9. a';/**/select/**/*/**/from/**/user_system_data;--

10. a';/**/seselectlect/**/*/**/fifromom/**/user_system_data;--

12) 104.130.219.202

A3):-

2.

Adapter for loop -

Browser => log in click

again wireshark

click=>lens icon

then type start

↓

Line-based Text data

Username & password

A7):-

2. right click => duplicate page

then click inspect

then click console

• >> alert(document.cookie);

---

7. remove credit card number ...

and copy query from 2nd one.

---

10. answer is in the same. Inspect => debug => Gruntgoat.js

lesson => test

-> .goatApp => views =>

goatRouter.js => see the code.

11. copy the ~~bright~~ bolded

Inspect -> console => paste it (for) => paste if

allow pastings

then copy the no.

12. 4
3
1
2
4

A4) X x E

1) ~~open~~ OWASP ZAP

click firefox ROM or .top

=) type in chat

zap=)

=) simple

then right click open/resend with Req Editor

~~keep~~ remove the line and type the query.

7) type hi

=) zap => content type

. two changes

=) remove text and type command

=) content type change

json => xml

4) Webwolf

take => Notepad

type (things)

webwolf -> files (number) → token 0.0.1

save files as name.dtd

come to W.W =>

file => browse => upload the file

now go to W.G

Hi => type and submit

zap

blind -> right click -> Request Editor

remove the line and type it.

now go to W.W

Incoming request

↓

landing

↓

copy URL

now go to W.G

paste

then edit

C%.20 remove/ enter space

A2)

=> ~~Password reset~~ - Authentication can bypass

Zap => Verify account => Request editor

edit 0 => 2

1 => 3

then send

=> Secure password:

4. set password

=) Password reset

2) Forget password

type username@webgoat.org => continue

the W.W => mail box

take the new password

account access

type name & password => Access

4)

tomm purple

admin green

5) security questions

6)

JWT Token

3) user

7) 1
3

5) change usr to tom

click delete icon

~~Burp~~ => waiting => R Editor.

remove ~~Cookie~~ => cookie access token (= to ;)

then with (b) last query copy and paste there (in editor) → Cast.a.add(6) before ;