

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'HTTP History' pane on the left lists several requests. A red box highlights the first request to 'https://admin-sb.konaplate.com:10443'. A red arrow points from this box to the 'Request' pane on the right, which displays the details of the selected POST request to '/api/login'. The request body is shown in the 'Raw' tab, with a red box highlighting the 'username' and 'password' fields. The 'Response' pane on the right shows the response details, including the status code 200 and the response body.

The screenshot displays the Burp Suite Community Edition interface, specifically the 'Intruder' tab. The 'Payloads' section is highlighted with a red box, showing a list of payload sets. The 'Payload settings [Simple list]' section is also highlighted with a red box, showing a list of payload strings. The 'Payload processing' section is also highlighted with a red box, showing a table for defining rules for each payload.

Navigation Bar: Burp Project Intruder Repeater View Help

Dashboard: Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Positions: **Payloads** Resource pool Settings

1 Payload sets Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 59
Payload type: Simple list Request count: 59

2 Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Buttons: Paste, Load ..., Remove, Clear, Deduplicate, Add, Add from list ... (Pro version only)

Payload List:

- ||e|t|-3+5,bin(15),ord(10),hex(char(45))|
- |l|6
- |' 6
- |@|
- |OR 1=1-
- |OR 1=1
- |OR '1'='1
- |OR '1'='1'
- |%22=or+isnull%201%2F0%29+%2F*

3 Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule
<input type="checkbox"/>	

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	e t (-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%28%2F0%29+%2F*	417			1250	
10	%27+OR+%277659%27%30%277659	417			1250	
11	%22+or+isnull%28%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-Fa-User-Agent: AP/0.0.1
9 Content-Type: application/json
10 Accept: application/json, text/plain, */*
11 X-Fa-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
21
22 {
  "username": "sys_admin",
  "password": "Konas1@91c3"
}
```

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	e t (-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%28%2F0%29+%2F*	417			1250	
10	%27+OR+%277659%27%30%277659	417			1250	
11	%22+or+isnull%28%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-Fa-User-Agent: AP/0.0.1
9 Content-Type: application/json
10 Accept: application/json, text/plain, */*
11 X-Fa-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
21
22 {
  "username": "|||e|t|(-3+5,bin(15),ord(10),hex(char(45)))|",
  "password": "Konas1@91c3"
}
```

Search 0 highlights

Finished

AttackSaveColumns

2. Intruder attack of https://admin-sb.konaplate.com:10443 - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	2567	
1	e!t(-3=5,bin(15),ord(10),hex(char(45)))	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
2	6	401	<input type="checkbox"/>	<input type="checkbox"/>	1402	
3	6	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
4	6	401	<input type="checkbox"/>	<input type="checkbox"/>	1402	
5	'OR 1=1--	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
6	OR 1=1	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
7	'OR '1='1	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
8	; OR '1='1	401	<input type="checkbox"/>	<input type="checkbox"/>	1402	
9	%22+or+isnull%28%2F0%29+%2F*	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
10	%27+OR+%277659%27%3D%277659	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
11	%22+or+isnull%28%2F0%29+%2F*	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
12	%27+--+	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
13	'or 1=1--	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
14	'or 1=1--	400	<input type="checkbox"/>	<input type="checkbox"/>	1388	
15	'or 1=1#	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
16	'or 1=1#	400	<input type="checkbox"/>	<input type="checkbox"/>	1388	
17	'or 1=1/"	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
18	or 1=1--	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	

RequestResponse

PrettyRawRender

61

62<div class="content">

63<div class="content">

64

417

65

66

Expectation Failed

67

68

The server cannot meet the requirements of the Expect request-header field.

69</div>

70</div>

71</body>

72</html>

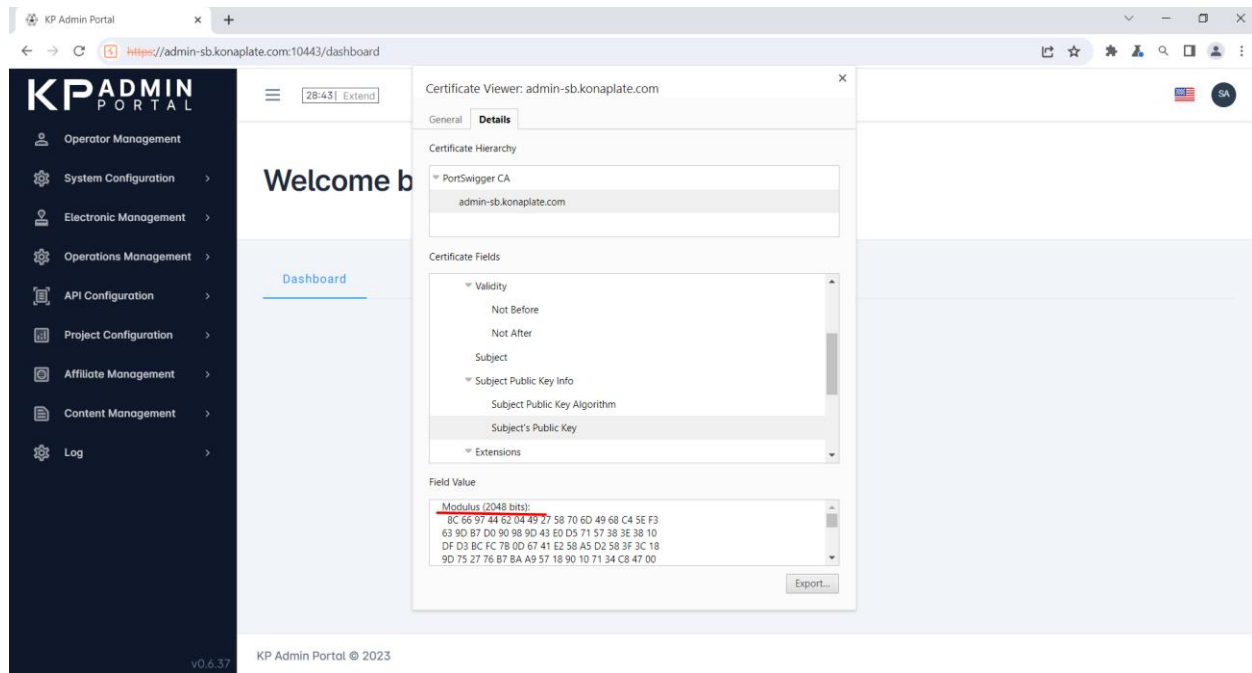
73

Search

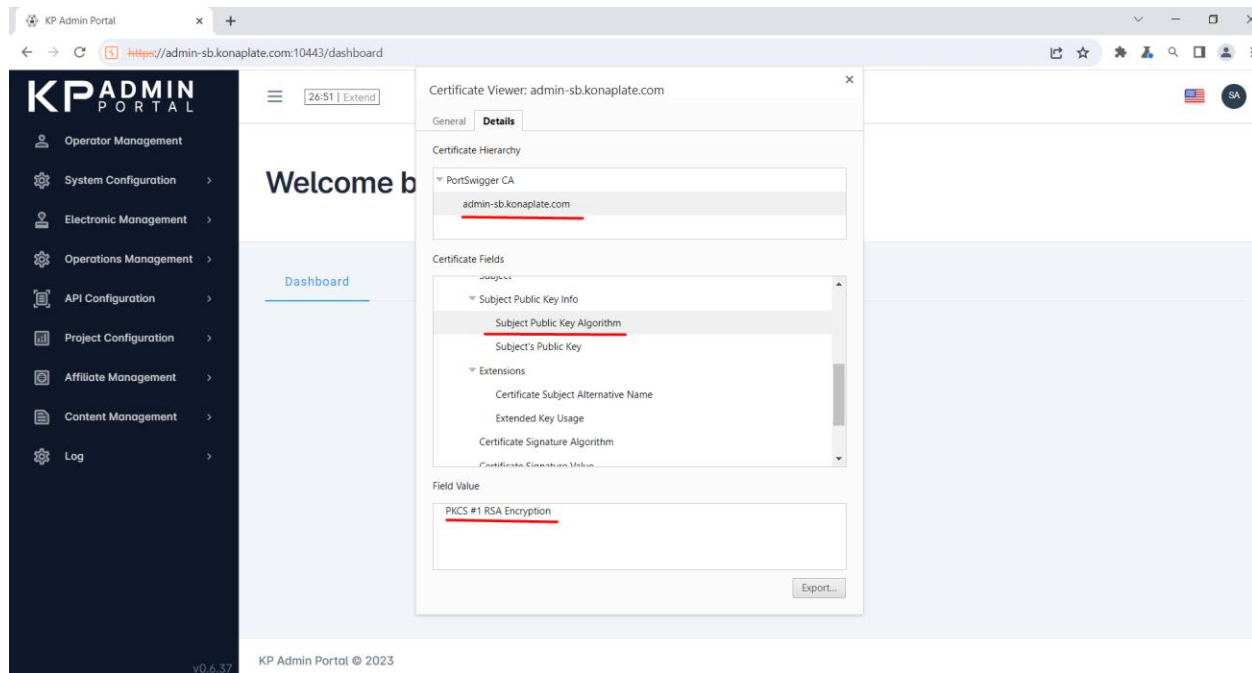
0 highlights

Finished

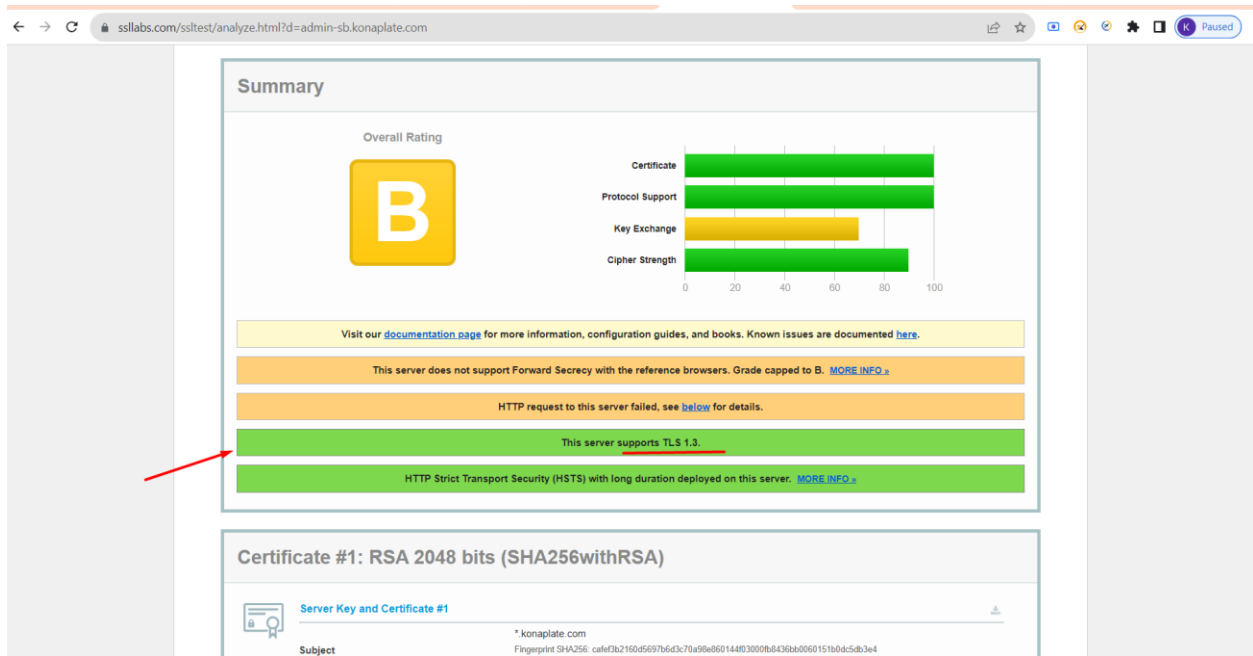
Test case 1: Check the crypto key length(strong length minimum 256 bytes/2048 bits)



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

The screenshot displays a database management interface with a table containing 35 records. The table has two columns: 'TRY' and 'PW1'. The 'PW1' column contains bcrypt hashes of passwords. The first record is highlighted, showing a hash for the password 'Korea XI'. The interface includes a sidebar with a tree view of the database structure, a top menu bar, and a bottom status bar.

TRY	PW1
1 Korea XI	{bcrypt}\$2a\$10\$PPE.wH07z3P31B1Qa6F0v.Z9F87A8Nqon28C8Y21D5AAyeL.38d..
2	{bcrypt}\$2a\$10\$PPE.wH07z3P31B1Qa6F0v.Z9F87A8Nqon28C8Y21D5AAyeL.38d..
3	{bcrypt}\$2a\$10\$D1JwmP4bQvJlNlXKw45ep8nPE/SUg3.8UTBvZu3kt13sY6x..
4 Korea XI	{bcrypt}\$2a\$10\$N.pf51eovP10gpxZVYKb40Mv97NbQjD08jzD4rXqb/n3dqf4kq5..
5	{bcrypt}\$2a\$10\$8BL/TB2mP/YQfKFSFgQp/eAX1oK8QVg40h2Lg296K8SGHS138..
6	{bcrypt}\$2a\$10\$e8L1A500dkCypa390eaded7EEftQw/Lcr2dKI15FRnArg/7eSA..
7	{bcrypt}\$2a\$10\$KJmEqWk/13179ZVMM5..je/wxVqWZ21M3SF87QhshrVesc/nac..
8	{bcrypt}\$2a\$10\$y0Qv1VsC0zhC8epoqHY9./872P23tLc1E1E1.31r7BB6SV3gA..
9	{bcrypt}\$2a\$10\$uHru.rF87XR0mDulcpQvXv93ov2f/I1uCYgu3nXjHcQh6hQ..
10	{bcrypt}\$2a\$10\$jt0wC5nKL3.v.g8lgo10gBz8.yaxy7MwAFZ0MMIEffTpyb0pH..
11	{bcrypt}\$2a\$10\$AXvZ0Y0VBTF8VKM0LTmV0LjUwQvLMYRVX/xEdF1f5YwHPot..
12	{bcrypt}\$2a\$10\$HF19cTqPMUAK5PmRC140suUeP/3.qwF1B1jzrQK0M0uMhKA..
13	{bcrypt}\$2a\$10\$S02.ctU179E2hyQ70ZyrQ0ec9zhnFSV4y1So05F0WV2Z190b3JmL..
14	{bcrypt}\$2a\$10\$txGErd1j0Ueav491j4e.o0KPv3GP7n0T5/66rKK1lnx88dzKSZ..
15	{bcrypt}\$2a\$10\$SDBAP/5WjFUXY6roA8p147.e31sTTT0yAU7NF0soZSQFUrj86a55..
16	{bcrypt}\$2a\$10\$4BundfT0srKc2YmN57uHe.0Lb1ev030L26t3C8V1/1D1Cs33So..
17	{bcrypt}\$2a\$10\$sn0FWeUr8vpQ8ns330VhM0INEhY879W0AGsF0dEzxx1820cy80B..
18	{bcrypt}\$2a\$10\$Nhej8637mUGIrehNly.ZhiuaH22P1ETfCYbYyQLP.pIaaqCjt12r..
19	{bcrypt}\$2a\$10\$7C3sQPUacEF3J1Mv0g3XG.v7CcyZm/DQSV0T6adrr8ZfX7ME..
20	{bcrypt}\$2a\$10\$851RVKjFDULK4N0c1gM9/0LVeaA.uRGfN1FT84g4u3.6Zx83CQ..
21	{bcrypt}\$2a\$10\$5NVOXNGUzvd.7Hvyswx0/cE1YSm3637j8jzvb74SCPEWjWj2..
22	{bcrypt}\$2a\$10\$41u9z15nYBhPCBhtx3sN/0s//Qv0ZuR3KICIS5Zsus0AN13M..
23	{bcrypt}\$2a\$10\$8rU/MSDQh0FfXhbnFp44P0uMx1C.vAstmpQLWHZ7xohuyLVdNq..
24	{bcrypt}\$2a\$10\$8Wxactq5mfcN8NP11W/n7MeB442K5c0G04XoFuj3HnngEL0rFlou3..
25	{bcrypt}\$2a\$10\$V1ed/OTQRuPuV75mu60R9eqQfrrn9.mB14u1D0W1z07Fc8Q0fcZ..
26	{bcrypt}\$2a\$10\$V8B0/v.RrtU3Z2F.pjWqAK6BLR9GWHa.v/PayNt2L/g5gkPWK0XK..
27	{bcrypt}\$2a\$10\$Vj2pU01m65JN3VQL6..h.nu7Kjy/K4MsXo2LHXVY1091sVQ798LD..
28	{bcrypt}\$2a\$10\$8nPHK1WK9C3nC8ESK82p0308HgaQKn0LNGrVc1oR/kakhL80MuvH..
29	{bcrypt}\$2a\$10\$XAJL.E./A708WauUlagZH.e.NCEAXQnXo1r1DakRoB1wVz3AcRZ..
30	{bcrypt}\$2a\$10\$5yR3MC8aT0p90MhcnPTLOFHxVjVzchW88HQ66ZXCrrRy60SCq..
31	{bcrypt}\$2a\$10\$Srziefy8y67Tzo15a..a.ofmcdSt4u2u80vniJ681ntXEscFC..
32	{bcrypt}\$2a\$10\$YH3dL/Mq11B96eubU6d18.kgoIAHKK0Htmnjo2Udftay/W7C...x..
33	{bcrypt}\$2a\$10\$3sFFv8cyLhz6VnmVQPhy3KQ/zzx/8Cy/r16fyUUYzRJNTEK..
34	{bcrypt}\$2a\$10\$8arQL3Ip03/os10AGsXDM.kx3C9q7e5Pdp1P0xHj1xe1U0WHTDM..
35	{bcrypt}\$2a\$10\$2Un2W6m/q7ov8Rak5Cd/0y5p9u0VarksXz01x0D12K283jyzJ7..

Test Case 5: Verify X-Type Option

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	<input type="checkbox"/>	<input type="checkbox"/>	2567	
1	' (t (-3+5,bin(15),ord(10),hex(char(45)))	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
2	j6	401	<input type="checkbox"/>	<input type="checkbox"/>	1402	
3	' j6	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
4	j6	401	<input type="checkbox"/>	<input type="checkbox"/>	1402	
5	'OR 1=1--	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
6	OR 1=1	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
7	'OR 1='1	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
8	;OR 1='1	401	<input type="checkbox"/>	<input type="checkbox"/>	1402	
9	%22-or=ismu%281%2F0%29-%2F*	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
10	%27-OR=%277659%27%3D%277659	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
11	%22-or=ismu%281%2F0%29-%2F*	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
12	%27-+--	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
13	'or 1=1--	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
14	"or 1=1"	400	<input type="checkbox"/>	<input type="checkbox"/>	1388	
15	'or 1=1#	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
16	"or 1=1#	400	<input type="checkbox"/>	<input type="checkbox"/>	1388	
17	'or 1=1/*	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	
18	or 1=1--	417	<input type="checkbox"/>	<input type="checkbox"/>	1250	

Request

Response

Pretty
Raw
Hex

```

5 Sec-Ch-Ua: "Not-A.Brand";v="59", "Chromium";v="110"
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/110.0.5993.90 Safari/537.36
8 X-Pw-User-Agent: AP/O.0.1
9 Content-Type: application/json
10 Accept: application/json, text/plain, */*
11 X-Pw-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
21
22 {
  "username": "'|(|t|(-3+5,bin(15),ord(10),hex(char(45)))",
  "password": "Komas1@9123"

```

Finished

0 highlights

Test Case 6: Verify Session Payload Object

[illegible]

Test Case 7: Verify Keys should not stored in DB

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