Ασφάλεια Συστημάτων Υπολογιστών
Εργασία εργαστήριου 4
Σάββας Λιάπης 57403

Άσκηση

Το αρχείο access_log περιέχει κάποιες από τις καταγραφές επισκεψιμότητας ενός web server.

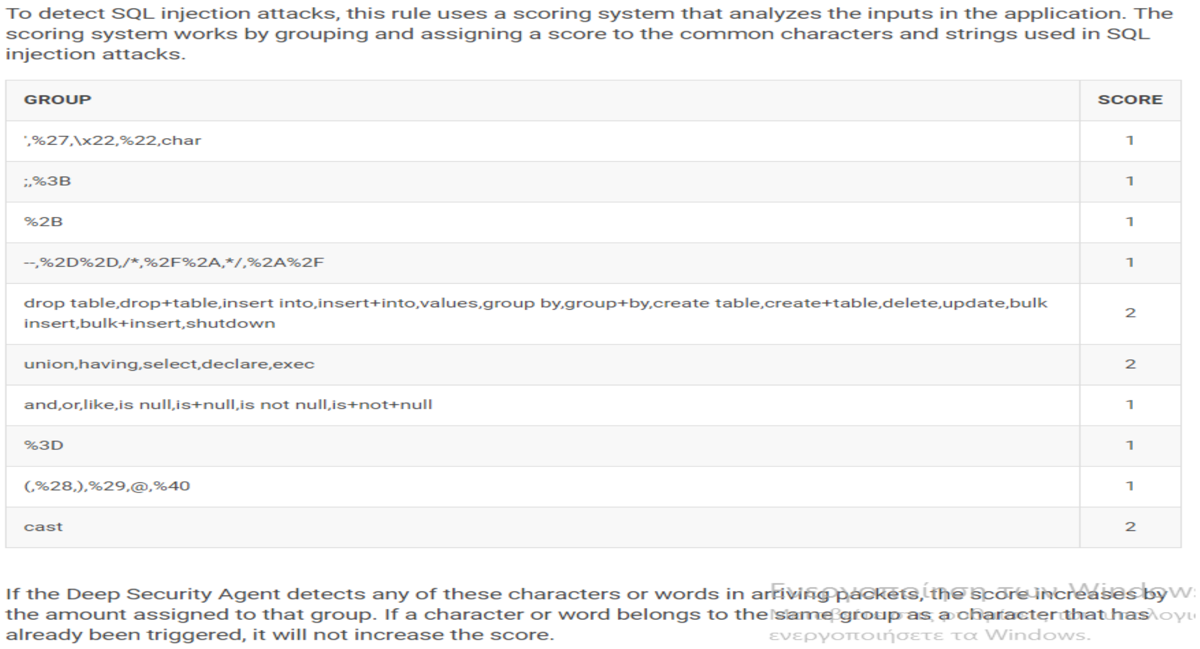
a. Να δημιουργήσετε ένα regular expression το οποίο να βρίσκει μόνο τις IP των clients που επιχειρούν SQL injections.
b. Να δημιουργήσετε ένα regular expression το οποίο να βρίσκει μόνο τις IP των clients που επιχειρούν SQL injections και το response status code του server είναι επιτυχές (success)
c. Να δημιουργήσετε ένα regular expression το οποίο να βρίσκει μόνο τις IP των clients που επιχειρούν SQL injections καθώς και την ημερομηνία & ώρα της επίθεσης και το response status code του server είναι επιτυχές (success)

Σημείωση 1: List of HTTP status codes: https://en.wikipedia.org/wiki/List_of_HTTP_status_codes
Σημείωση 2: Understanding the Apache Access Log: https://www.keycdn.com/support/apache-access-log (παράγραφος «Reading the Apache access logs»)

Απάντηση a

Αρχικά συντάσουμε το μοτίβο που να μας δίνει το IP: **\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b**

Έπειτα για να εντοπίσουμε sql injections υπάρχουν κάποια μοτίβα συνδυασμών χαρακτήρων και κάποιες λέξεις μέσω των οποίων μπορούμε να εντοπίσουμε μία πιθανή sql injection αυτά είναι :



To detect SQL injection attacks, this rule uses a scoring system that analyzes the inputs in the application. The scoring system works by grouping and assigning a score to the common characters and strings used in SQL injection attacks.

GROUP	SCORE
',%27,\x22,%22,char	1
;,%3B	1
%2B	1
--,%2D%2D,/*,%2F%2A,*/,%2A%2F	1
drop table,drop+table,insert into,insert+into,values,group by,group+by,create table,create+table,delete,update,bulk insert,bulk+insert,shutdown	2
union,having,select,declare,exec	2
and,or,like,is null,is+null,is not null,is+not+null	1
%3D	1
(,%28,),%29,@,%40	1
cast	2

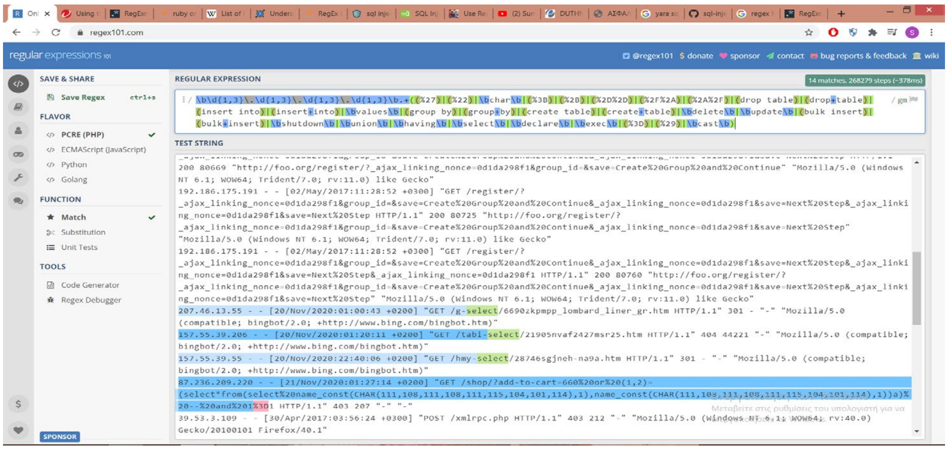
If the Deep Security Agent detects any of these characters or words in arriving packets, the score increases by the amount assigned to that group. If a character or word belongs to the same group as a character that has already been triggered, it will not increase the score.

Πηγή : https://success.trendmicro.com/solution/1098159-understanding-the-generic-sql-injection-prevention-rule#collapseFive

Έβαλα κάποιες (τις περισσότερες ακολουθίες από τις παραπάνω και κατέληξα στην εξής εντολή):

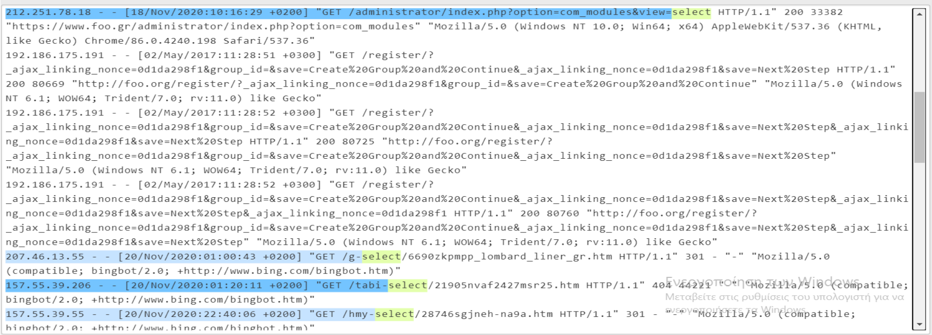
\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b.+((%27)|(%22)|\bchar\b|(%3B)|(%2B)|(%2D%2D)|(%2F%2A)|(%2A%2F)|(drop table)|(drop+table)|(insert into)|(insert+into)|\bvalues\b|(group by)|(group+by)|(create table)|(create+table)|\bdelete\b|\bupdate\b|(bulk insert)|(bulk+insert)|\bshutdown\b|\bunion\b|\bhaving\b|\bselect\b|\bdeclare\b|\bexec\b|(%3D)|(%29)|\bcast\b)

Και πήρα το εξής αποτέλεσμα : εντοπίστηκαν 14 IP που επιχείρησαν sql injection.

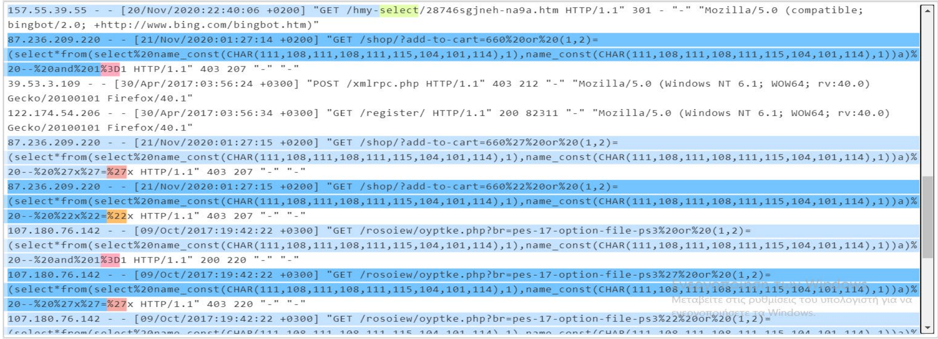


```
/ \b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b.+((%27)|(%22)|\bchar\b|(%3B)|(%2B)|(%2D%2D)|(%2F%2A)|(%2A%2F)|(drop table)|(drop+table)|(insert into)|(insert+into)|\bvalues\b|(group by)|(group+by)|(create table)|(create+table)|\bdelete\b|\bupdate\b|(bulk insert)|(bulk+insert)|\bshutdown\b|\bunion\b|\bhaving\b|\bselect\b|\bdeclare\b|\bexec\b|(%3D)|(%29)|\bcast\b) / gm
```

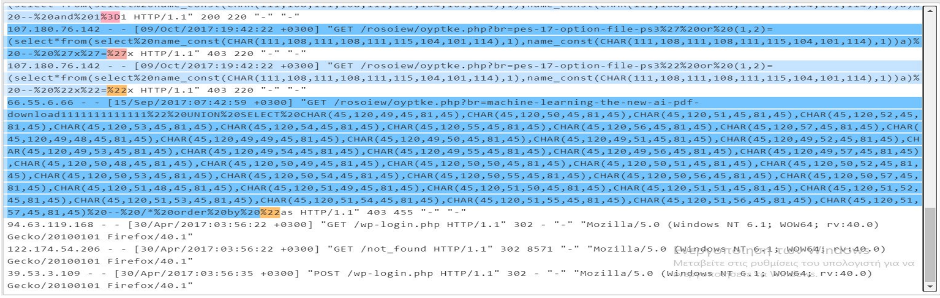
```
200 80669 "http://foo.org/register/?_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue" "Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.186.175.191 - - [02/May/2017:11:28:52 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step HTTP/1.1" 200 80725 "http://foo.org/register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step"
"Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.186.175.191 - - [02/May/2017:11:28:52 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step&_ajax_linking_nonce=0d1da298f1 HTTP/1.1" 200 80760 "http://foo.org/register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
207.46.13.55 - - [20/Nov/2020:01:00:43 +0200] "GET /g-select/6690zkpmpp_lombard_liner_gr.htm HTTP/1.1" 301 - "-" "Mozilla/5.0
(compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
157.55.39.206 - - [20/Nov/2020:01:20:11 +0200] "GET /tabi-select/21905nvaf2427msr25.htm HTTP/1.1" 404 44221 "-" "Mozilla/5.0 (compatible;
bingbot/2.0; +http://www.bing.com/bingbot.htm)"
157.55.39.55 - - [20/Nov/2020:22:40:06 +0200] "GET /hmy-select/28746sgjneh-na9a.htm HTTP/1.1" 301 - "-" "Mozilla/5.0 (compatible;
bingbot/2.0; +http://www.bing.com/bingbot.htm)"
87.236.209.220 - - [21/Nov/2020:01:27:14 +0200] "GET /shop/?add-to-cart=660%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 403 207 "-" "-"
39.53.3.109 - - [30/Apr/2017:03:56:24 +0300] "POST /xmlrpc.php HTTP/1.1" 403 212 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
```



```
212.251.78.18 - - [18/Nov/2020:10:16:29 +0200] "GET /administrator/index.php?option=com_modules&view=select HTTP/1.1" 200 33382
"https://www.foo.gr/administrator/index.php?option=com_modules" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36"
192.186.175.191 - - [02/May/2017:11:28:51 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step HTTP/1.1"
200 80669 "http://foo.org/register/?_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue" "Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.186.175.191 - - [02/May/2017:11:28:52 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step HTTP/1.1" 200 80725 "http://foo.org/register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step"
"Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.186.175.191 - - [02/May/2017:11:28:52 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step&_ajax_linking_nonce=0d1da298f1 HTTP/1.1" 200 80760 "http://foo.org/register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
207.46.13.55 - - [20/Nov/2020:01:00:43 +0200] "GET /g-select/6690zkpmpp_lombard_liner_gr.htm HTTP/1.1" 301 - "-" "Mozilla/5.0
(compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
157.55.39.206 - - [20/Nov/2020:01:20:11 +0200] "GET /tabi-select/21905nvaf2427msr25.htm HTTP/1.1" 404 44221 "-" "Mozilla/5.0 (compatible;
bingbot/2.0; +http://www.bing.com/bingbot.htm)"
157.55.39.55 - - [20/Nov/2020:22:40:06 +0200] "GET /hmy-select/28746sgjneh-na9a.htm HTTP/1.1" 301 - "-" "Mozilla/5.0 (compatible;
bingbot/2.0; +http://www.bing.com/bingbot.htm)"
```



```
157.55.39.55 - - [20/Nov/2020:22:40:06 +0200] "GET /hmy-select/28746sgjneh-na9a.htm HTTP/1.1" 301 - "-" "Mozilla/5.0 (compatible;
bingbot/2.0; +http://www.bing.com/bingbot.htm)"
87.236.209.220 - - [21/Nov/2020:01:27:14 +0200] "GET /shop/?add-to-cart=660%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 403 207 "-" "-"
39.53.3.109 - - [30/Apr/2017:03:56:24 +0300] "POST /xmlrpc.php HTTP/1.1" 403 212 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
122.174.54.206 - - [30/Apr/2017:03:56:34 +0300] "GET /register/ HTTP/1.1" 200 82311 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
87.236.209.220 - - [21/Nov/2020:01:27:15 +0200] "GET /shop/?add-to-cart=660%27%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%27x%27=%27x HTTP/1.1" 403 207 "-" "-"
87.236.209.220 - - [21/Nov/2020:01:27:15 +0200] "GET /shop/?add-to-cart=660%22%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%22x%22=%22x HTTP/1.1" 403 207 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 200 220 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%27%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%27x%27=%27x HTTP/1.1" 403 220 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%22%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
```



```
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 200 220 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%27%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%27x%27=%27x HTTP/1.1" 403 220 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%22%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%22x%22=%22x HTTP/1.1" 403 220 "-" "-"
66.55.6.66 - - [15/Sep/2017:07:42:59 +0300] "GET /rosoiew/oyptke.php?br=machine-learning-the-new-ai-pdf-
download1111111111111%22%20UNION%20SELECT%20CHAR(45,120,49,45,81,45),CHAR(45,120,50,45,81,45),CHAR(45,120,51,45,81,45),CHAR(45,120,52,45,
81,45),CHAR(45,120,53,45,81,45),CHAR(45,120,54,45,81,45),CHAR(45,120,55,45,81,45),CHAR(45,120,56,45,81,45),CHAR(45,120,57,45,81,45),CHAR(
45,120,49,48,45,81,45),CHAR(45,120,49,49,45,81,45),CHAR(45,120,49,50,45,81,45),CHAR(45,120,49,51,45,81,45),CHAR(45,120,49,52,45,81,45),CH
AR(45,120,49,53,45,81,45),CHAR(45,120,49,54,45,81,45),CHAR(45,120,49,55,45,81,45),CHAR(45,120,49,56,45,81,45),CHAR(45,120,49,57,45,81,45)
,CHAR(45,120,50,48,45,81,45),CHAR(45,120,50,49,45,81,45),CHAR(45,120,50,50,45,81,45),CHAR(45,120,50,51,45,81,45),CHAR(45,120,50,52,45,81,
45),CHAR(45,120,50,53,45,81,45),CHAR(45,120,50,54,45,81,45),CHAR(45,120,50,55,45,81,45),CHAR(45,120,50,56,45,81,45),CHAR(45,120,50,57,45,
81,45),CHAR(45,120,51,48,45,81,45),CHAR(45,120,51,49,45,81,45),CHAR(45,120,51,50,45,81,45),CHAR(45,120,51,51,45,81,45),CHAR(45,120,51,52,
45,81,45),CHAR(45,120,51,53,45,81,45),CHAR(45,120,51,54,45,81,45),CHAR(45,120,51,55,45,81,45),CHAR(45,120,51,56,45,81,45),CHAR(45,120,51,
57,45,81,45)%20--%20/*%20order%20by%20%22as HTTP/1.1" 403 455 "-" "-"
94.63.119.168 - - [30/Apr/2017:03:56:22 +0300] "GET /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
122.174.54.206 - - [30/Apr/2017:03:56:22 +0300] "GET /not_found HTTP/1.1" 302 8571 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
39.53.3.109 - - [30/Apr/2017:03:56:35 +0300] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
```

Κανονικά πρέπει να έχουμε όλα τα ευαίσθητα μοτίβα. Για την εξοικονόμηση χώρου, η παρακάτω regular expresion βγάζει τα ίδια αποτελέσματα :

\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b.+((%22)|\bselect\b)

*σημείωση : μπορεί αυτό (και το παραπάνω) regex να δουλέψει σε αυτό το αρχείο access log ωστόσο ο εντοπισμός του sql injection με key filtering δεν είναι τόσο αποτελεσματικός τρόπος καθώς υπάρχουν πολύ τρόποι να το επιτευχθεί bypass.

Απάντηση b

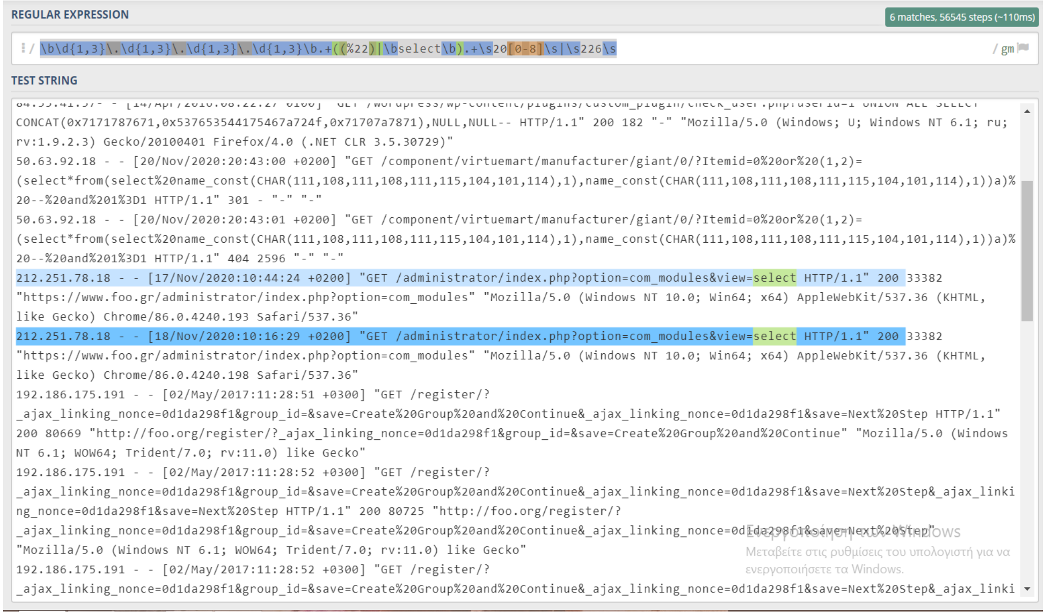
Αν το response status code του server είναι επιτυχές (success) τότε θα είναι ένα από τα παρακάτω :

200 , 201, 202, 203, 204, 205, 206, 207, 208, 226

Οπότε για να εντοπίσουμε κάποιο sql injection του οποίου το response status είναι επιτυχές μπορούμε να χρησιμοποιήσουμε την παρακάτω regular expression:

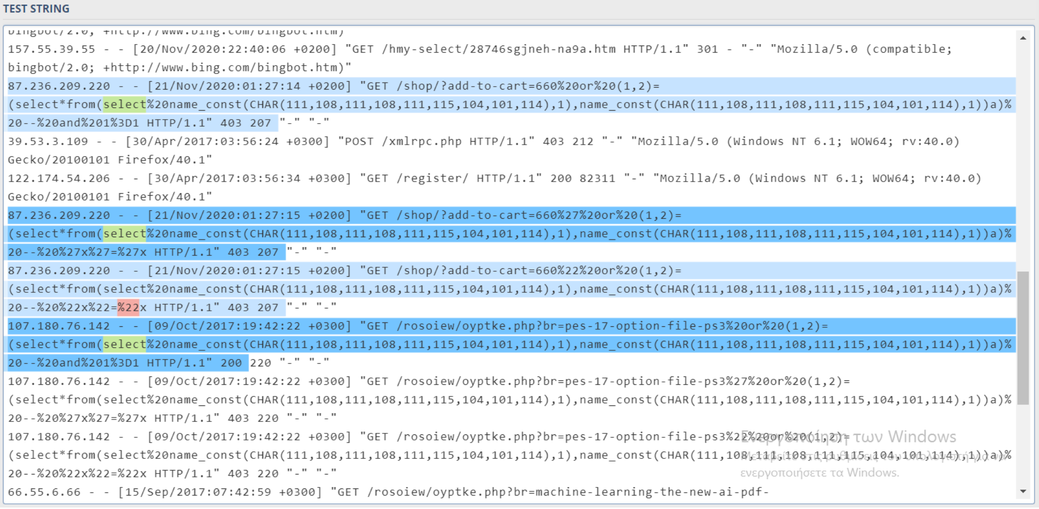
\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b.+((%22)|\bselect\b).+\s20[0-8]\s|\s226\s

και βλέπουμε ότι υπάρχουν 6 matches :



```
/ \b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b.+((%22)|\bselect\b).+\s20[0-8]\s|\s226\s / gm
```

```
84.55.41.57- - [14/Apr/2016:08:22:27 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru;
rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)"
50.63.92.18 - - [20/Nov/2020:20:43:00 +0200] "GET /component/virtuemart/manufacturer/giant/0/?Itemid=0%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 301 - "-" "-"
50.63.92.18 - - [20/Nov/2020:20:43:01 +0200] "GET /component/virtuemart/manufacturer/giant/0/?Itemid=0%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 404 2596 "-" "-"
212.251.78.18 - - [17/Nov/2020:10:44:24 +0200] "GET /administrator/index.php?option=com_modules&view=select HTTP/1.1" 200 33382
"https://www.foo.gr/administrator/index.php?option=com_modules" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.193 Safari/537.36"
212.251.78.18 - - [18/Nov/2020:10:16:29 +0200] "GET /administrator/index.php?option=com_modules&view=select HTTP/1.1" 200 33382
"https://www.foo.gr/administrator/index.php?option=com_modules" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36"
192.186.175.191 - - [02/May/2017:11:28:51 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step HTTP/1.1"
200 80669 "http://foo.org/register/?_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue" "Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.186.175.191 - - [02/May/2017:11:28:52 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step HTTP/1.1" 200 80725 "http://foo.org/register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step"
"Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.186.175.191 - - [02/May/2017:11:28:52 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
```



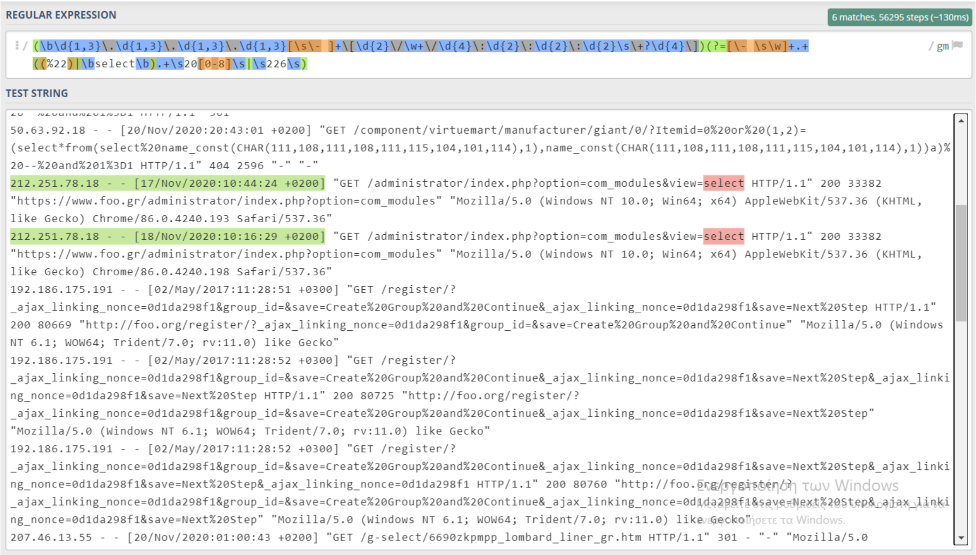
```
bingbot/2.0; +http://www.bing.com/bingbot.htm)
157.55.39.55 - - [20/Nov/2020:22:40:06 +0200] "GET /hmy-select/28746sgjneh-na9a.htm HTTP/1.1" 301 - "-" "Mozilla/5.0 (compatible;
bingbot/2.0; +http://www.bing.com/bingbot.htm)"
87.236.209.220 - - [21/Nov/2020:01:27:14 +0200] "GET /shop/?add-to-cart=660%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 403 207 "-" "-"
39.53.3.109 - - [30/Apr/2017:03:56:24 +0300] "POST /xmlrpc.php HTTP/1.1" 403 212 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
122.174.54.206 - - [30/Apr/2017:03:56:34 +0300] "GET /register/ HTTP/1.1" 200 82311 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
87.236.209.220 - - [21/Nov/2020:01:27:15 +0200] "GET /shop/?add-to-cart=660%27%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%27x%27=%27x HTTP/1.1" 403 207 "-" "-"
87.236.209.220 - - [21/Nov/2020:01:27:15 +0200] "GET /shop/?add-to-cart=660%22%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%22x%22=%22x HTTP/1.1" 403 207 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 200 220 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%27%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%27x%27=%27x HTTP/1.1" 403 220 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%22%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%22x%22=%22x HTTP/1.1" 403 220 "-" "-"
66.55.6.66 - - [15/Sep/2017:07:42:59 +0300] "GET /rosoiew/oyptke.php?br=machine-learning-the-new-ai-pdf-
```

Απάντηση c

Η νέα regular expression θα είναι :

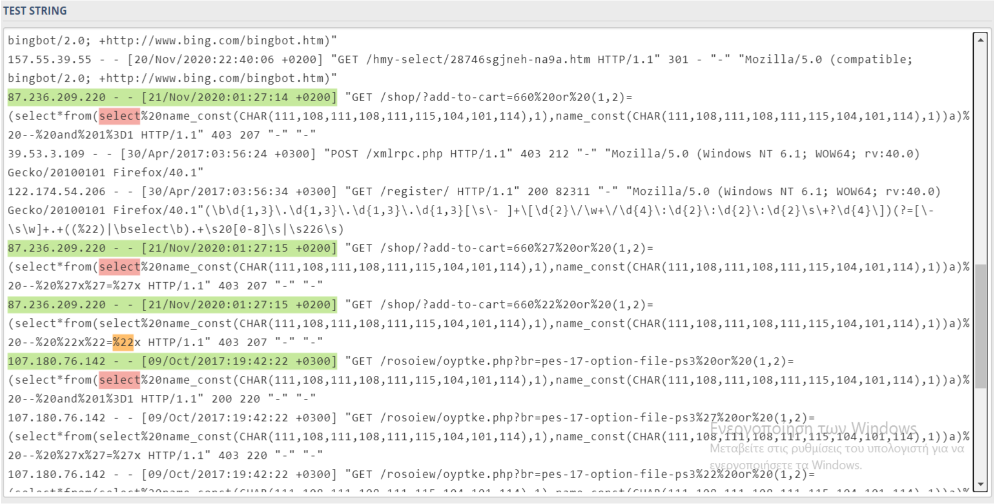
(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}[\s\-]+\[\d{2}\/\w+\/\d{4}\:\d{2}\:\d{2}\:\d{2}\s\+?\d{4}\])(?=[\-\s\w]+.+((%22)|\bselect\b).+\s20[0-8]\s|\s226\s)

Και τα αποτελέσματα θα εμφανίζονται ώς εξής :



```
/ (\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}[\s\- ]+\[\d{2}\/\w+\/\d{4}\:\d{2}\:\d{2}\:\d{2}\s\+?\d{4}\])(?=[\-\s\w]+.+
((%22)|\bselect\b).+\s20[0-8]\s|\s226\s)
```

```
20--%20and%201%3D1 HTTP/1.1" 301
50.63.92.18 - - [20/Nov/2020:20:43:01 +0200] "GET /component/virtuemart/manufacturer/giant/0/?Itemid=0%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 404 2596 "-" "-"
212.251.78.18 - - [17/Nov/2020:10:44:24 +0200] "GET /administrator/index.php?option=com_modules&view=select HTTP/1.1" 200 33382
"https://www.foo.gr/administrator/index.php?option=com_modules" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.193 Safari/537.36"
212.251.78.18 - - [18/Nov/2020:10:16:29 +0200] "GET /administrator/index.php?option=com_modules&view=select HTTP/1.1" 200 33382
"https://www.foo.gr/administrator/index.php?option=com_modules" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36"
192.186.175.191 - - [02/May/2017:11:28:51 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step HTTP/1.1"
200 80669 "http://foo.org/register/?_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue" "Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.186.175.191 - - [02/May/2017:11:28:52 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step HTTP/1.1" 200 80725 "http://foo.org/register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step"
"Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.186.175.191 - - [02/May/2017:11:28:52 +0300] "GET /register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step&_ajax_linking_nonce=0d1da298f1 HTTP/1.1" 200 80760 "http://foo.org/register/?
_ajax_linking_nonce=0d1da298f1&group_id=&save=Create%20Group%20and%20Continue&_ajax_linking_nonce=0d1da298f1&save=Next%20Step&_ajax_linki
ng_nonce=0d1da298f1&save=Next%20Step" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
207.46.13.55 - - [20/Nov/2020:01:00:43 +0200] "GET /g-select/6690zkpmpp_lombard_liner_gr.htm HTTP/1.1" 301 - "-" "Mozilla/5.0
```



```
bingbot/2.0; +http://www.bing.com/bingbot.htm)"
157.55.39.55 - - [20/Nov/2020:22:40:06 +0200] "GET /hmy-select/28746sgjneh-na9a.htm HTTP/1.1" 301 - "-" "Mozilla/5.0 (compatible;
bingbot/2.0; +http://www.bing.com/bingbot.htm)"
87.236.209.220 - - [21/Nov/2020:01:27:14 +0200] "GET /shop/?add-to-cart=660%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 403 207 "-" "-"
39.53.3.109 - - [30/Apr/2017:03:56:24 +0300] "POST /xmlrpc.php HTTP/1.1" 403 212 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"
122.174.54.206 - - [30/Apr/2017:03:56:34 +0300] "GET /register/ HTTP/1.1" 200 82311 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1"(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}[\s\- ]+\[\d{2}\/\w+\/\d{4}\:\d{2}\:\d{2}\:\d{2}\s\+?\d{4}\])(?=[\-
\s\w]+.+((%22)|\bselect\b).+\s20[0-8]\s|\s226\s)
87.236.209.220 - - [21/Nov/2020:01:27:15 +0200] "GET /shop/?add-to-cart=660%27%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%27x%27=%27x HTTP/1.1" 403 207 "-" "-"
87.236.209.220 - - [21/Nov/2020:01:27:15 +0200] "GET /shop/?add-to-cart=660%22%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%22x%22=%22x HTTP/1.1" 403 207 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20and%201%3D1 HTTP/1.1" 200 220 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%27%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
20--%20%27x%27=%27x HTTP/1.1" 403 220 "-" "-"
107.180.76.142 - - [09/Oct/2017:19:42:22 +0300] "GET /rosoiew/oyptke.php?br=pes-17-option-file-ps3%22%20or%20(1,2)=
(select*from(select%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a)%
```