

PSP0201

Week 3

Writeup

Group Name: ikun no 1

Members

ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 6 - [Web Exploitation] Be careful with what you wish on a Christmas night

Tool used: OWASP ZAP, firefox

Solution/Walkthrough:

Q1, Q2

Input validation strategies

Input validation should be applied on both **syntactical** and **Semantic** level.

Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).

Semantic validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).

Validating a U.S. Zip Code (5 digits plus optional -4)

```
^\d{5}(-\d{4})?$
```

Research from owasp cheat sheet.

Q3.

```
<!DOCTYPE html>

<html>
  <head>
    <meta charset="utf-8">
    <title>Santa's portal</title>
    <link rel="stylesheet" href="/static/style.css">
  </head>

  <body>
```

Inspect the site using inspect tools. The vulnerability can be found in the title tag.

Q4.

Welcome to Santa's official 'Make a Wish!' website


Here you can anonymously submit your Christmas wishes and see what other people wished too!


Santa's portal

← → ↻ 🏠 🔒 10.10.32.81:5000/?q=girlfriend



Put a random word in the make a wish section after it initiates, a q can be found on top of the address.

Q5.





Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:   Select...

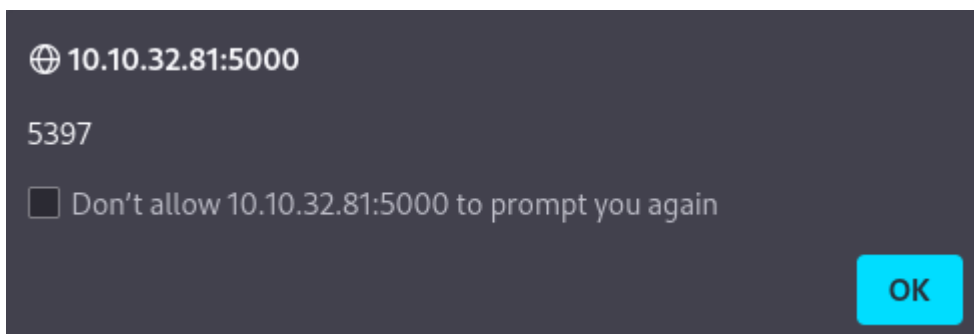
Use traditional spider: ☒

Use ajax spider: ☐ with

 Attack  Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

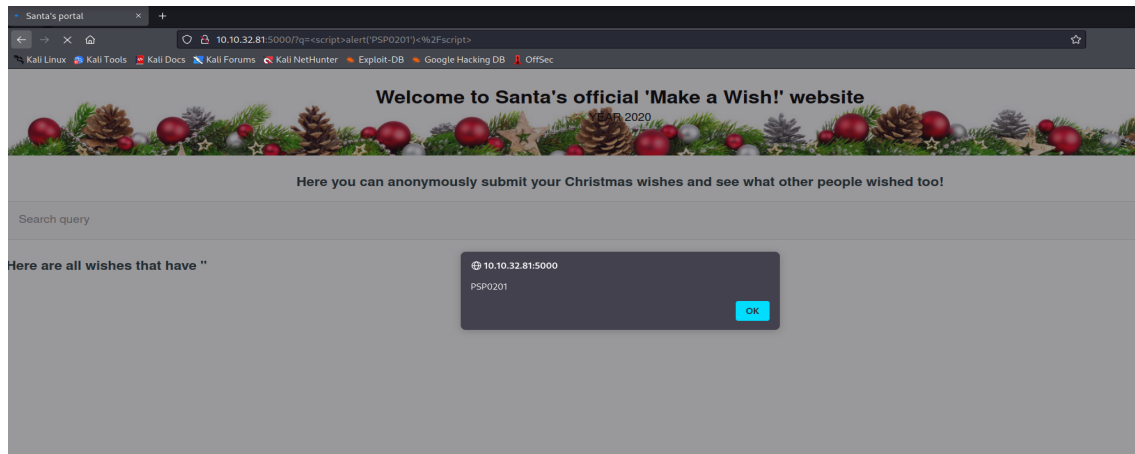
By using OWASP ZAP, scan the site and attack it.



2 pop out will prompt out after the scan is finished.

Q6.

A search query is put after this keyword parameter. The XSS can be exploited by putting a payload **instead** of the search query. The url starts with `10.10.100.27/reflected?keyword=`. By adding text onto the keyword, we can perform reflected XSS like `10.10.100.27/reflected?keyword=<script>alert(1)</script>` which results in an alert box with 1 on our screen.



From THM, we can know the way to prompt our own custom word. Copy the script and change the content inside the alert and it will show us the results. In this case I put in PSP0201 and it will prompt out an alert box.

Q7.

Close the page and open the page again. The xss attack can be experienced again.