**RBS PROJEKAT 2023**

**SQLi napad:**

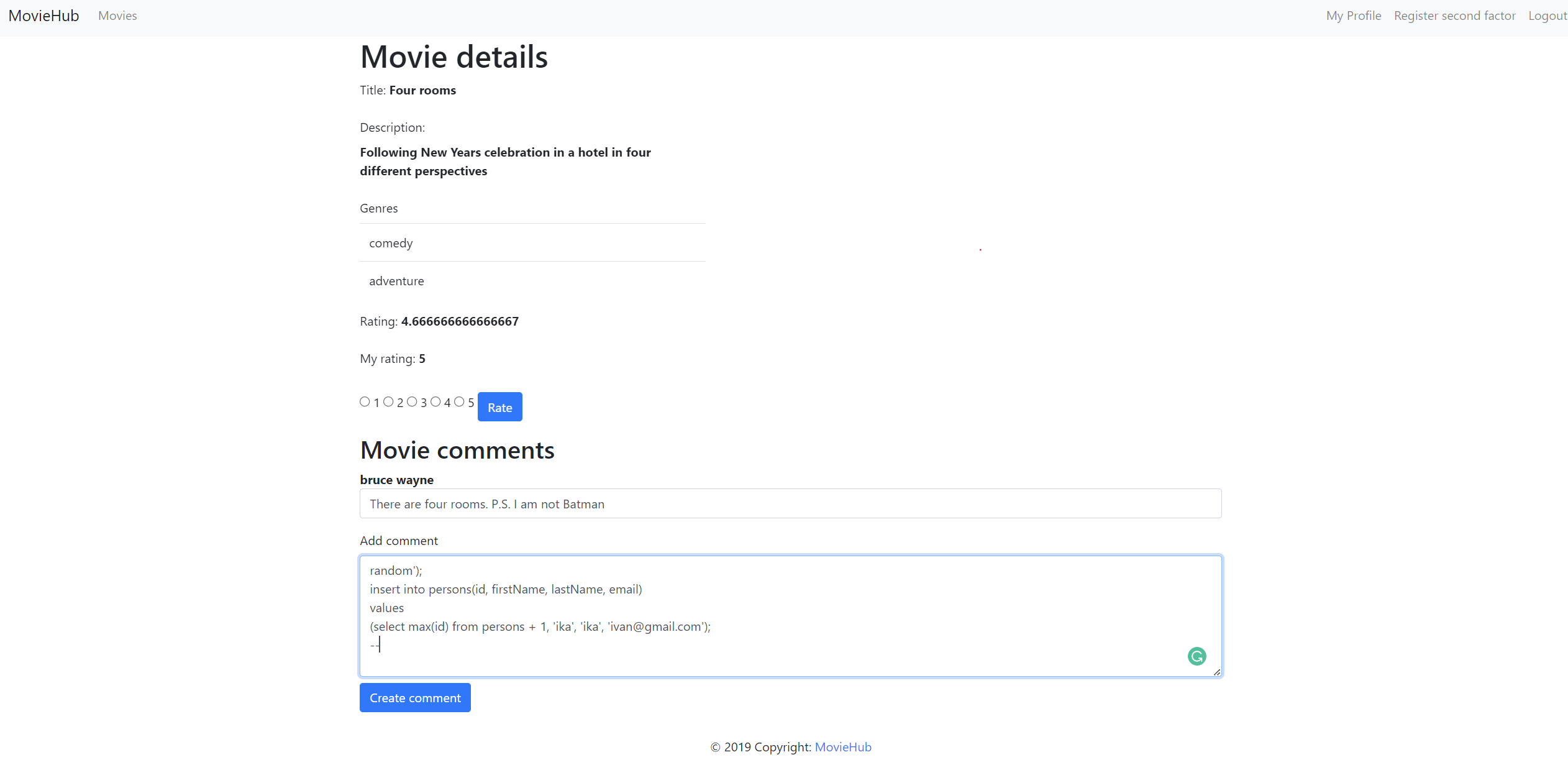
random');

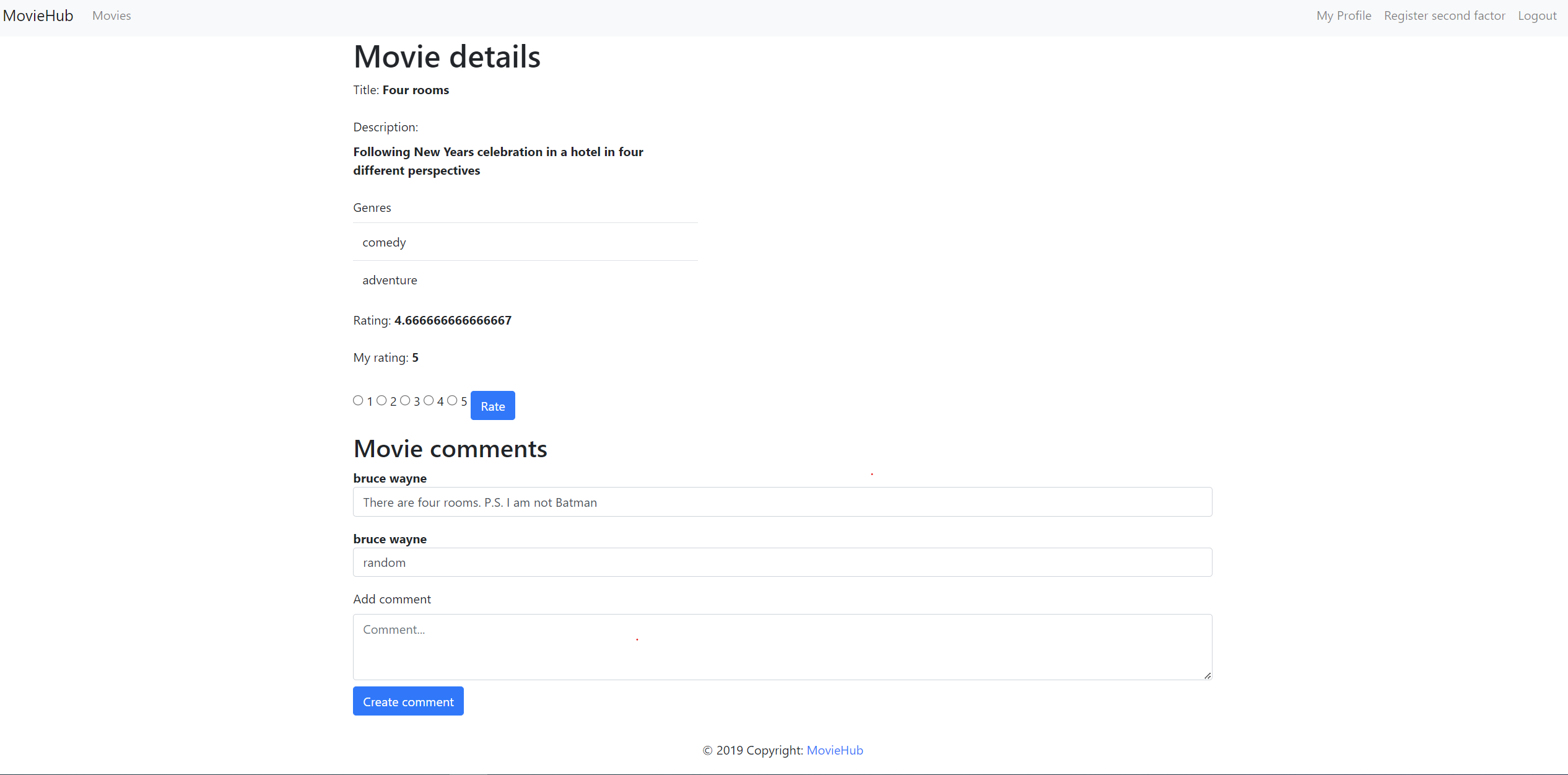
insert into persons(id, firstName, lastName, email)

values

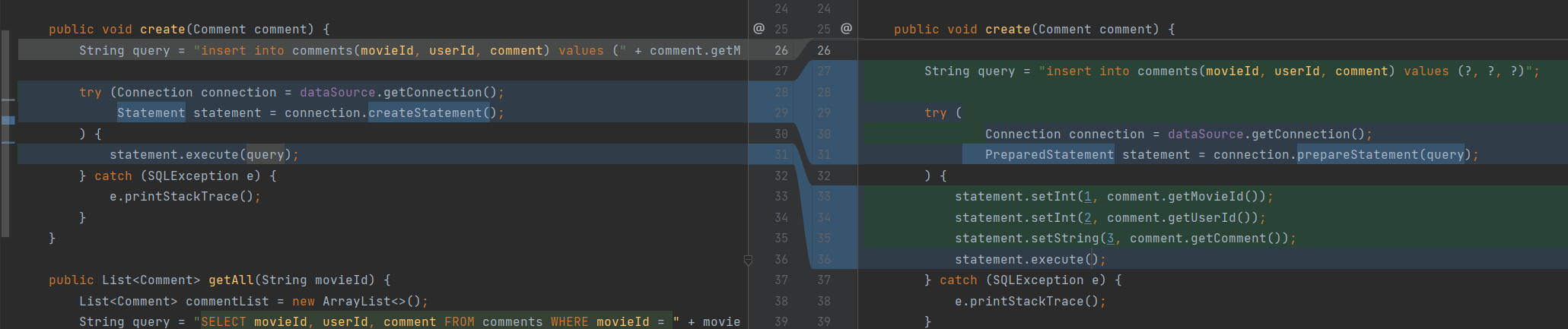
(select max(id) from persons + 1, 'ika', 'ika', 'ivan@gmail.com');

--

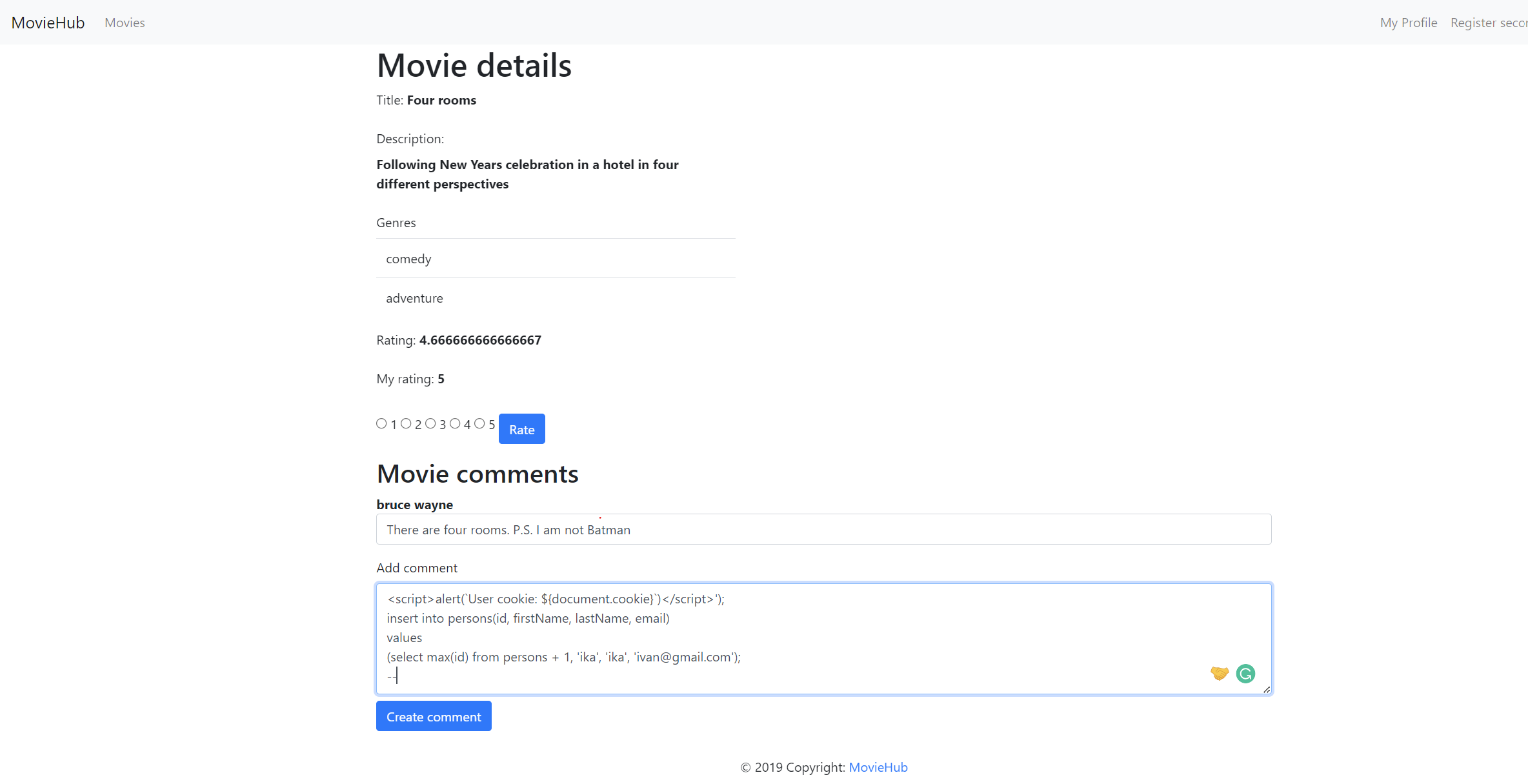


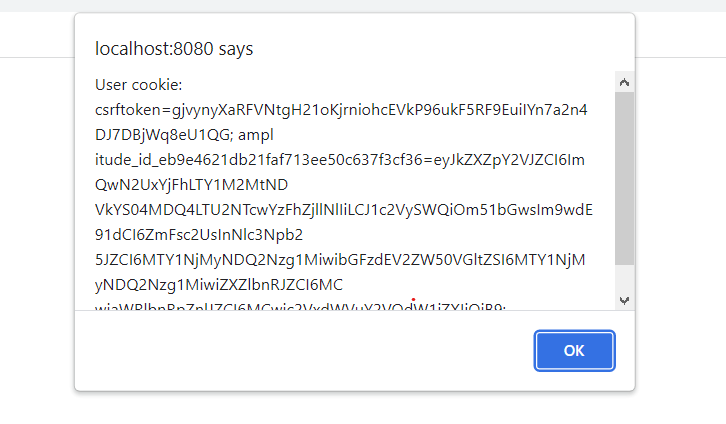


**SQLi odbrana:**

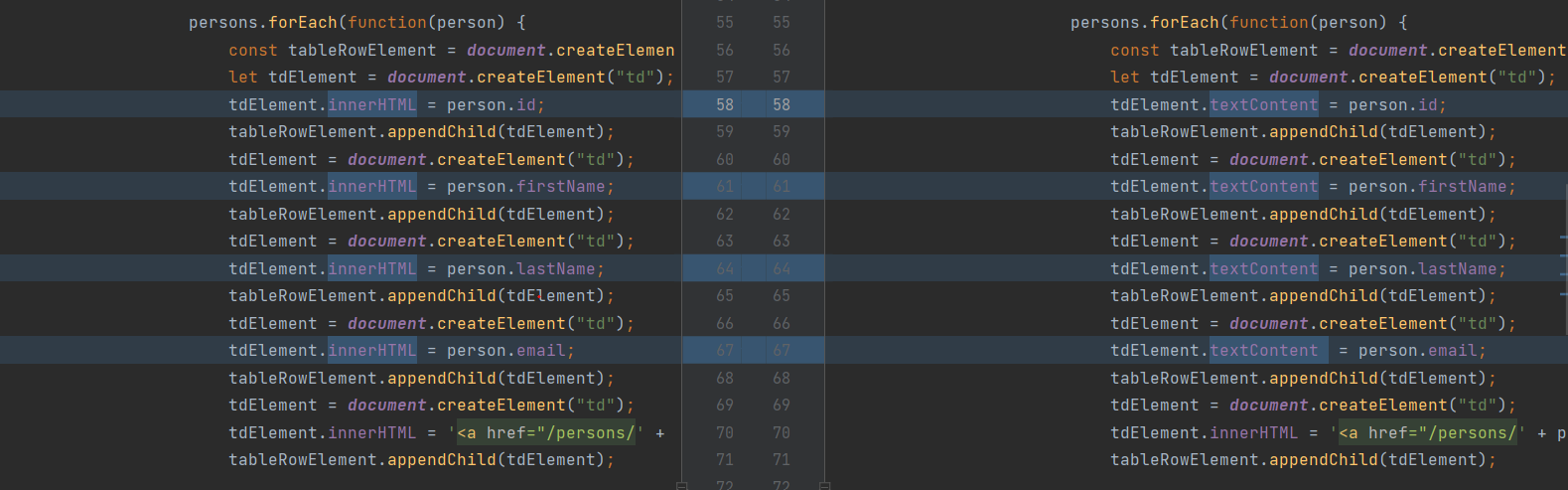
****

**XSS napad:**

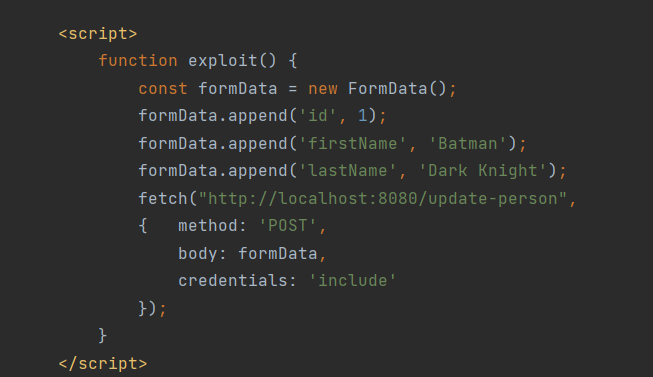
****

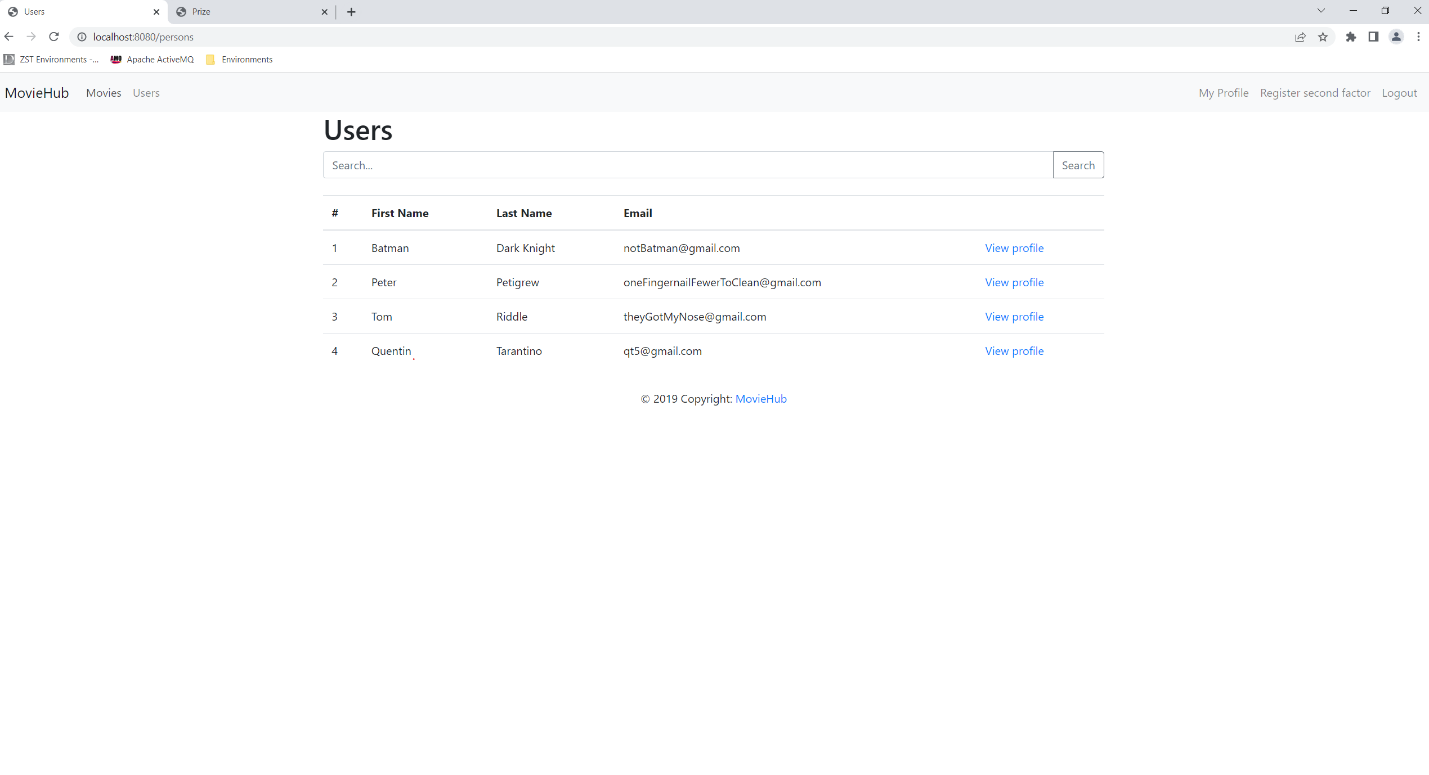
****

**XSS odbrana:**

****

**CSRF napad:**

****



**CSRF odbrana:**

@GetMapping("/persons/{id}")  
@PreAuthorize("hasAuthority('VIEW\_PERSON') || hasAuthority('UPDATE\_PERSON')")  
public String person(@PathVariable int id, Model model, HttpSession session) throws AccessDeniedException{  
 String csrfToken = session.getAttribute("CSRF\_TOKEN").toString();  
 model.addAttribute("CSRF\_TOKEN", csrfToken);  
 model.addAttribute("person", personRepository.get("" + id));  
 return "person";  
}

@PostMapping("/update-person")  
@PreAuthorize("hasAuthority('UPDATE\_PERSON')")  
public String updatePerson(Person person, HttpSession session, @RequestParam("csrfToken") String csrfToken) throws AccessDeniedException {  
  
 String sessionToken = session.getAttribute("CSRF\_TOKEN").toString();  
  
 if(!csrfToken.equals(sessionToken)){  
 *LOG*.error("Access denied! User " + SecurityUtil.*getCurrentUser*().getUsername() + " does not have necessary permissions to update person details.");  
 throw new AccessDeniedException("Access denied!");  
 }  
  
 return "redirect:/persons/" + person.getId();  
}

Takodje u formama se dodaje sledeci kod:

<input type="hidden" name="csrfToken" class="form-control" th:value="${CSRF\_TOKEN}">