Qradar Incident ID: Offense 49947

Web Attacks
(LFI)

Summery : Web application attack OR Web Exploit

Description

attacker use wordpress vulnerability to exploit website use wp-config.php

and used REQUEST-930-APPLICATION-ATTACK-LFI.conf to reconfigure wp-config.php

"OWASP_CRS/3.0.0" set rules for this type of vulnerability.

Event/Flow count 2 events and 0 flows in 1 categories

Relevance 0 Severity 9 Credibility 2 Magnitude 3

```
(Total Inbound Score: 8 -
SQLI=0,XSS=0,RFI=0,LFI=5,RCE=0,PHPI=0,HTTP=0,SESS=0)
```

Encoded log: - /wp-config.php~","http_user_agent":"Mozilla\/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko\/20100101 Firefox\/77.0","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1

Decoded log: -

Attacker Info:
IP: 89.40.227.242

User Agent: Mozilla\/5.0

Browser Name: - Firefox

Browser Version: - \/77.0

OS: - Intel Mac OS X
Accept-Encoding: gzip, deflate

Analyst Investigation Results:

Virus Total Result:

6 security vendors flagged this IP address as malicious

Security vendors' analysis : **Malicious**

[here| https://www.virustotal.com/gui/ip-address/89.40.227.242]

Security Vendors' Analysis from Talos Intelligence:

Talos Intelligence:

LOCATION DATA : Italy

REPUTATION DETAILS
IP Reputation: Poor
WEB REPUTATION: Untrusted
BLOCK LISTS:
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 Yes

CLASSIFICATION: Malware

[here|https://talosintelligence.com/reputation_center/lookup?search=89.40.227.242
]

Shodan Result:

Open Ports: - 80 443 995 2082 2086 2087

Domains : 3DO.it , CPRAPID.COM , EMAHT.COM , TEST3DO.IT

[here|https://www.shodan.io/host/89.40.227.242
]

Brief Community Comments: -

Victim: 38.242.128.144

Raw Data:

```
<168>Oct 11 13:04:26 websystem suricata[19132]: {"timestamp":"2023-10-11T13:04:26.727822+0200","flow_id":639424014238202,"in_iface":"eth0","event_type":"alert","src_ip":"89.40.227.242","src_port":37286,"dest_ip":"38.242.128.144","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009955,"rev":10,"signature":"ET WEB_SERVER Tilde in URI, potential .php~ source disclosure vulnerability","category":"Web Application Attack","severity":1},"http":{"hostname":"38.242.128.144","url":"\/wp-config.php~","http_user_agent":"Mozilla\/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko\/20100101 Firefox\/77.0","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":403,"length":279}}
```

Action

The results was **403 Forbidden**, so no need for an extra action.

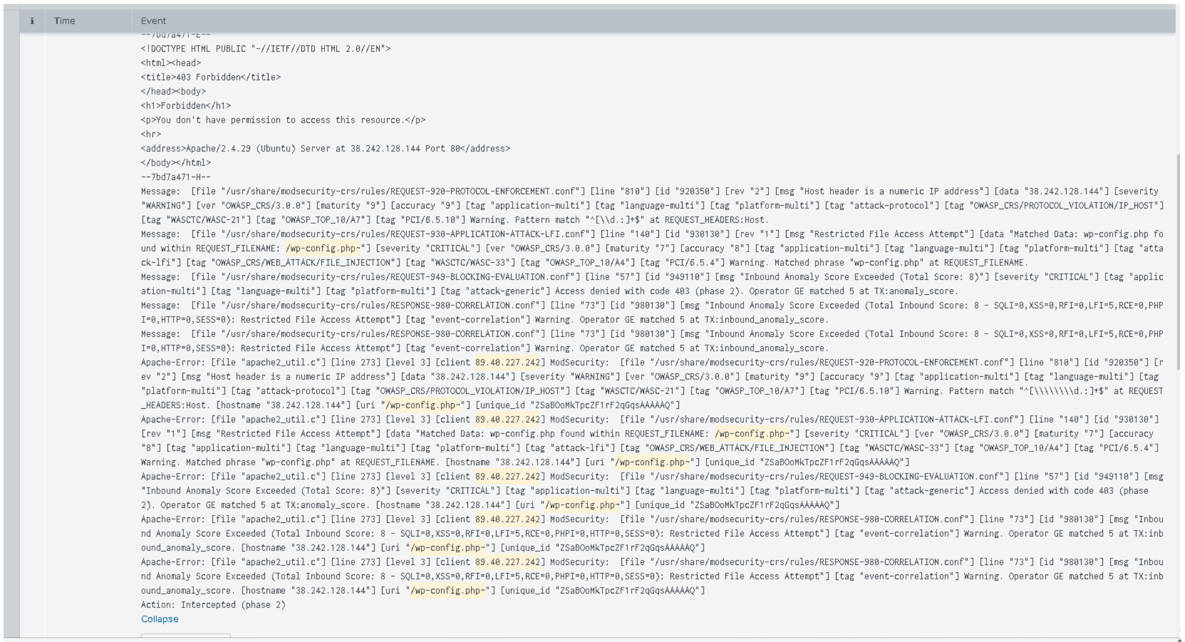
Requirement :

configuring your web application firewall to use the OWASP CRS rule set on web application firewall.

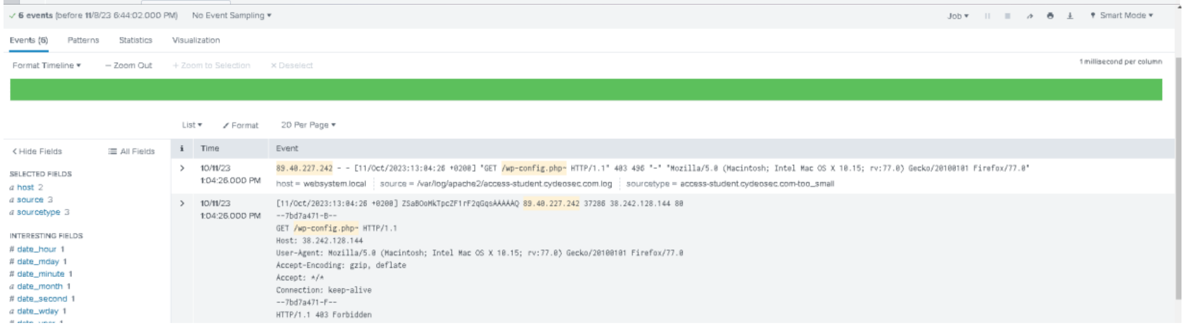
We can use This repository for this type of attack.

rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf

[here|https://github.com/SpiderLabs/owasp-modsecurity-crs/blob/v3.3/dev/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf
]



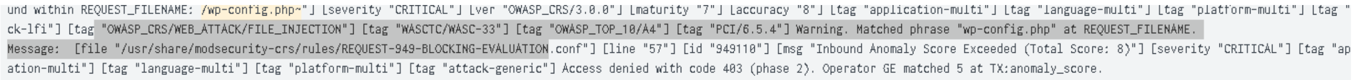
```
--7bd7a471-E--
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at 38.242.128.144 Port 80</address>
</body></html>
--7bd7a471-H--
Message:  [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "810"] [id "920350"] [rev "2"] [msg "Host header is a numeric IP address"] [data "38.242.128.144"] [severity
"WARNING"] [ver "OWASP_CRS/3.0.0"] [maturity "9"] [accuracy "9"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"]
[tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host.
Message:  [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "140"] [id "930130"] [rev "1"] [msg "Restricted File Access Attempt"] [data "Matched Data: wp-config.php fo
und within REQUEST_FILENAME: /wp-config.php~"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "7"] [accuracy "8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "atta
ck-lfi"] [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"] Warning. Matched phrase "wp-config.php" at REQUEST_FILENAME.
Message:  [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "57"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 8)"] [severity "CRITICAL"] [tag "applic
ation-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score.
Message:  [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=0,XSS=0,RFI=0,LFI=5,RCE=0,PHP
I=0,HTTP=0,SESS=0): Restricted File Access Attempt"] [tag "event-correlation"] Warning. Operator GE matched 5 at TX:inbound_anomaly_score.
Message:  [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=0,XSS=0,RFI=0,LFI=5,RCE=0,PHP
I=0,HTTP=0,SESS=0): Restricted File Access Attempt"] [tag "event-correlation"] Warning. Operator GE matched 5 at TX:inbound_anomaly_score.
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 89.40.227.242] ModSecurity:  [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "810"] [id "920350"] [r
ev "2"] [msg "Host header is a numeric IP address"] [data "38.242.128.144"] [severity "WARNING"] [ver "OWASP_CRS/3.0.0"] [maturity "9"] [accuracy "9"] [tag "application-multi"] [tag "language-multi"] [tag
"platform-multi"] [tag "attack-protocol"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] Warning. Pattern match "^[\\\\\\\\d.:]+$" at REQUEST
_HEADERS:Host. [hostname "38.242.128.144"] [uri "/wp-config.php~"] [unique_id "ZSaBOoMkTpcZF1rF2qGqsAAAAAQ"]
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 89.40.227.242] ModSecurity:  [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "140"] [id "930130"]
[rev "1"] [msg "Restricted File Access Attempt"] [data "Matched Data: wp-config.php found within REQUEST_FILENAME: /wp-config.php~"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "7"] [accuracy
"8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"]
Warning. Matched phrase "wp-config.php" at REQUEST_FILENAME. [hostname "38.242.128.144"] [uri "/wp-config.php~"] [unique_id "ZSaBOoMkTpcZF1rF2qGqsAAAAAQ"]
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 89.40.227.242] ModSecurity:  [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "57"] [id "949110"] [msg
"Inbound Anomaly Score Exceeded (Total Score: 8)"] [severity "CRITICAL"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] Access denied with code 403 (phase
2). Operator GE matched 5 at TX:anomaly_score. [hostname "38.242.128.144"] [uri "/wp-config.php~"] [unique_id "ZSaBOoMkTpcZF1rF2qGqsAAAAAQ"]
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 89.40.227.242] ModSecurity:  [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "73"] [id "980130"] [msg "Inbou
nd Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=0,XSS=0,RFI=0,LFI=5,RCE=0,PHPI=0,HTTP=0,SESS=0): Restricted File Access Attempt"] [tag "event-correlation"] Warning. Operator GE matched 5 at TX:inb
ound_anomaly_score. [hostname "38.242.128.144"] [uri "/wp-config.php~"] [unique_id "ZSaBOoMkTpcZF1rF2qGqsAAAAAQ"]
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 89.40.227.242] ModSecurity:  [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "73"] [id "980130"] [msg "Inbou
nd Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=0,XSS=0,RFI=0,LFI=5,RCE=0,PHPI=0,HTTP=0,SESS=0): Restricted File Access Attempt"] [tag "event-correlation"] Warning. Operator GE matched 5 at TX:inb
ound_anomaly_score. [hostname "38.242.128.144"] [uri "/wp-config.php~"] [unique_id "ZSaBOoMkTpcZF1rF2qGqsAAAAAQ"]
Action: Intercepted (phase 2)
```



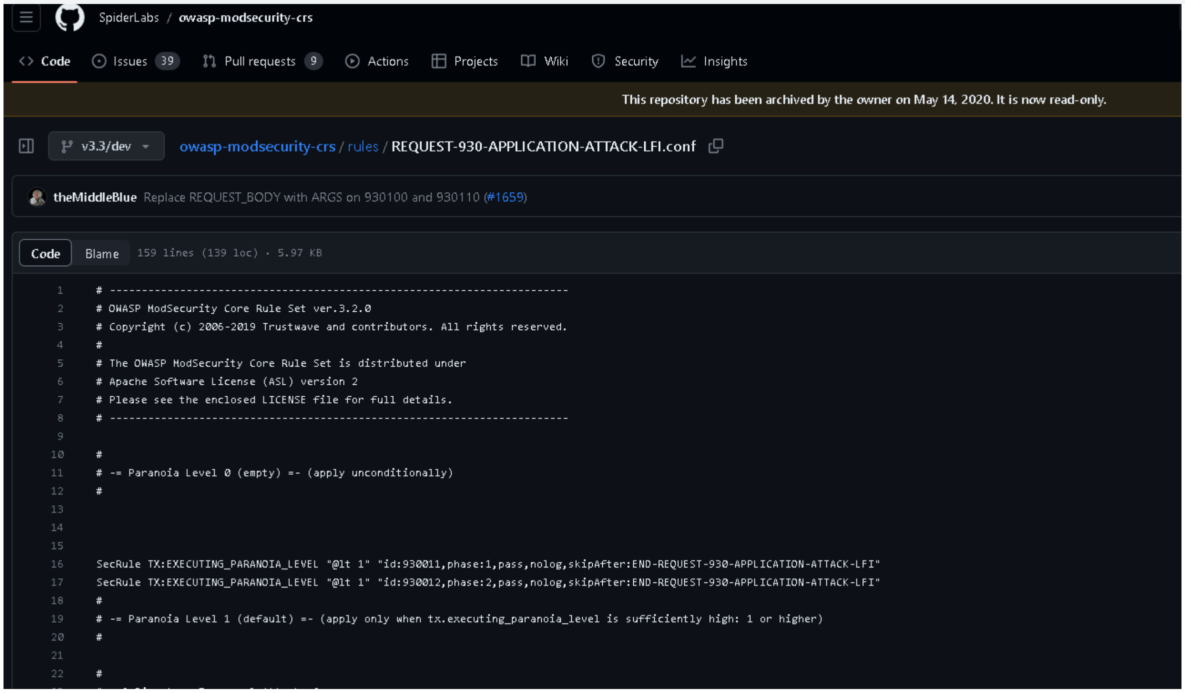
Time	Event

10/11/23
1:04:26.000 PM
	`89.40.227.242 - - [11/Oct/2023:13:04:26 +0200] "GET /wp-config.php~ HTTP/1.1" 403 496 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0"`
	host = websystem.local source = /var/log/apache2/access-student.cydeosec.com.log sourcetype = access-student.cydeosec.com-too_small

10/11/23
1:04:26.000 PM
	`[11/Oct/2023:13:04:26 +0200] ZSaBOoMkTpcZF1rF2qGqsAAAAAQ 89.40.227.242 37286 38.242.128.144 80`
	`--7bd7a471-B--`
	`GET /wp-config.php~ HTTP/1.1`
	`Host: 38.242.128.144`
	`User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0`
	`Accept-Encoding: gzip, deflate`
	`Accept: */*`
	`Connection: keep-alive`
	`--7bd7a471-F--`
	`HTTP/1.1 403 Forbidden`



```
und within REQUEST_FILENAME: /wp-config.php~"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "7"] [accuracy "8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "
ck-lfi"] [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"] Warning. Matched phrase "wp-config.php" at REQUEST_FILENAME.
Message:  [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "57"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 8)"] [severity "CRITICAL"] [tag "ap
ation-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score.
```



This repository has been archived by the owner on May 14, 2020. It is now read-only.

owasp-modsecurity-crs / rules / REQUEST-930-APPLICATION-ATTACK-LFI.conf

theMiddleBlue Replace REQUEST_BODY with ARGS on 930100 and 930110 (#1659)

159 lines (139 loc) · 5.97 KB

```
# ------------------------------------------------------------------------
# OWASP ModSecurity Core Rule Set ver.3.2.0
# Copyright (c) 2006-2019 Trustwave and contributors. All rights reserved.
#
# The OWASP ModSecurity Core Rule Set is distributed under
# Apache Software License (ASL) version 2
# Please see the enclosed LICENSE file for full details.
# ------------------------------------------------------------------------

#
# -= Paranoia Level 0 (empty) =- (apply unconditionally)
#



SecRule TX:EXECUTING_PARANOIA_LEVEL "@lt 1" "id:930011,phase:1,pass,nolog,skipAfter:END-REQUEST-930-APPLICATION-ATTACK-LFI"
SecRule TX:EXECUTING_PARANOIA_LEVEL "@lt 1" "id:930012,phase:2,pass,nolog,skipAfter:END-REQUEST-930-APPLICATION-ATTACK-LFI"
#
# -= Paranoia Level 1 (default) =- (apply only when tx.executing_paranoia_level is sufficiently high: 1 or higher)
#

#
```