

INFO & SEMICOLON;

2021

WSC

Web Security Consulting With
SEMICOLON;

Project Report

info



1. 웹 보안 컨설팅

1.1. 웹 보안

1.2. 웹 보안 컨설팅 프로젝트

1.3. 웹 보안 컨설팅 프로젝트의 목표

2. 취약점 리포트

2.1. 프로젝트 설명

2.2. 프로젝트 참여 인원

2.3. 프로젝트 진행 합의

3. 분석

3.1. 사이트 분석 결과

4. 평가

4.1. 사이트 보안성 평가

4.2. 일정 관리 문제

4.3. 팀원 관리 문제

4.4. 분석 정리 문제

4.5. 각 팀원의 고찰

5. 부록

5.1. 진행 일정표

5.2. 보고서 작성 참고 자료

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, 타겟(분석한 사이트), 명칭(공격 명칭), 우선순위(심각도 1(높음)~5(낮음)), 탐색일시, 발견자, 종류(취약점, 버그, 추가기능, 모바일 중) 등을 제공하는 프로젝트이다.

2.2. 프로젝트 참여 인원

2021년 상반기 웹 보안 컨설팅 프로젝트에 INFO 2학년 신희원, 이주석, 김민제, 고경태 학생과 3학년 민준혁, 손영웅, 심준호 학생이 참가하여 리포트를 작성하였으며 분석 목표 사이트인 대동여지도와 DSM_Auth에서는 SEMICOLON; 동아리의 2학년 안은결, 성예인, 정지원, 한준호, 조준서, 정지우, 이서준, 박상우, 손채건, 조호원 학생이 웹 사이트 개발팀으로 참가하였다.

2.3. 프로젝트 진행 합의

제 1항. 본 프로젝트의 분석 대상은 대동여지도와 DSM_Auth이다.

제 2항. 본 프로젝트는 2021년 3월 10일부터 2021년 4월 3일까지 진행한다.

제 3항. 본 프로젝트의 분석 대상은 서버를 자체적으로 운영함으로 서버에 무리가 갈 수 있는 무차별 대입 공격 혹은 분산 서비스 거부 공격 등의 기법을 이용해 모의 해킹을 하는 것은 금지한다. 단, 개발진의 허락하에 공격이 가능하다.

제 4항. 교내에서 학생을 대상으로 운영 중인 서비스이므로 서비스 이용에 무리가 가는 공격은 최대한 자제한다. 단, 공격은 하지 않으나 의심되는 취약점이 발견된다면 기술하여도 된다.

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 4월 3일부로 프로젝트의 진행 기간을 2021년 5월 15일까지로 연장하였다.

3. 분석

3.1. 사이트 분석 결과

취약점 분류

1. 취약한 인증 방식

타겟	DSM_Auth
명칭	취약한 인증 - Query문 노출
우선순위	우선순위 1위
탐색일시	2021년 3월 10일
발견자	신희원
종류	취약점

- 발견 경위

사이트에서 제공하는 서비스를 미리 살펴보던 중 발견했다.

- 공격 기법

우선 이 취약점은 취약한 인증 방식이라는 취약점으로 OWASP 2017에도 소개된 취약점이다. 여기서는 토큰 발급 시 서버에서 보내주는 code 값이 노출되는 것으로 발생하는 취약점이다.

해당 사이트는 로그인 시 다음과 같은 과정을 거친다. ID, PW, redirect_url, client_id를 body에 담아 보낸다. code, client_id, client_secret을 body에 담아 보낸다. 응답으로는 access_token과 refresh_token을 보내준다. 이 취약점이 해당 사이트에서 발생하는 이유는 리다이렉트 과정에서 노출되는 로딩 페이지에 code 값이 사용 뒤 만료되지 않고 계속 유지되기 때문이다. 로그인 시 리다이렉트 URL은 <https://ddyzd.dsmkr.com/callback?code={code값}> 형식인데, 위에서 설명했듯 code값이 만료되지 않아서 저 URL로 요청을 보내면 access_token을 발급해 로그인이 되는 것이다.

- 공격 시나리오

공격 시나리오는 다양하게 발생할 수 있다. code 값이 만료되지 않아 굳이 토큰을 힘들게 탈취할 필요 없이 URL에 노출되는 code값으로 access_token을 얻을 수 있기 때문이다. GET 방식으로 리다이렉트 되기 때문에 code값을 쉽게 찾을 수 있다. 예를 들어 타 컴퓨터에서 로그인을 했을 때 방문 기록을 살펴 URL에 노출되어 있는 code값으로 로그인이 가능하다. 한번 탈취한 리다이렉션 URL. 즉, code는 고정되어 있어서 여러 번 사용할 수 있다. 이 경우 URL의 callback?code={code값}에서 {code값}의 값을 무차별 대입 공격으로 알아낸다면 영구히 사용할 수 있다. 이 또한 계정 탈취를 당하는 것이다. code의 만료기간이 만약 길다면 수많은 로그인으로 code값이 겹쳐지는 경우가 발생해 타 계정으로 로그인이 될 가능성 또한 존재한다.

- 예상 피해

어떠한 공격 시나리오로 접근하건 최종적으로는 계정이 탈취당한다. 동아리장의 계정을 탈취당한다면 그것은 일반 유저의 계정을 탈취한 것보다 큰 피해를 끼칠 수 있다. 사이트 테러, 배너 변경, 프로필 변경, 게시물 삭제, 게시물 업로드, 테러, 탈취한 계정을 이용한 2차 공격, 사칭 등으로 계정 탈취를 통해 할 수 있는 악의적인 행동은 무궁무진하다.

- 대처 방안

위 사이트는 OAUTH형식의 로그인을 진행하고 있는데, 토큰 발급에 사용되는 code값의 만료기간을 최대한 짧게 설정하거나, 사용횟수를 지정해 code값을 만료해야 한다.

* 해당 취약점은 협의 사항 중 하나인 [사이트의 서비스 운영에 심각한 손해를 입힐 가능성이 존재하고 학생들이 비교적 수월하게 악용할 수 있는 취약점의 경우, 그 즉시 운영진에게 즉각적으로 전달한다.]의 규정에 따라 즉각적으로 개발진에게 전달되었다.

- 참고 자료

취약한인증 대처 - <https://bibimnews.com/entry/취약한-인증Broken-Authentication-사용자-정보보호를-위한-필수-보안-요소>
탈취한 토큰 값

안은결 (de2c522e-c48d-4b33-ab72-5bdeb1154f59)

이서준 (a3fa4249-3c36-4fc2-9c02-e7aa5ef2de18)

2. DSM_Auth 로그인 입력 수 무제한

타겟	DSM_Auth
명칭	버퍼 오버플로우
우선순위	우선순위 2위
탐색일시	2021년 3월 18일
발견자	김민제
종류	취약점

- 발견 경위

사이트에서 로그인, 비밀번호를 할 수 있는 페이지가 있다. 그런데 코드를 분석해 보니 코드에 입력 수 제한을 두고 있지 않았기 때문에 매우 긴 텍스트를 넣어 보면 서버에 영향을 줄 수 있겠다고 생각했다.

- 공격 기법

사이트에서 로그인, 비밀번호를 할 수 있는 페이지가 있다. 그런데 코드를 분석해 보니 코드에 입력 수 제한을 두고 있지 않았기 때문에 매우 긴 텍스트를 넣어 보면 서버에 영향을 줄 수 있겠다고 생각했다.

- 공격 시나리오

로그인 페이지에 약 50,000자를 넣고 입력하였다.

- 예상 피해

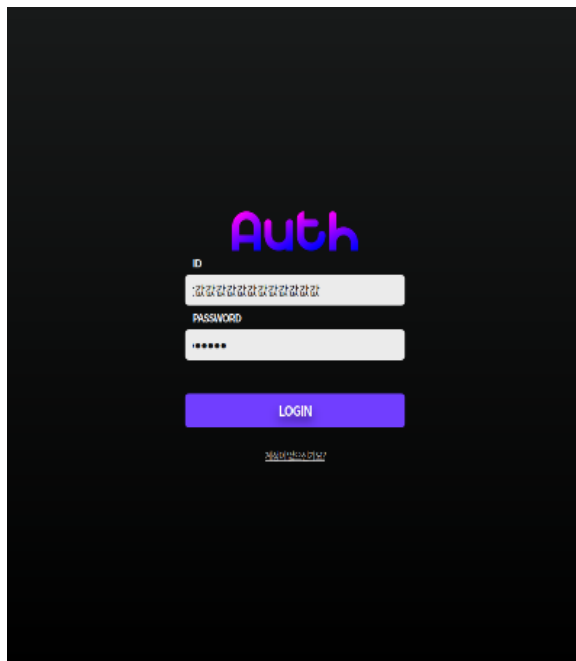
서버가 5만자를 입력하고 제출하였을 때 처리 속도가 약 3초가 느려졌다는 것을 확인하였다. 그런데 3초가 여러 번 시도 된다면 서버는 다운될 수밖에 없을 것이다. 그만큼 위험한 공격이라는 것이다. 이 로그인 페이지로 DOS 공격이 가능할 것이며, 왜 서버가 다운되었는지 영문도 모를 수 있는 위험이 있다.

- 대처 방안

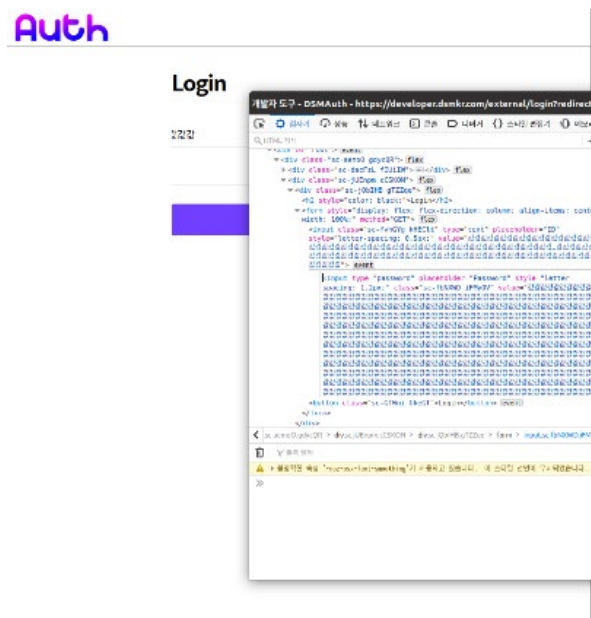
HTML에서 입력 수를 자르거나 input 태그에 `<input type="" maxlength="숫자">`로 최대 입력 글자 수를 제한하고, api로 데이터를 넘기기 전에 js를 활용하여 옆의 코드와 같이 데이터를 잘라 api로 전송하여도 된다.

- 참고 자료

공격화면(1)



공격화면(2)



```
function numbercheck(input) {
  if(input.value.length > input.maxLength) {
    input.value=input.value.slice(0, input.value.maxLength);
  }
}
```

3. 로그인 횟수 제한 부재

타겟	DSM_Auth
명칭	Brute Force
우선순위	우선순위 3위
탐색일시	2021년 3월 27일
발견자	손영웅
종류	취약점

- 발견 경위

로그인 관련 취약점의 탐색 중, 로그인 횟수 제한이 없다는 점을 발견했다.

- 공격 기법

무차별 대입 공격을 통해 로그인 시도를 할 경우, 로그인 시도에 대한 횟수 제한을 설정하지 않아 무차별 대입 공격이 성공할 수 있다.

- 공격 시나리오

무차별 대입 공격을 통해 로그인 시도를 자동화하여 불특정 다수의 계정을 탈취할 수 있다. 파이썬 코드를 활용하여 무차별 대입 공격 코드를 작성하고 실행한다. 공격이 성공함에 따라 불특정 다수의 계정에 대한 아이디와 비밀번호를 수직하여 기록한다.

- 예상 피해

계정이 탈취당한다면 사칭을 통해 2차 피해를 발생시킬 수 있으며, 이는 가능성이 무궁무진하기 때문에 간략히 서술하자면 사이트 테러, 권한 남용, 게시물 삭제, 프로필 변경, 게시물 업로드, 배너 변경, 홍보 문구 변경 등으로 피해를 줄 수 있다.

- 대처 방안

서버 측 자체에서 로그인 횟수에 대한 제한을 설정하는 것으로 손쉽게 해결할 수 있다.

- 참고 자료

보완 기능 참고 - <https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=p952973&logNo=220991799675>

4. Access Token 변조 후 요청 가능

타겟	ddyzd
명칭	토큰 변경
우선순위	우선순위 4위
탐색일시	2021년 5월 12일
발견자	고경태
종류	취약점

- 발견 경위

Access Token의 변조를 통한 공격 중 발견했다.

- 공격 기법

Access Token의 값을 관리 권한을 가진 Token으로 변조 시 Refresh Token + 유저 정보 + 소속동아리 변경 없이 권한이 별도로 필요한 행동이 가능하다. [취약한 인증]과 같은 부분에서 발생한 취약점이라고 예상된다.

- 공격 시나리오

Access Token의 변조한다. 권한이 필요한 작업을 수행한다.

- 예상 피해

권한의 탈취는 계정의 탈취라고 보아도 무방하다. 공격자가 계정의 주인이 사용할 수 있는 권한을 가지고 여러 작업을 한다는 것은 실질적으로 계정을 가지고 있지 않을 뿐, 여러 가지 작업 자체는 가능하다는 것을 의미하기 때문이다.

- 대처 방안

User Cache를 삭제 후 Token에 계정정보를 저장한다.

- 참고 자료

JWT - <http://www.opennaru.com/opennaru-blog/jwt-json-web-token/>

5. Click Jacking

타겟	DSM_Auth
명칭	Click Jacking
우선순위	우선순위 1위
탐색일시	2021년 3월 24일
발견자	이주석
종류	취약점

- 발견 경위

웹 서버에서 위험한 파일/CGI, 오래된 서버 소프트웨어 및 기타 문제를 검색하는 무료 소프트웨어 명령 줄 취약점 스캐너인 nikto를 사용해 DSM_Auth 사이트를 스캔하던 중 발견된 취약점이다.

- 공격 기법

Click Jacking이란 사용자의 클릭을 유도하는 공격으로, iframe 요소와 CSS를 교묘하게 이용해 투명하게 만든 공격 대상 사이트를 함정 사이트와 서로 겹쳐서 사용자가 모르는 사이에 공격 대상 사이트의 기능을 클릭하도록 유도하는 공격 방법이다.

- 공격 시나리오

Click Jacking의 대표적 예시는 피싱 사이트다. 사용자의 클릭을 유도하는 페이지를 구성한 후, 그 페이지 위에 iframe 등의 태그로 누르게 할 페이지를 호출한다. 그리고 CSS opacity(요소의 투명도를 조정)와 같이 사용자의 눈에는 보이지 않도록 숨겨 놓는 방법 등을 이용하여 공격을 할 수 있다. 예시 코드는 OWASP에서 제공한 Click Jacking Test 코드를 사용했다.

```
<!DOCTYPE html>
<html lang="en-US">
<head>
  <meta charset="UTF-8" />
  <title>DSMAuth</title>
  <link rel="shortcut icon" type="image/x-icon" href="https://developer.dsmkr.com/favicon3.ico">
  <style>
    body { margin: 0; } iframe { width:100vw; height: 100vh; position: relative; z-index: 0; }
  </style>
</head>
<body>
  <h3>clickjacking vulnerability</h3>
  <div class = "container">
    <iframe src="https://developer.dsmkr.com/login">
  </iframe>
  </div>
</body>
</html>
```

- 예상 피해

Click Jacking은 피싱 사이트를 만드는 데 굉장히 용이한 취약점으로, 특히 로그인을 하는 DSM_Auth를 사용해 피싱 사이트를 만들어 ID나 PW등 사용자의 개인정보를 가져올 수도 있다. 또는 피싱 사이트에 다른 링크를 걸어 다른 사이트로 접속하게끔 할 수 있다.

- 대처 방안

Click Jacking은 브라우저 측의 지원이 어느정도 필요하다. X-Frame-Options 라는 헤더를 사용해 frame 과 iframe의 참조를 제한하는 방법이 있고, Content Security Policy(CSP)의 frame-ancestors 지시어를 통해 값을 설정하여 제한하는 방식이 있다. 두 기술 중 대부분 브라우저에서는 호환성과 보안문제로 모든 parent URL들을 검사하면서 최신 기술인 CSP frame-ancestors를 권장하는 바이다.

- 참고 자료

Click Jacking? - <https://byounghee.tistory.com/146> , <https://owasp.org/www-community/attacks/Clickjacking>

6. Apache Range Header DoS

타겟	ddyzd
명칭	Dos
우선순위	우선순위 2위
탐색일시	2021년 4월 22일
발견자	이주석
종류	취약점

- 발견 경위

OWASP에서 개발한 오픈 소스 웹 애플리케이션 보안 스캐너이며, 개발 단계에서 개발자가 손쉽게 스스로 보안 취약점을 발견하고 조치할 수 있도록 하는 오픈소스 제품인 OWASP ZAP으로 DDYZD를 스캔 중 발견된 취약점이다.

- 공격 기법

일명 Apache Killer라고도 불리는 공격인데, HTTP Range 헤더를 이용한 DoS 공격이다. Range 필드를 포함한 요청을 보낼 때 공격자가 많은 범위의 서로 다른 요청을 보내면 비정상적인 많은 요청을 처리하는 과정에서 많은 CPU와 메모리를 소모하게 하고, 결국 무한루프에 빠진 것처럼 시스템을 불안하게 만들어 DoS 공격을 수행하게끔 하는 취약점이다.

- 공격 시나리오

[Range: byte=n-m] 형식으로 요청하며, 문서가 요구하는 부분적 범위를 명시하며 PDF나 동영상의 일부를 호출할 수 있다. 여기서 의문점이 든 것은 DDYZD는 nginx기반으로 돌아가는데 왜 Apache 관련 취약점이 발생하는지 의문이 들었는데, 위 취약점이 nginx에서도 발생했다고 한다.

```
GET https://ddyzd.dsmkr.com/_next/static/2rTbpRGXHvprlp-7za-fQ/_sfgManifest.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: */*
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.5,en;q=0.3
Connection: close Referer: https://ddyzd.dsmkr.com/
Cookie: __cfduid=d8f24945c35b8633d17ca312d85ab287e1619085799
Range: bytes=0,-5-0,5-1,5-2,5-3,5-4,5-5,5-6,5-7,5-8,5-9,5-10,5-11,5-12,5-13,5-14,5-15,5-16,5-17,5-18,5-19,5-20,5-21,5-22,5-23,5-24,5-25,5-26,5-27,5-28,5-29,5-30,5-31,5-32,5-33,5-34,5-35,5-36,5-37,5-38,5-39,5-40,5-41,5-42,5-43,5-44,5-45,5-46,5-47,5-48,5-49,5-50,5-51,5-52,5-53,5-54,5-55,5-56,5-57,5-58,5-59,5-60,5-61,5-62,5-63,5-64,5-65,5-66,5-67,5-68,5-69,5-70,5-71,5-72,5-73,5-74,5-75,5-76,5-77,5-78,5-79,5-80,5-81,5-82,5-83,5-84,5-85,5-86,5-87,5-88,5-89,5-90,5-91,5-92,5-93,5-94,5-95,5-96,5-97,5-98,5-99,5-100,5-101,5-102,5-103,5-104,5-105,5-106,5-107,5-108,5-109,5-1249,5-1250,5-1251,5-1252,5-1253,5-1254,5-1255,5-1256,5-1257,5-1258,5-1259,5-1260,5-1261,5-1262,5-1263,5-1264,5-1265,5-1266,5-1267,5-1268,5-1269,5-1270,5-1271,5-1272,5-1273,5-1274,5-1275,5-1276,5-1277,5-1278,5-1279,5-1280,5-1281,5-1282,5-1283,5-1284,5-1285,5-1286,5-1287,5-1288,5-1289,5-1290,5-1291,5-1292,5-1293,5-1294,5-1295,5-1296,5-1297,5-1298,5-1299
Content-Length: 0
Host: ddyzd.dsmkr.com
```

이러한 방식으로 Request를 전송하면 된다. 기본적으로 Range 필드는 첫 번째 바이트가 두 번째 바이트보다 같거나 작은 숫자이어야 하는데 이 payload에서는 이 법칙을 위반하는데, 이걸 서버에서는 허용한다. 또한 요청했던 Range 필드의 첫 번째 바이트(여기서는 5)를 중복해서 요청한다.

- 예상 피해

DoS공격인데 비해 요청 자체는 정상적인 요청으로 인식되므로 잘 차단되지 않고 많은 CPU와 메모리를 소모하게 되고, 결국 서버에 무리가 가게 된다.

- 대처 방안

인터넷에서는 Apache를 2.2.21이상으로 패치하라고 하지만 nginx 서버이기 때문에 해당사항이 없고, 개인적인 생각으로는 위 요청에 굳이 Range 헤더가 필요할 것이라고 생각되지 않아서 Range 헤더를 금지시키는 방법도 하나의 대처방안이 될 수 있다고 생각된다.

- 참고 자료

Apache Range Header DoS? - <https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=koromoon&logNo=120205479155>

nginx와 Apache Range Header DoS - <https://github.com/zaproxy/zaproxy/issues/6516>

7. Dos - File Upload

타겟	DSM_Auth
명칭	Dos
우선순위	우선순위 3위
탐색일시	2021년 5월 11일
발견자	신희원
종류	취약점

- 발견 경위

본 사이트에서는 파일 업로드 기능을 지원하고 있으며 파일 확장자가 jpg 혹은 png 파일만을 사용할 수 있도록 제한하고 있다. 그러나 이것은 파일의 확장자명에 jpg 혹은 png인 것만 확인하기 때문에 더미 파일의 파일 확장자를 임의로 변경하는 것만으로 더미 파일의 첨부가 가능하다. 이 점을 활용한 파일 업로드 취약점 공격 시도 중, 파일을 다량으로 첨부하자 서버의 속도가 느려지는 현상을 보고 시도한 공격이다.

- 공격 기법

개발진은 파일의 용량을 속도를 위해 약 1GB 용량 정도로 리사이징한다고 하였다. 때문에 두 번째 공격에서는 단순히 1GB 용량의 더미 이미지 파일을 수동으로 여러 번 첨부하였고 성공하였다. 수동으로 약 400개의 이미지. 즉, 400GB 정도의 용량을 두 명이 새벽 시간에 약 10분 내로 첨부하자 사이트의 처리 속도가 현저히 감소하였다. 공격 코드를 작성하여 자동화할 수 있었지만, 사이트의 변화가 감지되자마자 공격을 멈추고 복구할 수 있도록 수동으로 진행하였으며 실제 진행 중인 사이트이기 때문에 예상보다 서버의 처리 용량이 빠르게 소모된다면 공격을 즉각적으로 멈추기 힘들고 복구가 어렵기 때문이다. 또한, 혐의된 사항에 따라 공격은 새벽에 이용자 수가 적을 때 진행하였다.

- 공격 시나리오

Python을 이용해 공격 코드를 작성하여 이미지 파일 첨부을 빠르게 제한 없이 진행할 수 있다면 이는 사이트의 서버 처리 용량을 무서운 속도로 차지할 것이며, 결과적으로 서버의 모든 용량을 소비하여 서비스의 이용에 큰 불편함을 줄 것으로 예상된다. 코드를 작성한 후 가동한다. 그러면 서버의 용량을 급속도로 차지, 결국 사용자들의 접근이 차단된다.

- 예상 피해

일단 피해가 적은 쪽으로 생각하자면 사이트의 속도가 점차 느려진다. 이후 개발진 측이 사이트의 처리 속도의 저하를 확인하고 어떠한 유저가 공격을 가했는지 탐색하여 즉시 제재를 가하는 방법이 있다. 하지만 피해가 심각한 쪽으로 생각하자면 공격 즉시 최대 2분 내로 서버의 용량이 전부 할당되어 타 유저가 서비스를 이용하지 못하는 상황이 오는 것이다. 안타깝게도 해당 취약점의 경우 공격 실행이 비교적 간단하여 후자의 발생 확률이 높다.

- 대처 방안

서비스 거부 공격은 반복적으로 여러 번 진행하는 특정 작업을 통해 공격 타겟의 리소스를 차지하는 것이다. 즉, 서버의 용량을 차지하기 위해 파일의 첨부을 요청하는 반복적인 작업도 서비스 거부 공격의 일종이라고 보아도 무방하다. 이를 대처하기 위해서는 극단적인 방법으로 사용자 개인당 사이트에 첨부 가능한 이미지 파일의 용량을 제한하는 것도 있지만, 효율적인 방법으로는 반복적으로 서버의 용량을 차지하는 작업을 빠르게 요청하는 특정 사용자를 걸러내어 모든 요청을 무시하고 공격자를 찾아내어 책임을 지게 하는 방법이 있다.

- 참고 자료

서비스 거부 공격 - https://ko.wikipedia.org/wiki/서비스_거부_공격

8. Client secret 노출

타겟	DSM_Auth, ddyzd
명칭	민감한 데이터 노출
우선순위	우선순위 3위
탐색일시	2021년 4월 6일
발견자	이주석
종류	취약점

- 발견 경위

로그인 로직을 분석하기 위해 Request와 Respnese를 분석하던 중 발견했다. 본 사이트에서는 다음과 같은 로그인 로직을 사용한다. OAUTH 로그인 방식과 비슷한 것으로 보인다.

1. ID, PW, redirect_url, client_id를 body에 담아 보낸다. 응답으로는 code가 온다.
2. code, client_id, client_secret을 body에 담아 보낸다. 응답으로는 access_token과 refresh_token을 보내준다.

- 공격 기법

이 과정에서 문제되는 과정은 client_secret 값이다. OAUTH에서 토큰을 발급하는 과정에서 필요한 값으로 보이는데, 이러한 값을 각 서버의 상수 값으로 받게끔 해도 무방한데, 이 값을 프론트 코드에 암호화도 되어 있지 않게 그대로 노출되어 있다. client_id와 client_secret는 사용자가 사용하려는 서비스(Client)에 타사 서비스(Resource Server)가 발급해준 식별 코드와 같다. 여기서는 Resource Server가 DSM_Auth이고, Client가 DDYZD라고 가정하면 된다.

- 공격 시나리오

"민감한 데이터 노출" 취약점 같은 경우는 그 자체는 위험하지 않지만 이 취약점이 다른 취약점과 응용된다면 위험한 취약점으로 변모가 가능하다. Client를 식별하는 client_id와 client_secret 값이 모두 노출되어 있기 때문에 이 값을 가지고 피싱 서버를 만들어 Resource Server 내에 정보에 접근이 가능해진다. code값을 Brute Force하여 Access Token을 발급할 수도 있다.

- 예상 피해

예상되는 피해로는 client_secret값은 Client을 식별하는 식별자이면서 토큰을 발급할 때 사용되는 값이기도 하기에 아무래도 토큰 탈취나 피싱 서버를 통한 개인 정보 탈취 등의 피해가 생길 수 있다.

- 대처 방안

client_secret 값을 노출시키지 않으면 된다. 가장 확실한 방법은 Client 서비스의 서버에 env를 활용해 노출되지 않도록 하는 것이라고 생각된다.

- 참고 자료

OAuth란? - <https://programmingfbf7290.tistory.com/entry/11-이해하기-쉬운-OAuth-20>

OAuth 개요 및 보안 고려 사항 - <https://www.fsec.or.kr/common/proc/fsec/bbs/42/fileDownload/265.do>

버그 분류

1. File Extension

타겟	ddyzd
명칭	잘못된 함수 사용
우선순위	우선순위 2위
탐색일시	2021년 3월 16일
발견자	이주석
종류	버그

- 발견 경위

동아리 관리 페이지에서 File Upload 취약점을 목표로 확장자를 검증하는 코드를 읽어보던 중 발견하게 된 버그이다.

- 버그 개요

DDYZD 관리 페이지에서 사진 등을 올릴 때 화이트리스트 형식으로 확장자를 검증하는데, 이때 사용되는 함수가 **contain** 함수이다. 이 **contain** 함수는 문자열을 비교하는 함수인데, 특정 문자열이 "포함"되면 True를 반환하게 된다. 이 말은 즉, 확장자 안에 jpg, heic, png라는 문자열만 들어가면 확장자 검증을 통과하게 된다.

- 예상 피해

원래는 이 버그는 사실 취약점으로 분류하고 수많은 payload를 시도했었다. 파일 확장자에 Web Shell을 넣어보거나 BOF, Path Traversal, 세미콜론으로 코드를 강제 종료하는 등의 공격을 시도해보았으나 404 에러 등이 뜨면서 공격에 실패했고, 결국 위 취약점은 버그로 분류하게 되었다. 허나 분명 이 부분은 다른 취약점과 연계되어 악용될 가능성이 높아 보이는 것은 사실이다.

- 대처 방안

문자열이 포함되어 있음을 체크하는 **contain** 함수 대신 문자열이 동일함을 체크하는 **equals** 함수를 사용한다.

- 참고 자료

코드 - https://github.com/semicolonDSM/DDYZD_BACKEND_SPRING/blob/207ba0887228a025af6f550eef848f9f4bde2bfe/src/main/java/com/semicolon/spring/service/feed/FeedServiceImpl.java#L50

2. 면접일자 NaN월 NaN일 수정 필요

타겟	ddyzd
명칭	버그
우선순위	우선순위 3위
탐색일시	2021년 4월 14일
발견자	고경태
종류	버그

- 발견 경위

관리자 계정의 권한 허용 범위를 분석하던 중 발견했다.

- 버그 개요

면접일자 기능의 요일 표시에서 [NaN월 NaN일] 표시가 필터링 없이 표시된다.

- 예상 피해

면접일자는 본래 예민한 것이기 때문에 필터링은 있는 편을 추천한다.

- 대처 방안

필터링 기능을 추가한다.

- 참고 자료

NaN 값 처리 - <https://minu0807.tistory.com/1>

3. 당일 날 모집일정 개시 불가

타겟	ddyzd
명칭	버그
우선순위	우선순위 2위
탐색일시	2021년 3월 17일
발견자	고경태
종류	버그

- 발견 경위

모집 일정 설정 관련 취약점 탐색 중 발견했다.

- 버그 개요

모집 일정 설정 관련 취약점 탐색 중 발견했다.

- 예상 피해

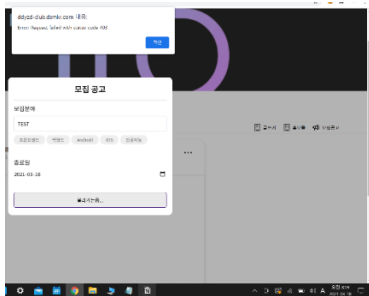
하루 한정 동아리원 모집의 진행 불가. 또한 버그로써 존재하기 때문에 수정이 필요하다.

- 대처 방안

당일에 모집 일정을 진행하여도 에러가 발생하지 않도록 수정한다.

- 참고 자료

403에러화면



4. User Cache 변조

타겟	ddyzd
명칭	버그
우선순위	우선순위 2위
탐색일시	2021년 5월 12일
발견자	고경태
종류	버그

- 발견 경위

User Cache 변조를 통한 취약점 분석 중 발견했다.

- 버그 개요

User Cache를 변경함에 따라 관리 동아리 및 프로필의 변경이 가능하며, 관리 동아리 페이지, 유저 이름, 동아리 이메일 등의 개인정보의 변조를 허용하고, Token 값을 NULL로 설정하여도 User Cache만 존재한다면 실질적인 권한 인증은 되지 않았으나 유저명과 로그아웃 요청 버튼이 활성화된다.

- 예상 피해

User Cache의 변조 같은 한 작업만으로 위에서 서술한 수많은 효과를 발생한다는 것은 바람직하지 않으며 각종 복합 취약점과 맞물려 심각한 문제가 될 수 있다.

- 대처 방안

User Cache를 없애고 User정보를 Token에 담는다.

- 참고 자료

토큰 - <https://krksap.tistory.com/1586>

5. 대동여지도 프로필 버그

타겟	ddyzd
명칭	잘못된 프로필 변경 설정
우선순위	우선순위 5위
탐색일시	2021년 4월 13일
발견자	신희원
종류	버그

- 발견 경위

해당 사이트에서의 프로필 설정 화면의 URL 주소에 프로필의 주인, 즉 이용자의 학번이 그대로 첨부되어 존재하였다. 때문에 그저 URL 주소에서 학번만 타 학생의 학번으로 변경하면 프로필 화면이 들어가졌다. 또한 프로필 업데이트 기능도 그대로 존재하였기 때문에 타 학생의 프로필 페이지에 들어가서 프로필 변경이 가능한지 확인상의 목적으로 타 학생의 프로필 페이지의 Github 아이디와 자기소개를 변경하고 [프로필 업데이트] 기능을 활성화하였다. 다시 본인의 프로필로 돌아가면 이름과 학번, 소속 중인 동아 제외한 모든 프로필이 위에서 변경한 설정 사항으로 똑같이 변경되어 있었다. 결론적으로 타 학생의 프로필에 접속하고 변경하지 않은 상태로 [프로필 업데이트] 기능을 활성화하자 똑같이 복사되었다.

- 버그 개요

타인의 프로필이 학번과 이름, 소속 동아리를 제외하고 복사된다.

- 예상 피해

우선 큰 피해는 사용자에게 줄 수 없다. 그저 자신이 들어간 프로필 창에서 업데이트를 실행하면 자신의 프로필이 바뀌는 것 외에는 어떠한 피해도 줄 수 없기 때문이다.

- 대처 방안

프로필 업데이트 기능에서 사용자를 확인해 타인이 자신의 프로필에 접근하여 프로필 업데이트 기능을 사용할 수 없게 한다.

- 참고 자료

타 학생의 프로필


이름
안은결

학번
No.2411

Github 아이디
eungyeole

자기소개
UI가 별루네 다크모드지원 애반데...

소속중인 동아리
SEMICOLON;
프로필 업데이트



복사된 자신의 프로필


이름
신희원

학번
No.2410

Github 아이디
eungyeole

자기소개
UI가 별루네 다크모드지원 애반데...

소속중인 동아리
프로필 업데이트



6. Access Token 변조 후 에러 불규칙

타겟	ddyzd
명칭	버그
우선순위	우선순위 4위
탐색일시	2021년 5월 12일
발견자	고경태
종류	버그

- 발견 경위

관리자 페이지의 Access Token의 변조를 통한 해킹 시도 중 발견했다.

- 버그 개요

본 페이지에서 Access Token의 값을 임의 값 X로 변경하여 배너 사진 변경 등의 권한이 필요한 요청을 시도하면 error 401 혹은 error 403이 랜덤하게 뜬다. 또한 Access Token의 변조 값을 동일하게 맞추고 다수의 시도에서 위의 error 표시의 규칙성이 발견되지 않았다.

- 예상 피해

에러 표시의 불규칙성이란 코드의 불안정성을 뜻한다고 볼 수 있다.

- 대처 방안

에러 처리에 대한 세심한 관리가 필요한 듯 보이며, 수정을 권장한다.

- 참고 자료

에러 처리의 필요성 - <https://velog.io/@jiwonsim/Exception%EC%9D%98-%ED%95%84%EC%9A%94%EC%84%B1-tqk5em3geo>

7. 회원가입 시 DSM_Auth 이메일 인증 관련 문제

타겟	DSM_Auth
명칭	잘못된 입력
우선순위	우선순위 5위
탐색일시	2021년 5월 13일
발견자	심준호
종류	버그

- 발견 경위

회원가입 도중, 이메일 입력란에 정규식을 사용할 것으로 예상하여 값들을 대입하던 도중 발견했다.

- 버그 개요

bypass(우회) 정규식을 우회하여 비정상적인 값을 입력하여 사이트에 오류를 일으킨다. 회원가입 시 이메일 입력 칸에 ‘.’ 대신 ‘,’를 입력한 경우 발생한다. (asdf@dsm.hs.kr)

- 예상 피해

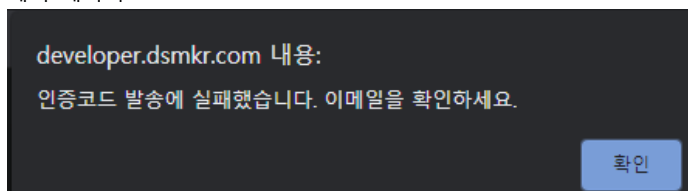
학교 이메일이 아닌 외부 이메일로 이메일 인증이 우회되면 추후 무분별한 계정 생성 등으로 연결될 수 있다. 또한 경우에 따라 정보 없는 계정들이 생성될 수 있다.

- 대처 방안

정규식을 수정한다.

- 참고 자료

에러 메시지



8. 관리자 페이지 변경 후 요청에 대한 에러 처리 미흡

타겟	ddyzd
명칭	버그
우선순위	우선순위 2위
탐색일시	2021년 5월 12일
발견자	고경태
종류	버그

- 발견 경위

타 동아리의 관리 페이지 접속 후 변조에 대한 연구 중 발견했다.

- 버그 개요

타 동아리의 관리 페이지에 접속하는 것은 URL 변경으로 간단하게 가능하다. 또한 타 동아리의 관리 페이지에 접속 후 해당 동아리의 동아리원 혹은 동아리장의 권한이 부여된 계정이 없는 상태에서 게시물 작성 요청 시 에러 표시가 뜨지 않고 그저 진행 중으로만 보인다.

- 예상 피해

타 동아리의 관리 페이지에 접속하는 것은 URL 변경으로 간단하게 가능하다. 또한 타 동아리의 관리 페이지에 접속 후 해당 동아리의 동아리원 혹은 동아리장의 권한이 부여된 계정이 없는 상태에서 게시물 작성 요청 시 에러 표시가 뜨지 않고 그저 진행 중으로만 보인다.

- 대처 방안

에러 처리를 통해 권한 없음을 고지한다.

- 참고 자료

HTTP 에러 코드 표 - <https://j07051.tistory.com/535>

9. 존재하지 않는 채팅페이지 URL접속

타겟	ddyzd
명칭	버그
우선순위	우선순위 2위
탐색일시	2021년 5월 12일
발견자	고경태
종류	버그

- 발견 경위

취약점 스캐너를 통해 산출된 채팅 페이지의 XSS취약점의 조사 중 발견했다.

- 버그 개요

존재하지 않는 '우리 동아리' 채팅방 관리자 계정으로 접속 시 아무런 오류나 경고 처리 없이 채팅방 목록만 뜬다. 존재하는 '우리 동아리' 채팅 방 '멤버'로 접속 시 경고 없이 이상한 페이지로 연결이 되며 새로 고치면 정상접속 된다. 존재하는 '타 동아리' 채팅방 관리자 계정으로 접속 시 404같은 에러 없이 그냥 빈 /chat 화면에서 멈춘다. 존재하는 '타동아리' 채팅 방 '일반 동아리 멤버'로 접속 시 404 에러 안 뜨고 채팅을 보낼 시 2번과 같은 증상이 반복되며 채팅이 보내지지 않으나 새로 고침 시 일정 확률로 채팅이 보내진다.

- 예상 피해

페이지 관리 및, 각종 에러 처리에 대한 미흡한 부분이다. 큰 피해는 줄 수 없으나 고치는 것이 바람직하다고 생각된다.

- 대처 방안

존재하지 않아야 하는 페이지에 대한 404 에러 처리에 대한 보수작업으로 해결이 가능하다.

- 참고 자료

404 에러 페이지 제작 - <https://kiss7.tistory.com/1196>

10. /clubinfo?id=(404 not found)

타겟	ddyzd
명칭	버그
우선순위	우선순위 1위
탐색일시	2021년 4월 23일
발견자	신희원
종류	버그

- 발견 경위

사이트 취약점 분석을 위해 사이트에 접근하였고 동아리 페이지를 보기위해 카테고리를 통해 접근하였으나 404 에러가 발생하며 막혔다. 이후 동아리 신청 페이지에서 접근이 가능하였으나 URL이 달랐고 이후 계정 프로필을 통해 접근하였으나 똑같이 막혔다. 이를 통해 /clubinfo?id=라는 URL 문장의 사용이 막혔음을 확인하였으며, 이는 개발진 측의 업데이트 작업 실수로 보인다.

- 버그 개요

사이트 취약점 분석을 위해 사이트에 접근하였고 동아리 페이지를 보기위해 카테고리를 통해 접근하였으나 404 에러가 발생하며 막혔다. 이후 동아리 신청 페이지에서 접근이 가능하였으나 URL이 달랐고 이후 계정 프로필을 통해 접근하였으나 똑같이 막혔다. 이를 통해 /clubinfo?id=라는 URL 문장의 사용이 막혔음을 확인하였으며, 이는 개발진 측의 업데이트 작업 실수로 보인다.

- 예상 피해

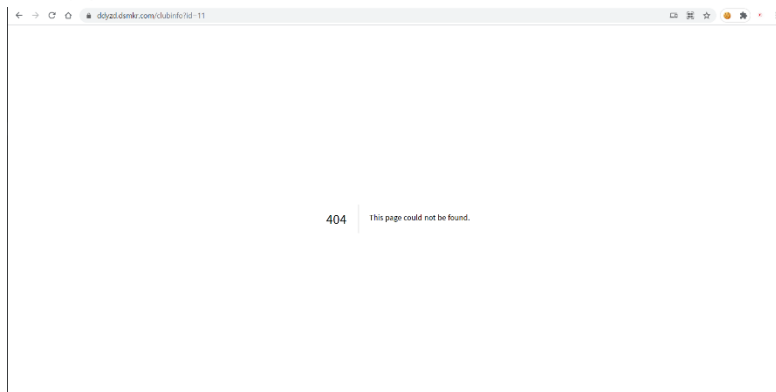
사용자들의 동아리 접근이 막힌다. 때문에 원활한 서비스 이용이 불가능하다. 다른 루트를 사용해 들어갈 수 있지만 이는 해결책이 아니다.

- 대처 방안

/clubinfo?id= 문장을 /club/ 으로 통일하면 원만히 해결된다.

- 참고 자료

404 에러



모바일 분류

1. 정직한 코드

타겟	ddyzd
명칭	추가기능
우선순위	우선순위 2위
탐색일시	2021년 5월 11일
발견자	심준호
종류	모바일

- 발견 경위

안드로이드 취약점을 탐색하기 위한 디컴파일 작업 후 발견했다.

- 기능의 필요성

코드 자체에 직접적이며 지금 당장 활용할 수 있는 보안상의 취약점이 존재하지는 않는 것으로 보인다. 허나 코드를 난독화 없이 표출함에 따라 추후 업데이트 등의 작업 시, 추가적으로 발생 가능한 취약점의 탐색이 쉬워진다. 때문에 난독화를 통하여 해커의 취약점 분석이 어려워지도록 해야 한다.

- 기능 구현

코드에 난독화 작업을 진행한다.

- 참고 자료

안드로이드 난독화 설명. - <https://dazemonkey.tistory.com/49>

추가기능 분류

1. DSM_Auth 비밀번호 찾기 기능 필요

타겟	DSM_Auth
명칭	추가기능
우선순위	우선순위 1위
탐색일시	2021년 4월 3일
발견자	민준혁
종류	추가기능

- 발견 경위

패스워드를 잊어서 복구를 시키거나 변경하려고 로그인 페이지에 접속했는데 패스워드 찾기 혹은 패스워드 변경 기능이 존재하지 않았다. 또한 이를 보고 ID 찾기 기능의 부재도 추가적으로 확인했다.

- 기능의 필요성

본인과 같이 패스워드 혹은 아이디를 잊은 사용자는 사이트의 계정 사용이 불가능하기 때문이다.

- 기능 구현

본인인증을 통한 아이디 확인 기능과 패스워드 확인 기능이 추가되거나 패스워드 변경 기능이 추가되면 해결이 된다.

- 참고 자료

아이디 및 패스워드 찾기 기능 구현 - <https://amazing96.tistory.com/11>

2. Port 스캐닝 방지 기능 필요

타겟	ddyzd
명칭	추가기능
우선순위	우선순위 3위
탐색일시	2021년 4월 14일
발견자	김민제
종류	추가기능

- 발견 경위

사이트에서 코드 보안에만 신경을 쓸 것이라 예상하고 포트 스캐닝 공격을 시도했다. 그런데 서버의 포트가 그대로 드러나 있고 다른 포트 또한 노출된 상태이다.

- 기능의 필요성

대동여지도의 URL ddyzd.dsmkr.com를 가지고 nmap에 인자 값으로 넘겨 일반 스캔을 진행하면 포트가 노출된다. 포트가 노출된다는 것은 다른 공격 경로가 있다는 것을 알 수 있는 중요한 정보가 되기 때문에 포트를 노출해선 안된다.

- 기능 구현

포트 스캐닝을 방지하기 위해서는 리눅스의 Port Sentry를 설치하여 실행하면 실제 실행되고 있지 않은 포트를 열고 특정 포트는 감지되지 않게 할 수 있기 때문에 이 방법을 사용하여도 좋다.

- 참고 자료

스캔 시 화면

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-14 19:58 KST
Nmap scan report for ddyzd.dsmkr.com (172.67.176.140)
Host is up (0.086s latency).
Other addresses for ddyzd.dsmkr.com (not scanned): 2606:4700:3034::6815:1f85 2606:4700:3030::ac43:b0
8c 104.21.31.133
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
```

3. 에러처리 통일 필요

타겟	ddyzd
명칭	추가기능
우선순위	우선순위 3위
탐색일시	2021년 5월 13일
발견자	고경태
종류	추가기능

- 발견 경위

관리자 페이지의 취약점 분석 도중 발견했다.

- 기능의 필요성

권한이 없는 한 종류의 에러에 대해서 여러 가지의 에러창으로 넘어가는 경우, 페이지에 자원을 불필요하게 소모하며 비효율적이다.

- 기능 구현

403 및 각종 에러 처리 통일

- 참고 자료

에러 처리 미흡에 대한 안내 - <https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=lascomco&logNo=221271580195>

4. 페이지 로그인 동기화

타겟	ddyzd
명칭	추가기능
우선순위	우선순위 1위
탐색일시	2021년 5월 12일
발견자	고경태
종류	추가기능

- 발견 경위

대동여지도 일반 페이지와 대동여지도 관리자 페이지를 통한 서비스 이용 중 발견했다.

- 기능의 필요성

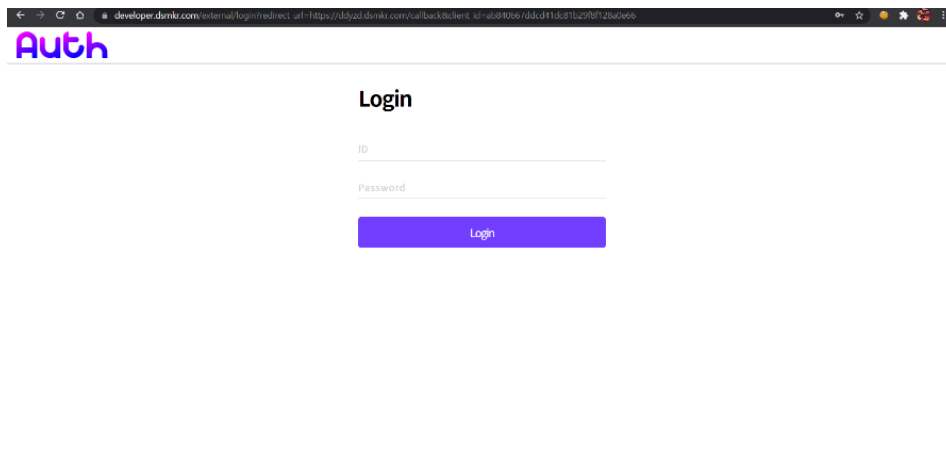
대동여지도의 일반 페이지 기능과 관리자 페이지 기능을 복합적으로 사용할 때 로그인 절차가 불필요하게 늘어나 있기 때문에 수정이 필요하다.

- 기능 구현

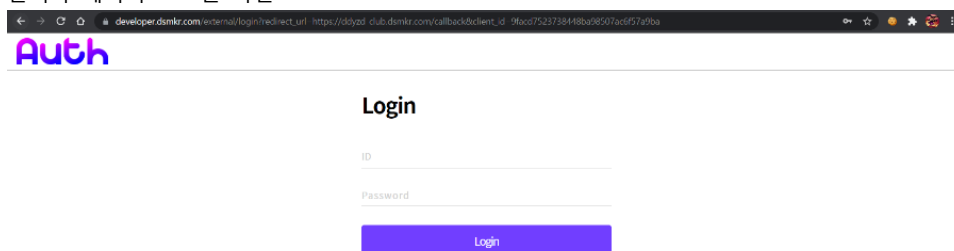
한쪽 로그인을 통한 인증으로 다른 쪽 페이지의 인증이 자동으로 진행되는 기능을 구현한다.

- 참고 자료

일반 페이지 로그인 화면



관리자 페이지 로그인 화면



4. 결론

4.1. 사이트 보안성 평가

전체적으로 보안의 수준은 중간 정도였다고 결론지었다. 물론 code 값의 유효기간이 없어 code 값으로 로그인되는 등의 위험한 취약점도 있었지만 발견된 대부분의 취약점이 서버에 큰 악영향을 끼치지 않았다. 하지만 파일 확장자 버그나 Access Token 변조 후 요청, User Cache 변조 등 좀 더 연구하면 사용 방법에 따라 취약점으로 발전할 가능성이 있는 버그들이 굉장히 많았다. 이러한 결과를 바탕으로 이 웹사이트의 보안 수준을 [상/중/하]로 평가할 때 [중] 정도였다고 결론을 내렸다.

4.2. 일정 관리 문제

프로젝트의 진행에 있어서 가장 중요한 일정 관리가 허술하였다. 우선 분석에 대해 각 인원이 언제부터 언제까지 어떠한 분석을 진행할 것인지에 대해 소통이 되지 않았으며 이에 따라 각 인원이 정확한 계획 없이 분석을 진행하였다. 이 때문에 같은 날짜에 동일인이 분석을 몰아서 진행하는 상황이 발생하기도 하였다. 또한 자신의 실력에 대한 판단 부족과 학교 일정 등의 복합적인 문제를 고려하지 않아 사이트의 분석 기간을 개발자 측에 요청하여 늘리기도 하였다. 추후 프로젝트의 일정 관리에 있어서 프로젝트 매니저는 개선방안을 찾아야 할 것이다.

4.3. 팀원 관리 문제

학교 측에 제출한 기획서에 서술된 분석 인원보다 리포트에 작성된 분석 인원의 수가 적었다. 이는 프로젝트 참여자 개개인의 역량 파악 부족과 학생의 개인적인 일정 등에 대한 고려 및 복수의 프로젝트를 진행하는 인원을 중복 참여시킨 것에 대한 결과이다. 이는 본 프로젝트에 참여하는 인원의 관리 방식이 미흡하다는 것을 나타낸다. 앞으로 프로젝트의 팀원 관리에 있어서 프로젝트 매니저는 이 부분에 대하여 개선방안을 찾아야 할 것이다.

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. 추후 프로젝트의 분석 정리에 있어서 프로젝트 보고서 작성자 및 프로젝트 매니저는 개선방안을 찾아야 할 것이다.

4.5. 각 팀원의 고찰

이주석 학생.

처음 진행하는 웹 컨설팅 프로젝트, 처음 맡아본 PM 자리라 많은 우여곡절이 있었지만 그래도 처음 진행한 프로젝트치고 잘 마무리되어서 다행이었다. 그리고 주말마다 진행한 멘토링을 통해 다음 진행할 컨설팅 프로젝트에서 추가할 점, 보완할 점을 알게 되어 좋았다. 이 프로젝트를 체계화, 세분화하여 앞으로 이 프로젝트를 동아리 대표 프로젝트로 남길 수 있도록 노력할 것이다.

신희원 학생.

취약점 분석 프로젝트의 기초 구상에 참여하고 진행하고 보고서를 작성하고 일정을 조율하며 취약점 분석이란 팀 프로젝트 자체가 동아리의 팀워크에 대한 평가라는 사실을 보았으며, 자신의 현재 상태에 대한 실력 미흡을 깊이 느꼈다.

김민제 학생.

처음 공식으로 해보는 취약점 분석 프로젝트여서 지식을 총동원해서 진행하였다. 중간에 개인 프로젝트로 빠지는 경우가 많아서 좀 아쉽지만, 다음에도 취약점 분석 프로젝트를 하게 된다면 이번보다는 열심히 할 것이다. 또, 취약점 중에 네트워크 단의 취약점을 분석해보려고 하였는데 은근히 포트가 많아서 놀랐다.

고경태 학생.

참여 인원 관리에 대해 좀 더 신경 쓸 필요가 있어 보인다.

손영웅 학생.

웹 보안은 개인적으로 경험이 많이 부족한 분야이기에 실전에서 웹 취약점 분석을 해보니 많이 공부가 되었다.

민준혁 학생.

취약점 분석 프로젝트에 뒤늦게 참석, 하지만 웹 해킹에 실력이 거의 없는 편인 내가 이미 쉬운 취약점이 다 찾아진 상태에서 할 수 있는 마땅한 것이 없었다. 그래서 이번에는 한 활동이 거의 없어 아쉬운 편이다. 다음 분기에 돌아오는 취약점 분석 때 성과를 만들어보도록 하겠다.

심준호 학생.

모바일 애플리케이션을 디컴파일하고 분석하는 과정에서 자바, 코틀린 등의 언어를 좀 더 깊게 공부해 보아야 코드를 이해하기 수월하리라 생각했고, 모바일 애플리케이션 분석 과정과 툴을 익힐 수 있었다.

5. 부록

5.1. 진행 일정표

- 2021년 03월 02일 - 대동여지도 및 DSM_Auth 서비스 개시.
- 2021년 03월 02일 - 웹 보안 컨설팅 프로젝트 참여 동아리 협력 회의.
- 2021년 03월 10일 - [취약한 인증 방식] 취약점 발견 후 즉시 전달.
- 2021년 03월 16일 - [File Extension] 버그 발견.
- 2021년 03월 17일 - [당일 날 모집일정 개시 불가] 버그 발견.
- 2021년 03월 18일 - [DSM Auth 로그인 입력 수 무제한] 취약점 발견.
- 2021년 03월 24일 - [Click Jacking] 취약점 발견.
- 2021년 03월 27일 - [로그인 횟수 제한 부재] 취약점 발견.
- 2021년 04월 02일 - 취약점 연구 기간 연장 합의.
- 2021년 04월 03일 - [DSM Auth 비밀번호 찾기 기능 필요] 추가기능 발견.
- 2021년 04월 06일 - [Client secret 노출] 취약점 발견.
- 2021년 04월 13일 - [대동여지도 프로필 버그] 버그 발견.
- 2021년 04월 14일 - [Port 스캐닝 방지 기능 필요] 추가기능 발견.
- 2021년 04월 14일 - [면접일자 NaN월 NaN일 수정 필요] 버그 발견.
- 2021년 04월 22일 - [Apache Range Header DoS] 취약점 발견.
- 2021년 04월 23일 - [/clubinfo?id=(404 not found)] 버그 발견.
- 2021년 05월 11일 - [정직한 코드] 모바일 발견.

2021년 05월 11일 - [Dos - File Upload] 취약점 발견.

2021년 05월 12일 - [User Cache 변조] 버그 발견.

2021년 05월 12일 - [관리자 페이지 변경 후 요청에 대한 에러 처리 미흡] 버그 발견.

2021년 05월 12일 - [존재하지 않는 채팅 페이지 URL접속] 버그 발견.

2021년 05월 12일 - [Access Token 변조 후 에러 불규칙] 버그 발견.

2021년 05월 12일 - [Access Token 변조 후 요청 가능] 취약점 발견.

2021년 05월 12일 - [페이지 로그인 동기화] 추가기능 발견.

2021년 05월 13일 - [회원가입 시 DMS_Auth 이메일 인증 관련 문제] 버그 발견.

2021년 05월 13일 - [에러처리 통일 필요] 추가기능 발견.

2021년 05월 15일 - 대동여지도 및 DSM_Auth 서비스 취약점 연구 종료.

5.2. 보고서 작성 시 참고 자료

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