

API Testing

Setup:

Target : Vulnerable Lab From Tryhackme (BookStore)

Target IP : 10.48.170.135

Overview:

Performed an API Testing on the vulnerable machine and identified critical weakness which may provide attacker an full knowledge of the other users data and can also end up in full system takeover, The bugs are “Information Disclosure” and “Path Traversal” .

Test ID	Vulnerability	Severity	Vulnerable Endpoint
01	Information Disclosure	Medium	/api
02	Path Traversal	Critical	/api/v1/resources/books?show=

Description:

Information Disclosure is said to be the protected information in the server which can be accessible to anyone visiting the page which may lead to sensitive details about the users and their accounts.

Path traversal is when an attacker is able to utilize the vulnerable parameter to read arbitrary files in the server or the system e.g. ../../etc/passwd

Findings:

1. Information Disclosure:

Request	Response
<pre>1 GET /api HTTP/1.1 2 Host: 10.48.163.65:5000 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:147.0) Gecko/20100101 Firefox/147 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.9 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Upgrade-Insecure-Requests: 1 9 X-FoxColor: red 10 Priority: u=0, i 11 12</pre>	<pre>1 HTTP/1.0 200 OK 2 Content-Type: text/html; charset=utf-8 3 Content-Length: 825 4 Access-Control-Allow-Origin: * 5 Server: Werkzeug/0.14.1 Python/3.6.9 6 Date: Thu, 22 Jan 2026 13:32:01 GMT 7 8 9 <title> 10 API Documentation 11 </title> 12 <h1> 13 API Documentation 14 </h1> 15 Since every good API has a documentation we have one as well! 16 </h1> 17 The various routes this API currently provides are: 18 <h2> 19 <div> 20 <p> 21 /api/v2/resources/books/all (Retrieve all books and get the output in a json format) 22 </p> 23 <p> 24 /api/v2/resources/books/random4 (Retrieve 4 random records) 25 </p> 26 <p> 27 /api/v2/resources/books?id=1(Search by a specific parameter , id parameter) 28 </p> 29 <p> 30 /api/v2/resources/books?author=J.K. Rowling (Search by a specific parameter, this que 31 will return all the books with author=J.K. Rowling) 32 </p> 33 <p> 34 /api/v2/resources/books?published=1993 (This query will return all the books publishe 35 the year 1993) 36 </p> 37 <p> 38 /api/v2/resources/books?author=J.K. Rowlingspublished=2003 (Search by a combination o 39 or more parameters) 40 </p></pre>

Identified on the Endpoint : /api
Result : Disclosure of all api endpoints

2. Path Traversal

1. Found an hidden parameter through Fuzzing

Request	Payload	Status code	Response received	Error	Timeout	Length
1623	show	500	99			23269
0		200	94			393
883	id	200	94			393
1	0	404	88			259
2	00	404	102			259
3	01	404	91			259
4	02	404	07			350

Request	Response
Pretty	Raw Hex Render
1	HTTP/1.0 500 INTERNAL SERVER ERROR
2	Content-Type: text/html; charset=utf-8
3	X-XSS-Protection: 0
4	Connection: close
5	Server: Werkzeug/0.14.1 Python/3.6.9
6	Date: Thu, 22 Jan 2026 13:24:47 GMT
7	
8	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
9	"http://www.w3.org/TR/html4/loose.dtd">
0	<html>
1	<head>
2	<title>
3	<link rel="stylesheet" href="__debugger__=yes&cmd=resource&f=style.css"
4	type="text/css">
5	<!-- We need to make sure this has a favicon so that the debugger does
6	not by accident trigger a request to /favicon.ico which might
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
0	
1	
2	
3	
4	
5	
6	
7	
8	

API Testing Summary:

Performed an API testing on the Bookstore Web page and identified two security weaknesses in the website which is "Information Disclosure" and "Path Traversal". On various endpoints `/api` and `/api/v1/resources/books?show=`. These vulnerabilities lead to providing an attacker sensitive information and the attacker able to read sensitive files from the server.