹 보안

해킹이란 본래의 의도와는 다른 동작을 일으키거나 주어진 권한 이상으로 정보를 열람, 복제, 변경 가능한 행위를 뜻하며 웹 해킹은 이러한 해킹이 웹 애플리케이션에서 발생하는 것이다. 이 웹 해킹을 사전에 취약점 진단을 통해 막거나 발생을 막고, 대처하는 등의 모든 과정을 웹 보안이라고 한다.

1.2. 웹 보안 컨설팅 프로젝트

웹 보안 컨설팅이란 현재 운영상태 혹은 운영 예정 상태인 웹 사이트 개발팀의 요청으로 사이트를 분석하여 발견된 취약점의 특징, 영향, 대응 방안 등을 종합적으로 리포트에 취합하여 사이트 개발진에게 제공하는 동아리 프로젝트이다.

1.3. 웹 보안 컨설팅 프로젝트의 목표

본 프로젝트의 취약점 분석 활동을 통해 위에 기술한 사항과 같은 실제 업무환경과 비슷한 환경에서 최소한의 간접적인 모의 해킹 작업을 진행하도록 하여 각 취약점에 대한 이해도의 향상과 연구 활동 및 경험을 쌓아 각자의 실력을 향상한다. 또한 각 동아리가 전공 분야를 초월한 협력을 통해 긍정적인 관계를 형성할 수 있도록 하고 보안 관련 경력으로 동아리원들이 자신 있게 자기소개서에 기술할 수 있는 것을 동아리의 목표로 두었다.

2. 취약점 리포트

2.1. 프로젝트 설명

본 프로젝트는 교내의 타 동아리에서 개발한 웹 사이트를 INFO의 웹 사이트 분석팀이 분석해 제목, 목표, 분류, 발견자, 발견일자, 취약점 명칭, 분석 내용을 작성해 제공하는 것이다.

2.2. 프로젝트 참여 인원

2021년 하반기 웹 보안 컨설팅 프로젝트에 동아리 INFO 2학년 신희원, 이주석, 김민제 학생이 참가하여 리포트를 작성하였다. 분석 목표가 되는 DMS는 새롭게 개발한 서비스가 아닌 본래 있던 서비스를 유지/보수하여 관리하였기 때문에 현재 DMS의 유지/보수를 맡고 있는 동아리 DMS에게 동의를 받았다.

2.3. 프로젝트 진행 합의

제 1항. 본 프로젝트의 분석 대상은 DMS이다.

제 2항. 본 프로젝트는 2021년 9월 13일부터 2021년 11월 14일까지 진행한다.

제 3항. 본 프로젝트의 분석 대상은 서비스의 소스 코드를 제공하여 분석팀이 유사한 가상 서비스를 구축할 수 있도록 하여 실제 서비스의 사용에 영향이 가지 않도록 한다

제 4항. 관리자 페이지의 경우 API를 통해 직접 연결되기 때문에 관리자 페이지에서 직접적으로 영향이 갈 수 있는 공격이나 테스트는 금지한다.

제 5항. 사이트의 서비스 운영에 심각한 손해를 입힐 가능성이 존재하고 학생들이 비교적 수월하게 악용할 수 있는 취약점의 경우, 그 즉시 운영진에게 즉각적으로 전달한다.

제 6항. 웹 취약점 스캐너의 사용을 허가한다.

제 7항. 본 분석 활동을 위한 계정을 만드는 것은 거부한다. 그 때문에 각 참가자 개인의 계정을 통해 프로젝트를 진행한다.

추가 사항. 2021년 11월 13일부로 프로젝트의 진행 기간을 2021년 12월 11일까지로 연장하였다.

3. 분석

3.1. 사이트 분석 결과

1. 관리자 페이지 노출

목표	DMS
제목	관리자 페이지 노출
분류	취약점
발견자	신희원
발견일자	2021년 10월 14일
취약점 명칭	보안 설정 오류

- 발견 경위

관리자 페이지 노출 테스트를 위하여 점검을 진행하였다. 추측하기 쉬운(/admin, /manager, /master, /system, /administrator 등)의 명칭을 사용하는 디렉터리 및 파일 관리자 페이지 존재 여부를 확인했다.

- 취약점 설명

웹 어플리케이션의 전반적인 기능 설정 및 회원 관리를 할 수 있는 관리자 페이지가 추측 가능한 형태로 구성되어 있을 경우 공격자가 관리자 페이지에 쉽게 접근할 수 있으며 무차별 대입 공격을 통해 관리자 권한을 획득할 수 있는 취약점이다.

- 공격 기법

웹 관리자의 권한이 노출될 경우 홈페이지의 변조뿐만 아니라 취약성 정도에 따라서 웹 서버의 권한까지도 노출될 수 있다.

- 공격 시나리오

무차별 대입 공격을 통해 관리자 페이지에 접속을 시도할 수 있다. 만약 공격이 성공한다면 관리자 페이지에 공격자가 로그인하여 서비스에 심각한 영향을 줄 수 있다. 또한 관리자 페이지 기준 권한 이하의 타 디렉토리에 접근이 가능하면 서비스의 운영이 반영구적으로 불가능 할 수 있다.

- 예상 피해

무차별 대입 공격을 통해 관리자 페이지에 접속을 시도할 수 있다. 만약 공격이 성공한다면 관리자 페이지에 공격자가 로그인하여 서비스에 심각한 영향을 줄 수 있다. 또한 관리자 페이지 기준 권한 이하의 타 디렉토리에 접근이 가능하면 서비스의 운영이 반영구적으로 불가능 할 수 있다.

- 대처 방안

가장 좋은 해결책은 관리자 페이지의 주소를 쉽게 예상할 수 없도록 설정하고, 관리자 페이지를 사용하는 인원이 고정되어 있거나 장소가 고정되어 있다면 MAC 주소 혹은 IP주소를 사용해 화이트 리스트 방식으로 접근을 통제하는 방법이 있다.

- 참고 자료

https://skynarciss.tistory.com/22

2. 관리자 패스워드 정책 부제

목표	DMS
제목	관리자 패스워드 정책 부제
분류	취약점
발견자	신희원
발견일자	2021년 10월 14일
취약점 명칭	식별 및 인증오류

- 발견 경위

무차별 대입 공격을 통한 관리자 페이지 로그인 시도가 서비스 관련 운영 사항으로 금지권고를 받아서 중지하고, 공격자가 유추한 ID 및 PASSWORD로 로그인을 다수 시도하자 성공했다.

- 취약점 설명

패스워드 유추가 쉽고, 구조가 단순하여 사회공학해킹 혹은 무차별 대입 공격 등을 하기 쉽다.

- 공격 기법

유추를 통한 아이디 및 패스워드 해킹 시도 혹은 무차별 대입 공격으로 탈취가 가능하다.

- 공격 시나리오

무차별 대입 공격 해킹 툴을 사용하거나 파이썬 등으로 쉽게 제작하여 포함될 것으로 예상되는 단어의 리스트와 아이디 및 패스워드의 길이, 구성 요소를 지정하고 실행하면 손쉽게 계정이 탈취될 것이다.

- 예상 피해

관리자 계정이 탈취됨에 따라 안정적인 서비스의 운영이 불가능하다.

- 대처 방안

관리자의 패스워드를 최소 8글자 이상으로 제한하고 영어 소문자, 영어 대문자, 숫자, 특수문자 모두를 강제적으로 사용하게 한다.

- 참고 자료

http://m.elec4.co.kr/article/articleView.asp?idx=27028

3. 관리자 로그인 횟수 제한 부제

목표	DMS
제목	관리자 로그인 횟수 제한 부제
분류	취약점
발견자	신희원
발견일자	2021년 10월 14일
취약점 명칭	식별 및 인증오류

- 발견 경위

관리자 페이지 접근이 허용된 상황에서 무차별 대입 공격을 시도하기 위해 로그인 관련 정책을 확인하던 중 발견했다.

- 취약점 설명

로그인 시도 횟수에 제약을 주지 않는다면 공격자는 툴 혹은 공격 코드를 이용하여 무차별 대입 공격을 시도해 사용자의 로그인 정보를 얻을 수 있다.

- 공격 기법

간단한 파이썬 코드를 사용하 무차별 대입 공격을 시하려고 하였으나, 관리자 페이지가 API를 통해 본 서버와 연결되어 있는 관계로 본 서버에 피해를 주지 않기 위해 공격을 가하지는 않았다. 그러나 유추한 아이디와 비번이 실제로 작용되는 것을 보아 무차별 대입 공격 과정도 그리 어렵지 많은 않았을 것으로 유추된다. 아이디와 비번이 동일하고 영어 소문자만으로 이루어진 8줄의 아이디와 패스워드는 하루면 충분히 탈취될 것이다.

- 공격 시나리오

파이썬 공격 코드 혹은 버프 스위트의 기능을 통해 문자 1~10기준, 영어 소문자, 대문자, 특수문자 점진적 증가를 통해 각각의 효율적인 방식으로 무차별 대입 공격을 진행. 현재 유추 작업을 통해 알아낸 ID:dsmadmin과 PASSWORD:dsmadmin은 8글자 영어 소문자로만 이루어져 있기에 단시간에 알 수 있다.

- 예상 피해

관리자 계정이 탈취됨에 따라 안정적인 서비스의 운영이 불가능하다.

- 대처 방안

관리자 로그인 페이지에 대한 로그인 횟수를 제한해야 한다.

- 참고 자료

http://gnujava.com/board/article_view.jsp?article_no=7143&menu_cd=16&idx_notice=NOTICE_FLAG+DESC%2C&board_no=3

4. 일반 회원 패스워드 정책 부제

목표	DMS
제목	일반 회원 패스워드 정책 부제
분류	취약점
발견자	신희원
발견일자	2021년 10월 21일
취약점 명칭	식별 및 인증오류

- 발견 경위

일반 회원이 회원가입 시도를 하는 경우에 대해 분석하여 나온 취약점이다.

- 취약점 설명

일반 회원이 회원가입을 시도할 때, 서비스 자체에서 패스워드 정책에 관한 설정 사항을 요구하지 않는다. 일부 회원의 패스워드가 보안 정책에서 권장하는 사항에 맞지 않게 설정됨에 따라, 무차별 대입 공격 또는 사회공학해킹 등을 통해 패스워드를 유추할 수 있다.

- 공격 기법

유추를 통한 아이디 및 패스워드 해킹 시도 혹은 무차별 대입 공격으로 탈취가 가능하다.

- 공격 시나리오

무차별 대입 공격 해킹 툴을 사용하거나 파이썬 등으로 쉽게 제작하여 포함될 것으로 예상되는 단어의 리스트와 아이디 및 패스워드의 길이, 구성 요소를 지정하고 실행하면 손쉽게 게정이 탈취될 것이다.

- 예상 피해

계정이 탈취됨에 따라 사칭, 테러 등등의 서비스 운영에 피해를 줄 수 있다. 또한, 타 학생의 개인정보를 빼앗을 수 있다. 혹은 악의적으로 피해를 주기 위한 수단으로 이용될 수 있다.

- 대처 방안

계정이 탈취됨에 따라 사칭, 테러 등등의 서비스 운영에 피해를 줄 수 있다. 또한, 타 학생의 개인정보를 빼앗을 수 있다. 혹은 악의적으로 피해를 주기 위한 수단으로 이용될 수 있다.

- 참고 자료

http://m.elec4.co.kr/article/articleView.asp?idx=27028

5. 일반 회원 로그인 횟수 제한 부제

목표	DMS
제목	일반 회원 로그인 횟수 제한 부제
분류	취약점
발견자	신희원
발견일자	2021년 10월 21일
취약점 명칭	식별 및 인증오류

- 발견 경위

무차별 대입 공격을 시도하기 위해 로그인 관련 정책을 확인하던 중 발견했다.

- 취약점 설명

로그인 시도 횟수에 제약을 주지 않는다면 공격자는 툴 혹은 공격 코드를 이용하여 무차별 대입 공격을 시도해 사용자의 로그인 정보를 얻을 수 있다.

- 공격 기법

로그인 시도 횟수에 제약을 주지 않는다면 공격자는 툴 혹은 공격 코드를 이용하여 무차별 대입 공격을 시도해 사용자의 로그인 정보를 얻을 수 있다.

- 공격 시나리오

파이썬 공격 코드 혹은 버프 스위트의 기능을 통해 문자 1~10기준, 영어 소문자, 대문자, 특수문자 점진적 증가를 통해 각각의 효율적인 방식으로 무차별 대입 공격을 진행. 현재 동의를 구하고 알아본 동아리원 학생의 아이디 패스워드를 확인한 결과 패스워드 보안 정책에 부합하지 않은 패스워드를 보유한 이용자가 존재하기 때문에 충분히 탈취가 가능하다.

- 예상 피해

계정이 탈취됨에 따라 사칭, 테러 등등의 서비스 운영에 피해를 줄 수 있다. 또한, 타 학생의 개인정보를 빼앗을 수 있다. 혹은 악의적으로 피해를 주기 위한 수단으로 이용될 수 있다.

- 대처 방안

로그인 페이지에 대한 로그인 횟수를 제한해야 한다.

- 참고 자료

http://gnujava.com/board/article_view.jsp?article_no=7143&menu_cd=16&idx_notice=NOTICE_FLAG+DESC%2C&board_no=3

6. 외출 신청 외출 사유 입력 수 제한 없음

목표	DMS
제목	외출 신청 외출 사유 입력 수 제한 없음
분류	취약점
발견자	김민제
발견일자	2021년 10월 21일
취약점 명칭	안전하지 않은 설계

- 발견 경위

외출 신청 페이지에서 외출 사유를 적는 텍스트 칸에 "테스트"라는 문자열을 계속해서 복사, 붙여넣기를 하여 입력 수 제한을 테스트했는데 무한정으로 텍스트가 입력되는 것을 확인하였다.

- 취약점 설명

이 취약점은 HTML 또는 JS에서 글자 수 제한을 안 걸어 놓은 것이 원인이다. 많은 양의 텍스트 데이터를 서버에 전송함으로써 순간적으로 서버의 자원을 낭비하여 부하를 일으킨다.

- 공격 기법

https://www.dsm-dms.com/apply/goingout에서 외출목록에서 '+'을 눌러 외출신청 입력 칸을 띄우고 외출 사유에 되도록 많은 양의 텍스트를 입력한 후 '신청'버튼을 눌러서 서버에 부하를 준다.

- 공격 시나리오

먼저 공격자가 DMS 임의의 계정 혹은 본인의 계정으로 로그인한 후 https://www.dsm-dms.com/apply/goingout에 접속한다. 그리고 외출사유에 많은 텍스트를 입력한 후 "신청" 버튼을 눌러 서버에 전송한다, 이 과정을 반복 또는 자동화하면 서버가 텍스트를 처리하는 동안 외부 사용자의 서비스 요청을 처리하지 못한다.

- 예상 피해

서버의 자원이 계속해서 낭비되어 서비스 불가 또는 성능 저하가 나타난다.

- 대처 방안

HTML에서 maxlength 속성을 명시를 하거나, JS로 클라이언트에서 서버로 텍스트가 전송되기 전에 문자열을 HTML에서 명시한 글자 수만큼 잘라서 전송한다. 이 대처방안을 도입하면 JS에서 강제로 글자수를 제한하기 때문에 서버에 부하가 가지 않는다.

- 참고 자료

https://www.dsm-dms.com/apply/goingout

https://squll1.tistory.com/entry/javascript-문자열-자르기-split-substring-substr

https://hianna.tistory.com/435

7. 로깅 및 모니터링 관리 불가 상태

목표	DMS
제목	로깅 및 모니터링 관리 불가 상태
분류	취약점
발견자	신희원
발견일자	2021년 10월 26일
취약점 명칭	보안 로깅 및 모니터링 실패

- 발견 경위

관리자 계정 탈취 이후, 공격자에 대한 추적 대책을 개발진에게 물었고 그 때에 대화를 통해 알 수 있다.

- 취약점 설명

보안 로깅 및 모니터링 실패는 사고 대응의 비효율적인 통합 또는 누락과 함께 공격자들이 시스템을 더 공격하고, 지속성을 유지하며, 더 많은 시스템을 중심으로 공격할 수 있도록 만들고, 데이터 변조, 추출 또는 파괴할 수 있다. 대부분의 침해 사례에서 침해를 탐지하는 기간이 200일이 넘는 통계 결과가 존재하고, 이는 일반적으로 내부 프로세스와 모니터링보다 외부 기관의 의심에 의한 감지 덕분에 탐지된다.

- 공격 기법

어떠한 공격 혹은 내부 문제가 발생할 경우, 안정적인 로깅과 모니터링이 불가능 함에 따라 즉각적인 대처가 불가능하다. DMS 같은 학생이 개발하고 운영하는 사이트의 경우 외부 기관의 관심을 받기 어려우며 로깅 및 모니터링이 불충분하다면 침해를 영원히 탐지하지 못 할 수도 있다.

- 공격 시나리오

계정을 탈취하여 웹 사이트에 접근에 보안 취약점을 이용하여 공격을 시행했다. 그러나 그를 확인하고 대처할 방안이 없어 계정 소유자가 개발진에게 전달하기 전까지 이를 탐지하고 못하고 방치하게 된다. 그 사이에 발생하는 피해는 충분히 막을 수 있었으나 막지 못한 피해가 된다.

- 예상 피해

계정 탈취 탐지 불가, 네트워크 공격 탐지 불가, DB 에러 확인 불가, 서버 이상 탐지 불가, 계정 권한 탐지 불가 등등 각종 권한 및 운영에 대한 문제점 확인 불가.

- 대처 방안

로깅 및 모니터링 인원을 특정해 배치하고 원활한 인수인계를 통해 유지되도록 한다. 현실적으로 로깅 및 모니터링을 24시간 할 수 없으므로, 최소 일주일에 한번 정도로 점검해야 한다고 권유한다.

- 참고 자료

https://ichi.pro/ko/a09-2021-boan-loging-mich-moniteoling-silpae-150365786469798

8. DB 세션 관리 미흡

목표	DMS
제목	DB 세션 관리 미흡
분류	취약점
발견자	이주석
발견일자	2021년 10월 26일
취약점 명칭	안전하지 않은 설계

- 발견 경위

기숙사에서 방송으로 공지가 올라왔다고 안내할 때가 있는데, DMS 앱으로 확인할 때마다 공지가 안 뜨는 경우가 자주 발생해, 에러 코드를 확인한 결과 500에러가 뜬다는 것을 확인했다.

- 취약점 설명

코드를 분석해본 결과, model에서 기본적인 모델로 사용하는 mixin.py에서 DB 세션 생성 후 close를 하지 않는다. DMS에서 사용하는 DB는 샘플서버 기준으로 MySQL인데, MySQL의 동시 접속 가능한 수는 기본적으로 100이며, 실 서비스는 AWS lambda를 사용하기 때문에 사용 횟수에 따라 돈이 부과되므로 우리 학교 학생 수를 고려해 더 줄였을 것이다. 또한 AWS 자체적으로 자주 사용하는 API는 더 빠른 호출을 위해 따로 관리하는 특징이 있어 이미 응답처리를 한 lambda 함수가 DB 세션을 종료하지 않아 다른 함수에서 사용할 수 있는 여유 session의 개수가 부족하여 DB에 접속하지 못하는 문제가 발생하는 것으로 보인다.

- 공격 기법

DB 세션에 접근하는 모든 api (auth, apply)에 동시 접속해 다른 접속자들이 서비스를 이용하지 못하게 한다.

- 공격 시나리오

공격자가 굳이 공격을 할 필요도 없이, 동시 접속자가 늘어나는 상황이 생기는 경우 접속자들이 서비스를 이용하지 못하는, DoS 공격이 성립되는 것이다. 이는 곧 동시 접속자를 조금만 늘려도 DoS 공격이 성립되는 것으로, 코드 상으로 충분히 막을 수 있음에도 불구하고 그 여지를 남겨두는 것이다.

- 예상 피해

DoS 공격에 대한 피해와 같다. 동시 접속자의 수가 늘어나면 접속자는 그 서비스를 이용하지 못하는 상황이 생긴다.

- 대처 방안

DB에 대한 커넥션을 각 API가 종료될 시 닫아주는 코드인 "`db.session.remove()`"를 추가한다.

- 참고 자료

없음

9. DB 세션 관리 미흡

목표	DMS
제목	DB 세션 관리 미흡
분류	취약점
발견자	이주석
발견일자	2021년 10월 26일
취약점 명칭	안전하지 않은 설계

- 발견 경위

기숙사에서 방송으로 공지가 올라왔다고 안내할 때가 있는데, DMS 앱으로 확인할 때마다 공지가 안 뜨는 경우가 자주 발생해, 에러 코드를 확인한 결과 500에러가 뜬다는 것을 확인했다.

- 취약점 설명

코드를 분석해본 결과, model에서 기본적인 모델로 사용하는 mixin.py에서 DB 세션 생성 후 close를 하지 않는다. DMS에서 사용하는 DB는 샘플서버 기준으로 MySQL인데, MySQL의 동시 접속 가능한 수는 기본적으로 100이며, 실 서비스는 AWS lambda를 사용하기 때문에 사용 횟수에 따라 돈이 부과되므로 우리 학교 학생 수를 고려해 더 줄였을 것이다. 또한 AWS 자체적으로 자주 사용하는 API는 더 빠른 호출을 위해 따로 관리하는 특징이 있어 이미 응답처리를 한 lambda 함수가 DB 세션을 종료하지 않아 다른 함수에서 사용할 수 있는 여유 session의 개수가 부족하여 DB에 접속하지 못하는 문제가 발생하는 것으로 보인다.

- 공격 기법

DB 세션에 접근하는 모든 api (auth, apply)에 동시 접속해 다른 접속자들이 서비스를 이용하지 못하게 한다.

- 공격 시나리오

공격자가 굳이 공격을 할 필요도 없이, 동시 접속자가 늘어나는 상황이 생기는 경우 접속자들이 서비스를 이용하지 못하는, DoS 공격이 성립되는 것이다. 이는 곧 동시 접속자를 조금만 늘려도 DoS 공격이 성립되는 것으로, 코드 상으로 충분히 막을 수 있음에도 불구하고 그 여지를 남겨두는 것이다.

- 예상 피해

DoS 공격에 대한 피해와 같다. 동시 접속자의 수가 늘어나면 접속자는 그 서비스를 이용하지 못하는 상황이 생긴다.

- 대처 방안

DB에 대한 커넥션을 각 API가 종료될 시 닫아주는 코드인 "`db.session.remove()`"를 추가한다.

- 참고 자료

없음

10. 디버그 모드로 켜져 있는 서버

목표	DMS
제목	디버그 모드로 켜져 있는 서버
분류	취약점
발견자	이주석
발견일자	2021년 11월 11일
취약점 명칭	보안 설정 오류

- 발견 경위

dms 자습실 자리 신청 부분에서 어떠한 취약점이 발생할 것인지 찾는 도중 시간대를 입력하는 부분에서 발견되었다.

- 취약점 설명

사용자 요청에 500에러가 발생하는 것도 모자라 500에러 발생 시 출력되는 디버그 내용이 응답으로 사용자에게 보내진다.

- 공격 기법

자리 신청 시, 보내는 요청인 POST /apply/extension/12 에서 11, 12시 연장신청 기능을 나타내는 12 부분을 다른 숫자로 변경해 요청을 보냈을 때 500 에러 메시지와 동시에 디버그 내용이 응답으로 오면서 소스 코드를 노출시킨다.

- 공격 시나리오

위 api에서 500에러와 에러 메시지를 보낸다는 것은 서버 전체가 디버그 모드로 켜져 있음을 파악할 수 있고, 이는 github에 공개되지 않는 config 파일을 참조하는 api나 소스코드들을 확인 할 수 있다.

- 예상 피해

일단 가장 첫 번째로 500 에러가 뜬 다는 것은 서버의 코드에 사용자의 값에 대한 제대로 된 검증 및 예외 처리가 미흡하는 점을 나타낸다. 두 번째로 비록 위 서비스의 소스코드를 깃허브에 올려놓았다고 하지만 토큰 키 값이나 .env 파일 등 숨겨야 하는 값들이 있는데, 500 에러와 더불어 디버그 내용을 응답으로 보내주기 때문에 소스코드 정보 유출 및 서버가 디버그 모드로 실행되고 있음을 파악하고, 다른 api에서 500 에러를 유발해 깃허브에 올려놓지 않은 secret 값을 얻어낼 수도 있다.

- 대처 방안

서버를 실행시킬 때 디버그모드가 아니라 배포용 모드로 실행시켜야 500 에러가 떠도 디버그 메시지가 사용자에게 가지 않는다.

- 참고 자료

없음

11. 관리자 외출자 관리 페이지 접속 가능 버그

목표	DMS
제목	관리자 외출자 관리 페이지 접속 가능 버그
분류	버그
발견자	신희원
발견일자	2021년 10월 21일
취약점 명칭	없음

- 발견 경위

관리자 페이지의 로그인 권한없이 접근할 수 있는 모든 경로를 찾아서 나온 단 하나의 경로이다.

- 버그 설명

관리자 페이지에 로그인도 하지 않고 관리자만 들어갈 수 있는 페이지에 접근을 허용했으니 해당 사항은 본래 취약점으로 분류되어야 한다. 그러나 외출 신청을 한 내용 자체는 권한 부족으로 인해 막혀 볼 수 없다. 때문에 이는 취약점이 아닌 버그로 분류되었다. 이 버그가 발생한 이유는 타 경로의 접근은 막았지만 실수로 해당 경로는 열어 놓은 개발자에게 있다.

- 버그 효과

해당 버그로 인해 관리자 페이지의 내부 구조를 알 수 있다. 접근이 된다는 것은 일부지만 내부의 통로를 열어준 것과 같기 때문이다.

- 예상 피해

해당 버그로 인해 관리자 페이지의 내부 구조를 알 수 있다. 접근이 된다는 것은 일부지만 내부의 통로를 열어준 것과 같기 때문이다.

- 대처 방안

다른 경로는 관리자로 로그인하지 않고 접근할 시, 접근이 불가능하게 박히고 리다이렉트한다. 이 페이지도 같은 원리로 막으면 된다.

- 참고 자료

https://www.dsm-dms.com/admin/goingout → 접근이 가능하다.

12. 백엔드 서버에서 비밀번호 공한 체크 안함

목표	DMS
제목	백엔드 서버에서 비밀번호 공란 체크 안함
분류	버그
발견자	김민제
발견일자	2021년 10월 26일
취약점 명칭	없음

- 발견 경위

dsm-dms.com에서 비밀번호 변경 칸에 공란을 사용할 수 없도록 설정이 되어 있는데 burp suite 웹 프록시로 값을 바꿀 비밀번호를 공란으로 변경하여 전송하니 공란으로 비밀번호가 변경되었다.

- 버그 설명

https://www.dsm-dms.com/에서 내 정보에 들어가고 burp suite 프록시를 설정한 후 비밀번호 변경을 시도한다. 그러면 burp suite에 비밀번호 변경 JSON이 잡히게 된다. JSON값을 "{"currentPassword":"현재 비밀번호","newPassword":""}"와 같이 변경하고 전송하면 공란이 비밀번호로 설정되고 웹 프록시 도구를 사용하지 않는 이상 로그인의 공란 체크로 인하여 정상적으로 이 계정에 로그인할 수 없다.

- 버그 효과

이 버그로 인해 프론트에서 제한한 공란 입력이 백엔드에서 체크하지 않아 비밀번호가 공란으로 설정되어 계정을 사용할 수 없다.

- 예상 피해

이 버그를 악용하면 남의 계정을 알고 있는 경우에 계정을 더 이상 쓸 수 없도록 잠그는게 가능하다.

- 대처 방안

백엔드에서 newPassword에 대해서 공란을 체크하여 오류를 반환한다.

- 참고 자료

파이썬 문자열 체크

12. 회원가입 요구 파라미터 다름

목표	DMS
제목	회원가입 요구 파라미터 다름
분류	버그
발견자	이주석
발견일자	2021년 12월 2일
취약점 명칭	없음

- 발견 경위

회원가입 기능에 취약점 분석을 진행하던 중 발견된 버그이다.

- 버그 설명

현재 Backend 코드를 보면 회원가입 시 개인 고유의 확인 코드와 id, password를 입력 받던 예전 방식이 아닌 id, password, name, number와 모두에게 동일한 key값을 요구한다. 하지만 Frontend에서 Backend로 요청을 보낼 때는 과거의 방식과 같이 코드를 전송한다. 결국 회원가입을 시도할 때 400 에러가 뜨는 상황이다. 이건 Frontend와 Backend의 소통 부재로 생긴 버그로 보인다.

- 버그 효과

위 버그 시점 기준으로 유지될 시 회원가입을 하지 못한다.

- 예상 피해

만약 내년 3월까지 수정을 하지 않고, 과거와 같이 개인코드를 각자 나눠주면 모두가 회원가입을 하지 않는 불상사가 생긴다.

- 대처 방안

Frontend에서 회원가입 페이지를 Backend의 기능명세에 맞게 수정한다.

- 참고 자료

없음

13. 월초 급식 업데이트 부진

목표	DMS
제목	월초 급식 업데이트 부진
분류	버그
발견자	신희원
발견일자	2021년 11월 1일
취약점 명칭	없음

- 발견 경위

아침 급식 메뉴 확인 중, 급식 업데이트가 느린 점을 발견했다.

- 버그 설명

API에서 급식 목록이 오지 않는다. API 오류 혹은 매크로를 통한 정규화 오류일 가능성이 높다. 혹은 매크로가 돌아가는 시간대에 대한 설정 오류일 수도 있다.

- 버그 효과

급식 목록 제공 서비스의 원활한 이용이 불가하다.

- 예상 피해

급식을 확인하지 못함. 핵심 서비스 이용이 불가하다.

- 대처 방안

API 수정 혹은 매크로를 수정한다.

- 참고 자료

없음

14. 실제로 존재하지 않는 페이지 예외 처리 없음

목표	DMS
제목	실제로 존재하지 않는 페이지 예외 처리 없음
분류	요구사항
발견자	김민제
발견일자	2021년 10월 19일
취약점 명칭	없음

- 요구 사항

실제로 존재하지 않는 페이지 경로에 아무런 오류 코드도 출력되지 않는다.

- 추가기능 설명

실제로 존재하지 않는 페이지는 적절한 오류 코드를 출력하거나, 홈페이지로 리다렉트될 수 있도록 수정한다.

- 참고 자료

https://www.dsm-dms.com/notfoundneededbypage

15. 외출 신청 칸 입력 범위 유효하지 않음

목표	DMS
제목	외출 신청 칸 입력 범위 유효하지 않음
분류	요구사항
발견자	김민제
발견일자	2021년 10월 21일
취약점 명칭	없음

- 요구 사항

외출 신청칸에서 외출 날짜칸이 0~12, 0~31로 설정되어 있고, 외출 시각이 0~24시 0~59분 ~ 0~24시 0~59분 로 설정되어 있다. 날짜를 1~12월 1~31일로 외출 시각의 시, 분에서 시를 0~23시으로 설정을 바란다.

- 추가기능 설명

HTML 파일에서 수정하면 된다.

- 참고 자료

https://www.dsm-dms.com/apply/goingout

16. 비밀번호 찾기 기능 부제

목표	DMS
제목	비밀번호 찾기 기능 부제
분류	요구사항
발견자	신희원
발견일자	2021년 11월 5일
취약점 명칭	없음

- 요구 사항

비밀번호 분실 시, 온라인을 통해 원활하게 해결 받을 수 없다.

- 추가기능 설명

회원가입 시 사용한 메일로 ID 입력 시, ID에 해당하는 메일에 비밀번호 변경 페이지를 첨부한다.

- 참고 자료

https://sowon-dev.github.io/2020/10/31/201101findpw/

4. 결론

4.1. 사이트 보안성 평가

전체적으로 보안의 수준은 낮은 정도였다고 결론지었다. 가장 핵심적인 문제점은 취약점의 양이 저번 분석에 비해 압도적으로 많았다는 점과 관리자 계정이 쉽게 뚫렸다는 점이다. 또한 버그 중 일부는 시간과 힌트만 주어졌다면 계정의 탈취보다 더욱 심각한 취약점으로 발달할 수 있던 부분이 존재했다. 본 프로젝트가 "웹" 취약점 분석 프로젝트여서 서술하지 않는 기타 WinApp 취약점도 존재하였으며 해당 취약점도 상당히 위험한 취약점이었다. 이러한 결과를 바탕으로 이 웹사이트의 보안 수준을 [상/중/하]로 평가할 때 [하] 정도였다고 결론을 내렸다.

4.2. 일정 관리 문제

일정은 이번 프로젝트에서도 연장을 요청하게 되었다. 가장 큰 문제는 학생이라는 특수한 직업 환경에서 발생하는 스케줄의 복잡함과 구체적인 취약점이 예측된 기간내에 도출되지 않는다는 문제점이다. 그 외 부가적인 요소로서 애초에 분석자가 적은 문제점도 있지만 해당 사항은 프로젝트가 아직 초창기임으로 시간이 자연스럽게 해결해 줄 것이라 믿는다. 학생 신분의 문제는 졸업과 버그바운티 형태의 프로젝트로 발전함에 따라 해결될 것이고 구체적인 취약점 도출은 단순 실력 문제인데 이 점은 반복되는 데이터를 통해 숙련해야 할 것 같다. 또한 이 반복되는 데이터를 사용해 DB를 구축하여 중복되는 취약점은 자동으로 처리할 수 있도록 노력해야 할 것이다.

4.3. 팀원 관리 문제

학교 측에 제출한 기획서에 서술된 분석 인원보다 리포트에 작성된 분석 인원의 수가 적었다. 이는 프로젝트 참여자 중 무책임하게 떠넘기거나 중간에 탈퇴를 하여 발생한 사항으로 버그바운티 형식으로 발전함에 따라 해결할 수 있을 것이라 예상된다.

4.4. 분석 정리 문제

분석 자체의 진행은 일정 관리와 실력의 문제 등을 포함하여 예상하지 못한 상황이 발생하였음에도 불구하고 수월하게 진행되어 분석된 취약점 및 버그 등에 관한 내용의 양과 질은 준수하다고 생각된다. 하지만 이를 정확히 집계하고 내용을 정리하는 작업에 있어서 형식과 수순을 사전에 고지하지 않아 리포트의 작성 및 분석 결과를 재조사하면서 불편함이 있었다. 전과 같은 문제점이 다시 발생함에 따라 "자동화 구축"이라는 방안을 찾았고 현재 개발을 위해 노력중이다.

4.5. 각 팀원의 고찰

이주석 학생.
상반기 프로젝트 경험을 겪고 진행해 확실히 저번 프로젝트 보다는 좀 더 체계화되어서 좋았다. 전체적인 리포트의 개수는 줄었지만 저번보다 취약점의 비율이 높고, 유효한 취약점이 많이 발견되어 성과가 어느정도 나왔다고 생각된다. Wargame 프로젝트를 겸해 진행하느라 제대로 분석하지 못해서 너무 아쉬웠다. 이 프로젝트를 동아리 정기 프로젝트로 남기지 못해 아쉽지만 다행히 졸업 후에도 같이 하고자 하는 친구들 덕분에 팀을 구성하고 버그바운티 형태로 발전시켜 구성할 계획이다. 마지막으로 프로젝트 중간중간 우여곡절과 여러 일들이 많았지만 그래도 포기하지 않고 여러 일들이 많았지만 그래도 포기하지 않고 끝까지 따라와준 멤버들, 친구들에게 감사한다.

신희원 학생.
저번 프로젝트와 비교하여 버그보다 취약점이 많이 발견되었다. 아직 프로젝트 초창기라 데이터가 쌓여야 특수성을 도출할 수 있을 것 같다. 오래 운영된 사이트인 만큼 취약점이 많은 상태를 보고 업데이트 과정에서 발생한 취약점인지 기존에 있던 취약점인지 구분할 수 없었던 아쉬움이 있었다. 유지/보수를 개발자 분들이 잘 관리해 주셔서 소스코드 관련 소통이 원활했으면 좋았다고 생각한다.

김민제 학생.
DMS 서비스의 취약점이나 버그 등을 분석하면서 가지각색의 버그를 보았다. 특히 기억에 남는 버그는 비밀번호 변경과정에서 공란을 서버에서 체크하지 않는다고 하던가 또는, 일부 텍스트 입력 칸에는 적당한 입력 수 제한이 걸려있지 않는다는 것이다. 하지만 알려진 것과 같이 DMS 서비스의 가치는 높고, 밝혀진 버그들과 취약점을 점차 고쳐 나간다면, 좋은 서비스를 유지할 수 있을 것이다. 이번 프로젝트로 취약점에 대해 경각심을 더욱 느낄 수 있었다.

5. 부록

5.1. 진행 일정표

2021년 09월 01일
- DMS 취약점 분석 공식 요청.

2021년 09월 13일
- DMS 취약점 분석 공식 승인 후 분석 시작.

2021년 10월 14일

- [관리자 패스워드 정책 부제] 취약점 발견.
- [관리자 페이지 노출] 취약점 발견.
- [관리자 로그인 횟수 제한 부제] 취약점 발견.

2021년 10월 19일
- [실제로 존재하지 않는 페이지 예외 처리 없음] 요구사항 발견.

2021년 10월 21일
- [관리자 외출자 관리 페이지 접속 가능 버그] 버그 발견.

2021년 10월 21일
- [일반 회원 패스워드 정책 부제] 취약점 발견.
- [일반 회원 로그인 횟수 제한 부제] 취약점 발견.
- [외출 신청 칸 입력 범위 유효하지 않음] 요구사항 발견.
- [외출 신청 사유 입력 수 제한 없음] 취약점 발견.

2021년 10월 26일
- [로깅 및 모니터링 관리 불가 상태] 취약점 발견.
- [DB 세션 관리 미흡] 취약점 발견.
- [백엔드 서버에서 비밀번호 공란 체크 안 함] 버그 발견.

2021년 11월 01일
- [월초 급식 업데이트 부진] 버그 발견.

2021년 11월 05일
- [비밀번호 찾기 기능 부제] 요구사항 발견.

2021년 11월 11일
- [디버그 모드로 켜져있는 서버] 취약점 발견.

2021년 12월 02일
- [회원가입 요구 파라미터 다름] 버그 발견.

5.2. 보고서 작성 시 참고 자료

본 보고서는 INFO 웹 취약점 분석 프로젝트의 분석 결과에 기반하여 작성되었습니다.