Offense IP: 53270

Description

This is SQL injection Attempt , Attacker used sqlmap for injection.

Decoded log:

/news-details.php?nid=13' OR EXP(~(SELECT * FROM (SELECT CONCAT(0x716a787871,(SELECT (ELT(5946=5946,1))),0x7178717071,0x78))x)) AND 'faGl'='faGl","http_user_agent":"sqlmap\/1.7.10#stable (https:\/\/sqlmap.org)"

/news-details.php?nid=13' AND EXP(~(SELECT * FROM (SELECT CONCAT(0x716a787871,(SELECT (ELT(1277=1277,1))),0x7178717071,0x78))x)) AND 'jwPt'='jwPt","http_user_agent":"sqlmap\/1.7.10#stable (https:\/\/sqlmap.org)"

/news-details.php?nid=13' OR (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x716a787871,(SELECT (ELT(7399=7399,1))),0x7178717071,0x78))s), 8446744073709551610, 8446744073709551610))) AND 'qoPz'='qoPz","http_user_agent":"sqlmap\/1.7.10#stable (https:\/\/sqlmap.org)"

/news-details.php?nid=13' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x716a787871,(SELECT (ELT(8495=8495,1))),0x7178717071,0x78))s), 8446744073709551610, 8446744073709551610))) AND 'TRyk'='TRyk","http_user_agent":"sqlmap\/1.7.10#stable (https:\/\/sqlmap.org)"

GET /news-details.php?nid=13' AND GTID_SUBSET(CONCAT(0x716a787871,(SELECT (ELT(1582=1582,1))),0x7178717071),1582) AND 'CaOQ'='CaOQ

Attacker Info:

IP: 31.61.233.203{*}:{*}

User Agent:

Browser: TOR

Analyst Investigation Results:

**

Virus Total Result: None

The processed IP address as the attacker:

[here|https:// https://www.virustotal.com/gui/ip-address/31.61.233.203]

Security Vendors' Analysis from Virus Total: Clear

Talos Intelligence: for 31.61.233.203{*}:{*}

[here|https://talosintelligence.com/reputation_center/lookup?search=31.61.233.203]

*LOCATION DATA * : Warsaw, Poland

*BLOCK LISTS *

SENDER IP REPUTATION Poor

WEB REPUTATION Unknown

BL.SPAMCOP.NET Not Listed

CBL.ABUSEAT.ORG NOT Listed

PBL.SPAMHAUS.ORG Listed

SBL.SPAMHAUS.ORG Not Listed

**

Shodan Result: for for 31.61.233.203{*}:{*} No results found

[here| https://www.shodan.io/search?query=31.61.233.203]

Victim: 38.242.128.144 vmi919546.contaboserver.net

Raw Data:

<168>Nov 12 14:09:35 websystem suricata[2154]: {"timestamp":"2023-11-12T14:09:35.436524+0100","flow_id":1682346450292449,"in_iface":"eth0","event_type":"alert","src_ip":"31.61.233.203","src_port":18531,"dest_ip":"38.242.128.144","dest_port":80,"proto":"TCP","http":{"hostname":"news.cydeosec.com","url":"\/news-details.php?nid=13%27%20OR%20EXP%28~%28SELECT%20%2A%20FROM%20%28SELECT%20CONCAT%280x716a787871%2C%28SELECT%20%28ELT%285946%3D5946%2C1%29%29%29%2C0x7178717071%2C0x78%29%29x%29%29%20AND%20%27faGl%27%3D%27faGl","http_user_agent":"sqlmap\/1.7.10#stable (https:\/\/sqlmap.org)","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":2089},"tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2011042,"rev":3,"signature":"ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt","category":"Web Application Attack","severity":1}}... 23 lines omitted ...

Investigation Result

Analysis

Attacker use sqlmap over tor and want to test Time-dependent SQL injection

Magnitude	(5)	Relevance	1	Severity	9	Credibility	5

Also I found 24 events on splunk with different URL on Qradar :

GET /news-details.php?nid=13' AND GTID_SUBSET(CONCAT(0x716a787871,(SELECT (ELT(1582=1582,1))),0x7178717071),1582) AND 'CaOQ'='CaOQ

And 345 events on splunk with : "HTTP\/1.1","status":200

Action

Disconnect the internet, see authentication on users,

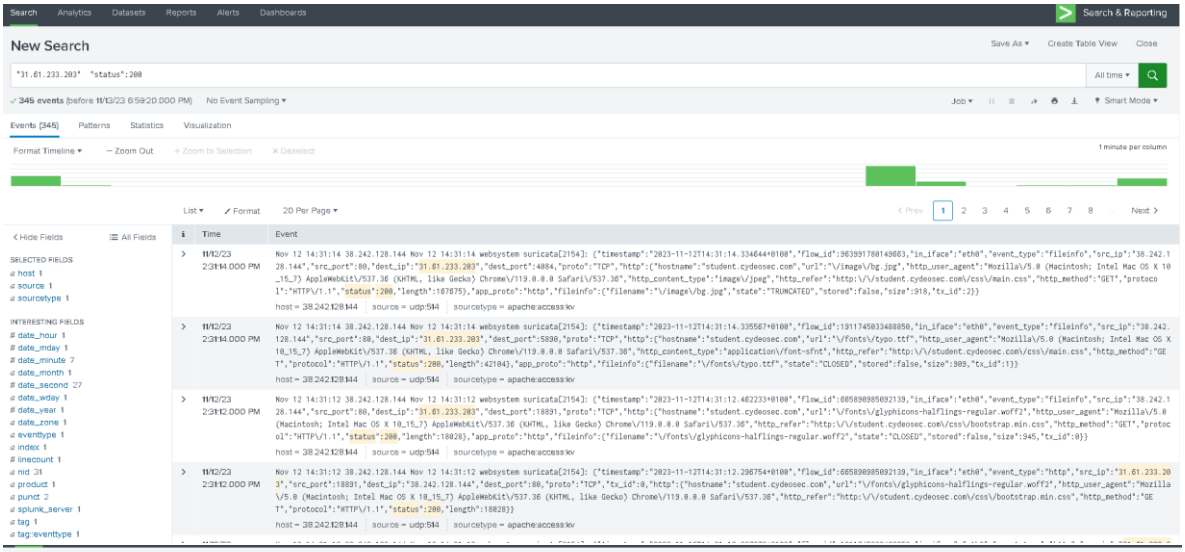
Use Parameterized Statements/Prepared Statements and Input Validation.

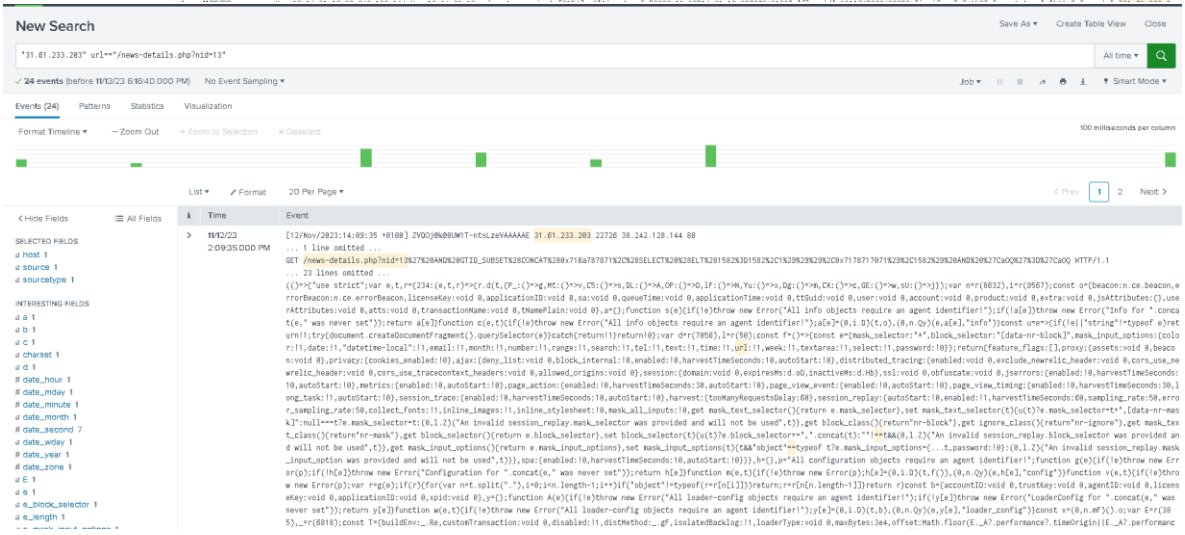
For API :

API Authentication and Authorization:

Implement strong authentication mechanisms for your API, ensuring that only authorized users can access the endpoints. Limit the permissions of each API key or user account to the minimum necessary.

Attachment:


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
"31.61.233.203" "status":200
All time
345 events (before 11/13/23 6:59:20.000 PM)
No Event Sampling
Job
Smart Mode
Events (345)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 minute per column
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 7
date_month 1
date_second 27
date_wday 1
date_year 1
date_zone 1
eventtype 1
index 1
linecount 1
nid 31
product 1
punct 2
splunk_server 1
tag 1
tag::eventtype 1
Time
Event
11/12/23 2:31:14.000 PM
Nov 12 14:31:14 38.242.128.144 Nov 12 14:31:14 websystem suricata[2154]: {"timestamp":"2023-11-12T14:31:14.334644+0100","flow_id":963991780143663,"in_iface":"eth0","event_type":"fileinfo","src_ip":"38.242.128.144","src_port":80,"dest_ip":"31.61.233.203","dest_port":4084,"proto":"TCP","http":{"hostname":"student.cydeosec.com","url":"\/image\/bg.jpg","http_user_agent":"Mozilla\/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/119.0.0.0 Safari\/537.36","http_content_type":"image\/jpeg","http_refer":"http:\/\/student.cydeosec.com\/css\/main.css","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":167675},"app_proto":"http","fileinfo":{"filename":"\/image\/bg.jpg","state":"TRUNCATED","stored":false,"size":918,"tx_id":2}}
host = 38.242.128.144 source = udp:514 sourcetype = apache:access:kv
11/12/23 2:31:14.000 PM
Nov 12 14:31:14 38.242.128.144 Nov 12 14:31:14 websystem suricata[2154]: {"timestamp":"2023-11-12T14:31:14.335567+0100","flow_id":1911745033488850,"in_iface":"eth0","event_type":"fileinfo","src_ip":"38.242.128.144","src_port":80,"dest_ip":"31.61.233.203","dest_port":5890,"proto":"TCP","http":{"hostname":"student.cydeosec.com","url":"\/fonts\/typo.ttf","http_user_agent":"Mozilla\/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/119.0.0.0 Safari\/537.36","http_content_type":"application\/font-sfnt","http_refer":"http:\/\/student.cydeosec.com\/css\/main.css","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":42104},"app_proto":"http","fileinfo":{"filename":"\/fonts\/typo.ttf","state":"CLOSED","stored":false,"size":909,"tx_id":1}}
host = 38.242.128.144 source = udp:514 sourcetype = apache:access:kv
11/12/23 2:31:12.000 PM
Nov 12 14:31:12 38.242.128.144 Nov 12 14:31:12 websystem suricata[2154]: {"timestamp":"2023-11-12T14:31:12.462233+0100","flow_id":66589085092139,"in_iface":"eth0","event_type":"fileinfo","src_ip":"38.242.128.144","src_port":80,"dest_ip":"31.61.233.203","dest_port":18891,"proto":"TCP","http":{"hostname":"student.cydeosec.com","url":"\/fonts\/glyphicons-halflings-regular.woff2","http_user_agent":"Mozilla\/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/119.0.0.0 Safari\/537.36","http_refer":"http:\/\/student.cydeosec.com\/css\/bootstrap.min.css","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":18028},"app_proto":"http","fileinfo":{"filename":"\/fonts\/glyphicons-halflings-regular.woff2","state":"CLOSED","stored":false,"size":945,"tx_id":0}}
host = 38.242.128.144 source = udp:514 sourcetype = apache:access:kv
11/12/23 2:31:12.000 PM
Nov 12 14:31:12 38.242.128.144 Nov 12 14:31:12 websystem suricata[2154]: {"timestamp":"2023-11-12T14:31:12.296754+0100","flow_id":66589085092139,"in_iface":"eth0","event_type":"http","src_ip":"31.61.233.203","src_port":18891,"dest_ip":"38.242.128.144","dest_port":80,"proto":"TCP","tx_id":0,"http":{"hostname":"student.cydeosec.com","url":"\/fonts\/glyphicons-halflings-regular.woff2","http_user_agent":"Mozilla\/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/119.0.0.0 Safari\/537.36","http_refer":"http:\/\/student.cydeosec.com\/css\/bootstrap.min.css","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":18028}}
host = 38.242.128.144 source = udp:514 sourcetype = apache:access:kv


New Search
Save As
Create Table View
Close
"31.61.233.203" url="*/news-details.php?nid=13"
All time
24 events (before 11/13/23 6:16:40.000 PM)
No Event Sampling
Job
Smart Mode
Events (24)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
100 milliseconds per column
List
Format
20 Per Page
Prev
1
2
Next
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
a 1
b 1
c 1
charset 1
d 1
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 7
date_wday 1
date_year 1
date_zone 1
E 1
e 1
e_block_selector 1
e_length 1
Time
Event
11/12/23 2:09:35.000 PM
[12/Nov/2023:14:09:35 +0100] ZVOOj0k00UWlT-ntsLzeYAAAAAE 31.61.233.203 22726 38.242.128.144 80
... 1 line omitted ...
GET /news-details.php?nid=13%27%20AND%20GTID_SUBSET%28CONCAT%288x716a787871%2C%28SELECT%20%28ELT%281582%3D1582%2C1%29%29%29%2C0x7178717071%29%2C1582%29%20AND%20%27CaOQ%27%3D%27CaOQ HTTP/1.1
... 23 lines omitted ...