

# WEB APPLICATION SECURITY ASSESSMENT REPORT

(Comprehensive Vulnerability Analysis & Penetration Testing)

## Project Details

**Project Title:** Web Application Security Testing – OWASP Juice Shop

**Task Number:** FUTURE\_CS\_01

**Client / Organization:** Future Interns

**Application Under Test (AUT): OWASP Juice Shop (Docker Deployment)**

**CIN ID :** FIT/OCT25/CS4249

**Submission Date:** 16/11/2025

**Prepared By:** Jeetesh Maurya)

# TABLE OF CONTENTS

- 1. Executive Summary**
- 2. Assessment Objectives**
- 3. Scope of Work**
  - o 3.1 In-Scope Components
  - o 3.2 Out-of-Scope Components
- 4. Testing Environment**
- 5. Tools and Resources Used**
- 6. Methodology**
  - o 6.1 Reconnaissance
  - o 6.2 Manual & Automated Testing
  - o 6.3 Exploitation
  - o 6.4 Verification & Evidence Collection
- 7. Summary of Vulnerabilities Identified**
- 8. Detailed Vulnerability Analysis**
  - o 8.1 F-01: Username Enumeration
  - o 8.2 F-02: Reflected Cross-Site Scripting (XSS)
  - o 8.3 F-03: Directory Browsing / Sensitive Data Exposure
- 9. OWASP Top 10 Mapping (2021)**
- 10. Risk Rating Matrix**
- 11. Recommendations & Best Practices**
- 12. Conclusion**

# 1. Executive Summary

This security assessment focused on identifying vulnerabilities in the OWASP Juice Shop web application, an intentionally insecure platform designed for hands-on security testing.

The assessment simulated real-world penetration testing activities that attackers commonly perform, including authentication testing, input validation checks, access control validation, and security misconfiguration assessment.

The testing revealed **three key vulnerabilities**, each of which could be exploited under real-world conditions:

- Username Enumeration
- Reflected Cross-Site Scripting
- Directory Browsing / Sensitive Data Exposure

While Juice Shop is intentionally vulnerable, these findings mimic realistic security flaws frequently found in modern web applications.

Addressing such vulnerabilities would significantly strengthen any system's security posture.

## 2. Assessment Objectives

The main objectives of this engagement were:

- To identify common and impactful vulnerabilities in a controlled environment
- To understand exploitation techniques used by attackers
- To learn and implement OWASP Top 10 testing standards
- To gain hands-on experience with security tools like Burp Suite, OWASP ZAP, and Docker
- To prepare a formal security assessment document suitable for professional portfolio use

# 3. Scope of Work

## 3.1 In-Scope Components

Component	Status
Application URL	<a href="http://localhost:3000">http://localhost:3000</a>
Authentication Pages	Included
Search Functionality	Included
Public Endpoints (e.g., /ftp directory)	Included
API Endpoints (as captured via Burp HTTP History)	Included

## 3.2 Out-of-Scope Components

Component	Reason
Denial of Service Attacks	Not permitted for local system stability
Backend Database Testing	Requires internal access
Source Code Review	Not included in black-box assessment
Server OS Exploitation	Beyond scope of web app testing

# 4. Testing Environment

Parameter	Details
Operating System	Windows 11
Deployment Method	Docker Desktop
Application Container	bkimminich/juice-shop
Browser Used	Burp-Suite Chromium
Network Configuration	Localhost (no VPN or proxy interference)

# 5. Tools and Resources Used

## ❖ Primary Tools

- **Burp Suite Community Edition** – Interception, manual testing, request manipulation
- **OWASP ZAP** – Automated scanning and spidering
- **Docker Desktop** – Running the Juice Shop container

## ❖ Supporting Tools

- Windows CMD / PowerShell
- Chromium browser (bundled with Burp Suite)
- Firefox (optional for comparison)

## ❖ Standards & Documentation

- OWASP Testing Guide v4
- OWASP Top 10 (2021)
- CVSS v3.1 Risk Calculator

# 6. Methodology

This assessment was executed in four main phases:

## 6.1 Reconnaissance

- Identified accessible endpoints through browsing and proxy logs
- Captured all HTTP/HTTPS requests using Burp Proxy
- Noted application behavior and error messages
- Mapped directory structures such as /ftp

## 6.2 Manual & Automated Testing

Techniques used:

- Input fuzzing
- HTML/JS payload injection
- Parameter tampering
- Directory traversal attempts
- Authentication bypass attempts

Automated Scans:

- OWASP ZAP passive scan
- Burp Suite issue alerts

## 6.3 Exploitation

Verified vulnerabilities using:

- Specially crafted payloads
- Manipulated HTTP request headers
- Path guessing
- Manual navigation to sensitive endpoint

## 6.4 Verification & Evidence Collection

- Screenshots of vulnerable pages
- Screenshot of impacted request in Burp Suite
- Consistent replication of vulnerabilities

# 7. Detailed Vulnerability Analysis

## 7.1 Finding F-01: Username Enumeration

**Severity:** Medium

**CVSS v3.1 Score:** 5.3

**OWASP Category:** A07 – Identification & Authentication Failures

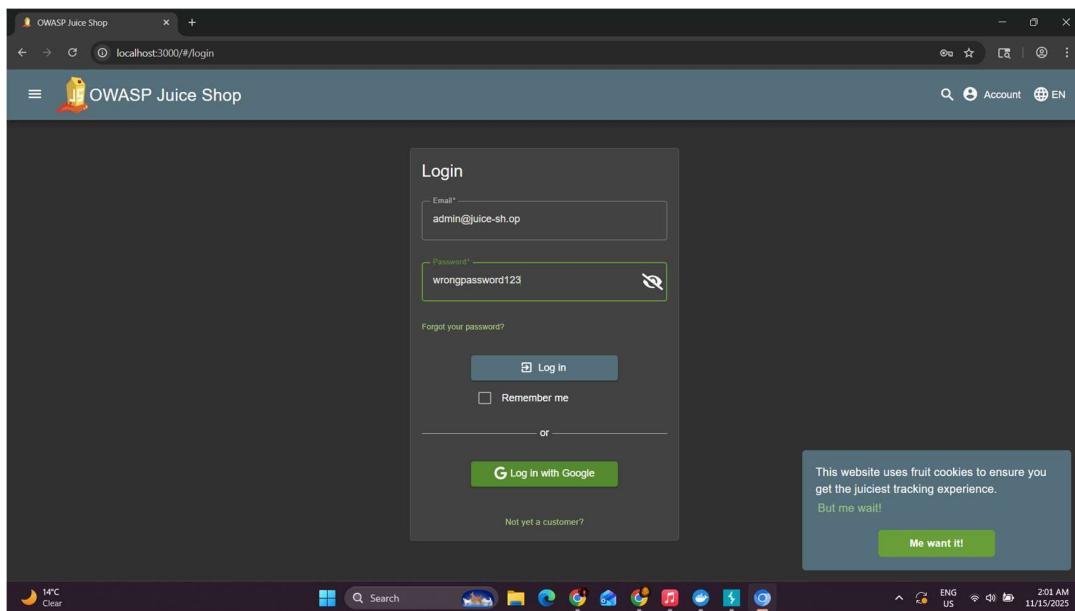
## Description

The login functionality displays **different error messages** depending on whether a username exists.

This allows attackers to verify if an account is registered.

## Technical Evidence

- Invalid user input → “User does not exist”
- Valid user input → “Invalid password”  
This discrepancy leaks user existence.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start resp...
1	http://localhost:3000	GET	/			304	393	JSON	json			127.0.0.1			02:00:21 15 ...	8080	4
7	http://localhost:3000	GET	/socket.io/1/socket.json			304	392	text	io/			127.0.0.1			02:00:21 15 ...	8080	5
9	http://localhost:3000	GET	/socket.io/1/4&transport=poll...	✓		200	326	text	io/			127.0.0.1			02:00:22 15 ...	8080	5
10	http://localhost:3000	GET	/rest/admin/application-configuration			304	324					127.0.0.1			02:00:22 15 ...	8080	39
11	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:00:22 15 ...	8080	14
12	http://localhost:3000	GET	/api/Challenges/?name=Score%20B...	✓		304	305					127.0.0.1			02:00:22 15 ...	8080	197
13	http://localhost:3000	GET	/rest/language			304	306					127.0.0.1			02:00:22 15 ...	8080	53
15	http://localhost:3000	POST	/socket.io/1/E0D+4&transport=poll...	✓		200	215	HTML	io/			127.0.0.1			02:00:22 15 ...	8080	3
16	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:00:22 15 ...	8080	9
17	http://localhost:3000	GET	/socket.io/1/E0D+4&transport=poll...	✓		200	262	text	io/			127.0.0.1			02:00:22 15 ...	8080	7
18	http://localhost:3000	GET	/socket.io/1/E0D+4&transport=web...	✓		101	129	text	io/			127.0.0.1			02:00:22 15 ...	8080	2
19	http://localhost:3000	GET	/rest/admin/application-configuration			304	304					127.0.0.1			02:00:22 15 ...	8080	10
20	http://localhost:3000	GET	/api/Challenges/?name=Score%20B...	✓		304	305					127.0.0.1			02:00:22 15 ...	8080	54
21	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:00:22 15 ...	8080	6
22	http://localhost:3000	GET	/socket.io/1/E0D+4&transport=poll...	✓		200	230	text	io/			127.0.0.1			02:00:22 15 ...	8080	92
23	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:00:23 15 ...	8080	3
24	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:00:23 15 ...	8080	6
25	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:00:23 15 ...	8080	3
26	http://localhost:3000	POST	/rest/user/login	✓		401	413	HTML				127.0.0.1			02:01:39 15 ...	8080	19
27	http://localhost:3000	GET	/rest/user/whoami			200	394	JSON				127.0.0.1			02:01:39 15 ...	8080	12
28	http://localhost:3000	GET	/rest/user/whoami			304	303					127.0.0.1			02:01:39 15 ...	8080	4

Event log (1) All issues

Memory: 150.3MB

Disabled |

## Impact

- Attackers can build a list of valid users
- Enables targeted password brute-force attacks
- Increases likelihood of credential stuffing attacks

## Attack Scenario

An attacker automates username attempts through a bot:  
If the system reveals correct usernames, attackers focus password attacks only on valid accounts.

## Recommendations

- Standardize error messages to a generic:  
**“Invalid username or password”**
- Add CAPTCHA or rate-limiting
- Implement account lockout mechanisms

## 7.2 Finding F-02: Reflected Cross-Site Scripting (XSS)

**Severity:** Medium–High

**CVSS v3.1 Score:** 6.4

**OWASP Category:** A03 – Injection

### Description

The search parameter reflects user input directly without sanitization.

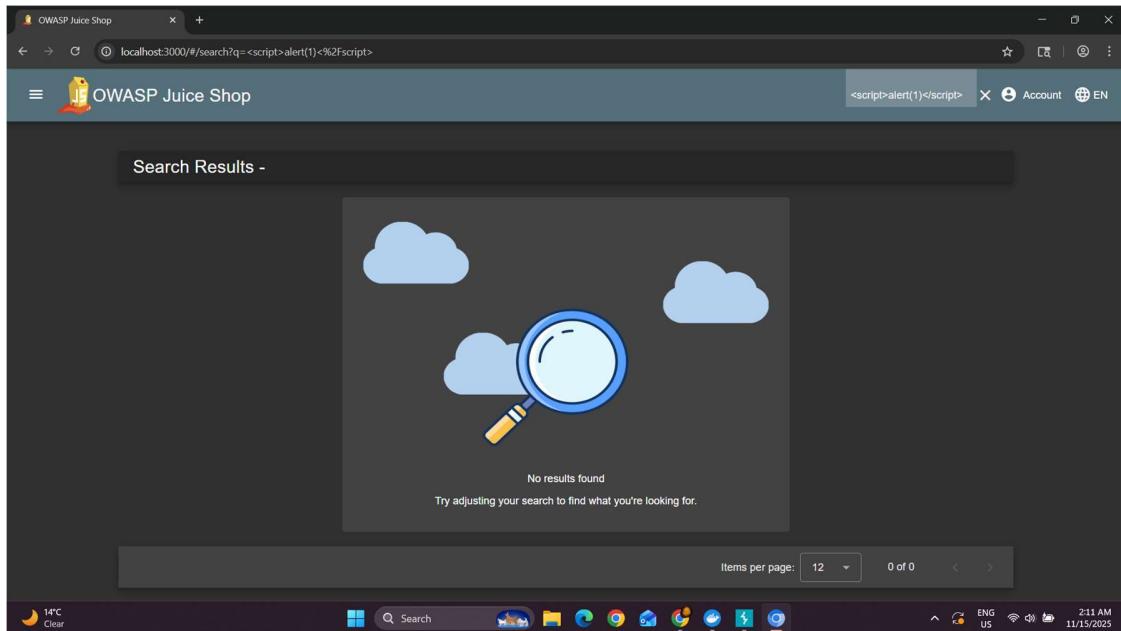
Testing with payload:

```
<script>alert(1)</script>
```

revealed potential XSS behavior (depending on version and context).

### Impact

- Execution of attacker-injected JavaScript
- Theft of session cookies
- Redirection to malicious pages
- Potential account compromise



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	http://localhost:3000	GET	/assets/18nen.json			200	393	text	io/			127.0.0.1	02:00:21 15 ...	8080	4		
7	https://localhost:3000	GET	/asset/18nen.json			304	392	JSON	json			127.0.0.1	02:00:21 15 ...	8080	5		
8	http://localhost:3000	GET	/socket.io/4/socket-transport-polling...		✓	200	226	text	io/			127.0.0.1	02:00:22 15 ...	8080	39		
10	http://localhost:3000	GET	/rest/admin/application-version...			304	304					127.0.0.1	02:00:22 15 ...	8080	14		
11	http://localhost:3000	GET	/rest/admin/application-configurat...			304	306					127.0.0.1	02:00:22 15 ...	8080	197		
12	http://localhost:3000	GET	/api/challenges/?name=Score%20B...		✓	304	305					127.0.0.1	02:00:22 15 ...	8080	53		
13	http://localhost:3000	GET	/rest/languages			304	306					127.0.0.1	02:00:22 15 ...	8080	3		
15	http://localhost:3000	POST	/socket.io/4/socket-transport-polling...		✓	200	215	HTML	io/			127.0.0.1	02:00:22 15 ...	8080	9		
16	http://localhost:3000	GET	/rest/admin/application-configurat...			304	306					127.0.0.1	02:00:22 15 ...	8080	7		
17	http://localhost:3000	GET	/rest/admin/application-version...			200	252	text	io/			127.0.0.1	02:00:22 15 ...	8080	2		
18	https://localhost:3000	GET	/socket.io/4/socket-transport-web...		✓	101	129	text	io/			127.0.0.1	02:00:22 15 ...	8080	10		
19	http://localhost:3000	GET	/rest/admin/application-version...			304	304					127.0.0.1	02:00:22 15 ...	8080	54		
20	http://localhost:3000	GET	/api/challenges/?name=Score%20B...		✓	304	305					127.0.0.1	02:00:22 15 ...	8080	92		
21	http://localhost:3000	GET	/rest/admin/application-configurat...			304	306					127.0.0.1	02:00:22 15 ...	8080	6		
22	http://localhost:3000	GET	/socket.io/4/socket-transport-polling...		✓	200	230	text	io/			127.0.0.1	02:00:22 15 ...	8080	3		
23	http://localhost:3000	GET	/rest/admin/application-configurat...			304	306					127.0.0.1	02:00:23 15 ...	8080	6		
24	http://localhost:3000	GET	/rest/admin/application-configurat...			304	306					127.0.0.1	02:00:23 15 ...	8080	62		
25	http://localhost:3000	GET	/rest/admin/application-configurat...			304	306					127.0.0.1	02:00:23 15 ...	8080	14		
26	http://localhost:3000	POST	/rest/user/login		✓	401	112	HTML				127.0.0.1	02:01:39 15 ...	8080	4		
27	http://localhost:3000	GET	/rest/user/whohami			200	394	JSON				127.0.0.1	02:01:39 15 ...	8080	5		
28	http://localhost:3000	GET	/rest/user/whohami			304	303					127.0.0.1	02:01:39 15 ...	8080	4		
29	http://localhost:3000	POST	/rest/user/login		✓	401	413	HTML				127.0.0.1	02:06:01 15 ...	8080	14		
30	http://localhost:3000	GET	/rest/user/whohami			304	303					127.0.0.1	02:06:01 15 ...	8080	5		
31	http://localhost:3000	GET	/rest/user/whohami			304	303					127.0.0.1	02:06:01 15 ...	8080	4		
32	http://localhost:3000	GET	/api/Quantify/			304	306					127.0.0.1	02:08:17 15 ...	8080	62		
33	http://localhost:3000	GET	/rest/products/search?q=		✓	304	306					127.0.0.1	02:08:17 15 ...	8080	39		

## Attack Scenario

A victim receives a link such as:

`http://localhost:3000/#/search?q=<script>alert("pwned")</script>`

If clicked, attacker code executes instantly.

## Recommendations

- Use server-side sanitization libraries
  - Encode all output using HTML entity encoding
  - Deploy Content Security Policy (CSP)
  - Validate inputs using whitelist filters

## 7.3 Finding F-03: Directory Browsing / Sensitive Data Exposure

**Severity:** High

**CVSS v3.1 Score:** 7.1

**OWASP Category:** A01 – Broken Access Control  
**Secondary Category:** A05 – Security Misconfiguration

## Description

The `/ftp` directory is publicly accessible and lists internal files:

`http://localhost:3000/ftp`

This is a common misconfiguration where a server exposes its internal filesystem.

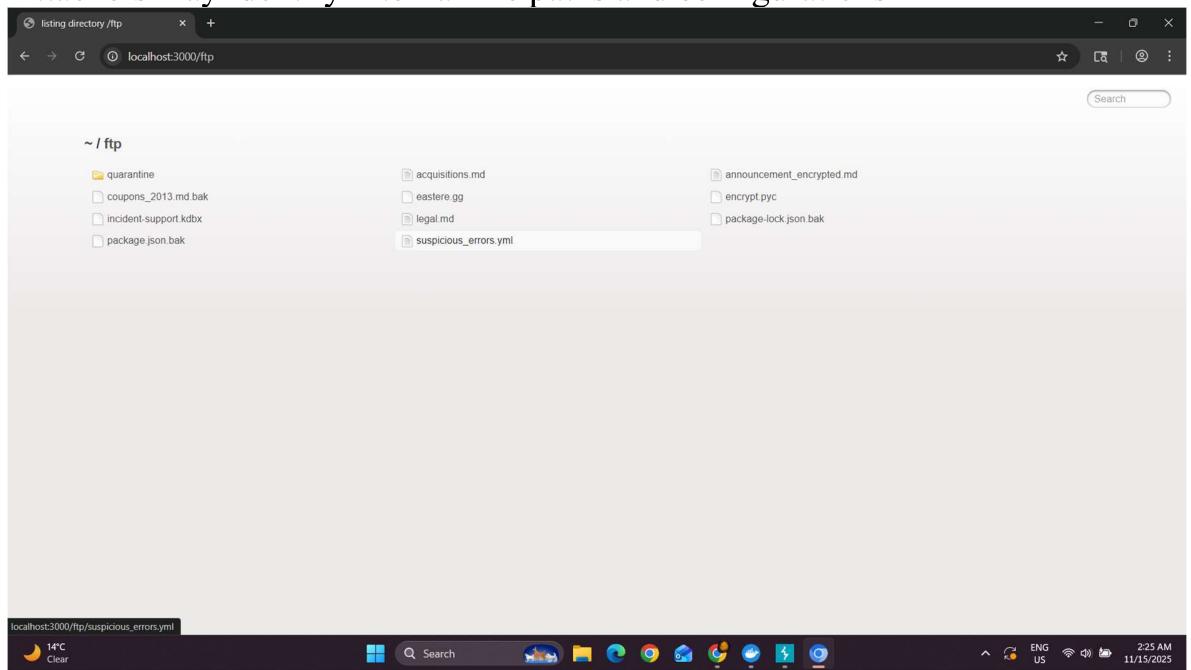
## Technical Evidence

Accessible files included:

- Invoices
- Images
- Log files
- Data exports (depending on version)

## Impact

- Leakage of confidential information
- Data theft
- Increased attack surface
- Attackers may identify internal file paths and configurations



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
1	http://localhost:3000	GET	/			304	393					127.0.0.1			02:20:31 15 ...	8080	2
7	http://localhost:3000	GET	/assets/i18n/en.json			304	392	JSON	json			127.0.0.1			02:20:32 15 ...	8080	34
9	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:20:32 15 ...	8080	3
10	http://localhost:3000	GET	/socket.io/?EIO=4&transport=poll...	✓		200	326	text	io/			127.0.0.1			02:20:32 15 ...	8080	50
11	http://localhost:3000	GET	/rest/admin/application-version			304	304					127.0.0.1			02:20:32 15 ...	8080	175
12	http://localhost:3000	GET	/api/Challenges?nameScore%20B...	✓		304	305					127.0.0.1			02:20:32 15 ...	8080	53
13	http://localhost:3000	GET	/rest/language			304	306					127.0.0.1			02:20:33 15 ...	8080	29
14	http://localhost:3000	GET	/api/Quantities/			304	306					127.0.0.1			02:20:33 15 ...	8080	16
15	http://localhost:3000	GET	/rest/products/search?q=	✓		304	306					127.0.0.1			02:20:33 15 ...	8080	3
17	http://localhost:3000	POST	/socket.io/?EIO=4&transport=poll...	✓		200	215	HTML	io/			127.0.0.1			02:20:33 15 ...	8080	3
18	http://localhost:3000	GET	/socket.io/?EIO=4&transport=poll...	✓		200	262	text	io/			127.0.0.1			02:20:33 15 ...	8080	3
19	http://localhost:3000	GET	/rest/admin/application-configuration	✓		304	129					127.0.0.1			02:20:33 15 ...	8080	7
20	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:20:33 15 ...	8080	8
21	http://localhost:3000	GET	/rest/admin/application-version			304	304					127.0.0.1			02:20:33 15 ...	8080	1
22	http://localhost:3000	GET	/api/Challenges?nameScore%20B...	✓		304	305					127.0.0.1			02:20:33 15 ...	8080	26
28	http://localhost:3000	GET	/socket.io/?EIO=4&transport=poll...	✓		200	230	text	io/			127.0.0.1			02:20:33 15 ...	8080	100
29	http://localhost:3000	GET	/rest/admin/application-configuration			304	306					127.0.0.1			02:20:33 15 ...	8080	3
37	http://localhost:3000	GET	/ftp			200	11636	HTML		listing directory /ftp		127.0.0.1			02:25:11 15 ...	8080	18

**Request**

```

1 GET /ftp HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua-platform: "A Brand" ;v="99", "Chromium" ;v="14"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua: "Windows"
6 Accept-Language: en-GB,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 Windows NT 10.0; Win64; x64 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/webp,*/*

```

**Response**

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: text/html; charset=utf-8
8 Date: Fri, 14 Nov 2025 20:55:11 GMT
9 Keep-Alive: timeout=5
10 Connection: keep-alive
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
617
618
619
619
620
621
622
623
624
625
625
626
627
627
628
629
629
630
631
632
633
634
634
635
636
636
637
637
638
638
639
639
640
640
641
641
642
642
643
643
644
644
645
645
646
646
647
647
648
648
649
649
650
650
651
651
652
652
653
653
654
654
655
655
656
656
657
657
658
658
659
659
660
660
661
661
662
662
663
663
664
664
665
665
666
666
667
667
668
668
669
669
670
670
671
671
672
672
673
673
674
674
675
675
676
676
677
677
678
678
679
679
680
680
681
681
682
682
683
683
684
684
685
685
686
686
687
687
688
688
689
689
690
690
691
691
692
692
693
693
694
694
695
695
696
696
697
697
698
698
699
699
700
700
701
701
702
702
703
703
704
704
705
705
706
706
707
707
708
708
709
709
710
710
711
711
712
712
713
713
714
714
715
715
716
716
717
717
718
718
719
719
720
720
721
721
722
722
723
723
724
724
725
725
726
726
727
727
728
728
729
729
730
730
731
731
732
732
733
733
734
734
735
735
736
736
737
737
738
738
739
739
740
740
741
741
742
742
743
743
744
744
745
745
746
746
747
747
748
748
749
749
750
750
751
751
752
752
753
753
754
754
755
755
756
756
757
757
758
758
759
759
760
760
761
761
762
762
763
763
764
764
765
765
766
766
767
767
768
768
769
769
770
770
771
771
772
772
773
773
774
774
775
775
776
776
777
777
778
778
779
779
780
780
781
781
782
782
783
783
784
784
785
785
786
786
787
787
788
788
789
789
790
790
791
791
792
792
793
793
794
794
795
795
796
796
797
797
798
798
799
799
800
800
801
801
802
802
803
803
804
804
805
805
806
806
807
807
808
808
809
809
810
810
811
811
812
812
813
813
814
814
815
815
816
816
817
817
818
818
819
819
820
820
821
821
822
822
823
823
824
824
825
825
826
826
827
827
828
828
829
829
830
830
831
831
832
832
833
833
834
834
835
835
836
836
837
837
838
838
839
839
840
840
841
841
842
842
843
843
844
844
845
845
846
846
847
847
848
848
849
849
850
850
851
851
852
852
853
853
854
854
855
855
856
856
857
857
858
858
859
859
860
860
861
861
862
862
863
863
864
864
865
865
866
866
867
867
868
868
869
869
870
870
871
871
872
872
873
873
874
874
875
875
876
876
877
877
878
878
879
879
880
880
881
881
882
882
883
883
884
884
885
885
886
886
887
887
888
888
889
889
890
890
891
891
892
892
893
893
894
894
895
895
896
896
897
897
898
898
899
899
900
900
901
901
902
902
903
903
904
904
905
905
906
906
907
907
908
908
909
909
910
910
911
911
912
912
913
913
914
914
915
915
916
916
917
917
918
918
919
919
920
920
921
921
922
922
923
923
924
924
925
925
926
926
927
927
928
928
929
929
930
930
931
931
932
932
933
933
934
934
935
935
936
936
937
937
938
938
939
939
940
940
941
941
942
942
943
943
944
944
945
945
946
946
947
947
948
948
949
949
950
950
951
951
952
952
953
953
954
954
955
955
956
956
957
957
958
958
959
959
960
960
961
961
962
962
963
963
964
964
965
965
966
966
967
967
968
968
969
969
970
970
971
971
972
972
973
973
974
974
975
975
976
976
977
977
978
978
979
979
980
980
981
981
982
982
983
983
984
984
985
985
986
986
987
987
988
988
989
989
990
990
991
991
992
992
993
993
994
994
995
995
996
996
997
997
998
998
999
999
1000
1000
1001
1001
1002
1002
1003
1003
1004
1004
1005
1005
1006
1006
1007
1007
1008
1008
1009
1009
1010
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1
```

## 8. OWASP Top 10 Mapping (2021)

Vulnerability	OWASP Category	Explanation
Username Enumeration	A07: Identification & Authentication Failures	Leaks authentication state information
Reflected XSS	A03: Injection	Unsanitized input directly reflected into HTML
Directory Browsing	A01: Broken Access Control / A05: Security Misconfiguration	Unauthorized access to internal directories

## 9. Risk Rating Matrix

Severity	Description
Low	Minimal impact, no sensitive data exposed
Medium	Potential information leakage, minor exploitation
High	Significant risk, sensitive data exposed, real exploitation possible
Critical	Full system compromise, remote code execution

All identified vulnerabilities fall under Medium to High-risk categories.

# 10. Recommendations & Best Practices

## ✓ Strengthen Authentication

- Implement login throttling
- Use generic error messages
- Add multi-factor authentication (MFA)

## ✓ Improve Input Security

- Enforce input validation
- Encode all outputs
- Implement CSP headers
- Avoid dynamic HTML generation

## ✓ Restrict File Access

- Disable directory indexing
- Implement RBAC for sensitive paths
- Enforce secure server configurations

## ✓ General Best Practices

- Conduct regular security audits
- Perform code reviews
- Keep frameworks updated
- Use automated scanners during CI/CD

# Conclusion

The assessment successfully identified three realistic and high-impact vulnerabilities in the OWASP Juice Shop application. These findings reflect common security issues that occur in production environments due to misconfiguration, poor validation, or weak access control.

By following the recommended fixes, the application's overall security posture can be dramatically improved.

This project provided hands-on experience with industry-standard testing methodologies, tools, and vulnerability reporting practices.