Vulnerabilidades Web y uso de mod-security

Luis Miguel Raña Cortizo

Ejercicio 1: Vulnerabilidades típicas en aplicaciones web

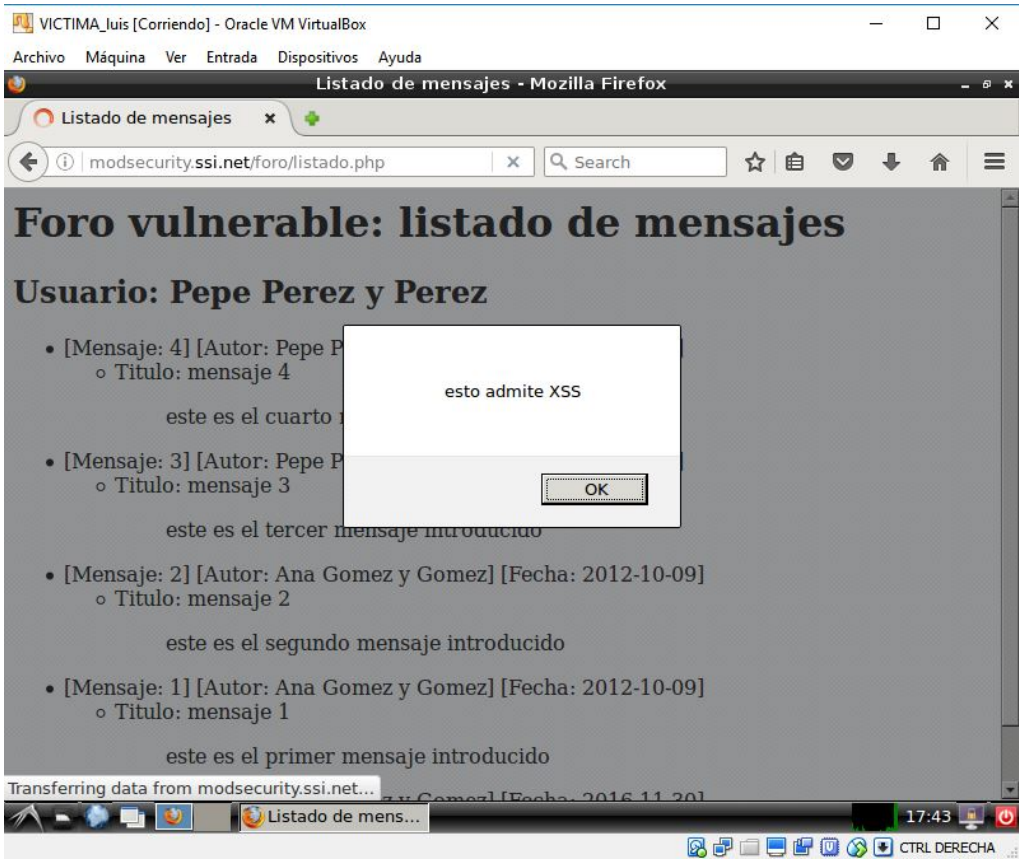
Aplicaciones vulnerables (Cross Site Scripting: XSS)

Foro "simple" vulnerable

En la máquina **modsecurity** hay una implementación de un foro de juguete en PHP.

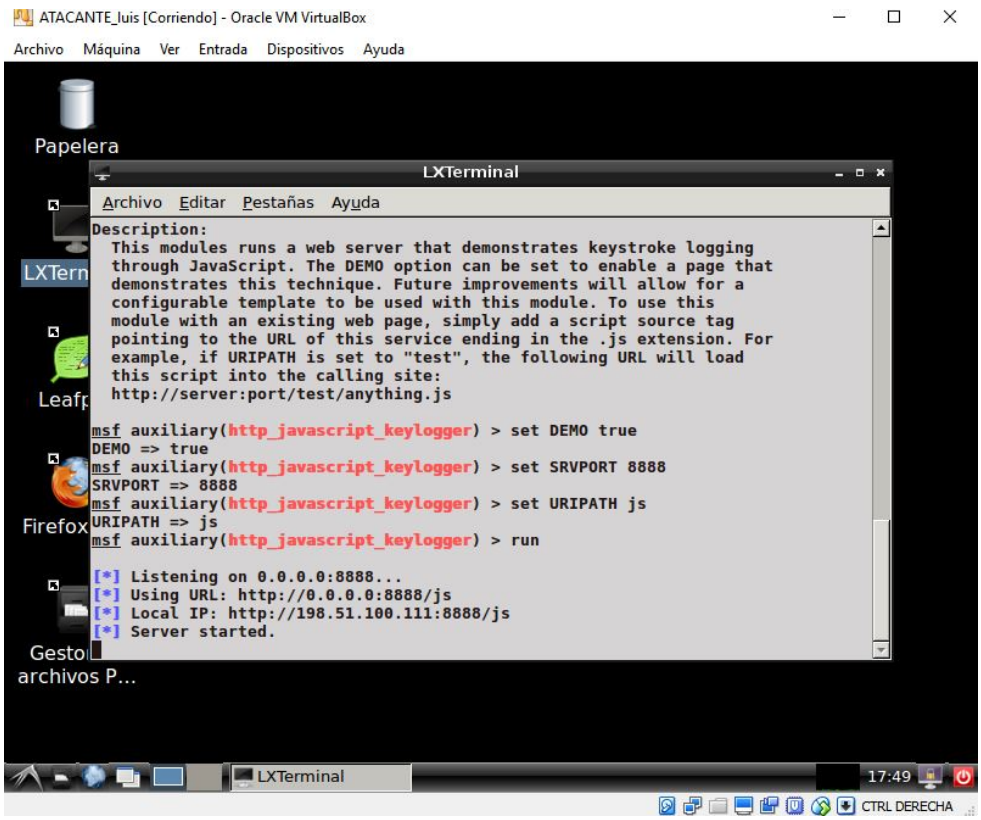
Desde la máquina atacante accedemos a http://modsecurity.ssi.net/foro y nos logueamos con login ana y password ssi y enviamos un ataque de XSS mediante el siguiente mensaje:

Ahora desde la máquina víctima accedemos a `http://modsecurity.ssi.net/foro` y nos logueamos con login pepe y password ssi y accedemos al listado de mensajes para comprobar la ejecución del ataque XSS:

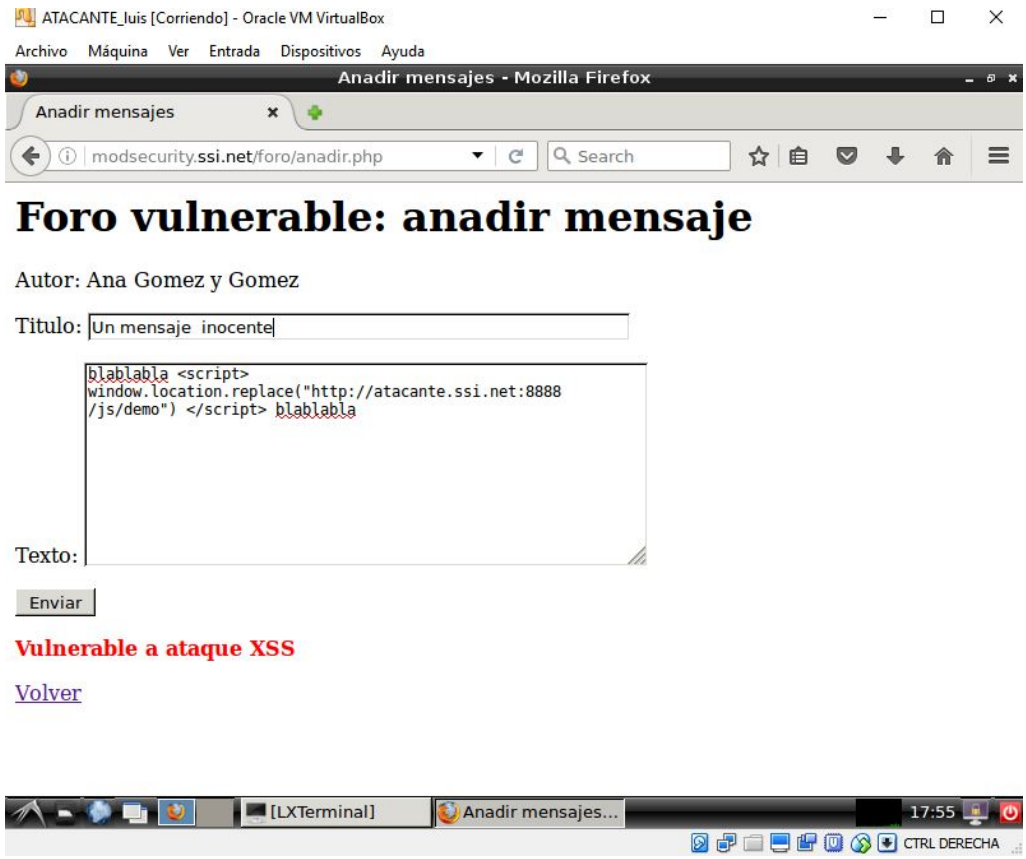


Carga de librerías Javascript "maliciosas"

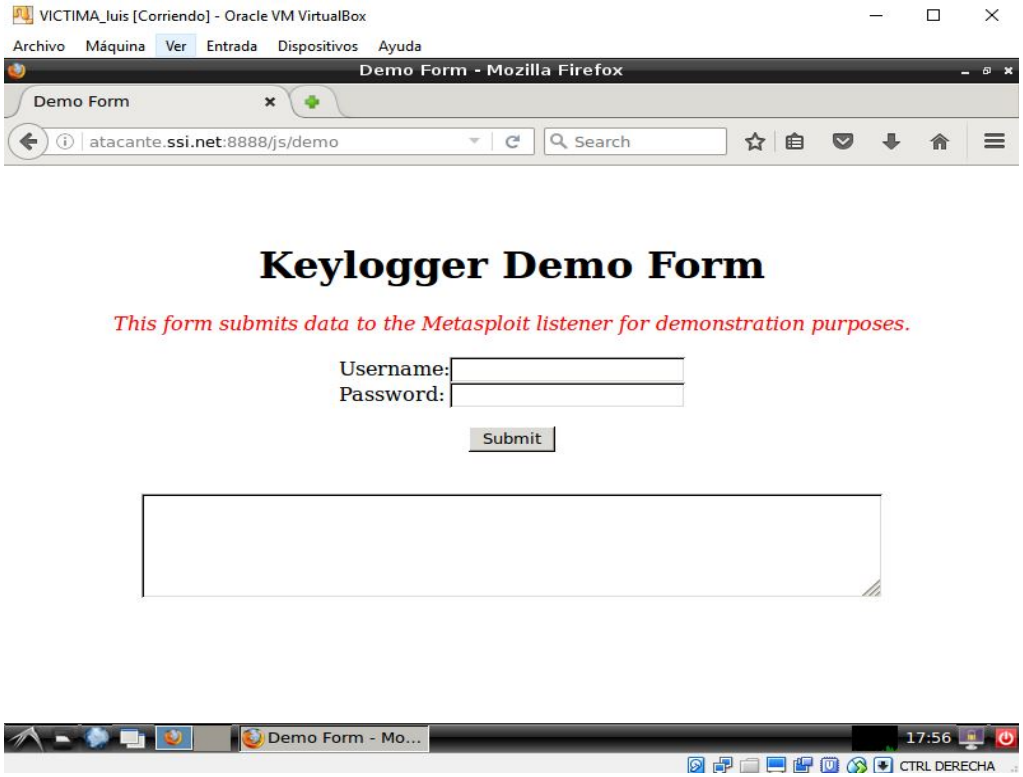
Lo primero es preparar la librería Javascript y el servidor de escucha en la máquina atacante. El módulo *keylogger* Javascript quedará disponible en cualquier URL de la forma http://atacante.ssi.net:8888/js/[...].js, de modo que cuando se cargue esa librería Javascript se inicie la captura de pulsaciones de teclado.



Ahora vamos a probarlo enviado el siguiente mensaje desde la máquina atacante:



Para comprobar el resultado accedemos desde la máquina víctima a la lista de mensajes:



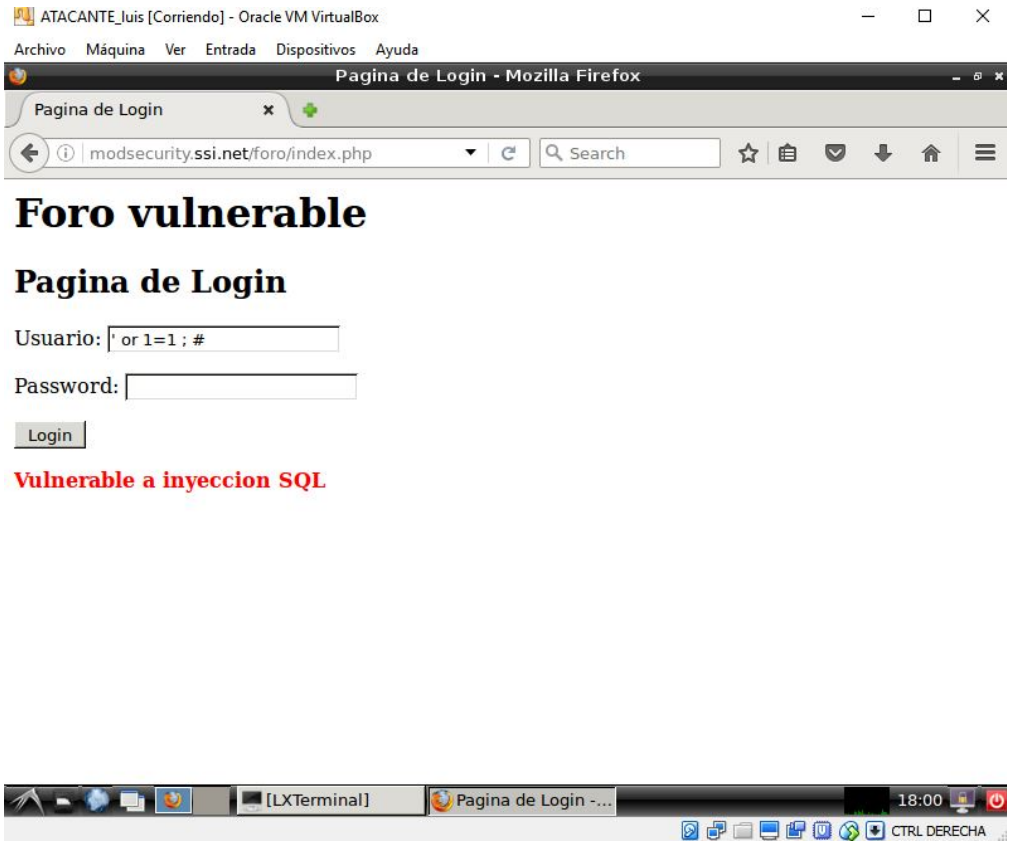
Observamos que nos redirige a una página de login falsa creada por Metasploit donde capturará las pulsaciones de teclado.

Aplicaciones vulnerables (Inyección SQL)

Inyección SQL Foro "simple" vulnerable

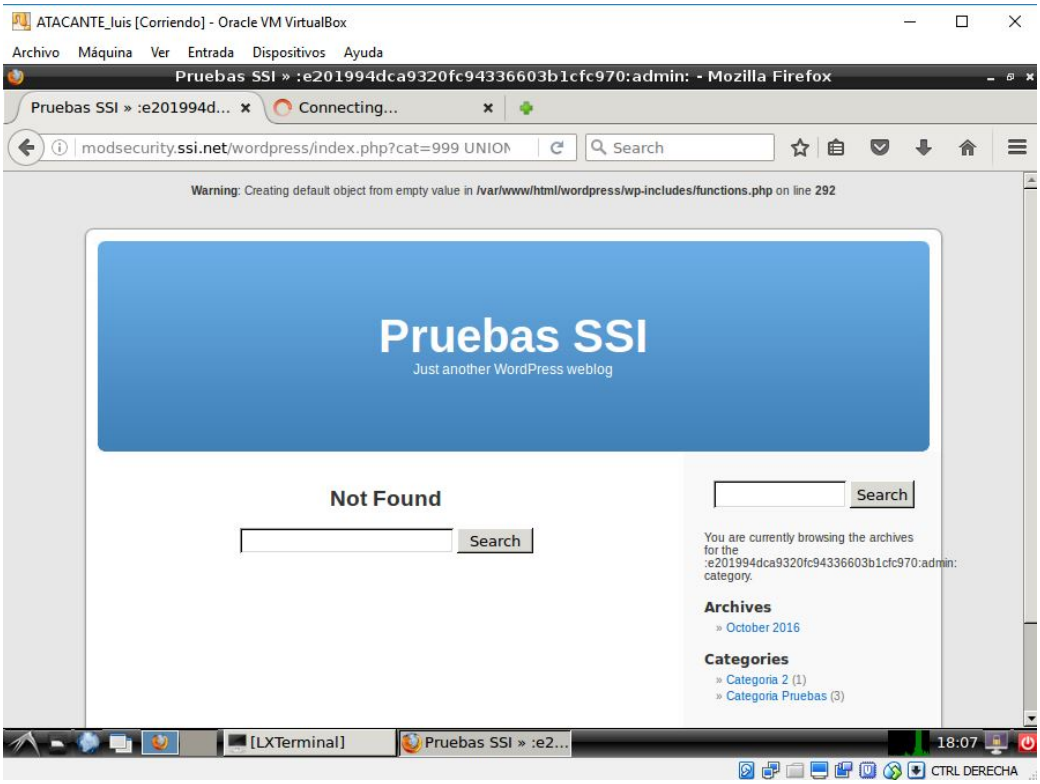
Volver a la página de inicial del foro: http://modsecurity.ssi.net/foro. Ahora veremos como acceder sin disponer de nombre de usuario ni clave en la página de login.

Accedemos con usuario: ' or 1=1 ; # y password: <vacío>



Inyección SQL en Wordpress 1.5.1.1

En la maquina atacante ponemos en la barra de direcciones: http://modsecurity.ssi.net/wordpress/index.php?cat=999%20UNION%20SELECT%20null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null%20FROM%20wp_users



Vemos que en la columna de la derecha pone admin:e201994dca9320fc94336603b1cfc970 que es el resumen md5 de la password para entrar(usuario: admin, pass: secreto). Podemos comprobar mismo poniéndolo en google que efectivamente se corresponde con el resumen md5 de la palabra secreto.

Ejercicio 2: Instalación y experimentación con mod-security

Seguimos los pasos de instalación y configuración: instalar los paquetes debian, descargar las reglas del *OWASP ModSecurity Core Rule Set Project, a*justar la configuración por defecto de mod-security e indicar el uso de las reglas , *c*onfigurar y habilitar las reglas OWASP.
A continuación repetimos las pruebas anteriores de inyección SQL y XSS y vemos el funcionamiento a través del error.log.

Mod-security en modo detención:

[Wed Nov 30 18:29:09.888576 2016] [:error] [pid 29654] [client 198.51.100.111:44841] PHP Warning: Creating default object from empty value in /var/www/html/wordpress/wp-includes/functions.php on line 292
[Wed Nov 30 18:29:09.908773 2016] [:error] [pid 29654] [client 198.51.100.111:44841] PHP Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html/wordpress/wp-includes/functions-formatting.php on line 76
[Wed Nov 30 18:29:09.909320 2016] [:error] [pid 29654] [client 198.51.100.111:44841] PHP Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html/wordpress/wp-includes/functions-formatting.php on line 76

[Wed Nov 30 18:29:09.909763 2016] [:error] [pid 29654] [client 198.51.100.111:44841] PHP Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html/wordpress/wp-includes/functions-formatting.php on line 76
[Wed Nov 30 18:29:09.910102 2016] [:error] [pid 29654] [client 198.51.100.111:44841] PHP Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html/wordpress/wp-includes/functions-formatting.php on line 76
[Wed Nov 30 18:29:42.037935 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 3 at TX:sqli_select_statement_count. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "108"] [id "981317"] [rev "2"] [msg "SQL SELECT Statement Anomaly Detection Alert"] [data "Matched Data: Connection found within TX:sqli_select_statement_count: 3"] [ver "OWASP_CRS/2.2.9"] [maturity "8"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038038 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:\\\\b(?:(?:s(?:t(?:d(?:dev(_pop|_samp)?)?|r(?:_to_date|cmp))|u(?:b(?:str(?:ing(_index)?)?|(?:dat|tim)e)|m)|e(?:c(?:_to_time|ond)|ssion_user)|ys(?:tem_user|date)|ha(1|2)?|oundex|chema|ig?n|pace|qrt)|i(?:s(null|_(free_lock|ipv4_compat|ipv4_mapped|ipv4| ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "125"] [id "950001"] [rev "2"] [msg "SQL Injection Attack"] [data "Matched Data: UNION SELECT found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038152 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:(?:s(?:t(?:d(?:dev(_pop|_samp)?)?|r(?:_to_date|cmp))|u(?:b(?:str(?:ing(_index)?)?|(?:dat|tim)e)|m)|e(?:c(?:_to_time|ond)|ssion_user)|ys(?:tem_user|date)|ha(1|2)?|oundex|chema|ig?n|pace|qrt)|i(?:s(null|_(free_lock|ipv4_compat|ipv4_mapped|ipv4|ipv ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "143"] [id "959073"] [rev "2"] [msg "SQL Injection Attack"] [data "Matched Data: UNION SELECT found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038196 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "([\\\\~\\\\!\\\\@\\\\#\\\\$\\\\%\\\\^\\\\&*\\\\(\\\\)\\\\-\\\\+\\\\=\\\\{\\\\}\\\\[\\\\]\\\\|\\\\:\\\\;\\"\\\\'\\\\\\xc2\\xb4\\\\\\xe2\\x80\\x99\\\\\\xe2\\x80\\x98\\\\\`\\\\<\\\\>].*?){5,}" at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "159"] [id "981173"] [rev "2"] [msg "Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded"] [data "Matched Data:) found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM

wp_users"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038306 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:\\\\sexec\\\\s+xp_cmdshell)|(?:[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]\\\\s*?!\\\\s*?[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\w])|(?:from\\\\W+information_schema\\\\W)|(?:(?:(?:current_)?user|database|schema|connection_id)\\\\s*?\\\\([^\\\\)]*?)|(?:[\\\"'`\\xc2\\xb4\\xe2 ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "207"] [id "981255"] [msg "Detects MSSQL code execution and information gathering attempts"] [data "Matched Data: UNION SELECT found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038356 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:;.*?[)\\\\da-f\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98][\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98](?:[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98].*?[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]|\\\\Z|[^\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]+))|(?:\\\\Wselect.+\\\\W*?from)|((? ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "209"] [id "981257"] [msg "Detects MySQL comment-/space-obfuscated injections and backtick termination"] [data "Matched Data: SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038477 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:union\\\\s*?(?:all|distinct|[(!@]*?)?\\\\s*?[([]*?\\\\s*?select\\\\s+)|(?:\\\\w+\\\\s+like\\\\s+[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98])|(?:like\\\\s*?[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]\\\\%)|(?:[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]\\\\s*?like\\\\W*?[\\\"'`\\xc2\\xb4 ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "223"] [id "981245"] [msg "Detects basic SQL authentication bypass attempts 2/3"] [data "Matched Data: UNION SELECT found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038522 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:(union(.*?)select(.*?)from)))" at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "225"] [id "981276"] [msg "Looking for basic sql injection. Common attack string for mysql, oracle and others."] [data "Matched Data: UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM found within ARGS:cat: 999 UNION SELECT

null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038580 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:\\\\)\\\\s*?when\\\\s*?\\\\d+\\\\s*?then)|(?:[\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]\\\\s*?(?:#|--|{))|(?:\\\\/*!\\\\s?\\\\d+)|(?:ch(?:a)?r\\\\s*?\\\\(\\\\s*?\\\\d)|(?:(?:(n?and|x?x?or|div|like|between|and|not)\\\\s+|\\\\|\\\\||\\\\&\\\\&)\\\\s*?\\\\w+\\\\())" at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "231"] [id "981240"] [msg "Detects MySQL comments, conditions and ch(a)r injections"] [data "Matched Data: CHAR(5 found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.038842 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:[\\\\d\\\\W]\\\\s+as\\\\s*?[\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\w]+\\\\s*?from)|(?:^[\\\\W\\\\d]+\\\\s*?(?:union|select|create|rename|truncate|load|alter|delete|update|insert|desc))|(?:(?:select|create|rename|truncate|load|alter|delete|update|insert|desc)\\\\s+ ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "243"] [id "981247"] [msg "Detects concatenated basic SQL injection and SQLLFI attempts"] [data "Matched Data: 999 UNION found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]
[Wed Nov 30 18:29:42.040435 2016] [:error] [pid 29655] [client 198.51.100.111:44846] PHP Warning: Creating default object from empty value in /var/www/html/wordpress/wp-includes/functions.php on line 292
[Wed Nov 30 18:29:42.047512 2016] [:error] [pid 29655] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_60_correlation.conf"] [line "37"] [id "981204"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 46, SQLi=21, XSS=0): 981247-Detects concatenated basic SQL injection and SQLLFI attempts"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8MhsYzZHAAAHPXt4oAAAAB"]

--02a94c66-H--
Message: Warning. Pattern match "\\W{4,}" at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_40_generic_attacks.conf"] [line "37"] [id "960024"] [rev "2"] [msg "Meta-Character Anomaly Detection Alert - Repetitive Non-Word Characters"] [data "Matched Data: ") </ found within ARGS:mensaje: <script> alert("esto admite XSS") </script>"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"]
Message: Warning. Pattern match "(?i:([\\s'\"`\xc2\xb4\xe2\x80\x99\xe2\x80\x98\\(\\)]*?)\\b([\\d\\w]++)([\\s'\"`\xc2\xb4\xe2\x80\x99\xe2\x80\x98\\(\\)]*?)(?:(?:=|<=>|r?like|sounds\\s+like|regexp)([\\s'\"`\xc2\xb4\xe2\x80\x99\xe2\x80\x98\\(\\)]*?)\\2\\b|(?:!=|<=|>=|<>|<|>|\\^|is\\s+not ..." at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "77"] [id "950901"] [rev "2"] [msg "SQL Injection Attack: SQL Tautology Detected."] [data "Matched Data: script> alert found within ARGS:mensaje: <script> alert("esto admite XSS") </script>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag

"OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"]
Message: Warning. Pattern match "([\\~\\!\\@\\#\\$\\%\\^\\&*\\(\\)\\-\\+\\=\\{\\}\\[\\]\\|\\:\\;\"\\'\\xc2\xb4\\xe2\x80\x99\\xe2\x80\x98\\`\\<\\>].*?){5,}" at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "159"] [id "981173"] [rev "2"] [msg "Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded"] [data "Matched Data: ' found within ARGS:mensaje: <script> alert("esto admite XSS") </script>"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"]
Message: Warning. Pattern match "(?i:(?:union\\s*?(?:all|distinct|[(!@]*?)?\\s*?[([]*?\\s*?select\\s+)|(?:\\w+\\s+like\\s+[\"'`\xc2\xb4\xe2\x80\x99\xe2\x80\x98])|(?:like\\s*?[\"'`\xc2\xb4\xe2\x80\x99\xe2\x80\x98]\\%)|(?:[\"'`\xc2\xb4\xe2\x80\x99\xe2\x80\x98]\\s*?like\\W*?[\"'`\xc2\xb4 ..." at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "223"] [id "981245"] [msg "Detects basic SQL authentication bypass attempts 2/3"] [data "Matched Data: "esto a found within ARGS:mensaje: <script> alert("esto admite XSS") </script>"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"]
Message: Warning. Pattern match "(?i)(<script[^>]*>[\\s\\S]*?<\\/script[^>]*>|<script[^>]*>[\\s\\S]*?<\\/script[[\\s\\S]]*[\\s\\S]|<script[^>]*>[\\s\\S]*?<\\/script[\\s]*[\\s]|<script[^>]*>[\\s\\S]*?<\\/script|<script[^>]*>[\\s\\S]*?)" at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_xss_attacks.conf"] [line "14"] [id "973336"] [rev "1"] [msg "XSS Filter - Category 1: Script Tag Vector"] [data "Matched Data: <script> alert("esto admite XSS") </script> found within ARGS:mensaje: <script> alert("esto admite XSS") </script>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "1"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/XSS"] [tag "WASCTC/WASC-8"] [tag "WASCTC/WASC-22"] [tag "OWASP_TOP_10/A2"] [tag "OWASP_AppSensor/IE1"] [tag "PCI/6.5.1"]
Message: Warning. Pattern match "\\balert\\b\\W*?\\(" at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_xss_attacks.conf"] [line "163"] [id "958052"] [rev "2"] [msg "Cross-site Scripting (XSS) Attack"] [data "Matched Data: alert(found within ARGS:mensaje: <script> alert("esto admite xss") </script>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "8"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/XSS"] [tag "WASCTC/WASC-8"] [tag "WASCTC/WASC-22"] [tag "OWASP_TOP_10/A2"] [tag "OWASP_AppSensor/IE1"] [tag "PCI/6.5.1"]
Message: Warning. Pattern match "\\< ?script\\b" at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_xss_attacks.conf"] [line "211"] [id "958051"] [rev "2"] [msg "Cross-site Scripting (XSS) Attack"] [data "Matched Data: <script found within ARGS:mensaje: <script> alert("esto admite xss") </script>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "8"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/XSS"] [tag "WASCTC/WASC-8"] [tag "WASCTC/WASC-22"] [tag "OWASP_TOP_10/A2"] [tag "OWASP_AppSensor/IE1"] [tag "PCI/6.5.1"]
Message: Warning. Pattern match "<(a|abbr|acronym|address|applet|area|audioscope|b|base|basefront|bdo|bgsound|big|blackface|blink|blockquote|body|bq|br|button|caption|center|cite|code|col|colgroup|comment|dd|del|dfn|dir|div|dl|dt|em|embed|fieldset|fn|font|form|frame|frameset|h1|head|h ..." at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_xss_attacks.conf"] [line "301"] [id "973300"] [rev "2"] [msg "Possible XSS Attack Detected - HTML Tag Handler"] [data "Matched Data: <script> found within ARGS:mensaje: <script> alert("esto admite xss") </script>"] [ver "OWASP_CRS/2.2.9"] [maturity "8"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/XSS"] [tag "WASCTC/WASC-8"] [tag "WASCTC/WASC-22"] [tag "OWASP_TOP_10/A2"] [tag "OWASP_AppSensor/IE1"] [tag "PCI/6.5.1"]

Message: Warning. Pattern match "(?:fromcharcode|alert|eval)\\s*(?:\\(|`)" at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_xss_attacks.conf"] [line "391"] [id "973307"] [rev "2"] [msg "XSS Attack Detected"] [data "Matched Data: alert(found within ARGS:mensaje: <script> alert("esto admite xss") </script>"] [ver "OWASP_CRS/2.2.9"] [maturity "8"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/XSS"] [tag "WASCTC/WASC-8"] [tag "WASCTC/WASC-22"] [tag "OWASP_TOP_10/A2"] [tag "OWASP_AppSensor/IE1"] [tag "PCI/6.5.1"]
Message: Warning. Pattern match "(?i:<script.*?>)" at ARGS:mensaje. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_xss_attacks.conf"] [line "472"] [id "973331"] [rev "2"] [msg "IE XSS Filters - Attack Detected."] [data "Matched Data: <script> found within ARGS:mensaje: <script> alert("esto admite XSS") </script>"] [ver "OWASP_CRS/2.2.9"] [maturity "8"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/XSS"] [tag "WASCTC/WASC-8"] [tag "WASCTC/WASC-22"] [tag "OWASP_TOP_10/A2"] [tag "OWASP_AppSensor/IE1"] [tag "PCI/6.5.1"]
Message: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_60_correlation.conf"] [line "37"] [id "981204"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 46, SQLi=7, XSS=30): IE XSS Filters - Attack Detected."]
Apache-Handler: application/x-httpd-php
Stopwatch: 1480526793325585 27850 (- - -)
Stopwatch2: 1480526793325585 27850; combined=3626, p1=223, p2=3298, p3=1, p4=47, p5=57, sr=12, sw=0, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.8.0 (http://www.modsecurity.org/); OWASP_CRS/2.2.9.
Server: Apache/2.4.10 (Debian)
Engine-Mode: "DETECTION_ONLY"

Mod-security en modo rechazo:

[Wed Nov 30 18:37:52.921632 2016] [:error] [pid 29666] [client 198.51.100.111:44849] PHP Warning: Creating default object from empty value in /var/www/html/wordpress/wp-includes/functions.php on line 292
[Wed Nov 30 18:37:52.930213 2016] [:error] [pid 29666] [client 198.51.100.111:44849] PHP Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html/wordpress/wp-includes/functions-formatting.php on line 76
[Wed Nov 30 18:37:52.930806 2016] [:error] [pid 29666] [client 198.51.100.111:44849] PHP Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html/wordpress/wp-includes/functions-formatting.php on line 76
[Wed Nov 30 18:37:52.931198 2016] [:error] [pid 29666] [client 198.51.100.111:44849] PHP Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html/wordpress/wp-includes/functions-formatting.php on line 76
[Wed Nov 30 18:37:52.931582 2016] [:error] [pid 29666] [client 198.51.100.111:44849] PHP Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html/wordpress/wp-includes/functions-formatting.php on line 76
[Wed Nov 30 18:38:00.288681 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 3 at TX:sqli_select_statement_count. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "108"] [id "981317"] [rev "2"] [msg "SQL SELECT Statement Anomaly Detection Alert"] [data "Matched Data: Connection found within TX:sqli_select_statement_count: 3"] [ver "OWASP_CRS/2.2.9"] [maturity "8"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag

"WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.288793 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:\\\\b(?:(?:s(?:t(?:d(?:dev(_pop|_samp)?)?|r(?:_to_date|cmp))|u(?:b(?:str(?:ing(_index)?)?|(?:dat|tim)e)|m)|e(?:c(?:_to_time|ond)|ssion_user)|ys(?:tem_user|date)|ha(1|2)?|oundex|chema|ig?n|pace|qrt)|i(?:s(null|_(free_lock|ipv4_compat|ipv4_mapped|ipv4| ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "125"] [id "950001"] [rev "2"] [msg "SQL Injection Attack"] [data "Matched Data: UNION SELECT found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.288915 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:(?:s(?:t(?:d(?:dev(_pop|_samp)?)?|r(?:_to_date|cmp))|u(?:b(?:str(?:ing(_index)?)?|(?:dat|tim)e)|m)|e(?:c(?:_to_time|ond)|ssion_user)|ys(?:tem_user|date)|ha(1|2)?|oundex|chema|ig?n|pace|qrt)|i(?:s(null|_(free_lock|ipv4_compat|ipv4_mapped|ipv4|ipv ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "143"] [id "959073"] [rev "2"] [msg "SQL Injection Attack"] [data "Matched Data: UNION SELECT found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.288966 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "([\\\\~\\\\!\\\\@\\\\#\\\\$\\\\%\\\\^\\\\&*\\\\(\\\\)\\\\-\\\\+\\\\=\\\\{\\\\}\\\\[\\\\]\\\\|\\\\:\\\\;\\\"\\\\'\\\\\\xc2\\xb4\\\\\xe2\\x80\\x99\\\\\xe2\\x80\\x98\\\\`\\\\<\\\\>].*?){5,}" at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "159"] [id "981173"] [rev "2"] [msg "Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded"] [data "Matched Data:) found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.289118 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:\\\\sexec\\\\s+xp_cmdshell)|(?:[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]\\\\s*?!\\\\s*?[\\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\w])|(?:from\\\\W+information_schema\\\\W)|(?:(?:(?:current_)?user|database|schema|connection_id)\\\\s*?\\\\([^\\\\)]*?)|(?:[\\\"'`\\xc2\\xb4\\xe2 ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "207"] [id "981255"] [msg "Detects MSSQL code execution and information gathering attempts"] [data "Matched Data: UNION SELECT found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM

wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.289186 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:;.*?[)\\\\da-f\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98][\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98](?:[\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98].*?[\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]|\\\\Z|[^\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]+))|(?:\\\\Wselect.+\\\\W*?from)|((? ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "209"] [id "981257"] [msg "Detects MySQL comment-/space-obfuscated injections and backtick termination"] [data "Matched Data: SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.289322 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:union\\\\s*?(?:all|distinct|[(!@]*?)?\\\\s*?[([]*?\\\\s*?select\\\\s+)|(?:\\\\w+\\\\s+like\\\\s+[\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98])|(?:like\\\\s*?[\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]\\\\%)|(?:[\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]\\\\s*?like\\\\W*?[\\"'`\\xc2\\xb4 ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "223"] [id "981245"] [msg "Detects basic SQL authentication bypass attempts 2/3"] [data "Matched Data: UNION SELECT found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.289368 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:(union(.*?)select(.*?)from)))" at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "225"] [id "981276"] [msg "Looking for basic sql injection. Common attack string for mysql, oracle and others."] [data "Matched Data: UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.289430 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:\\\\)\\\\s*?when\\\\s*?\\\\d+\\\\s*?then)|(?:[\\"'`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98]\\\\s*?(?:#|--|{))|(?:\\\\/*!\\\\s?\\\\d+)|(?:ch(?:a)?r\\\\s*?\\\\(\\\\s*?\\\\d)|(?:(?:(n?and|x?x?or|div|like|between|and|not)\\\\s+|\\\\|\\\\||\\\\&\\\\&)\\\\s*?\\\\w+\\\\()" at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "231"] [id "981240"] [msg "Detects MySQL comments, conditions and ch(a)r injections"] [data "Matched Data: CHAR(5 found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM

wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.289628 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Pattern match "(?i:(?:[\\\\d\\\\W]\\\\s+as\\\\s*?[\\'"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\w]+\\\\s*?from)|(?:^[\\\\W\\\\d]+\\\\s*?(?:union|select|create|rename|truncate|load|alter|delete|update|insert|desc))|(?:(?:select|create|rename|truncate|load|alter|delete|update|insert|desc)\\\\s+ ..." at ARGS:cat. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "243"] [id "981247"] [msg "Detects concatenated basic SQL injection and SQLLFI attempts"] [data "Matched Data: 999 UNION found within ARGS:cat: 999 UNION SELECT null,CONCAT(CHAR(58),user_pass,CHAR(58),user_login,CHAR(58)),null,null,null FROM wp_users"] [severity "CRITICAL"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]
[Wed Nov 30 18:38:00.291300 2016] [:error] [pid 29657] [client 198.51.100.111:44850] PHP Warning: Creating default object from empty value in /var/www/html/wordpress/wp-includes/functions.php on line 292
[Wed Nov 30 18:38:00.296776 2016] [:error] [pid 29657] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/etc/modsecurity/owasp-modsecurity-crs/activated_rules/modsecurity_crs_60_correlation.conf"] [line "37"] [id "981204"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 46, SQLi=21, XSS=0): 981247-Detects concatenated basic SQL injection and SQLLFI attempts"] [hostname "modsecurity.ssi.net"] [uri "/wordpress/index.php"] [unique_id "WD8OeMYzZHAAAHPZcakAAAAD"]