

Advanced Web Application Defense with ModSecurity

! " # \$%
& " ' (&)
* # % + % + ! " , " \$
! ! ')
* % - + ! " . & # !
+ ! " \$/ . %)
++ ' \$* ' + .

+ !" / & 0 ! #)
" # + !" * &
+ / * \$ %1 \$ * ++. %)
* # % + % + !" , " \$
! ! %1)
++' \$ +2\$* ' +. 3' +2 .

2 % # '

+ !" # 1 !

"! !"

+ ! " ! " 1

!

+ " 4 & # " #

% ")

2! " +!

1 2 ! !"

. % -" 1 #! %

"!")

/ - !4 ! & &

+56 7!

8++

%% 7!

"## * - #

+ % "

/ !))

2! " +!

. 9" #-" 1 & &
:;< # =; ; % & 1
2 ! \$' 11\$8%(!\$!)
! # # # ##!
4 - \$1" 2 ! - \$ "
* \$-))
. !" 4 !" !
7 !" # ! %)

' 1 %

. 1 - % ! !

6 !4 # 1 !")

" 9" % \$!" # %

4 > "! 1" "

!"

- # \$ #

" ++6\$ #

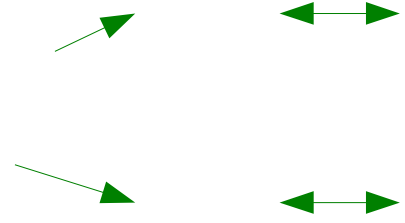
' 1 %

? 4 # > & -

1 - 1 1

1

@@=



+ ! "

" ! 3' - # 1 2 !

* 2 ! ")

* + " ! , ' 6

- % 1 - A !

The purpose of ModSecurity is to increase web application security by protecting them from known and unknown attacks

! "

2 ! " ! >% # &! ! \$!

! 4 B ! \$' \$!)

? -" 1 ! - \$ % ! " !

)

" !)

/ # !")

. ! 1 - !)

1 ! 1 &

-)

"

Request filtering: ! % & 9"

! % \$ 1 # & 1 1 -
% ")

Output Filtering: ! " -)

/ \$! \$/) ' C' /

Understanding of the HTTP protocol ! &

" C. . ' \$ # % - ! #! #

& " # &)

''

Anti-evasion techniques

%

%

1 #

4

!

#&

- ! 9")

A % - %" # ! !

. 1 !4 # ! ! 9"

A % - ! # # !

! % - " (1 < ; ;

! DA6 ! ! !

”

POST payload analysis

! % " & ' * +. %)

HTTPS and Compression

! & %1
1 - \$ & !! 9" #
! ! % 4 !)

" E

Audit logging #

- 9" ! " &' * +.

! 1 && #)

& ## ! - # ! - & 1 !4\$

+ " ! '

. % %

C. ! %

DA 9"

" C

+ ! 1" (! ! 4

DA6 ! &-

D ! ! &-

& - #! F, (G00H ! 7!

(+ !

(A 9" % & A\$

&" & " " ! / & ! %

1 & F=G(I G H)

A"

"

A" # % " & &"

2 " %1 #! " % " "

2 & " "

2

C - " & - 1

/ - % - 1

' * + .

+ - - 1

+! " "

- " ! 4

2!

!

A 7! 9"

" !

F@,=\$0; ; \$))H

A 7! 9"

!

/ !"

1

" % !

6 & 9"

2!

+ " ! & 9" "&

A" ! &

+4 " % !

' " # "%1 #% !

D

! # 1 &" " & 1 -
+ " # 4
/ !" ! - 7! # %2E
(- "

*

&

#

1

-

!

!

&

+

-

-

\$

!

&

-

-

%

&

\$ 4

\$# 1

\$!)

/

"

!

#

!

)

C

4

I) ' 9")

G)' # % ! ! (- !)

=)' # % ! 1" (! !4)

@y !" " "

9" \$!

!")

2# 9"

I) / !" " " ")

G) 6 & 9")

+ ! " %

2 ! " " 4 % # & "

" ! %)

. ! " %

' -

? & -

+ ! " % ' -

4 & #)

6 4 4 # % J 2 (2 K

,

% !

6 # -

! % \$ % ! % " # !
! \$! " # %) # !

/ %

' & &) \$ # 6 & ! " !! ! ! F (2(B; (LH
! " 1 | G! &)

+ ! "

? & -

& "

4 - & 1 # " !

,

6 % % % \$! & ## !
!)

-
! & %

/ % 8++

. # & ! " 4 # 8++\$! %
% # % - & !)

+ ! "

? & -

M 17! N)))MB 17! N

M %1 N)))MB %1 N

M N)))MB N

M! N)))MB! N

M! !OP)))FNMB! N

M# % !OP)))FN

M%& !OP7 - !)))FN

M1 " * - OP)))FN

Q)))FS

#&"

' ! #&"

! E " C ! ! "

! #&" # + -) + % # !

E " C)

. " &)))

1 " % 1 - \$ > " 2 !)))

A -

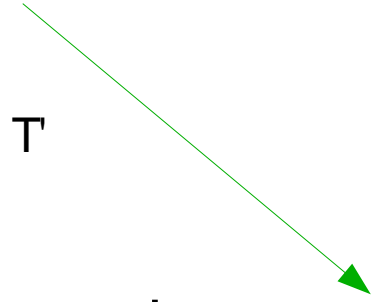
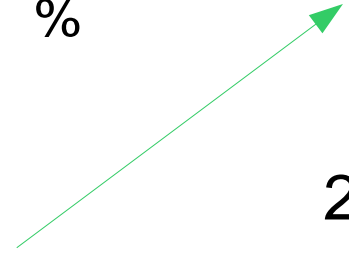
'

+

)%)!	%	
)%	!)!	%
)%)!	%	

1

2 !



T !"

T

% T !"

% T

O "

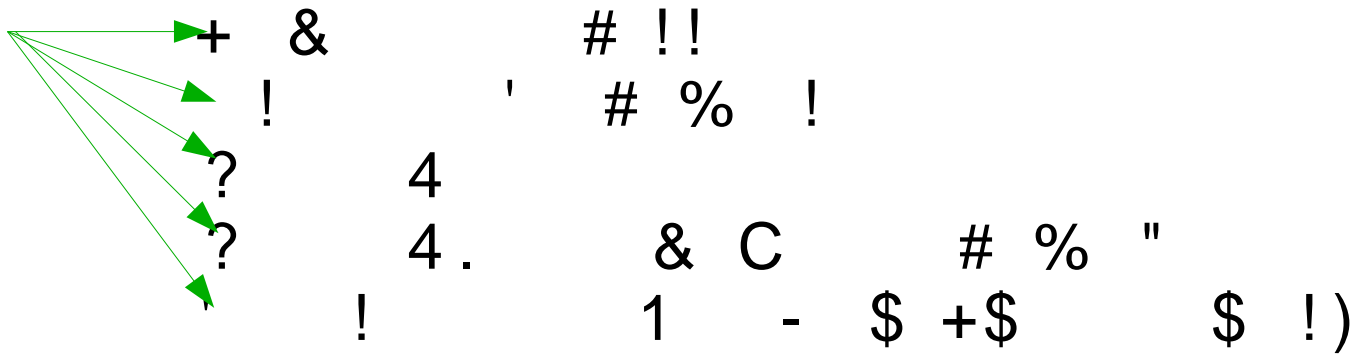
! #

!

A -

'

Advantages:



Disadvantages:



/ & "

+ %%

4 ! (& &

6 4! (& &

C # & &

1 1 & !

+ % # # " ! %% ! # \$

" & 1 & # * + " ! 7! 4

!" ! " %)

+ % %

D & 6 1 % G " 1" C. 6 #
 ! ")

C - & \$! " 4 4 & # ! %%

MQ((N

!" % #)

+ 7 & ! -

SecStripCommentCode On/Off

+

% %

!"

!

! %%

!

1 #

&

9"

&

")

!

! %%

"

#! %%

!

!

1 !4

! % 1

1

).

! %%

)

4 &

#! %%

!

##

!

&" &

7 -

!

\$! \$!

)

4 + & &

2 # " ! (& & #! 4 \$ -
% & ! 4 &\$ #
! -

SecSignCookies On/Off

SecEncryptionPassword "password"

" & 1 ! (&
2 - ! / ! + 2/ + & %)
+ 4 &

6 4 + & &

2 # !" - &
4 1 1 # % J K \$ " 1
J # K # !)

2& " 1\$ & 4 2/ + & %)

. ! - !

SecSignLinks On/Off

SecEntryPoint "/index.asp" "/images" ... "entry page n"

SecEncryptionPassword "password"

6 4 + & &

Signing the links we can tackle this threats:

' ! 1 A " ! 6 !
! # & !4 P# ! P DA6 1
!! & ! ## & 4)

2" % ! 4 ? 4 \$ 1\$ \$ 1

)

/ % # 4! (&

3) !" &)! %3) & O " (

&) **Secsign=MIHVBgkqhkiG9w0BBwOggccwgc**

QCAQAxcaNvAgEAOBsGCSqGSib3DQEFDDAObAhyxt

2Mf3s4KQICAfQwIwYlKoZ...6DQDpC

% C ! (& &

2 !" % " ! (& & ## %
& & # % # \$ -
- " # % 1 & % # 9" \$ % \$!)
" # # %)

6 &

1 1

6 &

!

&

4

+ 2! +

+ % # & -

. !; !4 !4

. !4

6 ! 0 2 !4

* ! ! !

2 !4

+ !

!

6 &

6 &

*

'

C

Web App Security Consortium (WASC)

. 7! " # 1 !4 > % "

& % (* ' -) #1 &

& # !4 \$ 1 " ! " #

!4 & " & !)

& %" \$! ! #&" -

\$ % 4 1 (4 #

% ! " ##! - %)

*

'

C

.

%

!

"!

(%

C. . '

##!

!

&

9"

!

#!

"

1

1 + !"

.

#!

&& &

!

!

)

/ %

+5 6 7!

8++ +! &

& ! !4

"## * - #

' -

* " " # &\$)

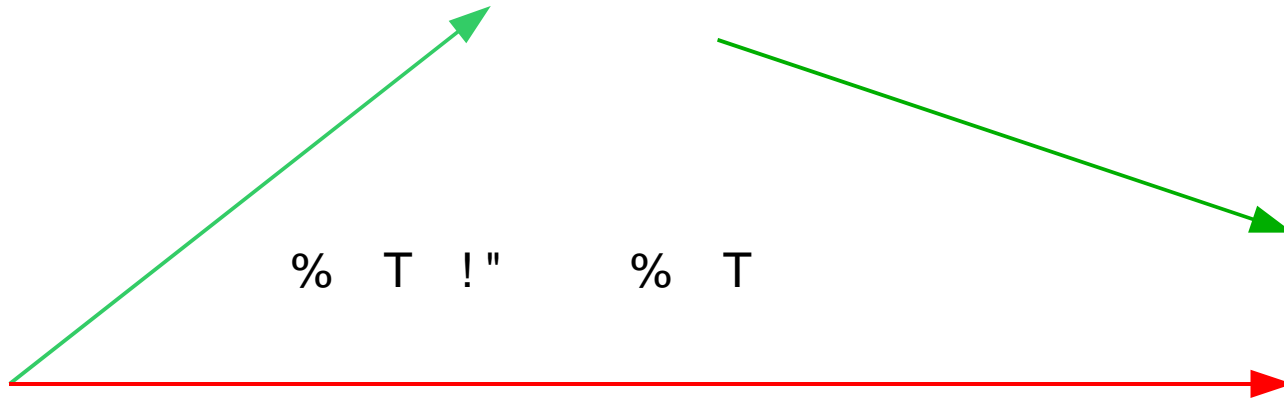
A " ! ! !

+ ! %% !

&3 " % % !

/ % +!

) ! ")! %



)- " 1)! %

+56 7!

Vulnerable parameter: 6 &

Test String:

> | a \$(

Modsecurity rule:

+ !# > ((! 3) !")! %3 | G=) %

Positive way:

+ !# + ! - 2A, T & UF (2(BHW

8++ ' -

Vulnerable parameter: &

Test String:

M! N > % " ! 4 >SB! N

Hex Encoded:

< = < X=< =<X G< L< X; <X @< =/ < I< < 0< XG< X@< G
< GX< @< 0< X: < X@< G; < X@< L< < 0< G; < @< G; < XX
< L< < < G; < 0< I< X@< G; < XL< < X0< XG< G; < =
< < < < L< 0< X=< G; < GX< GL< = <= <G < X=< =
< XG< L< X; < X@< =/

Modsecurity rule:

+ !# JM)Z NK ! 3) !")! %3) %

,

!

-

Vulnerable parameter: &

Test String:

. | Q

| Q Q Q

Modsecurity rule:

+ !# + ! - 2A, T & \WF (2(BHW

6 4 - - U

/ ' !

File extension to protect: [)

Requested file % 3)

Modsecurity rule

+ !# + ! - + A ' . T 6 / ? 2 /) Z W

' - + A ' . T 6 / ? 2 / U Z W

" 6 4 + & & > 1 " ")

*" / ' !

Vulnerable parameter

Test String

> & 9" | ! & 1 ! " # "

1 #)

Modsecurity rule

+ !# + ! - * D. ' D. J ! # * 6/ ' - K

J ! 33) ! ")! %3 # ") K

+ % %

Vulnerable page:)

Commented code:

MQ(% %1 % 3 % 3((N

Modsecurity option:

+ !+ %% *

& +

% +!

\$

)% 1 &! %



1

2 ! 3

C

!"

4 &

% -

! &)

&3 " % + % ' !

Vulnerable parameter: comments

Spam message:

J - & K

J -6 & K

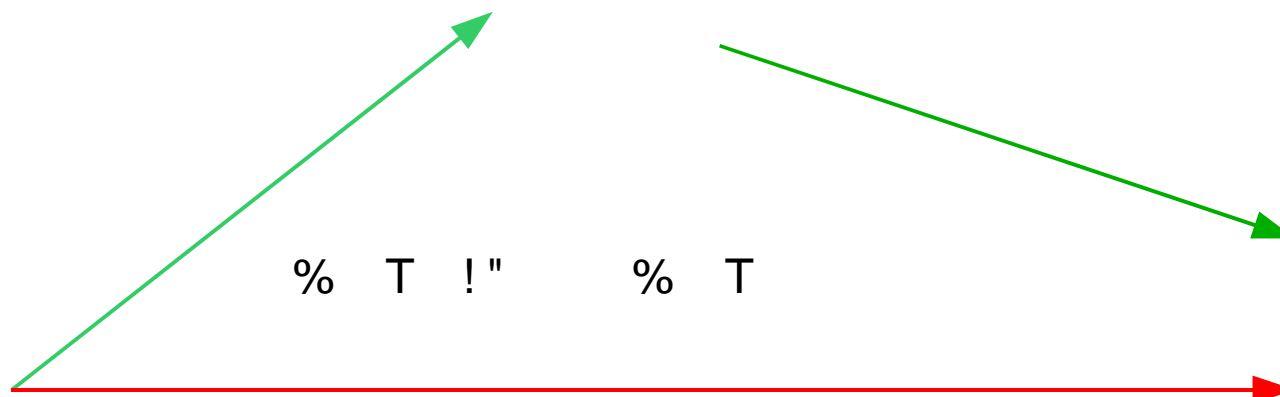
J -l & K

Modsecurity Rule:

+ !# 2A, + J F 6l H& K
! 3)% 1 &! %3 %) #

6 4 + & & 2! -

) !" &)! %



% T !" % T

)- " 1)! %

A " ! 6 ! ' !

Attack tool: ? 4

Attack options:

4 ()- " 1)! %
4 () ! " &)! %

Modsecurity options:

+ !+ & 6 4 *
+ !/ ! ' J " T' [(WK

A

"

!

6

!

"

&

?

4

A

"

!

6

!

"

&

?

4

8++ ! (& 4 1

Vulnerable parameter: &

Test String:

M! N >? % " ! 4 >S/B! N

Modsecurity rule:

+ !# JM)Z NK

Same for all other type of injection and variable manipulation, that involves a link, or direct access to URL.

/

+ & 6 4 *

Vulnerable file extension: [)

Requested file 3 % 3)

Modsecurity rule

+ !# + ! - + A ' .T 6/ ?2 /) Ț W

' - + A ' .T 6/ ?2 / U Ț W

We don't need to worry about this rules anymore!

!"

!" & ! ! # ! & " 1
!

/ ! #&"

E ## ! -

A % %1 !" " "
! ! % \$ - !" " !
- !)

. %"! 4 % - # " \$
-)

5"

\$

" 1

A # !

Download Modsecurity:

)% !") &

Mailing List:

% (!" (" \) " ! # &)

Cryptlib:

3)!) "!4) !) 3 &" ; ; | 3 13

Libxml2:

3 % #) &3

. 4 " U

2 - ! 1 ! # !"

\ ! ")! %

!% \ ! ")! %

" & %%