

PSP0201

Week 2

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

cheat sheets but can significantly contribute to reducing their impact if implemented properly.

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).

Research and study from OWASP Cheat Sheet.

Q2

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

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

Research and study from OWASP Cheat Sheet.

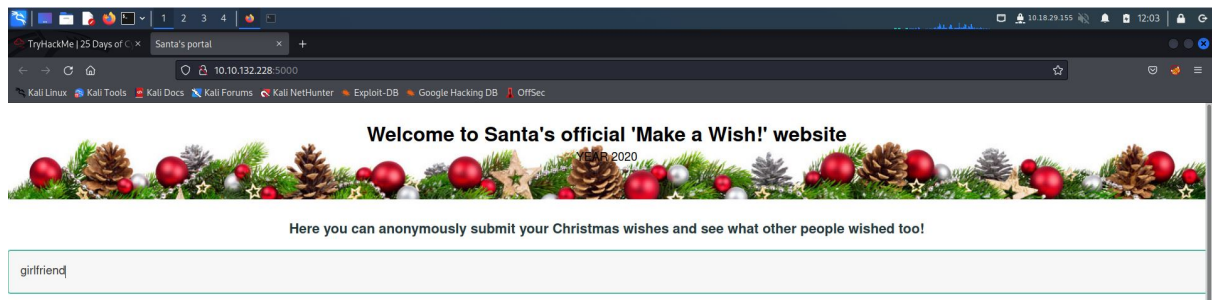
Q3

Search HTML

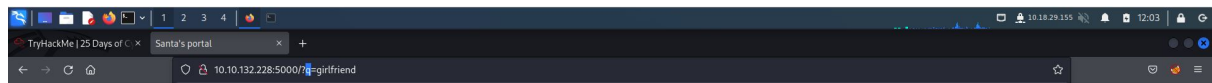
```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>Santa's portal</title>
    <link rel="stylesheet" href="/static/style.css">
  </head>
  <body>
```

Inspect the webpage. Examine the html page. The vulnerability is found.

Q4

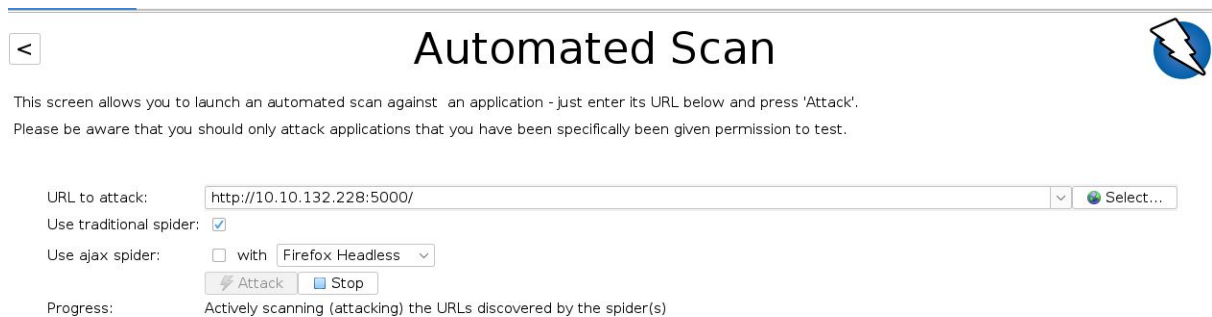


on the "Make a wish" website search for random text.

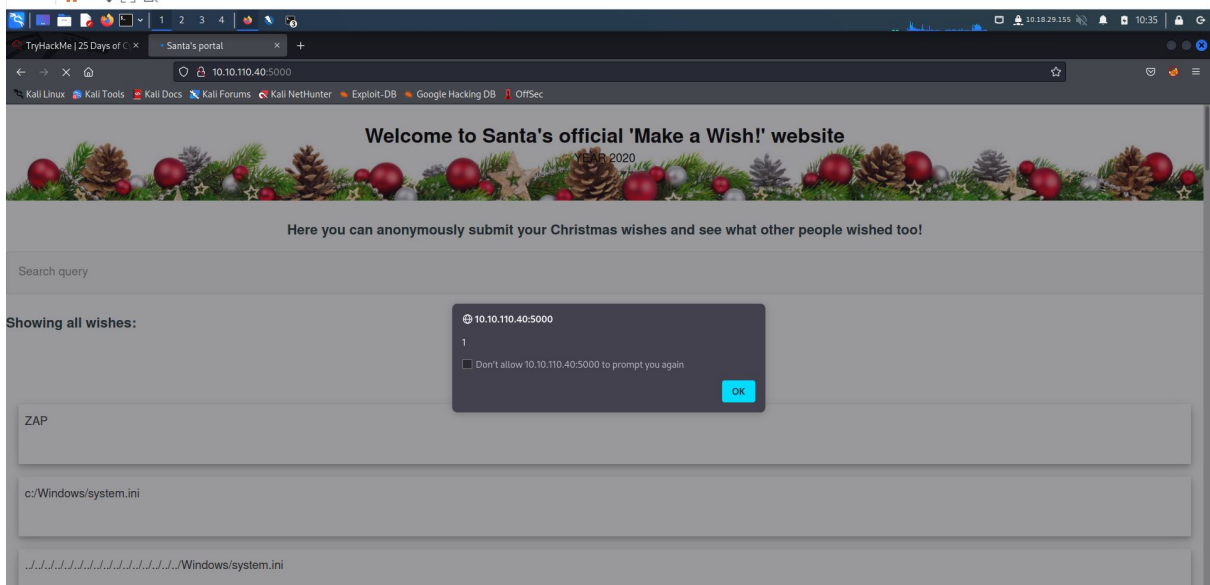
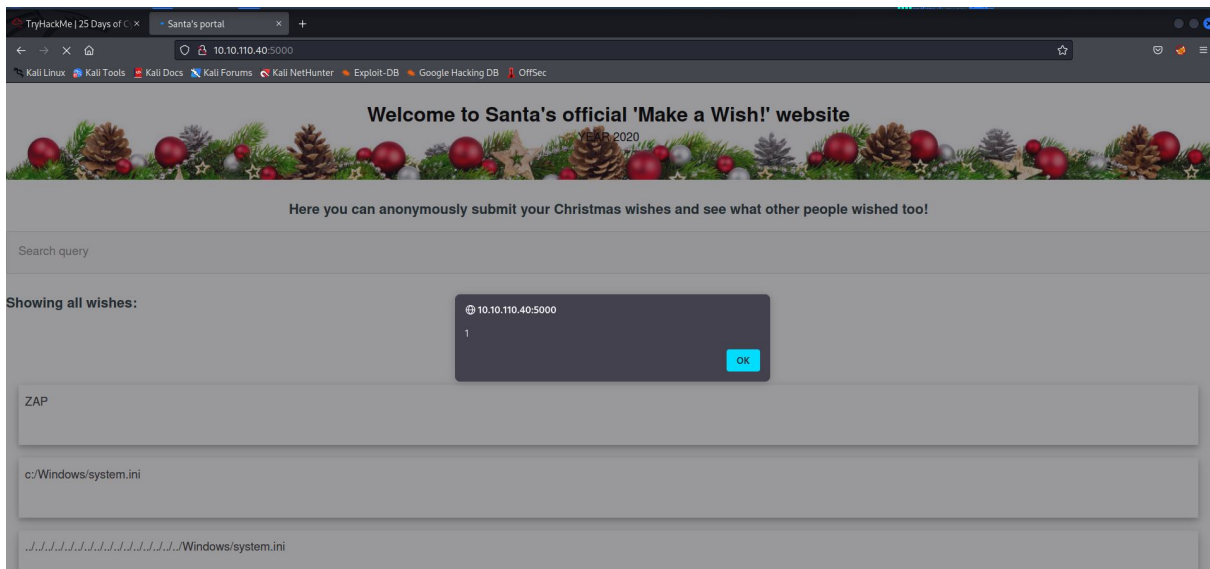


Initiate it, on the search bar, a 'q' is found.

Q5

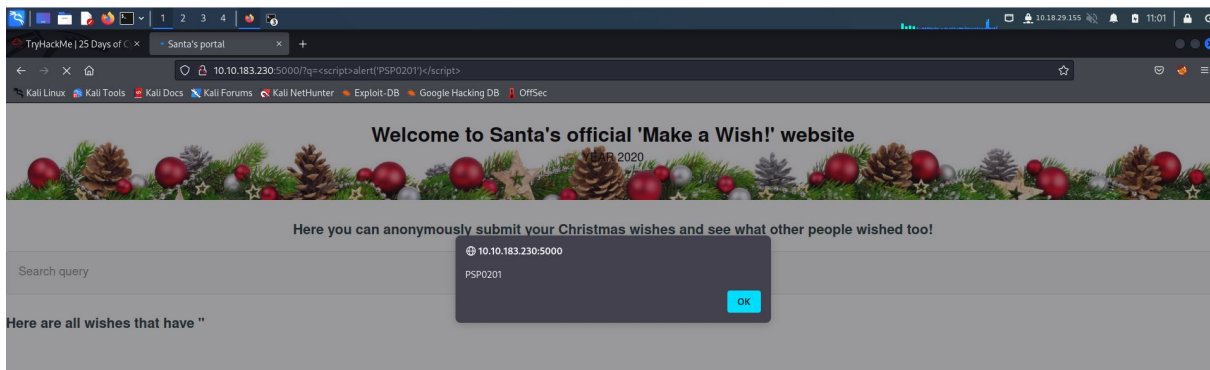


Open OWASP ZAP, copy the webpage link and attack it using zap.



After the automatic scan is finished, refresh the site. Automatically 2 alerts will pop out.

Q6



An alert saying 'PSP0201' can be produced by search [`<script>alert('PSP0201')</script>`] in the wish text box.

Q7

Close the page and revisit it. The XSS attack is re-experienced.