

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:// www.virustotal.com/gui/ip-address/31.61.233.203](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.

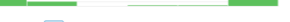
Attachment:

All time ▾

Job ▾ || || ▸ 🔍 ⬆ Smart Mode ▾

Job ▾ || || ▸ 🔍 ⬆ Smart Mode ▾

1 minute per column



< Prev **1** 2 3 4 5 6 7 8 ... Next >

i	Time	Event
---	------	-------

i	Time	Event
---	------	-------

```
Nov 12 14:31:14 38.242.128.144 Nov 12 14:31:14 websystem suricata[2194]: {"timestamp": 2023-11-12T14:31:14.334644+0100", "flow_id": 363591780148663, "in_iface": "eth0", "event_type": "fileinfo", "src_ip": "38.242.128.144", "src_port": 80, "dest_ip": "31.61.233.283", "dest_port": 4884, "proto": "TCP", "http": {"hostname": "student.cydeosec.com", "url": "\/image\/bg.jpg", "http_user_agent": "Mozilla\/5.0 (Macintosh; Intel Mac OS X 10_11_2) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/44.0.2403.157 Safari\/537.36"}}
```

```

..._15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36"; "http_content_type": "image/jpeg", "http_referer": "http://student.cybersec.com/css/main.css", "http_method": "GET", "proto
": "HTTP/1.1", "status": 200, "length": 167875, "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
```

2:31:14.000 PM 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

```
T", "protocol": "HTTP/1.1", "status": 200, "length": 42184, "app_proto": "http", "fileinfo": {"filename": "\/fonts\/typo.ttf", "state": "CLOSED", "stored": false, "size": 989, "tx_id": 1}}
```

host = 39.242.128.144	source = udp:144	sourcetype = apache-access-xy
-----------------------	------------------	-------------------------------

```
23112.000 PM 28.144,"src_port":80,"dest_ip":"31.61.233.283","dest_port":18891,"proto":"TCP","http":{"hostname":"student.cydeosec.com","url":"/fonts/glyphicons-halflings-regular.woff2","http_user_agent":"Mozilla/5.0
```

```
ol":{"HTTP/1.1","status":200,"length":18828,"app_prot":"http","fileinfo":{"filename":"/fonts/glyphicons-halflings-regular.woff2","state":"CLOSED","stored":false,"size":945,"tx_id":0}}
```

```
2/31/2000 PM 3", "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/cso/boosterplan.php", "http_method": "GET" }
```

```
T*, "protocol": "HTTP/1.1", "status": 200, "length": 18828}}
```

Save As ▼ Create Table View Close

All time ▾ 🔍

Job ▾ || || ↗ 🔍 ⬆ ⚡ Smart Mode ▾

0.00 milliseconds per column



< Prev **1** 2 Next >

i	Time	Event
---	------	-------

```
> 11/12/23 [12/Nov/2023:14:09:35 +0100] ZVO0jEN@BUMIT-ntsLzeVAAAAAE 31.61.233.203 22726 38.242.128.144 80
200/200000000 1 line omitted
```

```
GET /news-details.php?id=13k27K2bANDK2bGTID_SUBSETK28CONCATK28x716a787871K2Ck28SELECTK28K28ELTK281582K3D1582K2C1K29K29K29K2C8x7178717871K29K2C1582K29K2bANDK28K27C8xK27K3Dk27C8x HTTP/1.1
33 lines omitted
```

```
((*)%*use strict*;var e,t,r=(234:(e,t,r)%>f.d(t,{P_:(*)%>,MC:({}%>,CS:({}%>,DL:({}%>,AP:({}%>,IF:({}%>,Yu:({}%>,Dg:({}%>,CX:({}%>,GE:({}%>,SU:({}%>));var n=r(8632),r(9567);const o={beacon:n.ca.beacon,e}
```

```
rAttributes(void 0,atts:void 0,transactionName:void 0,tNamePlain:void 0),a=c);function s(e){if(!e)throw new Error("All info objects require an agent identifier!");if(!a[e])throw new Error("Info for '"+e+"' was never set");return c[a][e]}function g(a,t){if(!t)throw new Error("All info objects require an agent identifier!");var f=a[t];if(f){f["info"]||c.set(a,"info",{});f["info"].toString=function(){return f["info"]}}
```

```
url||try(document.createDocument().querySelector(e).catch{return||return||var d=r(755),i=r(58);const f={}>>const e={mask_selector:"*",block_selector:["data-nr-block"],mask_input_options:{color:1,date:1,"datetime-local":1,email:1,month:1,number:1,password:1,search:1,tel:1,text:1,time:1,url:1,week:1,textarea:1,color:1,password:1},return(f.feature_flags||{}).passwords:1;# bo
```

```

n: void 0, privacy: {cookies_enabled: 10}, ajax: {deny_list: void 0, block_internal: 10, enabled: 10, harvestTimeSeconds: 10, autostart: 10}, distributed_tracing: {enabled: void 0, exclude_newrelic_header: void 0, cors_use_newrelic_header: void 0, cors_use_tracertext_headers: void 0, allowed_origins: void 0}, session: {domain: void 0, expiresMs: d 0, inactiveMs: d 40}, ssl: void 0, obfuscate: void 0, iserrors: {enabled: 10, harvestTimeSeconds:

```

```
10,autoStart:{0},metrics:{enabled:{0},autoStart:{0}},page_action:{enabled:{0},harvestTimeSeconds:30,autoStart:{0}},page_view_event:{enabled:{0},autoStart:{0}},page_view_timing:{enabled:{0},harvestTimeSeconds:30,autoStart:{0}},single_task:{1,autoStart:{0}},session_trace:{enabled:{0},harvestTimeSeconds:10,autoStart:{0}},harvest:{tooManyRequestsDelay:60},session_replay:{autoStart:{0},enabled:{1},harvestTimeSeconds:60,sampling_rate:50,errors:{0}}
```

```

r_sampling_rate:50,collect_fonts:1,inline_images:1,inline_stylesheet:10,mask_all_inputs:1,get_mask_text_selector(){return e.mask_selector},set_mask_text_selector(f){u(f)%e.mask_selector+="",[data-nr-mask
k?":null***?e.mask_selector+f:(0.1.2)"/An invalid session replay mask selector was provided and will not be used*:f}}.get_block_class(){return"nr-block*}.get_ignore_class(){return"nr-ignore*}.get_mask_tex

```

```

t.class()return "nr-mask",get_block_selector()return e.block_selector,set_block_selector(t){u(t)%=block_selector+*,.concat(t):""+t%t%["An invalid session_replay_block_selector was provided and
d will not be used".t]}get_mask_input_options()return e.mask_input_options.set_mask_input_options(t){t%t%object""typeof t%e.mask_input_options%...t.password:0:0.1.2}["An invalid session_replay_mask

```

```

    _input_option was provided and will not be used.");spc:(enabled:0,numberOfTimeSeconds:1,accuracy:0));n["j",p="All configuration objects require an agent identifier";function g(e){if(!e)throw new Error("Agent identifier is required");if(!e.startsWith("agent:"))throw new Error("Agent identifier must start with 'agent:'");return e.startsWith("agent:")?e.substring(7):e;}function h(e){if(!e)throw new Error("Configuration for 'concat' was never set");return h(e)}function m(e,t){if(!e)throw new Error(a:h["j"]+(0-i-1)+t.f+"): (0-p-0x)(e-h["j"].config)}function y(e,t){if(!e)throw

```

```

    w new Error(D);var f=g(e);if(f){f=(var n=c.split( ,1+0;1;n.length-1;));if(!Object.prototype.hasOwnProperty(f[n]))return f=f[n];return f}const o={accountId:void 0,trustKey:void 0,agentId:void 0,itemId:
    eKey:void 0,applicationID:void 0,xpid:void 0},v={};function A(e){if(!e)throw new Error("All loader-config objects require an agent identifier!");if(!e)throw new Error("LoaderConfig for ".concat(e," was

```

```

never set >>:return ylo))function (o,t){if(!o)throw new Error("All loader-config objects require an agent identifier!");ylo=(o,i,o)(o),(o,n,o)(o,ylo, loader_config ))const x=(o,n,nr){>:o:var x=(38
5),_r(5818);const T=(buildEnv:_Re,customTransaction:void 0,disabled:!1,distMethod:_gf,isolatedBacklog:!1,loaderType:void 0,maxBytes:3e4,offset:Math.floor(E_A?.performance?.timeOrigin)/E_A?.performanc

```