cloudbric

WordPress Security Plugins vs. WAF Services

A Comparative Test of WAF Accuracy Rates in Security Solutions

Contents

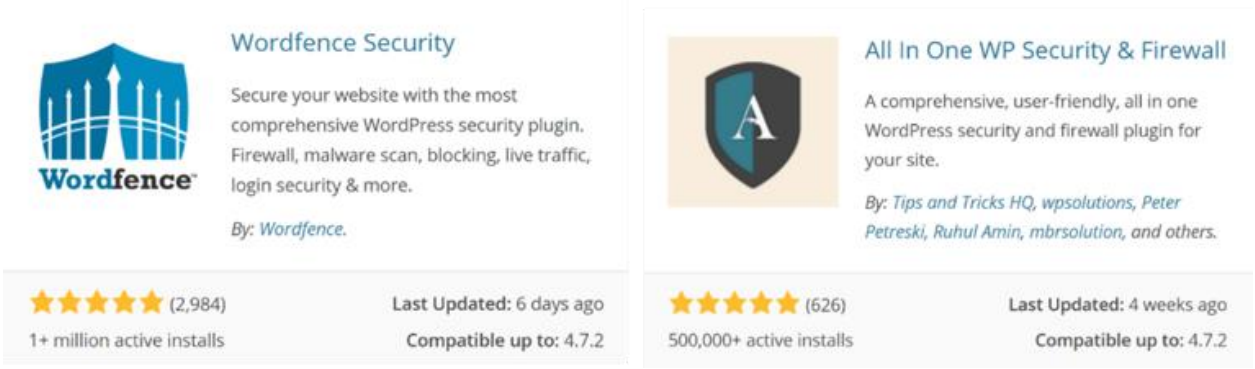
Abstract

This report contains the results of a comparative penetration test, the practice of testing a system in the same way a hacker would to identify security weaknesses, conducted by the research team at Cloudbric against two WordPress security plugins, Wordfence Security("Wordfence") and All In One WP security & Firewall ("All In One"), and Cloudbric's website protection service. Unlike other web application security tests that generate only attack traffic for testing, this test generated not only attack traffic but also legitimate traffic in order to test the ability of the WAF to detect web attacks and distinguish malicious traffic from legitimate traffic. Through testing, the research team concluded that Cloudbric has the highest true positive rate and the lowest false positive rate when tested against these security plugins. The results show that Cloudbric has superior detection capabilities in terms of both depth and accuracy. This is because Cloudbric uses a "logic-based detection engine" to understand the structure and meaning of the attack by analyzing traffic. This report also provides a pattern analysis for purpose to figure out why these patterns causes WAFs to generate false negatives or false positives.

Introduction

There is no doubt that WordPress is the CMS (Content Management System) of choice for most people. Because of its open source nature and ease of use, it has become a popular target for hackers. Therefore, many WordPress site operators have begun installing security plugins that offers WAF (Web Application Firewall) features as an attempt to secure their website. However, the question that remains is - can one protect a website from dangerous web attacks with a simple WAF provided by the plugin?

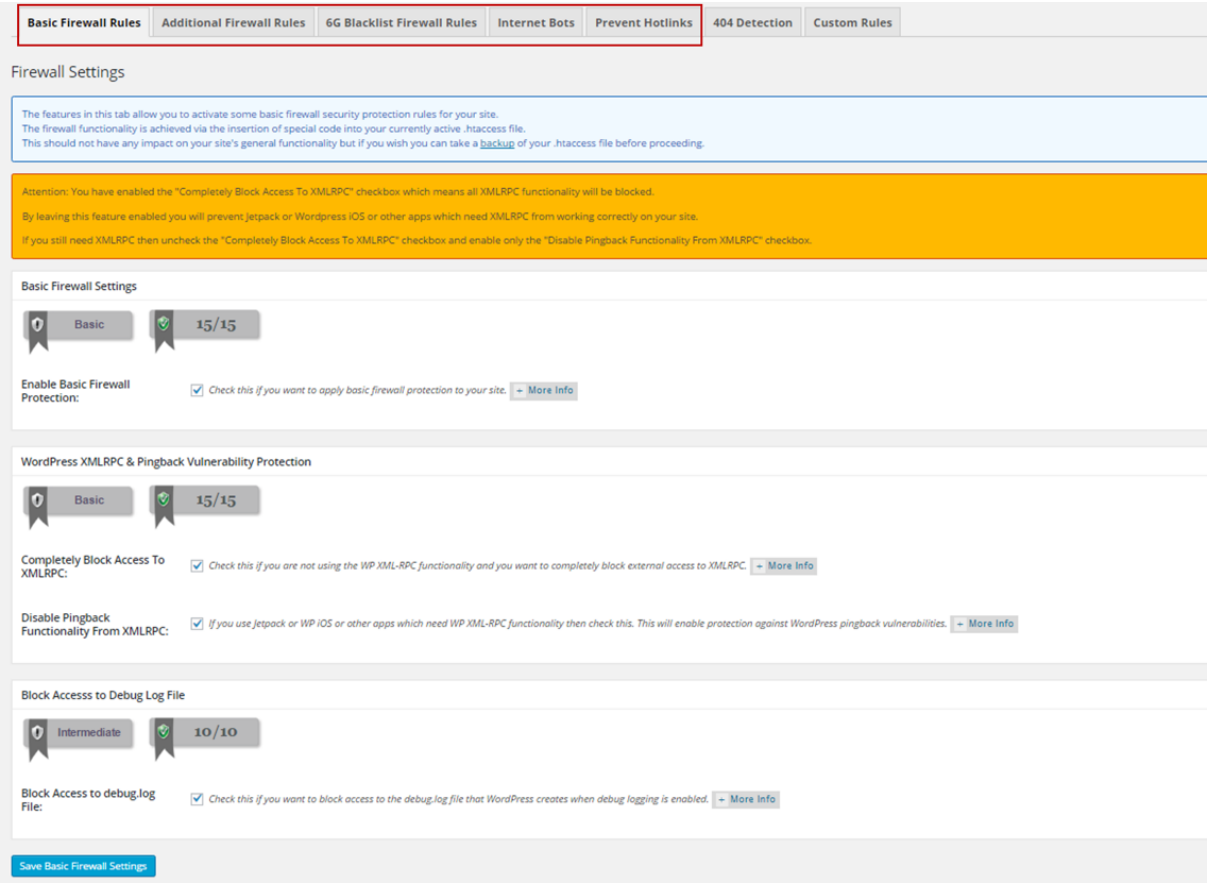
In order to investigate the quality of WAF security provided by security plugins, the research team at Cloudbric conducted a comparative penetration test, the practice of testing a system in the same way a hacker would to identify security weaknesses. This report will show the results of a test comparing the WAF detection capabilities of popular security plugins Wordfence Security ("Wordfence") and All In One WP Security & Firewall ("All In One"), against Cloudbric's website protection service.



Wordfence & All In One

Wordfence is one of the most downloaded WordPress security plugins with one million downloads and a rating of 4.9/5. It provides security features including WAF, malware scanner, and login security. Though a free plugin, Wordfence also offers a premium version covering country blocking, remote scans and more. For this particular test, Wordfence plugin free version 6.2.5 was used.

All In One is another popular WordPress security plugin with over 500,000 downloads. It differs from Wordfence in offering greater customizability of security deployed. By enabling more security features than the default, users can increase site security levels. While All In One's default security setting for firewall was 'OFF', all options in 'Basic Firewall Rules', 'Additional Firewall Rules', '6G Blacklist Firewall Rules', 'Internet Bots' and 'Prevent Hotlinks' tab of 'Firewall Settings' were set to 'ON' for the test (refer to figure below). All In One plugin version 4.1.9 was used.



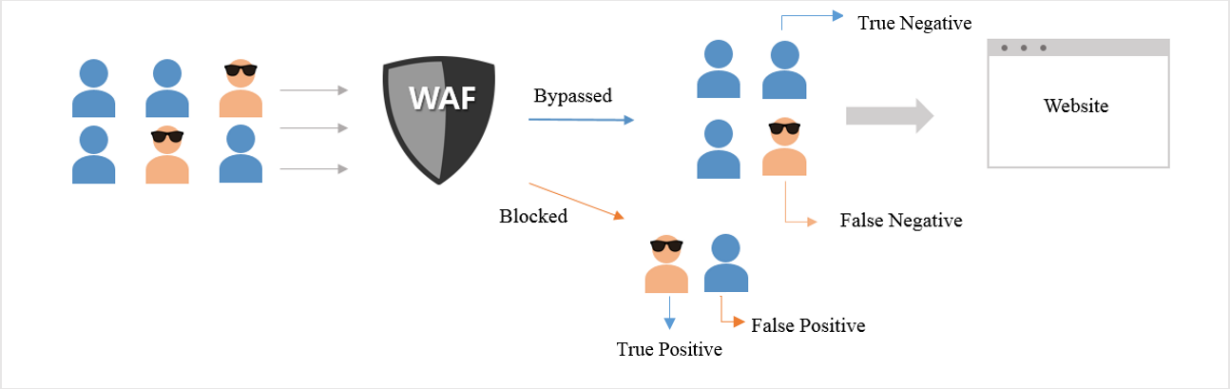
Firewall Setting of All In One (v4.1.9)

Cloudbric, is a cloud-based security service offering WAF, SSL and DDoS protection. A comprehensive list of premium security features is provided to all users regardless of pricing as usage is priced on monthly website traffic. In any case, the test website used for this research qualifies for free Cloudbric usage.

WAF Evaluation Criteria

Before testing the plugins, there are two criteria that should be considered when choosing a WAF service: True Positives and False Positives. True positives are cases in which the WAF correctly identifies attack traffic and blocks it. On the other hand, if the WAF failed to identify and block attack traffic, this instance is referred to as a false negative. Therefore, the true positive rate represents the WAF's detection ability. The higher the true positive rate, the more kinds of attacks the WAF is capable of blocking.

False positives are cases in which the WAF incorrectly identifies legitimate traffic as an attack. The opposite case, where legitimate traffic passes through as it should, is called True Negative (or often termed "Normal"). If the false positive rate is too high, it means the WAF is not sensitive enough to distinguish legitimate traffic from malicious traffic.



Four cases of WAF detection

There is a trade-off between false negatives and false positives. The more restrictive the rules configured in a WAF, the more likely malicious traffic will be blocked (low false negatives). Consequently, however, more legitimate traffic may be mistakenly blocked as well (high false positives). On the contrary, the more tolerant the rules configured in a WAF, the more freely legitimate traffic can access a site (low false positives). Similarly, malicious traffic from hackers will less likely be blocked (high false negatives).

In conclusion, an accurate WAF is one that prevents more web attacks while blocking fewer legitimate users. In other words, a WAF with a higher true positive rate and lower false positive rate is ideal.

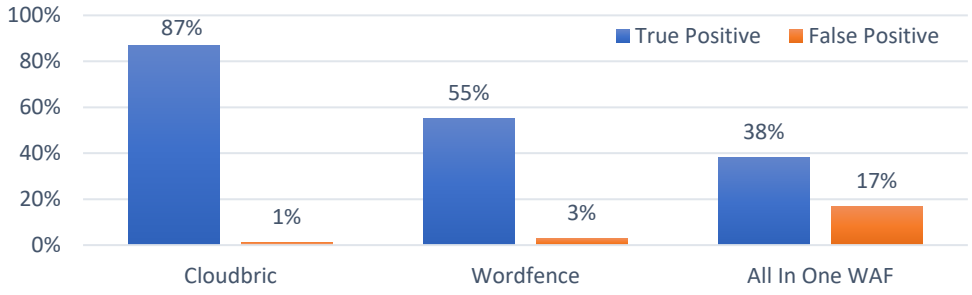
Therefore, it is important to consider both True Positives and False Positives to evaluate the performance of a WAF. However, most existing web application security tests focus only on attack detection abilities. Unlike those tests, this test generated legitimate traffic along with attack traffic to test the WAF's ability to correctly detect web attacks and distinguish malicious traffic from legitimate traffic.

Results

This test was conducted using 1524 web attack patterns published by Exploit-DB ("EDB") and 661 legitimate patterns developed by Cloudbric (see Appendix).

EDB(www.exploit-db.com) is a comprehensive database of exploit codes maintained by Offensive Security, an information security training company that provides various information security certifications as well as high end penetration testing services.

The true positive rate achieved against attack patterns published by EDB was found to be significantly higher through Cloudbric than through the two plugins. Cloudbric detected 87% of the attacks, on average, a 41% higher true positive rate against EDB attack patterns than the two plugins. Cloudbric also had 1% false positives compared to 3% for Wordfence and 17% for All In One. While both Cloudbric and Wordfence demonstrated few false positives, All In One blocked legitimate traffic 113 times, causing customer inconvenience.



True Positive vs. False Positive Rates

	Attack Traffic			Legitimate Traffic		
	True Positives	False Negatives	True Positive Rate	True Negatives	False Positive	False Positive Rate
Cloudbric	1326	198	87%	655	6	1%
Wordfence	839	685	55%	640	21	3%
All In One	583	941	38%	548	113	17%

Pattern Analysis

In order to figure out why some patterns cause false negatives or false positives results, patterns which leads false negatives or false positives are analyzed. The following patterns used method that pass data in the query portion of the requested URL.

True Positives

While there were several attack patterns that only Cloudbric was able to correctly detect, below is a thorough explanation of two particular attack patterns that the other WordPress security plugins' WAF failed to detect.

Basic LFI attack pattern

Pattern 1: Basic pattern including NULL character
http://test.com/pages/../../../../../../../../../../etc/passwd%00

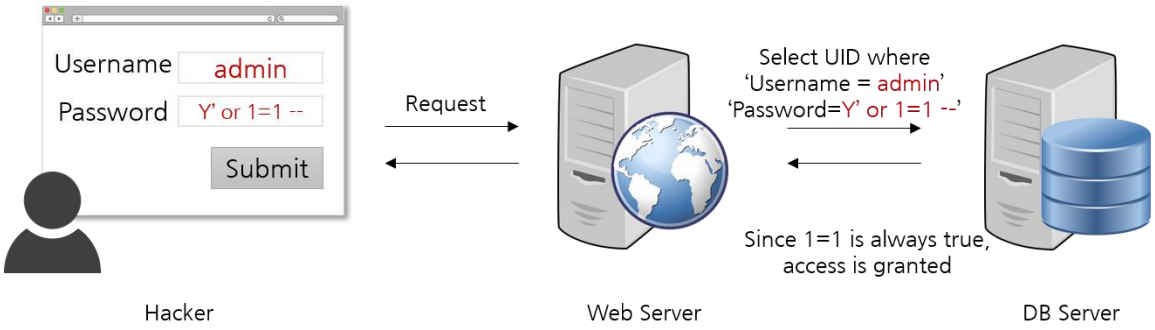
Pattern 1 is a prime example of avoiding detection by adding meaningless characters to a basic LFI (Local File Inclusion) attack pattern.

LFI is an attack that targets files that are already locally present on the server. In the attack pattern example above, hackers can read the "/etc/passwd" file after accessing the top level directory using '../'(move to parent directory). This file contains basic information necessary for hackers to gain entry into the system and access user account information. Though it is regarded as a basic pattern among LFI attack patterns, Wordfence and All In One did not detect this attack.

SQL injection attack pattern

SQL injection is another common web attack, and can be fatal, causing all data to be leaked or deleted. In the worst- case scenario, it can completely compromise the application system. Despite its potentially catastrophic consequences, the principle behind SQL injection is quite simple.

For example, in a standard login process, the user enters an ID and password on the site, and then a server verifies whether this information matches the information that was stored in the database.



The SQL injection process

However, in login processes affected by SQL injection, a hacker enters SQL statements that will behave abnormally in the database, rather than normal data such as an ID or password. For example, if “or 1=1 --” is inserted in the ID or password field, the server will recognize the condition as true even if the password is not correct (because 1=1 is always true), and will output the information requested.

Within the test, there were several SQL injection patterns that Cloudbric was able to detect correctly, but the other plugins could not detect.

Pattern 2: Basic SQL Injection attack pattern
http://test.com/admin/admin.php?username=admin%27+and+substring%28user%28%29,1,4%29=%27root%27+--+&session=c8d7ebc95b9b1a72d3b54eb59bea56c7*

Decoding this pattern:

http://test.com/admin/admin.php?username=admin' and substring(user(),1,4) ='root' -- &session=c8d7ebc95b9b1a72d3b54eb59bea56c7*

In the above pattern, ‘and substring(user(),1,4)='root' -- &session=c8d7ebc95b9b1a72d3b54eb59bea 56c7*’ is inserted in the username field. When this pattern works, the code after the '--' is commented out, thus preventing it from being interpreted, and the following query is executed into MySQL:

Select * from users where id=’admin’ and substring(user(),1,4)=’root’

This is a SQL SELECT statement with the common structure “Select [Field(column)] from [Table_name] where [Condition]”. It can be understood as a command to retrieve information about a user whose ID is 'admin' and ‘substring (user (), 1,4)’ is 'root' from the ‘users’ table. Therefore, the database server that receives this query will look for a user according to those requirements. With this attack pattern, ‘admin’ can be replaced with any other username registered on the site. This pattern is an attack because of the 'substring (user (), 1,4) =' root '' syntax.

To break down this pattern for easier understanding, substrring (str, start, length) is a MySQL default method that returns a portion of a string, extracting 'length' number of consecutive characters, beginning with the character in the 'start' position. For example, substring ('abcd', 2, 3) returns 'bcd' because it will return three characters from the character in the second position within the string 'abcd'. Next, user(), which is used as an argument of substring() in the above pattern, is a function of MySQL that returns the username of the database. Combined, substring (user (), 1, 4) means the string from the first to the fourth character of the database username. If the database username is root, substring (user (), 1, 4) will also be 'root.'

The purpose of this attack is to confirm if the database username is 'root'. This is because the most commonly used database user name in SQL is ‘root’. If the database user name is not 'root', the hacker would receive a pop up informing him that there is no matching information. If the database username is indeed 'root', the hacker will be prompted to enter a password. In this way, hackers can gain information about the site by using the fact that the response of the site varies according to the input value. This attack is a prelude to a full-blown SQL injection attack.

Pattern 2 is a relatively well-known SQL injection basic pattern. Pattern 3 is a modified SQL injection attack pattern with complex parentheses as shown below:

Pattern 3: Modified SQL Injection attack pattern with multiple parentheses
http://test.com/40/PetRatePro/index.php?cmd=4ntand(select1from(selectcount(*),concat((selectconcat(CHAR(52),CHAR(67),CHAR(117),CHAR(121),CHAR(82),CHAR(65),CHAR(101),CHAR(74),CHAR(100),CHAR(109),CHAR(55)) from information_schema.tables limit 0,1),floor(rand(0)*2))x frominformation_schema.tables group by x)a)and'

Pattern 3 attempts SQL injection using double, triple complex parentheses. The key code hidden in multiple parentheses is simply:

select concat(CHAR(52), … ,CHAR(109),CHAR(55)) from information_schema.tables limit 0,1

This syntax consists of a 'select A from B' SQL SELECT statement, which extracts the 'A' column from the 'B' table. Within 'A', 'concat' is used to add strings together and CHAR(52) … CHAR(55), ASCII code, are used as those strings. It is intended to represent column names in a complex way by using ASCII code. On the other hand, 'information_schema.tables', which is equivalent to ' B ' in the syntax, is the default database for MySQL and has the entire structure and content of the database. When this table is exposed, manipulating or releasing data on the website is facilitated. Therefore, attacks of this pattern attempt to subtract some information from the information_schema.tables. Because of complex parentheses and the obfuscation of column names via 'A', it is difficult to detect this type of attack pattern.

False Positives

Below is a thorough explanation of two legitimate patterns that WordFence or All In One blocked.

WordFence and All In One False Positive Patterns

Pattern 4: WordFence and All In One False Positive Patterns
http://test.com/865/sendmsg.jsp?subj=&text=There+are+many+possible+encodings+for+data%3A+UTF-7%2C+UTF-8%2C+base64+and+so+on&Username=Anonymous &x=32&y=7

The above pattern is a legitimate pattern that only Cloudbric has properly identified.
The decoded pattern is as below:

http://test.com/865/sendmsg.jsp?subj=&text=There are many possible encodings for data: UTF-7, UTF-8, base64 and so on&Username=Anonymous&x=32&y=7

WordFence and All In One identified this pattern as an attack due to the value in text, suggesting that "**There are many possible encodings for data: UTF-7, UTF-8, base64 and so on**" in the pattern. This is a simple sentence, but the WAF considers this sentence as [There ... Base 64] and [so on], in other words, an attack with 'A and B' structures. The 'A and B' structures are especially common for SQL injection attacks. In this case, the pattern corresponding to 'A' contains several words frequently used in attack patterns such as 'encodings', ':', 'UTF-7' and 'UTF-8', triggering false positives. In reality, these patterns are harmless when embedded as text; hence, it should not have been blocked. While traffic may contain patterns commonly associated with attacks, Cloudbric does not block it unless such patterns are determined to accompany a malicious intent to attack the website. In pattern 4, the text input triggering the plugins' false positives were not intended as an attack, and so Cloudbric allowed it to access the website. WAFs that block the above pattern are likely to generate many false positives for websites with forum postings or discussions about coding.

All In One False Positive Patterns

Pattern 5: All In One False Positive Patterns
http://test.com/board.php?text=lsof%20is%20a%20command%20meaning%20%22ist%20open%20files%22%2C%20which%20is%20used%20in%20many%20Unixlike%20systems%20to%20report%20a%20list%20of%20all%20open%20files%20and%20the%20processes%20that%20opened%20them.

This pattern is a legitimate pattern that only the All In One has incorrectly detected. The decoded pattern is:

http://test.com/board.php?text=lsof is a command meaning "list open files", which is used in many Unix-like systems to report a list of all open files and the processes that opened

The element triggering the false positive is "lsof". lsof is a system command that prints all the information about the files utilized by the system. This command is useful when managing a system, but it can lead to an attack that leaks information about all files when manipulated. Some WAFs register lsof as a signature and block the request containing this word. For All In One, it has identified this particular pattern as an attack. However, when blocking a pattern containing lsof, WAF needs to make sure that this command is intended to be an attack, which is only when an additional filename or directory name follows lsof. Looking back at the above pattern, lsof does not have any effect on the system because no filename or directory name follows. Therefore, the above pattern is a legitimate pattern that should not have been identified as an attack.

Conclusion

The penetration test has shown that the WAF of WordPress security plugins performed poorly in terms of both true positives and false positives as compared to Cloudbric. All In One, especially, showed the lowest true positive rate and the highest false positive rate. The results demonstrated that Cloudbric's WAF provides more effective and accurate security, delivering more powerful attack detection while retaining a low false positives rate.

Cloudbric uses not only a "signature-based detection method" which identifies attacks by finding a match against a database of existing attack patterns, but also a "logic-based detection engine" which analyzes traffic through a set of 26 preset security policies. This is the main reason why there were several patterns which only Cloudbric was able to identify correctly, while the other plugins failed to detect or even mistakenly blocked. Utilizing a logic-based detection engine to understand the structure and meaning of the attack enables more accurate detection of hidden or modified attacks.

Appendix

The following patterns (legitimate) were used to test false positives. If you want a complete list of test patterns, then please contact support@cloudbric.com.

No.	Pattern
1	/board.php?id=1%20UNIunionON+SeLselectECT+1,2,3,4,5,6,7--
2	/sendmsg.jsp?subj=&text=select+one+item+from+these+funny+things+%3D%29&Username=Anonymous&x=32&y=7
3	/sendmsg.jsp?subj=&text=message=this+is+not+good%3B+drop+the+item+you+are+holding&Username=Anonymous&x=32&y=7
4	/sendmsg.jsp?subj=&text=I+have+selected+an+instrument+%28a+new+one%29+for+today&Username=Anonymous&x=32&y=7
5	/sendmsg.jsp?subj=&text=send+me+a+check+or+100000%24+cash&Username=Anonymous&x=32&y=7
6	/sendmsg.jsp?subj=&text=There+are+many+possible+encodings+for+data%3A+UTF-7%2C+UTF-8%2C+base64+and+so+on&Username=Anonymous&x=32&y=7
7	/sendmsg.jsp?subj=&text=Sun+Wu+and+his+Book%0D%0A----------%0D%0A%0D%0A%0D%0A+++++Ssu-ma+Ch%60ien+gives+the+following+biography+of+Sun+Tzu%3A++%5B1%5D%0D%0A--%0D%0A%0D%0A+++++++Sun+Tzu+Wu+was+a+native+of+the+Ch%60i+State.++His+ART+OF%0D%0A++WAR+brought+him+to+the+notice+of+Ho+Lu%2C+%5B2%5D+King+of+Wu.++Ho%0D%0A++Lu+said+to+him%3A++%22I+have+carefully+perused+your+13+chapters.%0D%0A++May+I+submit+your+theory+of+managing+soldiers+to+a+slight%0D%0A++test%3F%22%0D%0A++++++Sun+Tzu+replied%3A++%22You+may.%22%0D%0A+++++++Ho+Lu+asked%3A++%22May+the+test+be+applied+to+women%3F%22%0D%0A+++++++The+answer+was+again+in+the+affirmative%2C+so+arrangements%0D%0A++were+made+to+bring+180+ladies+out+of+the+Palace.++Sun+Tzu%0D%0A++divided+them+into+two+companies%2C+and+placed+one+of+the+King%27s%0D%0A++favorite+concubines+at+the+head+of+each.++He+then+bade+them%0D%0A++all+take+spears+in+their+hands%2C+and+addressed+them+thus%3A+++%22I%0D%0A++presume+you+know+the+difference+between+front+and+back%2C+right%0D%0A++hand+and+left+hand%3F%22%0D%0A+++++++The+girls+replied%3A++Yes.%0D%0A+++++++Sun+Tzu+went+on%3A++%22When+I+say+%22Eyes+front%2C%22++you+must%0D%0A++look+straight+ahead.++When+I+say+%22Left+turn%2C%22+you+must+face%0D%0A++towards+your+left+hand.++When+I+say+%22Right+turn%2C%22++you+must%0D%0A++face+towards+your+right+hand.++When+I+say+%22About+turn%2C%22++you%0D%0A++must+face+right+round+towards+your+back.%22%0D%0A+++++++Again+the+girls+assented.++The+words+of+command+having%0D%0A++been+thus+explained%2C+he+set+up+the+halberds+and+battle-axes%0D%0A++in+order+to+begin+the+drill.++Then%2C+to+the+sound+of+drums%2C+he%0D%0A++gave+the+order+%22Right+turn.%22++But+the+girls+only+burst+out%0D%0A++laughing.++Sun+Tzu+said%3A++%22If+words+of+command+are+not+clear%0D%0A++and+distinct%2C+if+orders+are+not+thoroughly+understood%2C+then%0D%0A++the+general+is+to+blame.%22%0D%0A+++++++So+he+started+drilling+them+again%2C+and+this+time+gave%0D%0A++the+order+%22Left+turn%2C%22+whereupon+the+girls+once+more+burst%0D%0A++into+fits+of+laughter.++Sun+Tzu%3A++%22If+words+of+command+are%0D%0A++not+clear+and+distinct%2C+if+orders+are+not+thoroughly%0D%0A++understood%2C+the+general+is+to+blame.++But+if+his+orders+ARE%0D%0A++clear%2C+and+the+soldiers+nevertheless+disobey%2C+then+it+is+the%0D%0A++fault+of+their+officers.%22&&Username=Anonymous&x=32&y=7
8	/sendmsg.jsp?subj=&text=%0D%0AShopping-list%3A%0D%0A%0D%0AMilk%0D%0AHot+dogs%0D%0ACheese&Username=Anonymous&x=32&y=7
9	/Extension_Filtering/test.exe
10	/Extension_Filtering/test.png
11	/Extension_Filtering/test.ico
12	/Extension_Filtering/test.asf
13	/Extension_Filtering/test.tif
14	/Extension_Filtering/test.zip
15	/Extension_Filtering/test.aspx
16	/Extension_Filtering/test.rar
17	/board.php?text=An%20additional%20important%20file%20is%20boot.ini%2C%20which%20contains%20boot%20configuration%20(if%20missing%2C%20NTLDR%20will%20default%20to%20%3Findows%20on%20the%20first%20partition%20of%20the%20first%20hard%20drive).
18	/board.php?text=Apache%20is%20a%20marvelous%20web%20server%20that%20offers%20.htpasswd%20and%20.htgroup%20for%20controlling%20restricted%20access%20to%20your%20website.

19	/board.php?text=Find%20out%20what%20telnet.exe%20is%20doing%20on%20computer%2C%20whether%20it%27s%20safe%2C%20info%20on%20related%20errors%20and%20how%20to%20remove%20it.
20	/board.php?text=Many%20people%20just%20have%20this%20wrong%20notion%20that%20windows%20command%20line%20FTP.exe%20can%20not%20be%20run%20in%20passive%20mode.%20
21	/board.php?text=So%20Typescript%20compiled%20Javascript%20actually%20works%20in%20WSH.exe?%20Thats%20so%20awesome.
22	/board.php?text=nothing%20can%20be%20more%20frustrated%20than%20running%20into%20error%20message%20like%20rcmd.exe%20error%20when%20you%20playing%20or%20working%20with%20the%20computer.
23	/board.php?text=The%20problem%20is%20that%20when%20i%20am%20open%20nc.exe%20from%20the%20CMD%20using%20the%20nc%20syntax%20as%20in%20the%20above%20code%20it%20works%20and%20is%20connecting%20to%20my%20server.
24	/board.php?text=Information%20about%20the%20Unix%20kill%20command%2C%20including%20examples%20and%20syntax.
25	/board.php?text=Used%20without%20parameters%2C%20net%20localgroup%20displays%20the%20name%20of%20the%20server%20and%20the%20names%20of%20local%20groups%20on%20the%20computer.
26	/board.php?text=National%20Association%20of%20Schools%20of%20Music.%20Welcome%20to%20the%20NASM%20web%20site.
27	/board.php?text=I%27m%20using%20tcl8.4%20and%20I%27m%20trying%20to%20do%20a%20little%20tclsh%20scripting.%20I%27m%20trying%20to%20execute%20a%20shell%20command%20using%20a%20tcl%20variable%20that%20has%20embedded%20spaces.
28	/board.php?text=In%20computer%20networking%2C%20the%20Name%2FFinger%20protocol%20and%20the%20Finger%20user%20information%20protocol%20are%20simple%20network%20protocols%20for%20the%20exchange%20of%20human-oriented%20status%20and%20user%20information.
29	/board.php?text=lsof%20is%20a%20command%20meaning%20%22list%20open%20files%22%2C%20which%20is%20used%20in%20many%20Unix-like%20systems%20to%20report%20a%20list%20of%20all%20open%20files%20and%20the%20processes%20that%20opened%20them.
30	/board.php?text=Information%20and%20examples%20on%20the%20Unix%20and%20Linux%20rm%20command.
31	/board.php?text=Python%20is%20a%20widely%20used%20general-purpose%2C%20high-level%20programming%20language.
32	/board.php?text=How%20to%20perform%20a%20traceroute%20to%20a%20domain%20or%20website%20-%20this%20will%20help%20identify%20connection%20problems.
33	/board.php?text=Information%20about%20the%20Unix%20and%20Linux%20chmod%20command%20including%20the%20full%20syntax%20and%20several%20different%20examples.
34	/board.php?text=onSubmit%20is%20a%20scripting%20event%20that%20occurs%20when%20the%20user%20attempts%20to%20submit%20the%20form%20to%20the%20CGI.
35	/board.php?text=Tutorials%20and%20over%20400%20free%20scripts.%20Also%20JavaScript%20objects%2C%20properties%2C%20and%20methods%20reference.
36	/board.php?text=Visual%20Meta%20GmbH%20operates%20multiple%20shopping%20platforms%20across%20Europe%20under%20the%20brands%20LadenZeile%20and%20ShopAlike.
37	/board.php?text=The%20ActiveXObject%20object%20is%20used%20to%20create%20instances%20of%20OLE%20Automation%20objects%20in%20Internet%20Explorer%20on%20Windows%20operating%20systems.
38	/board.php?text=VBScript%20(Visual%20Basic%20Scripting%20Edition)%20is%20an%20Active%20Scripting%20language%20developed%20by%20Microsoft%20that%20is%20modeled%20on%20Visual%20Basic.
39	/board.php?text=The%20onkeypress%20event%20occurs%20when%20the%20user%20presses%20a%20key%20(on%20the%20keyboard).
40	/board.php?text=This%20event%20triggers%20when%20a%20JavaScript%20%27unescape()%27%20or%20%27eval()%27%20contains%20the%20%27String%27%20method%20%27.fromCharCode()%27.
41	/board.php?text=For%20example%2C%20a%20script%20could%20generate%20a%20pop-up%20alert%20box%20message%2C%20or%20provide%20a%20dropdown%20menu.
42	/board.php?text=An%20application%20is%20a%20program%20or%20group%20of%20programs%20designed%20for%20end%20users.
43	/board.php?text=The%20background%20CSS%20property%20is%20a%20shorthand%20for%20setting%20the%20individual%20background%20values%20in%20a%20single%20place%20in%20the%20style%20sheet.
44	/board.php?text=I%20have%20been%20using%20GetSpecialFolder%20from%20madshell%20unit%2C%20I%20looked%20at%20the%20source%20examples%20provided%20with%20madcollection%20documentation.%20
45	/board.php?text=For%20the%20most%20part%2C%20customization%20is%20different%20in%20the%20new%20Disqus%20because%20we%20decided%20to%20completely%20re-implement%20our%20commenting%20embed%20inside%20of%20an%20iframe
46	/board.php?text=print%20is%20not%20actually%20a%20real%20function%20(it%20is%20a%20language%20construct)%20so%20you%20are%20not%20required%20to%20use%20parentheses%20with%20its%20argument%20list.

47	/board.php?text=The%20INSTR%20functions%20search%20string%20for%20substring.%20The%20function%20returns%20an%20integer%20indicating%20the%20position%20of%20the%20character%20in%20string%20that%20is%20the%20first%20character%20of%20this%20occurrence.%20INSTR%20calculates%20strings%20using%20characters%20as%20defined%20by%20the%20input%20character%20set.%20INSTRB%20uses%20bytes%20instead%20of%20characters.%20INSTRC%20uses%20Unicode%20complete%20characters.%20INSTR2%20uses%20UCS2%20code%20points.%20INSTR4%20uses%20UCS4%20code%20points.
48	/board.php?text=The%20public%20synonyms%20are%20not%20de?ned%20in%20all%20Oracle%20installations%20(at%20least%20for%20the%20DBA-views).%20Then%20one%20must%20write%2C%20e.g.%2C%20SYS.USER_CATALOG.
49	/board.php?text=check%20out%20what%20your%20database%20support%20on%20constraint_type.
50	/board.php?text=Was%20a%20little%20perplexed%20about%20the%20MsysObjects.Flags%20and%20how%20they%20figured%20into%20the%20equation.%20
51	/board.php?text=Phim%20Local%20User_Group%20-%20download%20at%204shared.%20Phim%20Local%20User_Group%20is%20hosted%20at%20free%20file%20sharing%20service%204shared.
52	/board.php?text=In%20SQL%20Enterprise%20Manager%2C%20when%20you%20expand%20a%20database%20you%20are%20shown%20the%20database%27s%20tables%2C%20views%2C%20stored%20procedures%2C%20and%20other%20useful%20database%20objects.%20Have%20you%20ever%20wondered%20how%20in%20the%20world%20SQL%20Server%20keeps%20track%20of%20the%20many%20objects%20for%20each%20database?%20Not%20surprisingly%2C%20SQL%20Server%20uses%20a%20table%20to%20store%20the%20object%20information%20for%20each%20database.%20This%20table%2C%20sysobjects%2C%20can%20be%20queried%20just%20like%20any%20other%20table!
53	/board.php?text=There%20is%20the%20customer%20who%20suspect%20the%20mib%20info%20on%20Appliance%202.0.3%20is%20incorrect%20since%20almost%20all%20the%20trpas%20are%20the%20object_type%20and%20the%20customer%20think%20those%20traps%20should%20be%20the%20notification_type%20by%20comparing%20with%20the%20showmib%20output%20in%20Appliance%202.5.%20
54	/board.php?text=I%20realize%20that%20I%27m%20not%20using%20information%20from%20mb_users%20table%20but%20by%20just%20adding%20them%20in%20there%2C%20I%20get%20the%20error.%20With%20that%20I%27m%20assuming%20that%20this%20is%20the%20line%20where%20I%20should%20be%20concerned.%20I%20dropped%20the%20ORDER%20BY%20as%20it%20doesn%27t%20change%20the%20meaning%20of%20the%20statement%2C%20just%20the%20ordering%20(duh%20:)%20).%20
55	/board.php?text=For%20%22normal%22%20indexes%2C%20USER_IND_COLUMNS%20will%20contain%20the%20column%20name(s)%20for%20an%20index%2C%20but%20things%20go%20astray%20when%20looking%20at%20function-based%20indexes.
56	/board.php?text=The%20INSERT%20INTO%20statement%20is%20used%20to%20insert%20new%20records%20in%20a%20table.%20The%20SQL%20INSERT%20INTO%20Statement.
57	/board.php?text=I%20was%20thinking%20of%20using%20AUTONOMOUS_TRANSACTION%20Pragma%20for%20some%20logging%20in%20a%20batch%20process.%20Does%20anyone%20have%20any%20experience%20with%20this%20?%20If%20so%20any%20pros%20and%20cons%20would%20be%20appreciated.
58	/board.php?text=If%20you%27re%20looking%20for%20how%20to%20do%20a%20nested%20IFNULL%2C%20you%20probably%20need%20to%20be%20looking%20at%20how%20to%20use%20COALESCE%20instead.
59	/board.php?text=Ciel%2C%20a%20tincture%20in%20heraldry%20also%20called%20bleu%20celeste%20or%20celeste%20(sky-blue)
60	/board.php?text=MySQL%20BIT_OR()%20function%20returns%20the%20bitwise%20OR%20of%20all%20bits%20in%20a%20given%20expression.
61	/board.php?text=This%20is%20a%207.2%20database.%20I%20am%20trying%20to%20test%20this%2C%20but%20having%20resource%20troubles%2C%20and%20running%20out%20of%20time.%20I%20want%20to%20delete%20rows%20from%20myschema.
62	/board.php?text=The%20time()%20function%20shall%20return%20the%20value%20of%20time%20[Option%20Start]%20in%20seconds%20since%20the%20Epoch.
63	/board.php?text=month%20(plural%20months)%20The%20plural%20is%20occasionally%20seen%20as%20month%20(unchanged).%20
64	/board.php?text=If%20get_class()%20is%20called%20with%20anything%20other%20than%20an%20object%2C%20an%20E_WARNING%20level%20error%20is%20raised.
65	/board.php?text=You%20can%20use%20the%20undocumented%20extended%20stored%20procedure%20xp_regread%20to%20access%20registry%20entries%20using%20T-SQL.
66	/board.php?text=MySQL%20EXPORT_SET()%20returns%20the%20string%20such%20a%20way%20that%20every%20bit%20set%20in%20the%20value%20bits%2C%20user%20can%20get%20an%20on%20string%20and%20get%20an%20off%20string%20for%20every%20reset%20bit.
67	/board.php?text=MySQL%20AES_DECRYPT()%20decrypts%20an%20encrypted%20string%20to%20return%20the%20original%20string.%20It%20returns%20NULL%20if%20detects%20invalid%20data.
68	/board.php?text=CURRENT_DATE%20returns%20a%20DATE%20value%20representing%20the%20current%20date%20in%20local%20time.
69	/board.php?text=Share%20our%20extensive%20collection%20of%20famous%20quotes%20by%20authors%2C%20celebrities%2C%20newsmakers%2C%20and%20more.%20Enjoy%20our%20Quotes%20of%20the%20Day%20on%20the%20web%2C%20Facebook%2C%20and%20blogs.

70	/board.php?text=Review%20the%20categories%20of%20user%20that%20might%20want%20to%20use%20with%20Citrix%2C%20and%20how%20to%20configure%20for%20concurrent%20multi-users.
71	/board.php?text=Locate32%20finds%20files%20and%20directories%20based%20on%20file%20and%20folder%20names%20stored%20in%20a%20database.
72	/board.php?text=The%20EXP%20function%20returns%20the%20exponential%20of%20the%20value%20specified%20by%20NumericExpression.%20The%20parameter%20can%20be%20any%20built-in%20numeric%20data%20type.
73	/board.php?text=CURRENT_TIMESTAMP%20returns%20a%20TIMESTAMP%20value%20representing%20the%20current%20date%20and%20local%20time.
74	/board.php?text=Returns%20a%20new%20string%20with%20some%20or%20all%20matches%20of%20a%20pattern%20replaced%20by%20a%20replacement.
75	/board.php?text=The%20@XmlType%20annnotation%20can%20be%20used%20with%20the%20following%20program%20elements
76	/board.php?text=The%20CHARACTER_LENGTH%20function%20returns%20the%20length%20of%20the%20first%20argument%20in%20the%20specified%20string%20unit
77	/board.php?text=CAST%20addresses%20issues%20of%20animal%20sciences%2C%20food%20sciences%20and%20agricultural%20technology%2C%20plant%20and%20soil%20sciences%2C%20and%20plant%20protection%20sciences%20with%20input%20from%20throughout%20the%20scientific%20and%20legal%20community.
78	/board.php?text=A%20varchar%20or%20Variable%20Character%20Field%20is%20a%20set%20of%20character%20data%20of%20indeterminate%20length.%20
79	/board.php?text=Look%20up%20position%20in%20Wiktionary%2C%20the%20free%20dictionary.%20Position%20refers%20to%20the%20spatial%20location%20(rather%20than%20orientation)%20of%20an%20entity.
80	/board.php?text=The%20DB2%20Administration%20Tool%20panel%20ADB21TAB%20%22Alter%20Table%22%20does%20not%20quality%20the%20SELECT%20from%20SYSIBM.SYSCOLUMNS%20with%20the%20TBCREATOR.
81	/board.php?text=Remove%20WEIGHT_STRING()%20from%20parser%20(where%20it%20does%20not%20belong).%20If%20someone%20wants%20to%20they%20can%20reimplement%20this%20as%20a%20straight%20function.%201295.
82	/board.php?text=A%20microsecond%20is%20an%20SI%20unit%20of%20time%20equal%20to%20one%20millionth%20(10?6%20or%201%2F1%2C000%2C000)%20of%20a%20second.%20Its%20symbol%20is%20.%20One%20microsecond%20is%20to%20one%20second%20as%20one%20second%20is%20to%2011.574%20days.
83	/board.php?text=The%20SYSTEM_USER%20special%20register%20specifies%20the%20authorization%20ID%20of%20the%20user%20that%20connected%20to%20the%20database.
84	/board.php?text=In%20a%20SQL%20Server%202005%20trace%2C%20I%27ve%20got%20lots%20of%20%22exec%20sp_execute%22%20statements.%20I%20know%20they%20are%20connected%20to%20a%20corresponding%20%22exec%20sp_prepare%22%20statement%20which%20specifies%20the%20actual%20SQL.
85	/board.php?text=I%20found%20the%20command%20%22SELECT%20CONNECTION_ID()%22%20in%20mysql%20which%20returns%20the%20connection%20ID%20with%20the%20server.%20Is%20there%20any%20equivalent%20command%20in%20PostgreSQL?
86	/board.php?text=The%20encryption%20key%20to%20use%20is%20chosen%20based%20on%20the%20second%20argument%20to%20DES_ENCRYPT()%2C%20if%20one%20was%20given.
87	/board.php?text=It%27s%20burdened%20by%20a%20predictable%2C%20overly%20melodramatic%20story%2C%20but%20The%20Greatest%20benefits%20from%20strong%20performances%20by%20its%20talented%20cast.
88	/board.php?text=Reading%20and%20Writing%20Server-side%20Files.%20UTL_FILE%20is%20a%20package%20that%20has%20been%20welcomed%20warmly%20by%20PL%2FSQL%20developers
89	/board.php?text=If%20the%20optional%20base%20parameter%20is%20specified%2C%20log()%20returns%20logbase%20arg%2C%20otherwise%20log()%20returns%20the%20natural%20logarithm%20of%20arg.
90	/board.php?text=I%20am%20not%20generally%20a%20proponent%20of%20creating%20tables%20with%20columns%20of%20datatype%20sql_variant%20in%20them.
91	/board.php?text=How%20to%20use%20encrypt%20in%20a%20sentence.%20Example%20sentences%20with%20the%20word%20encrypt.
92	/2225/board.php?text=the%20capital%20of%20Upper%20Canada%20was%20moved%20from%20Newark%20(now%20Niagara-on-the-Lake)%20to%20York%20(now%20Toronto)%2C%20which%20was%20judged%20to%20be%20less%20vulnerable%20to%20attack%20by%20the%20Americans.
93	/board.php?text=A%20small%20comment%20on%20phpdev-dunnbypauls%20conclusion%20that%20rand()%20only%20generates%20numbers%20that%20are%20a%20multiply%20of%203.%20
94	/board.php?text=The%20names%20of%20the%20days%20of%20the%20week%20(aste)%20in%20Guipuscoan%20Basque%20point%20to%20an%20earlier%20three-day%20week.
95	/board.php?text=If%20the%20first%20and%20only%20parameter%20is%20an%20array%2C%20min()%20returns%20the%20lowest%20value%20in%20that%20array.

96	/board.php?text=This%20article%20mentions%20How%20to%20Enable%20&%20Disable%20XP_CMDSHELL%20using%20SP_CONFIGURE.
97	/board.php?text=This%20will%20allow%20you%20to%20call%20sp_executesql%20with%20@eStatus%20as%20a%20parameter%20instead%20of%20embedding%20it%20into%20the%20SQL.
98	/board.php?text=THE%20EUROPEAN%20EXTREMELY%20LARGE%20TELESCOPE%20(%22E-ELT%22)%20PROJECT.
99	/board.php?text=The%20new%20Oracle%20built-in%20package%20DBMS_JAVA%20gives%20you%20access%20to%2C%20and%20the%20ability%20to%20modify%2C%20various%20characteristics%20of%20the%20Aurora%20Java%20Virtual%20Machine.
100	/board.php?text=Serene%20is%20a%20truly%20beautiful%20blogging%20theme%20with%20post%20format%20support.

Penta Security Systems Corp.

6220 Westpark Drive, Suite 222 Houston, TX 77057
www.pentasecurity.com