Proteger site com modsecurity

### What is ModSecurity?

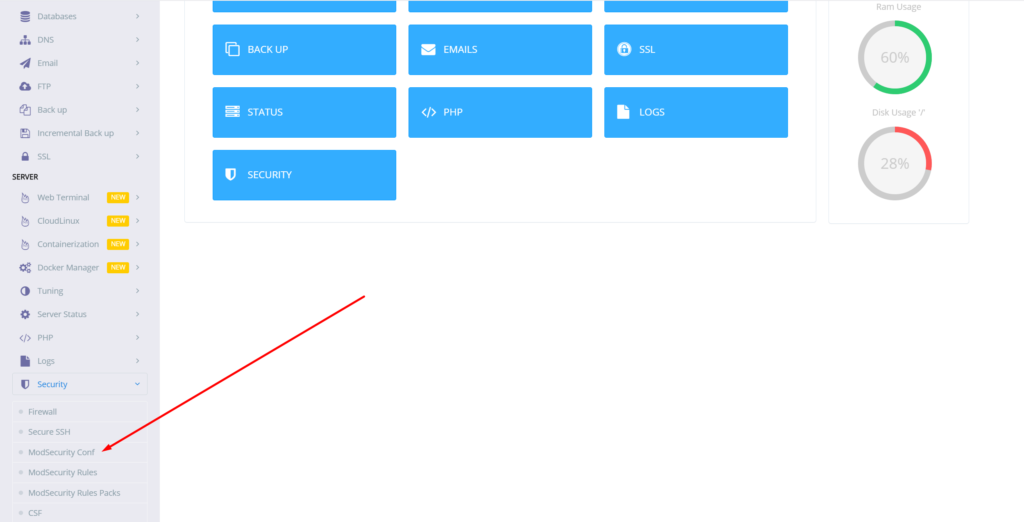
ModSecurity is an open-source web application firewall (or WAF). There are different sorts of firewalls available in today’s market but ModSecurity is [signature based firewall](https://www.informit.com/articles/article.aspx?p=31945&seqNum=5). LiteSpeed Web Server has its own high-performance ModSecurity engine, offering excellent compatibility and performance. LiteSpeed/OpenLiteSpeed works well with popular ModSecurity rules sets such as OWASP, Atomicorp, Comodo, and CloudLinux Imunify360.

Even though its a signature based firewall but in most of the cases it can prevent your site from getting compromised. Because usually hackers have automatic bots scanning for vulnerable sites with multiple attack payloads and these payloads are blocked by ModSecurity signature based rules.

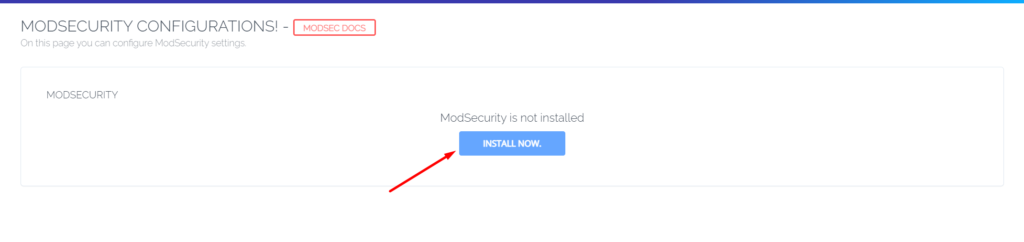
Apart from that CloudLinux Imunify360 rules are constantly updated with new signatures to cover newly introduced threats. (CyberPanel also support Imunify360 ModSecurity rules, but for that you need to i[nstall Imunify360](https://cyberpanel.net/docs/how-to-install-and-use-imunify360-on-cyberpanel/))

### Setup ModSecurity using CyberPanel

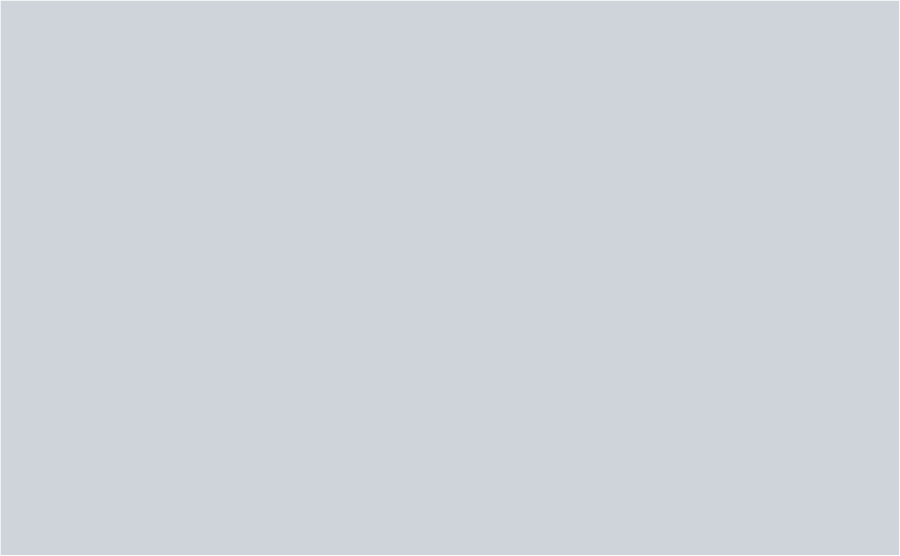
First of all login to the CyberPanel, on the main dashboard click on Security, and then click on ModSecurity Conf.



Then you will land on ModSecurity configuration page and if you already have ModSecurity installed, you will be allowed to configure ModSecurity other wise you will be opted to install first.



Once you click Install Now, CyberPanel will take few seconds to install ModSecurity for you and then redirect you to configurations page, which will look something like the image below. You can read and learn more about this page in our [ModSecurity Configurations](https://cyberpanel.net/docs/2-mod-security-configurations/) guide.



### ModSecurity Rules Packages

As mentioned above, ModSecurity is signature based firewall, so you need to provide ModSecurity with set of rules against which it can scan your web requests and protect your web application and if you don’t provide rules to ModSecurity it will not be able to protect your sites.

And CyberPanel provides you with two rules set out of the box, you can enable them with one-click.

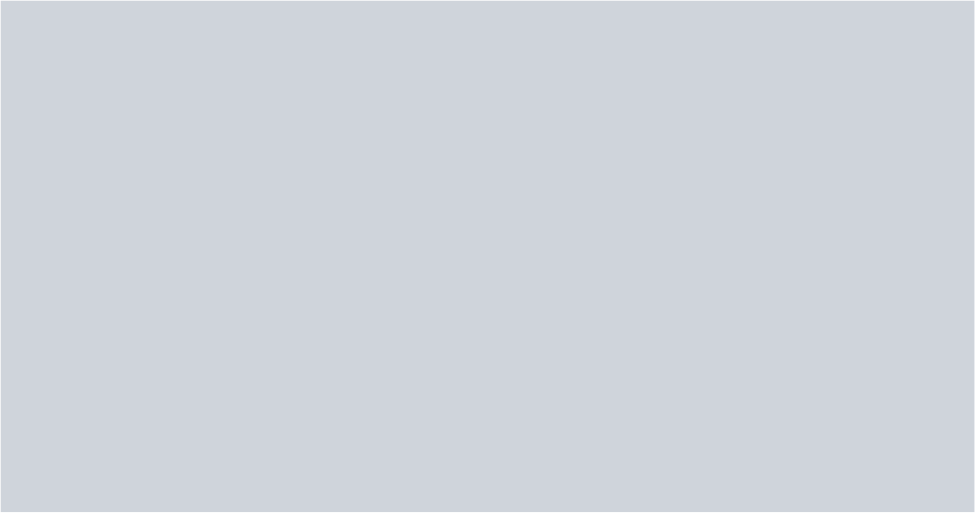
1. OWASP ModSecurity Core Rules
2. COMODO ModSecurity 3.0 Rules

In this tutorial, we will enable COMODO ModSecurity rules set, you can similarly enable OWASP ModSecurity Rules too.

Before moving forward visit your site with an attack payload such as

http://example.com/?a=b AND 1=1

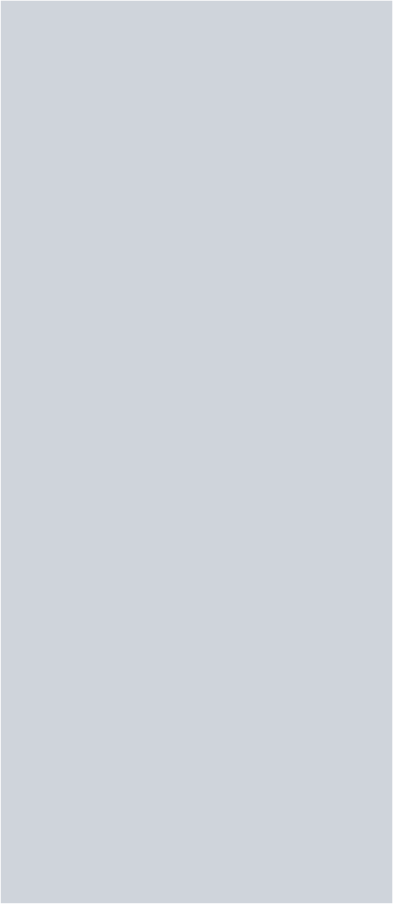
And you should be able to see your site just fine.



However, once we enable Comodo Rules Package, you should see a 403 error.

### Enable COMODO ModSecurity Rules Package

Go to the sidebar of CyberPanel=>Security=>ModSecurity Rules Packages

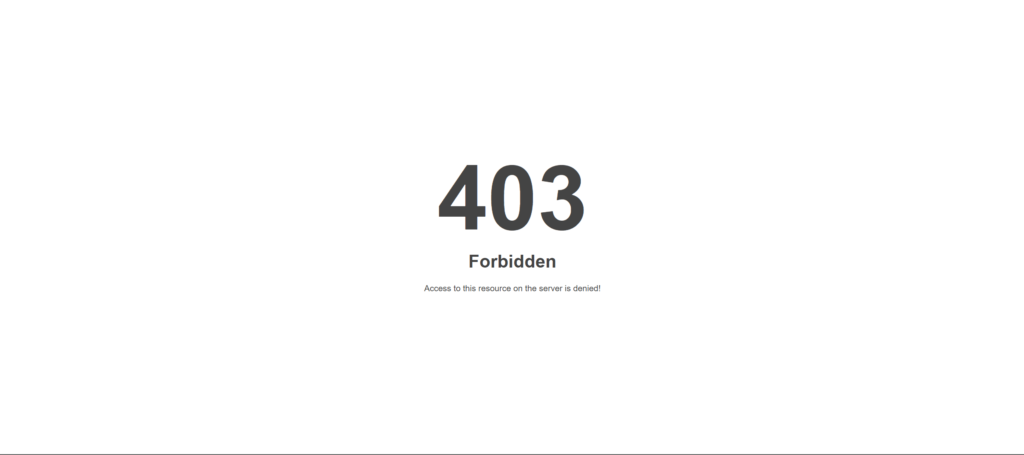


On the next screen, you can see OWASP ModSecurity and COMODO ModSecurity click on the second one to enable COMODO ModSecurity rules package.



Click the switch and it will turn on COMODO Rules, to verify if COMODO rules are installed successfully, open:

http://example.com/?a=b AND 1=1

You should get 403 Forbidden error

You can also see your ModSecurity Audit logs from CyberPanel=>logs=>ModSecurity Audit logs

HTTP/1.1 403

Content-Type: text/html

Cache-Control: private, no-cache, max-age=0

Pragma: no-cache

---PHfMHO9k---H--

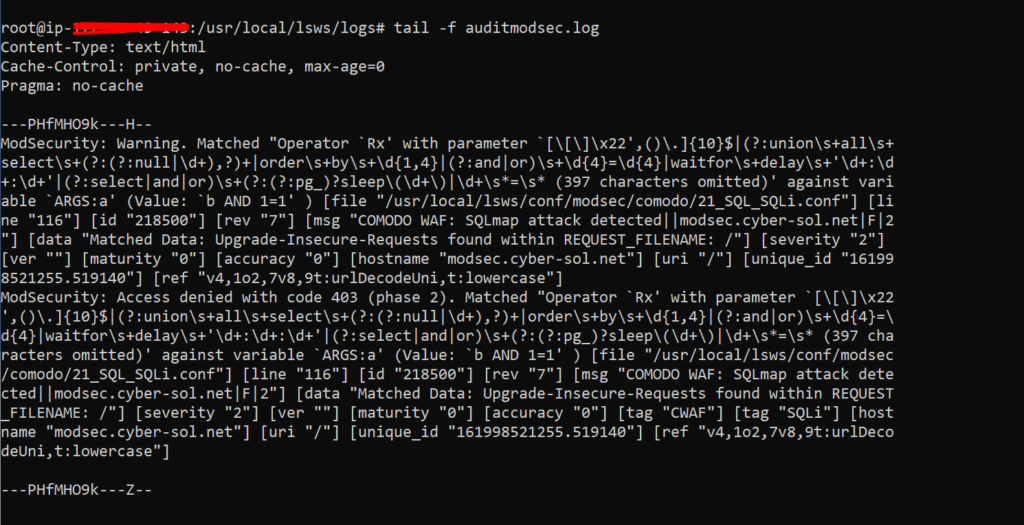
ModSecurity: Warning. Matched "Operator `Rx' with parameter `[\[\]\x22',()\.]{10}$|(?:union\s+all\s+select\s+(?:(?:null|\d+),?)+|order\s+by\s+\d{1,4}|(?:and|or)\s+\d{4}=\d{4}|waitfor\s+delay\s+'\d+:\d+:\d+'|(?:select|and|or)\s+(?:(?:pg\_)?sleep\(\d+\)|\d+\s\*=\s\* (397 characters omitted)' against variable `ARGS:a' (Value: `b AND 1=1' ) [file "/usr/local/lsws/conf/modsec/comodo/21\_SQL\_SQLi.conf"] [line "116"] [id "218500"] [rev "7"] [msg "COMODO WAF: SQLmap attack detected||modsec.cyber-sol.net|F|2"] [data "Matched Data: Upgrade-Insecure-Requests found within REQUEST\_FILENAME: /"] [severity "2"] [ver ""] [maturity "0"] [accuracy "0"] [hostname "modsec.cyber-sol.net"] [uri "/"] [unique\_id "161998521255.519140"] [ref "v4,1o2,7v8,9t:urlDecodeUni,t:lowercase"]

ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Rx' with parameter `[\[\]\x22',()\.]{10}$|(?:union\s+all\s+select\s+(?:(?:null|\d+),?)+|order\s+by\s+\d{1,4}|(?:and|or)\s+\d{4}=\d{4}|waitfor\s+delay\s+'\d+:\d+:\d+'|(?:select|and|or)\s+(?:(?:pg\_)?sleep\(\d+\)|\d+\s\*=\s\* (397 characters omitted)' against variable `ARGS:a' (Value: `b AND 1=1' ) [file "/usr/local/lsws/conf/modsec/comodo/21\_SQL\_SQLi.conf"] [line "116"] [id "218500"] [rev "7"] [msg "COMODO WAF: SQLmap attack detected||modsec.cyber-sol.net|F|2"] [data "Matched Data: Upgrade-Insecure-Requests found within REQUEST\_FILENAME: /"] [severity "2"] [ver ""] [maturity "0"] [accuracy "0"] [tag "CWAF"] [tag "SQLi"] [hostname "modsec.cyber-sol.net"] [uri "/"] [unique\_id "161998521255.519140"] [ref "v4,1o2,7v8,9t:urlDecodeUni,t:lowercase"]

---PHfMHO9k---Z--

You can also see your ModSecurity Audit logs from ssh terminal through this command:

tail -f usr/local/lsws/logs/auditmodsec.log

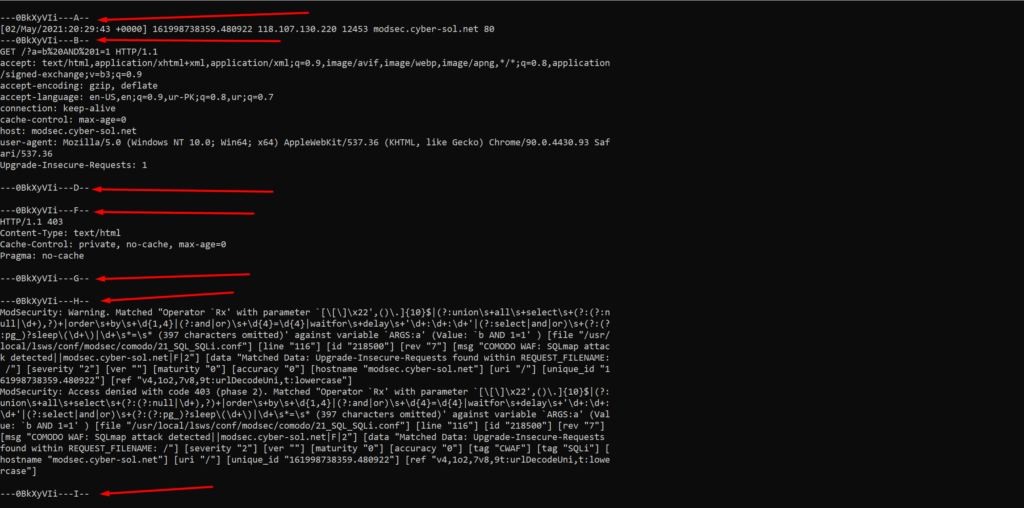


If you want to see the detail log you can change the

* A. Audit Logs Headers
* B. Best Headers
* C. Request Body
* D. Reserved and not used yet.
* E. Intermediary response body.
* F. Final response headers
* G. Reserved, and not used yet.
* H. Audit log trailer.
* I. Special Replacement for part C



After saving these changes you can refresh your website with SQL injection payload and run the previous command again on your terminal and you will be able to see more detailed logs on your screen.



Similarly ModSecurity will protect your site against other online attacks payloads using the signatures defined in Comodo Rules package, you can monitor the log files from time to time and see what is going on with your server.

https://cyberpanel.net/blog/2021/05/03/protect-your-websites-from-online-attacks-using-modsecurity-on-cyberpanel/