



TECH WITH Z

Hack Smarter: Hunter

Web Application Penetration Test Report

Business Confidential

Date: Decemeber 15th, 2025

Project: Hunter

Version 1.0

Table of Contents

Confidentiality Statement.....	3
Disclaimer.....	3
Contact Information.....	3
Assessment Overview	4
Assessment Components.....	4
Web Application Penetration Test.....	4
Finding Severity Ratings	5
Risk Factors.....	5
Likelihood	5
Impact.....	5
Scope	6
Scope Exclusions	6
Client Allowances	6
Executive Summary	7
Scoping and Time Limitations	7
Testing Summary	7
Tester Notes and Recommendations	8
Key Strengths and Weaknesses	8
Vulnerability Summary & Report Card	9
Web Application Penetration Test Findings.....	9
Technical Findings	10
Web Application Penetration Test Findings.....	10
Finding WPT-001: Insufficient Lockout Policy (High)	10
Finding WPT-002: Insufficient Encryption (Medium)	12
Finding WPT-003: Lack of rate limiting on Login and Password Reset endpoints (Medium)	13
Finding WPT-004: Username Enumeration via Password Reset response timing (Medium)	14
Finding WPT-005: Hidden Endpoint Exposure via HTTP Response (Informational)	16
Conclusion & Next Steps	17

Confidentiality Statement

This article is the sole property of Hunter and Tech With Z (TWZ). This document includes private and confidential information. Duplication, dissemination, or use, in whole or in part, in any form, requires the permission of both Hack Smarter and TWZ.

Hunter may share this material with auditors under non-disclosure agreements to verify compliance with penetration testing requirements.

Disclaimer

A penetration test is viewed as a snapshot in time. The findings and recommendations are based on the information obtained during the evaluation and do not include any changes or revisions made beyond that period.

Time-limited engagements do not allow for a comprehensive assessment of all security controls. TWZ prioritized the evaluation to find the most vulnerable security controls an attacker may exploit. TWZ suggests that similar assessments be conducted on an annual basis by internal or third-party assessors to verify that the controls remain effective.

Contact Information

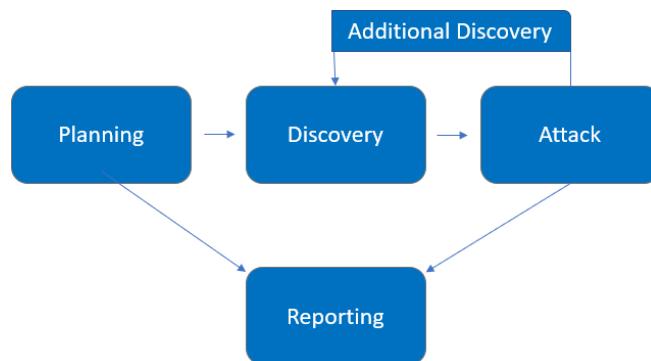
Tech With Z		
Name	Title	Contact Information
Zandro Dadulla Jr.	Penetration Tester	zandro@techwithz.com

Assessment Overview

Hunter engaged Tech With Z to assess the security status of its Web Application in relation to the latest industry standards, which involved conducting a web application penetration test. The testing conducted is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and tailored testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are identified, and rules of engagement are established.
- Discovery – Perform scanning and enumeration to identify possible vulnerabilities, weak points, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation, then conduct additional discovery with new access.
- Reporting – Document all discovered vulnerabilities and exploits, unsuccessful attempts, and company strengths and weaknesses.



Assessment Components

Web Application Penetration Test

This web application penetration test was conducted to simulate an attacker with no internal access or prior knowledge of the environment attempting to compromise the organization's exposed web assets. The objective was to identify security weaknesses that could be exploited to gain unauthorized access to sensitive data or application functionality.

The assessment involved active reconnaissance, including scanning and enumeration of the target's publicly accessible web infrastructure. Discovered endpoints, directories, and services were analyzed for common vulnerabilities, misconfigurations, and access control flaws. The testing process focused on identifying issues that could result in unauthorized data exposure, authentication bypass, privilege escalation, and improper access to application resources.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Web Application Penetration Test	http://10.1.42.12

Scope Exclusions

TWZ did not conduct any of the following attacks during testing:

- Denial of Service (DoS) attacks against production infrastructure.
- Phishing / Social Engineering attacks.

Client Allowances

No allowances provided by the client.

Executive Summary

On December 12th, 2025, TWZ performed a web application penetration test targeting Hunter's external login portal. The objective of this assessment was to evaluate the security posture of Hunter's web application by identifying vulnerabilities and assessing the effectiveness of implemented security controls. This report provides a high-level overview of the findings, including both successful and unsuccessful exploitation attempts, as well as identified strengths and weaknesses in the application's security architecture.

Scoping and Time Limitations

Throughout the engagement, TWZ did not perform denial of service or social engineering in any testing components.

Testing was limited in duration. Web application penetration testing was approved until December 15th, 2025.

Testing Summary

The assessment evaluated Hunter's web application security posture specifically the external login portal. From an external perspective, the TWZ team performed information gathering techniques to identify possible entry points for future attacks and gather sensitive information.

The TWZ team discovered a flaw in the password reset portal where a valid username can be enumerated by analyzing server response time (Finding WPT-004). Utilizing this flaw, the TWZ team were able to send multiple requests without rate limiting (Finding WPT-003) and identified one valid username.

The team was then able to perform password brute-forcing to gain access to the account. The application allowed sending multiple requests without locking out the account (Finding WPT-001). However, even after multiple attempts of password attacks, the TWZ team were unsuccessful in gaining access to the account due to strong password complexity.

For further details on the findings, please see the [Technical Findings](#) section.

Tester Notes and Recommendations

During testing, a few things stood out: insufficient encryption on the website, insufficient authentication controls, and lack of rate limiting. The lack of rate limiting resulted in username enumeration which identified one valid account.

We advise that Hunter review its current web application infrastructure and implement TLS encryption (HTTPS). We also advise to implement rate limiting, response time delay, and CAPTCHA to reduce the number of requests in the reset password portal which could result in username enumeration.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Effective protection against injection attacks (XSS, SQLi).
2. Effective protection against username enumeration in the Login page as there are no unique messages shown for both valid and invalid accounts.
3. Effective protection against username enumeration in the Password reset page using generic response message.
4. Excellent password complexity.

The following identifies the key weaknesses identified during the assessment:

1. Username enumeration via response time in the password reset page.
2. Insufficient lockout policy / rate limiting.
3. Insufficient encryption (HTTP).

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Web Application Penetration Test Findings

0	1	3	0	1
Critical	High	Medium	Low	Informational

Web Application Penetration Test		
Finding	Severity	Recommendation
WPT-001: Insufficient Lockout Policy	High	Restrict logon attempts against the login portal.
WPT-002: Insufficient encryption	Medium	Enforce HTTPS across the entire application.
WPT-003: Lack of rate limiting on Login and Password Reset endpoints	Medium	Implement request rate limiting / Implement CAPTCHA.
WPT-004: Username Enumeration via Password Reset response timing	Medium	Introduce delays to make response time for valid and invalid accounts the same.
WPT-005: Information Disclosure via HTTP Response Headers	Informational	Remove unnecessary information from HTTP response headers.

Technical Findings

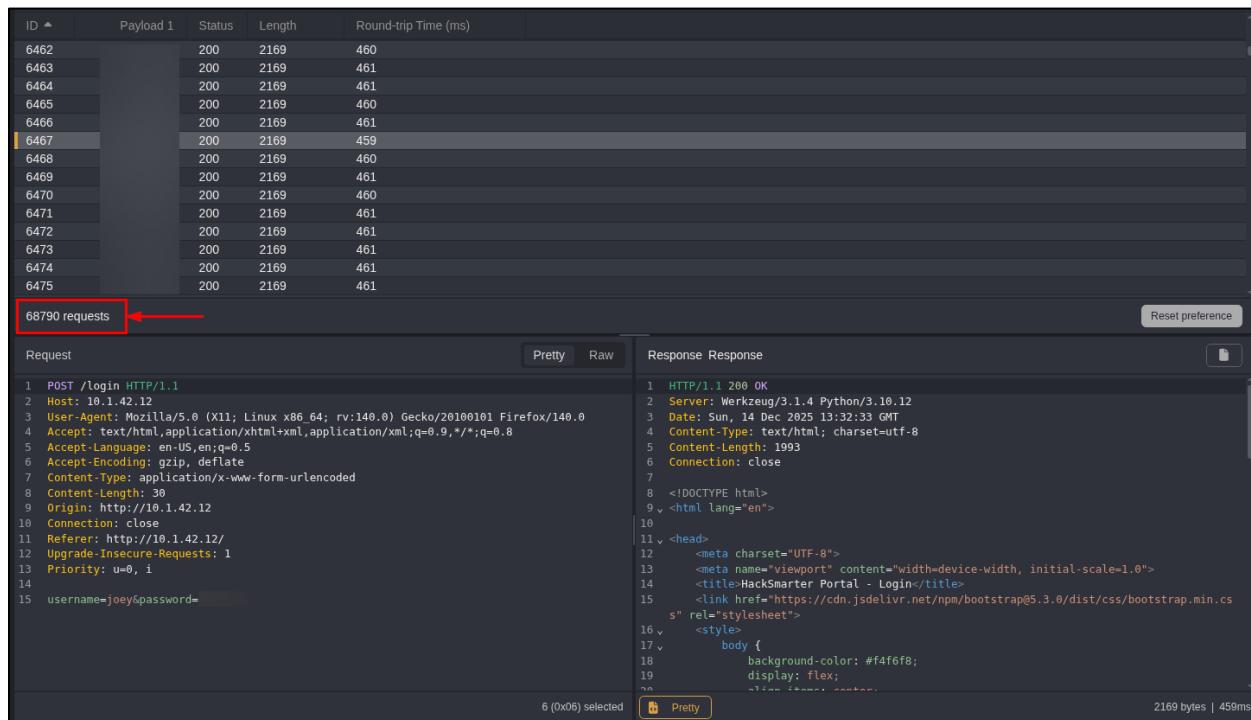
Web Application Penetration Test Findings

Finding WPT-001: Insufficient Lockout Policy (High)

Description	Hunter allowed unlimited logon attempts against login portal. This configuration allowed brute force and password spraying attacks. However, due to excellent password complexity, the tester was unsuccessful in accessing the account.
CVSS Score	8.2 (High) – CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
Risk	Likelihood: High – An attacker can utilize readily available tools such as Burp Suite, Caido, THC Hydra, etc. to perform brute-force and password spraying attacks without any restrictions to login attempts. Impact: High – If successful and given unlimited time, an attacker can gain access to a user's account sensitive information.
System	http://10.1.42.12
Tools Used	Caido
References	CWE-307: Improper Restriction of Excessive Authentication Attempts (4.17) Unsuccessful Logon Attempts: NIST SP 800-53 AC-07

Evidence / Steps to Reproduce

After identifying the valid user discussed in [WPT-004](#), TWZ was able to perform a password spraying attack against the account without getting locked out. However, the test was unsuccessful in gaining access to the account due to excellent password complexity.



The screenshot shows the Caido Automate tool interface during a password spraying attack. At the top, a table lists 68790 requests, with the 6467th request highlighted. Below the table, the 'Request' tab is active, displaying a POST request to '/login' with various headers and a body containing 'username=joey&password='.

The 'Response' tab is also visible, showing the server's response in JSON format, which includes the HTTP status code, server details, date, content type, content length, connection, and the HTML response body.

At the bottom, there are buttons for 'Pretty' and 'Raw' views, and a status bar indicating '6 (0x06) selected' and '2169 bytes | 459ms'.

Figure 1: Caido Automate – Password Spraying Attack.

Remediation

TWZ recommends Hunter to implement lockout policy and apply rate limiting and delay mechanisms to prevent or slow down any brute-force attempts.

Finding WPT-002: Insufficient Encryption (Medium)

Description	Hunter does not use encryption on their website. Allowing cleartext transmission enables potential adversary-in-the-middle eavesdropping.
CVSS Score	5.4 (Medium) – CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
Risk	Likelihood: Low – To conduct an adversary-in-the-middle attack, the attacker must be on the same network as the victim. Impact: High – Inadequate encryption may allow attackers to modify web content delivered to end users because it is not cryptographically signed via HTTPS.
System	http://10.1.42.12
Tools Used	Manual review
References	CWE-1428: Reliance on HTTP instead of HTTPS A02:2021: Cryptographic Failures OWASP Cheat Sheet: Transport Layer Security Cheat Sheet

Evidence / Steps to Reproduce

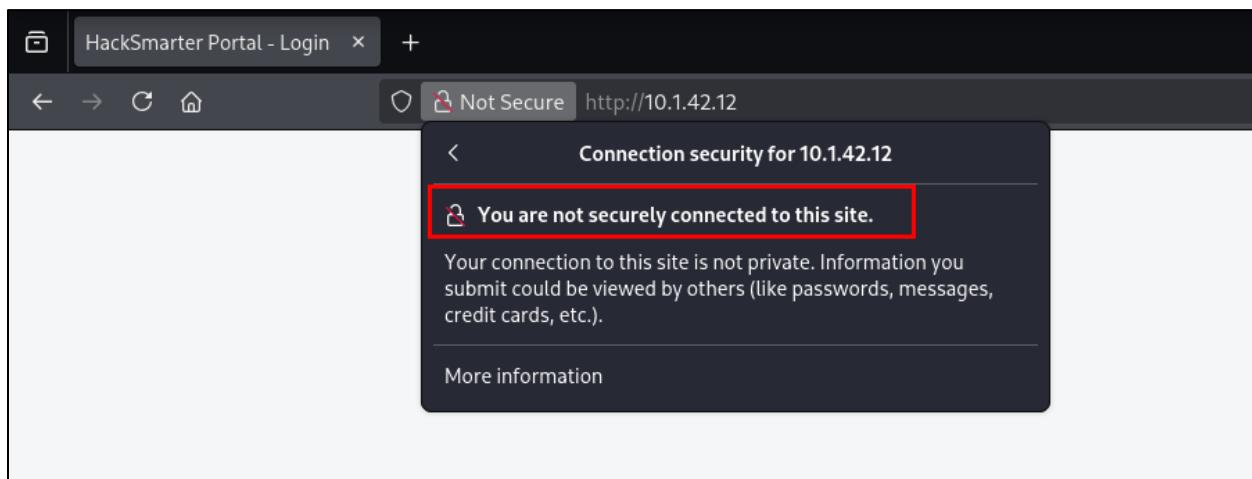


Figure 2: Hunter Login Portal – HTTP Only.

Remediation

Enable and enforce site-wide encryption.

Finding WPT-003: Lack of rate limiting on Login and Password Reset endpoints (Medium)

Description	The application does not enforce rate limits on the login and password reset (/reset) endpoints. This enables an attacker to submit unlimited login and password reset requests, aiding brute-force, password spraying, and enumeration attacks.
CVSS Score	5.3 (Medium) – CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Risk	Likelihood: High – Easily exploitable using automated tools. Impact: High – Can lead to account compromise and denial-of-service scenarios.
System	http://10.1.42.12
Tools Used	Caido
References	CWE - CWE-770: Allocation of Resources Without Limits or Throttling (4.19) CWE - CWE-799: Improper Control of Interaction Frequency (4.19)

Evidence / Steps to Reproduce

The TWZ team was able to submit multiple requests to the Login page and the Password Reset page (/reset) without getting rate limited. This allowed the team to perform username enumeration and successfully identified the valid user discussed in [WPT-004](#).

ID	Payload 1	Status	Length	Round-trip Time (ms)
1	james	200	2160	607
2	john	200	2160	560
3	robert	200	2160	590
4	michael	200	2160	527
5	william	200	2160	547
6	david	200	2160	587
7	richard	200	2160	526
8	charles	200	2160	553
9	joseph	200	2160	597
10	thomas	200	2160	526
11	christopher	200	2160	518
12	daniel	200	2160	533
13	paul	200	2160	583
14	mark	200	2160	515
15	donald	200	2160	571
16	george	200	2160	524
17	kenneth	200	2160	590
18	steven	200	2160	602
19	edward	200	2160	580
20	brian	200	2160	532
21	ronald	200	2160	569
22	anthony	200	2160	564
23	kevin	200	2160	608
24	jason	200	2160	588
25	matthew	200	2160	551
26	gary	200	2160	571
27	timothy	200	2160	542
28	jose	200	2160	575
29	larry	200	2160	532
30	jeffrey	200	2160	574
31	frank	200	2160	566

Figure 3: Caido Automate – Username Enumeration in Password Reset endpoint.

Remediation

Implement request rate limiting / Implement CAPTCHA.

Finding WPT-004: Username Enumeration via Password Reset response timing (Medium)

Description	<p>During testing of the password reset functionality (/reset), the TWZ team discovered that the application replies differently depending on whether the specified username exists. Valid usernames might be reliably identified by sending several password reset requests and evaluating response times. This behavior enables an attacker identify real user accounts without authentication.</p> <p>Username enumeration greatly reduces the work necessary to carry out credential-based attacks like password spraying or brute-force attacks.</p>
CVSS Score	5.3 (Medium) – CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Risk	<p>Likelihood: High – Timing-based enumeration is easy to automate.</p> <p>Impact: Medium – Enables targeted attacks against valid accounts.</p>
System	http://10.1.42.12/reset
Tools Used	Caido
References	Testing for Account Enumeration and Guessable User Account Time based username enumeration

Evidence / Steps to Reproduce

Using the usernames list provided by the OSINT analysts, the TWZ team was able to enumerate valid usernames by sending multiple requests to the password reset page (/reset) and analyzing the Response Time of the server.

One request stood out with a response time of 1362ms which suggest that the username used in that request is valid.

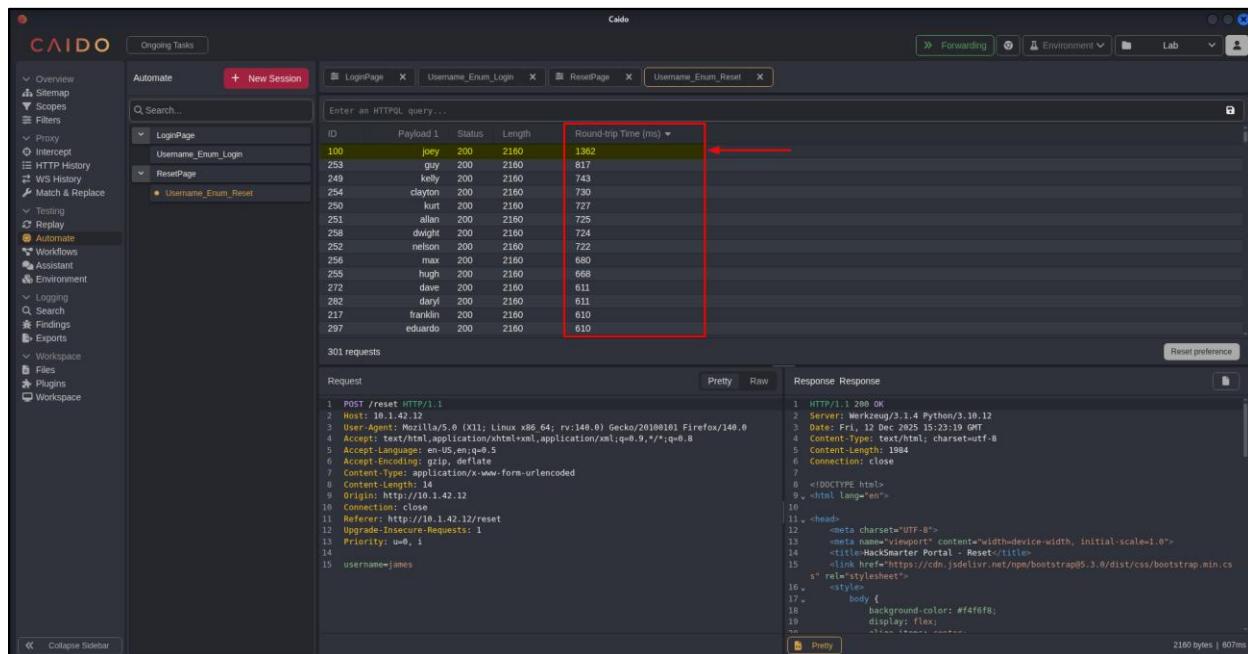


Figure 04: Caido Automate – Username Enumeration via Response Time Analysis

Remediation

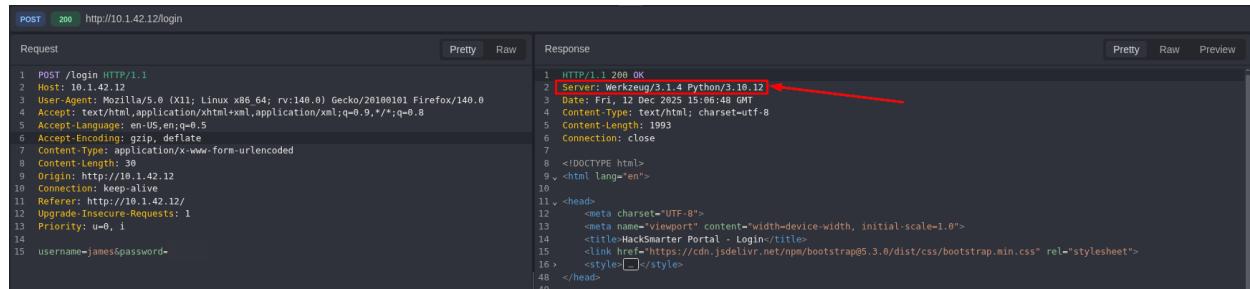
Introduce delays to make response time for valid and invalid accounts the same. Implement server-side rate limiting on password reset requests ([WPT-003](#)).

Finding WPT-005: Hidden Endpoint Exposure via HTTP Response (Informational)

Description	Hunter's web server discloses detailed backend technology information through HTTP response headers. Specifically, the following information was observed: <ul style="list-style-type: none"> • Web Server: Werkzeug/3.1.4 • Programming Language: Python/3.10.12
CVSS Score	N/A
Risk	Likelihood: Medium – The system is accessible from the internet and is passively observable with any HTTP client or proxy tool. Impact: Low – This information could allow an attacker to fingerprint the web server to better target future exploit attempts.
System	http://10.1.42.12/
Tools Used	Caido, Manual Review
References	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere OWASP Secure Headers Project: OWASP Secure Headers Project OWASP Foundation Nginx: Module ngx_http_headers_module

Evidence / Steps to Reproduce

While analyzing HTTP response headers of the website, the TWZ team discovered that the web server reveals the server version running which is unnecessary and could allow attackers to fingerprint the server.



```

POST 200 http://10.1.42.12/login
Request
Pretty Raw
Response
Pretty Raw Preview
1 POST /login HTTP/1.1
2 Host: 10.1.42.12
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 30
9 Origin: http://10.1.42.12
10 Connection: keep-alive
11 Referer: http://10.1.42.12/
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 username=james&password=
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
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
288
289
289
290
291
292
293
294
295
296
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
547
548
549
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
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
878
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
978
979
980
981
982
983
984
985
986
987
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
```

Conclusion & Next Steps

The web application penetration test discovered multiple medium to high severity vulnerabilities that, while not causing immediate compromise, collectively weakened the application's overall security posture. The detected concerns mostly concern information disclosure, authentication hardening gaps, and transport-layer security flaws.

Findings such as username enumeration via response timing, server version disclosure, lack of HTTPS enforcement, and lack of rate limiting provide attackers with valuable reconnaissance capabilities and increase the likelihood of successful credential-based attacks. Although no single vulnerability resulted in a direct system breach during this phase of testing, these flaws dramatically reduce the barrier to attackers performing targeted brute-force, password spraying, and man-in-the-middle attacks in real-world scenarios.

To improve the security posture of the application and reduce attack surface exposure, the following actions are recommended:

1. Harden Authentication and Account Recovery Mechanisms
 - Implement consistent responses and response timings for authentication and password reset workflows.
 - Enforce rate limiting, CAPTCHA challenges, and progressive delays to mitigate automated attacks.
 - Monitor authentication endpoints for abnormal or high-volume request patterns.
2. Secure Transport Layer Communications
 - Enforce HTTPS across the entire application.
 - Implement HTTP Strict Transport Security (HSTS) to prevent protocol downgrade attacks.
 - Redirect all HTTP traffic to HTTPS automatically.
3. Reduce Information Disclosure
 - Remove or obfuscate server and framework version information from HTTP response headers.
 - Regularly review application responses to ensure no unnecessary technical details are exposed.
4. Re-Assessment
 - Conduct a follow-up penetration test after remediation efforts are completed to validate the effectiveness of implemented controls and ensure no regressions were introduced.

LAST PAGE