*텍스트이(가) 표시된 사진

자동 생성된 설명2023년 lsb커뮤니티 모의해킹*

*2023 / 07 / 19*

2023년LSB 커뮤니티 모의해킹

모의해킹 결과 보고서 v1.0

**Copyright © SegFault**

세그폴트의 사전 승인 없이 본 내용의 전부 또는 일부에 대한 복사, 전재, 배포, 사용을 금합니다.

목 차

1. 모의해킹 수행 정보 2

1.1. 개요 2

1.2. 대상 2

1.3. 수행 기간 2

1.4. 수행 인력 2

2. 모의해킹 결과 3

2.1. 총평 3

2.2. 결과 요약 4

3. 취약점 상세 내용 5

3.1. [LSB 커뮤니티] (http://ctf.segfaulthub.com:9575/login.php) 5

3.1.1. XSS 5-10

3.1.2. 악성파일업로드 11-13

3.1.3. 자동화공격 14-15

3.1.4. 유추가능한 세션ID, 불충분한 세션 종료 16-17

3.1.5. 유추가능한 인증정보 이용 18-20

3.1.6. 데이터 평문전송 21-25

4. 보안 권고안 26

4.1. XSS 26

4.2. 악성파일업로드 26

4.3. 자동화공격 27

4.4. 유추가능한 세션ID, 불충분한 세션 종료 28

4.5. 유추가능한 인증정보 이용 29

4.6. 데이터 평문전송 29

1. 모의해킹 수행 정보
   1. 개요

본 프로젝트는 LSB 커뮤니티의 웹 애플리케이션에 대한 모의 해킹을 수행한 후 발견된 취약점에 대한 대응 방안을 제시함으로써 차후 발생할 수 있는 침해 사고를 예방하고 정보 보호 수준을 향상할 수 있는 대책을 수립하는 데 기여하는 것을 목적으로 합니다.

* 1. 대상

본 프로젝트 점검 대상은 다음과 같습니다.

|  |  |  |
| --- | --- | --- |
| No | Platform | URL |
| 1 | **WEB** | http://ctf.segfaulthub.com:9575/login.php |

* 1. 수행 기간

🡪 2023년 07월 15일 ~ 2023년 07월 19일

* 1. 수행 인력

|  |  |  |
| --- | --- | --- |
| 소속 | 성명 | 담당 업무 |
| SegFault | **박주형** | **- 웹 모의해킹** |

1. 모의해킹 결과
   1. 총평

LSB 커뮤니티에 대해 모의 해킹을 진행한 결과, 총 몇건의 취약점의 발견되었습니다. 해당 취약점은 사용자의 중요 정보를 탈취 및 변조가 가능하며, 서버의 소스코드 탈취 및 데이터 베이스 정보 노출로 인하여 2차 피해가 발생할 수 있습니다.

* **사용자의 중요 정보 탈취 및 변조**

사용자의 중요 정보가 탈취되게 된다면, 공격자는 이를 이용해 악의적인 의도로 사용이 가능하며, 다른 사용자의 권한을 이용하여 여러 피해를 발생시킬 수 있습니다.

* **서버의 상세 정보 및 소스코드 탈취**

서버의 정보 또는 소스코드가 탈취되면 공격자가 이를 악용해 다른 사용자의 권한을 악용할 수 있으며, 심각한 경우 최고 사용자의 권한이 탈취당해 다른 사용자가 서버를 이용할 수 없게 됩니다.

* **데이터 베이스 정보 노출 및 탈취**

데이터 베이스가 탈취당하면, 개인의 정보를 이용해 악의적인 행위를 할 수 있으며, 법적 물 의를 일으켜 기업에 치명적인 손실을 입힐 수 있습니다.

이러한 취약점들은 기업 가치를 하락 시킬 뿐 아니라 금전적인 피해, 법적 피해를 일으킬 수 있기 때문에 빠른 조치를 필요로 합니다.

* 1. 결과 요약

|  |  |  |  |
| --- | --- | --- | --- |
| No | 대상 | 취약점 | 내용 |
| 1 | **http://ctf.segfaulthub.com:9575/mypage/mod\_addr.php** | **XSS** | 파라미터 값을 이용하여 페이지를 만들 때 클라이언트 측에서 실행할 수 있는 스크립트에 대한 필터링이 미흡하여 악의적인 스크립트가 클라이언트 측에서 실행될 수 있습니다. 이러한 취약점은 사용자의 민감한 정보를 탈취하거나 서버를 장악 할 수 있습니다. |
| 2 | **http://ctf.segfaulthub.com:9575/user\_board/board.php** | **악성 파일 업로드** | 서버에 업로드 되는 파일의 확장자를 검증하는 로직이 미흡하여 웹 서버에 명령을 내릴 수 있는 웹 쉘을 업로드 할 수 있습니다. 이러한 웹 쉘은 사용자의 정보를 탈취하거나 DB 정보를 탈취하는 공격이 가능합니다. |
| 3. | **http://ctf.segfaulthub.com:9575/user\_board/board.php** | **자동화 공격** | 일정시간 내 게시글 작성 횟수에 제한을 두지 않는 취약점이 발견되었으며 이러한 취약점은 애플리케이션의 자원을 고갈시킬 수 있습니다. |
| 4. | **http://ctf.segfaulthub.com:9575/login.php** | **유추 가능한 세션ID, 불충분한 세션 종료** | 로그인 전과 로그인 후의 세션 ID가 일정하게 고정된 취약점이 발견되었습니다. 또한 일정시간이 지난 후에도 동일한 세션으로 로그인이 가능한 취약점이 발견되었습니다. 해당 취약점을 통해 세션 ID를 도용하여 악용하는 사례가 발생할 수 있습니다 |
| 5. | **http://ctf.segfaulthub.com:9575/login.php** | **유추가능한 인증정보 이용** | 사용자의 입력 값의 적절성 및 복잡성을 검증하는 필터링이 미흡하여 쉽게 유추할 수 있는 계정과 비밀번호를 생성 및 사용할 수 있는 취약점이 발견되었습니다. 이러한 취약점을 통해 계정 및 패스워드를 쉽게 유추할 수 있어 개인 정보 유출 및 침해가 발생할 수 있습니다. |
| 6. | [**http://ctf.segfaulthub.com:9575/login.php**](http://ctf.segfaulthub.com:9575/login.php)**,**  **http://ctf.segfaulthub.com:9575/user\_board/board.php** | **데이터 평문 전송** | 네트워크 데이터 전송 시 중요정보가 평문으로 전송되는 취약점을 발견하였습니다. 이러한 취약점은 공격자가 사용자의 정보를 탈취해 악용할 수 있습니다. |

1. 취약점 상세 내용
   1. LSB 커뮤니티 (http://ctf.segfaulthub.com:9575/login.php)
      1. XSS 크로스 사이트 스크립트

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 설명 | | |
| 발견URL | **URL** | **파라미터** | **메뉴** |
| http://ctf.segfaulthub.com:9575/mypage/mod\_addr.php |  | 로그인 > 마이페이지 > 주소 변경 |
| http://ctf.segfaulthub.com:9575/main.php | Title, content | 로그인 페이지 > 문의 게시판 |
| 취약점 상세내역 | 파라미터 값을 이용하여 페이지를 만들 때 클라이언트 측에서 실행할 수 있는 스크립트에 대한 필터링이 미흡하여 악의적인 스크립트가 클라이언트 측에서 실행될 수 있습니다. 이러한 취약점은 사용자의 민감한 정보를 탈취하거나 서버를 장악 할 수 있습니다. | | |

**Reflected XSS**

**스크린샷, 텍스트, 소프트웨어, 운영 체제이(가) 표시된 사진

자동 생성된 설명1. 회원 가입 후 로그인을 합니다.**

**2. 마이페이지 접속 후 주소변경으로 접속합니다.**

텍스트, 스크린샷, 인간의 얼굴, 만화 영화이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 디스플레이, 폰트이(가) 표시된 사진

자동 생성된 설명**3. 취약점 확인을 위하여 스크립트를 삽입하였습니다.**

**4. 아래 사진과 같이 Reflected XSS 취약점을 발견 할 수 있었습니다.**

텍스트, 소프트웨어, 스크린샷이(가) 표시된 사진

자동 생성된 설명

텍스트, 소프트웨어, 폰트, 웹 페이지이(가) 표시된 사진

자동 생성된 설명

**문의게시판 XSS**

**1. 문의 게시판에 접속합니다.**

텍스트, 스크린샷, 번호, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**2. 글쓰기 버튼을 누른 후 스크립트를 작성해 줍니다.**

텍스트, 스크린샷, 번호, 라인이(가) 표시된 사진

자동 생성된 설명

**3. 아래와 같이 XSS 취약점을 발견할 수 있었습니다.**

**제목부분**

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**내용부분**

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**Stored XSS**

**4. 내용부분에 alert 대신 세션값을 가져오는 스크립트를 삽입합니다.**

텍스트, 스크린샷, 디스플레이, 번호이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

자동 생성된 설명5**. 사이트 클릭 시 공격자의 사이트에 세션 ID가 전달되는 것을 확인하였습니다.**

**[보안권고안]**

**HTML Entity를 사용하여 입력 값에 대해 검증 및 필터링을 통해 XSS 공격을 방지 할 수 있습니다.**

* + 1. 악성 파일 업로드

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 설명 | | |
| 발견URL | **URL** | **파라미터** | **메뉴** |
| http://ctf.segfaulthub.com:9575/user\_board/write.php |  | 로그인 > 마이페이지 > 게시판 > 글쓰기 |
| 취약점 상세내역 | 서버에 업로드 되는 파일의 확장자를 검증하는 로직이 미흡하여 웹 서버에 명령을 내릴 수 있는 웹 쉘을 업로드 할 수 있습니다. 이러한 웹 쉘은 사용자의 정보를 탈취하거나 DB 정보를 탈취하는 공격이 가능합니다. | | |

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명**1. 게시판에 접속합니다.**

1. 텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

   자동 생성된 설명**글쓰기 버튼을 클릭하여 파일을 업로드 합니다.**
2. 텍스트, 소프트웨어, 멀티미디어 소프트웨어, 그래픽 소프트웨어이(가) 표시된 사진

   자동 생성된 설명**확장자를 변경한 파일을 올립니다.**
3. **웹 쉘 코드가 삽입된 파일이 정상적으로 올라가는 걸 확인 할 수 있습니다.**

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

자동 생성된 설명

**[보안 권고안]**

**파일 업로드 공격을 예방하기 위한 가장 효과적인 방법은 업로드하는 파일을 DB에 바이너리 형태로 저장해주는 것입니다.**

* + 1. 자동화공격

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 설명 | | |
| 발견URL | **URL** | **파라미터** | **메뉴** |
| http://ctf.segfaulthub.com:9575/user\_board/board.php |  | 로그인 > 게시판 페이지> 글쓰기, 수정 |
| 취약점 상세내역 | 일정 시간 내 게시글 작성 횟수에 제한을 두지 않는 취약점이 발견되었으며 이러한 취약점은 애플리케이션의 자원을 고갈시킬 수 있습니다. | | |

**1. 로그인 페이지에 접속합니다.**

텍스트, 스크린샷, 소프트웨어, 운영 체제이(가) 표시된 사진

자동 생성된 설명

**2. 게시판에 자동화를 통해 계속해서 게시글을 작성하였고, 시간내 횟수 제한이 없어 계속해서 만들어지는 것을 확인할 수 있었습니다.**

텍스트, 스크린샷, 번호, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**[보안 권고안]**

**웹 사이트의 과부화를 줄이기 위해 게시글 등록 등과 같은 서버에 요청을 보내는 행위에 일정시간을 정해 횟수를 지정해야한다.**

**CAPTCHA**

**컴퓨터와 사람을 구분하기 위한 완전 자동화 된 공개 튜링 테스트로 사람인지 자동화인지 구별해 예방할 수 있습니다.**

* + 1. 유추 가능한 세션ID(세션 고정), 불충분한 세션 종료

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 설명 | | |
| 발견URL | **URL** | **파라미터** | **메뉴** |
| http://ctf.segfaulthub.com:9575/login.php |  | 로그인 |
| 취약점 상세내역 | 로그인 전과 로그인 후의 세션 ID가 일정하게 고정된 취약점이 발견되었습니다. 또한 일정시간이 지난 후에도 동일한 세션으로 로그인이 가능한 취약점이 발견되었습니다. 해당 취약점을 통해 세션 ID를 도용하여 악용하는 사례가 발생할 수 있습니다 | | |

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명**1. 로그인전 세션 ID (h7b9au4lt82t4lc3jov04djoso)**

**2. 로그인 후 세션ID**

텍스트, 스크린샷, 소프트웨어, 웹 페이지이(가) 표시된 사진

자동 생성된 설명

**3. 일정시간이 지난 후에도 동일한 세션 ID**

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

자동 생성된 설명

**[보안 권고안]**

**웹 사이트는 사용자가 로그인을 할 때마다 새로운 세션ID를 생성하는 로직을 구현하고 기존 세션 ID는 파기하여야 한다.**

* + 1. 유추 가능한 인증정보 이용

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 설명 | | |
| 발견URL | **URL** | **파라미터** | **메뉴** |
| http://ctf.segfaulthub.com:9575/login.php | User\_id,  pw | 로그인 , 회원가입 |
|  | http://ctf.segfaulthub.com:9575/register.php |
| 취약점 상세내역 | 사용자의 입력 값의 적절성 및 복잡성을 검증하는 필터링이 미흡하여 쉽게 유추할 수 있는 계정과 비밀번호를 생성 및 사용할 수 있는 취약점이 발견되었습니다. 이러한 취약점을 통해 계정 및 패스워드를 쉽게 유추할 수 있어 개인 정보 유출 및 침해가 발생할 수 있습니다. | | |

**1.회원가입 페이지에 접속한 후 값을 입력합니다.**

텍스트, 스크린샷, 우주이(가) 표시된 사진

자동 생성된 설명

**2. 버프 스윗을 사용하여 공격한 결과 12값이 들어갔을 때 길이가 변화한 것을 발견하였습니다.**

텍스트, 스크린샷, 번호, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**3. 해당 정보로 로그인 시도 결과 로그인이 되는 걸 볼 수 있었습니다.**

텍스트, 스크린샷, 그래픽 디자인, 그래픽이(가) 표시된 사진

자동 생성된 설명

**[보안 권고안]**

**강력한 암호 정책 도입**

**강력한 암호를 사용할 수 있도록 특수문자, 대문자, 최소한의 비밀번호 길이를 사용하여 암호 강도를 높여야 합니다. 또한 강도를 평가하는 기능을 추가하여 강력한 암호를 생성하도록 요구 해야 합니다.**

* + 1. 데이터 평문전송

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 설명 | | |
| 발견URL | **URL** | **파라미터** | **메뉴** |
| http://ctf.segfaulthub.com:9575/login.php | uId, pwd | 로그인 |
| http://ctf.segfaulthub.com:9575/mypage/mypage.php | JUSO, detail,  Mod\_pw | 로그인 >마이페이지>주소변경 |
| http://ctf.segfaulthub.com:9575/user\_board/write.php | No, name,subject,memo,pwd | 로그인 > 게시판 >글 쓰기 |
| http://ctf.segfaulthub.com:9575/ask\_board/ask\_write.php | No,name,subject,memo,phone,pwd | 로그인페이지 >문의게시판 |
| 취약점 상세내역 | 네트워크 데이터 전송 시 중요정보가 평문으로 전송되는 취약점을 발견하였습니다. 이러한 취약점은 공격자가 사용자의 정보를 탈취해 악용할 수 있습니다. | | |

1. **로그인 페이지에 접속후 ID, PW를 입력 후 로그인을 진행해 줍니다.**

텍스트, 스크린샷, 소프트웨어, 운영 체제이(가) 표시된 사진

자동 생성된 설명

1. 텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

   자동 생성된 설명**버프 스윗으로 살펴 본 결과 유저의 ID, PW가 그대로 노출되는 것을 확인 할 수 있었습니다.**

**3. 마이페이지 접속 후 주소 변경에 접속합니다.**

텍스트, 스크린샷, 디자인이(가) 표시된 사진

자동 생성된 설명

4. 버프 스윗으로 살펴 본 결과 데이터가 평문으로 나오는 걸 확인 할 수 있었습니다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명5. 게시판 페이지에 접속 후 글쓰기 페이지에 접속합니다.

텍스트, 스크린샷, 소프트웨어, 번호이(가) 표시된 사진

자동 생성된 설명**6. 버프 스윗으로 확인해본 결과 데이터가 평문으로 나오는 걸 확인 할 수 있었습니다.**

**[보안 권고안]**

**민감한 정보를 통신 채널을 통하여 내보낼 때 반드시 암호화를 거쳐야 하며 , 필요할 경우 SSL, HTTPS 등과 같은 보안 채널을 사용해야 한다.**

1. 보안 권고안
   1. XSS 크로스 사이트 스크립트

|  |  |  |
| --- | --- | --- |
| 취약점 항목 | XSS | |
| 취약점 개요 | 웹 페이제에 악의적인 스크립트를 포함시켜 사용자 측에서 실행되게 유도할 수 있음. 예를 들어, 검증되지 않은 외부 입력이 동적웹페이지 생성에 사용될 경우, 전송된 동적 웹페이지를 열람하는 접속자의 권한으로 부적절한 스크립트가 수행되어 정보유출 등의 공격을 유발할 수 있음 | |
| 보안 조치 방법 | | |
| * 보안 조치 방법  1. HTML Entity   HTML Entity 을 통하여 특수문자를 필터링하여 예방할 수 있음 | |

* 1. 악성 파일 업로드

|  |  |  |
| --- | --- | --- |
| 취약점 항목 | 악성 파일 업로드 | |
| 취약점 개요 | 일반적으로 웹사이트내에 게시판 내 파일업로드가 가능한 곳에서는 확장자 제한을 두는데 파일 확장자를 제한하지 않거나 파일에 실행 권한을 제공해 공격자가 웹을 통해 직접 실행시킬 수 있는 경우 시스템 내부명령어를 실행하거나 외부와 연결하여 시스템을 제어할 수 있음 | |
| 보안 조치 방법 | | |
| * 보안 조치 방법  1. 업로드 되는 파일을 DB에 저장하기   업로드 되는 파일이 저장되는 서버를 웹서버와 분리시켜 예방 할 수 있음   1. 웹 서버에 업로드 대상 파일의 확장자를 검증하는 처리 프로그램을 통해 서버 사이트 스크립트 (JSP, PHP, JSP, 등) 파일의 업로드 차단 | |

|  |  |  |
| --- | --- | --- |
| 취약점 항목 | 자동화 공격 | |
| 취약점 개요 | 애플리케이션 운영시 특정 프로세스에 대한 접근시도 횟수 제한을 설정하지 않을 경우 공격자가 자동화 툴 및 봇을 활용하여 1분에 수백 번의 접근을 시도할 수 있음, 단 시간동안 특정 프로세스를 반복 실행하여 시스템 성능에 영향을 미칠 수 있음 | |
| 보안 조치 방법 | | |
| * 보안 조치 방법   1.보안 장비에서 조치  시스템 과부하를 방지하기 위해 패킷량을 모니터링 할 수 있는 시스템(IDS/IPS)을 구축하여 다량의 패킷이 유입될 경우 해당 접속을 차단    2. 홈페이지 개발 보안 조치  2.1   특정 시간 내 동일 프로세스가 반복 실행되지 않도록 시간제한 설정    2.2   웹 애플리케이션 로그인 관련 테이블에 로그인 시도 횟수를 저장하는 컬럼을 추가하여 로그인 시도가 있을 때마다 횟수를 증가시키고, 일정 횟수 이상이 되면 자동화 공격으로 인식하여 로그인을 할 수 없도록 차단    2.3   게시물 등록, 메일 발송 등의 기능에서 사용자의 요청이 일회성이 될 수 있도록 캡챠(이미지를 이용하여 확인 값을 표시하고 사용자가 값을 입력하여 인증) 등을 이용 | |

* 1. 자동화공격
  2. 유추 가능한 세션 ID , 불충분한 세션 종료

|  |  |  |
| --- | --- | --- |
| 취약점 항목 | 유추 가능한 세션 ID , 불충분한 세션 종료 | |
| 취약점 개요 | 사용자에 따라 고정된 세션ID를 발행하는 사이트에 공격자는 다른 사용자의 세션ID를 가지고 유효화되는 것을 자동으로 체크하여 유효화된 세션 ID로 정상적인 사이트를 이용 | |
| 보안 조치 방법 | | |
| * 보안 조치 방법  1. 고정 세션ID 금지   사용자에 따른 고정 세션ID를 발행하지 말고, 상용 웹서버나 웹 애플리케이션 플래폼에서 제공하는 세션ID를 사용하고, 가능하다면 맞춤형 세션 관리 매커니즘을 권고한다.   1. 인증한 후 새로운 세션 ID 발행   인증 기능에서 사용자가 인증을 받은 후 새로운 세션 ID를 할당 받도록 한다. | |

* 1. 유추가능한 인증정보 이용

|  |  |  |
| --- | --- | --- |
| 취약점 항목 | 유추가능한 인증정보 이용 | |
| 취약점 개요 | 유추 가능한 문자열 사용으로 계정 및 패스워드가 탈취 위험이 존재하며, 해당 위험을 방지하기 위해 값의 적절성 및 복잡성을 검증하는 로직을 구현 해야함 | |
| 보안 조치 방법 | | |
| * 보안 조치 방법  1. 패스워드 규정이 반영된 체크 로직을 적용하여 예방한다.   Ex>영문+ 대문자+ 특수문자 + 최소한의 비밀번호 길이 사용 | |

* 1. 데이터 평문전송

|  |  |  |
| --- | --- | --- |
| 취약점 항목 | 데이터 평문전송 | |
| 취약점 개요 | 개인 정보를 암호화하지 않고 평문으로 전송 처리하여 도청을 통해 노출되는 취약점으로 암호화를 통해 최소화 할 수 있다. 웹 상의 데이터 통신은 대부분 텍스트 기반으로 이루어져 있으며 이는 간단한 도청을 통해 쉽게 개인 정보의 탈취 및 도용이 가능하다. | |
| 보안 조치 방법 | | |
| * 보안 조치 방법   1. 웹 상에서의 전송 정보를 제한하여 불필요한 비밀번호, 주민등록번호, 계좌정보 와 같은 중요 정보의 전송을 최소화 해야 하며, 중요 정보에 대해서는 반듯이 SSL 등의 암호화를 사용하여 도청으로부터의 위험을 없애야 한다.  또한 쿠키와 같이 조작이 가능한 방식이 아닌 세션을 사용하여 공격자에 의한 데이터 위/변조를 차단해야 한다. | |

|  |  |
| --- | --- |
| 취약점 항목 | 유추가능한 인증정보 이용 |