Web Security Platform – documentaţie tehnică

- ## Ce este Web Security Platform (WSP) ?

Web Security Platform este o platformă web ce încearcă îmbunătăţirea şi reducerea riscurilor ca o persoană rău-intenţionată sa compromita informatii private.Platforma vine in ajutorul administratorului prin panoul de comanda ce pune la dispozitie o serie de statistici, functii si extensii ce incearca reducerea riscurilor de penetrare a securitatii.

Platforma **este la baza un schelet** ce pune in miscare o **serie de mini-aplicatii, denumite generic extensii**, care folosesc diverse informatii puse la dispozitie de schelet pentru a stabili daca avem de-a face cu atacuri web. Una din extensiile platformei WSP detecteaza cu succes atacurile de tip Cross Side Scripting(XSS), Remote File Inclusion(RFI), Local File Inclusion (LFI),SQL Injection (SQLI), File Path Disclosure (FPD) , Cross Site Request Forgery(CSRF) si Remote Code Execution(RCE). O alta extensie are grija de blocarea unui mare volum din atacurile de tip DDOS care incearca sa aduca un website la o incarcare foarte mare. Alte doua extensii analizeaza fisierele si continutul acestora, urmarind modificarile,adaugarile sau disparitia fisierelor (WSP File Monitor) sau prezenta unor virusi (WSP Antivirus).

Aceste extensii sunt completate de diverse facilitati pre-instalate in schelet :

- ## Instalarea și configurarea platformei WSP

Web Security Platforma are nevoie pentru a accesa panoul de administrare de un utilizator şi o parolă alaturi de o conexiune la o bază de date MySQL. Acestea pot fi configurate inainte de instalare in fisierul **wspConfig.php .** Dacă dorim să adăugăm mai multe persoane cu permisiuni de administrator va trebuie să-i punem intr-un mod asemanator cu imaginea de mai jos, aceasta reprezentand configurarea a 3 persoane.

```
$users = array('Andrei',
               'User2',
               'User3'
               );
$passs  = array('wsp',
                'pass2',
                'pass3'
               );
```

Pentru a seta conexiunea către serverul MySQL trebuie doar să configuram fisierul **wspConfig.php** ca in imaginea de mai jos .Sub setarile de baza , avem posibilitatea de a seta numele tabelelor precum si prefixul acestora.

```
$connection = array('server'       => 'localhost',
                    'username'     => 'root',
                    'password'     => '',
                    'database'     => 'wss');


 $tablePrefix = 'prt_sys';
 $tables = array(
              'settings'     => $tablePrefix.'_settings',
              'banlist'      => $tablePrefix.'_banlist',
              'adminlog'     => $tablePrefix.'_adminlog',
              'whitelist'    => $tablePrefix.'_whitelist',
              'protected'    => $tablePrefix.'_protected',
              'attackstats'  => $tablePrefix.'_astats',
              'plugins'      => $tablePrefix.'_plugins',
              'restrictions' => $tablePrefix.'_restrictions'
              );
```

- ## Instalarea sistemului de protecție

  - **Instalarea manuala –** consta in editarea fisierelor PHP care se doresc a fi protejate. Aceasta instalare necesita includerea unor fisiere in fiecare pagina ce va urma sa fie protejata de WSP astfel :

1. Inainte de deschiderea tagului HTML si de inceperea tuturor codului, adaugati urmatoarele linii :

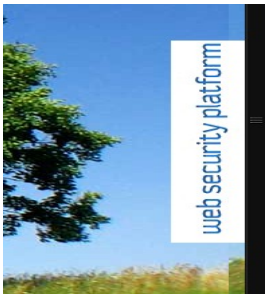
```
<?php
    $pathToWSP = 'path_to_WSP/';
    include_once($pathToWSP.'preWSP.php');
?>
```

2. Imediat dupa inchiderea tagului HTML si terminarea tuturor liniilor de cod PHP, adaugati urmatoarea linie :

```
</html>
<?php include_once($pathToWSP.'postWSP.php'); ?>
```

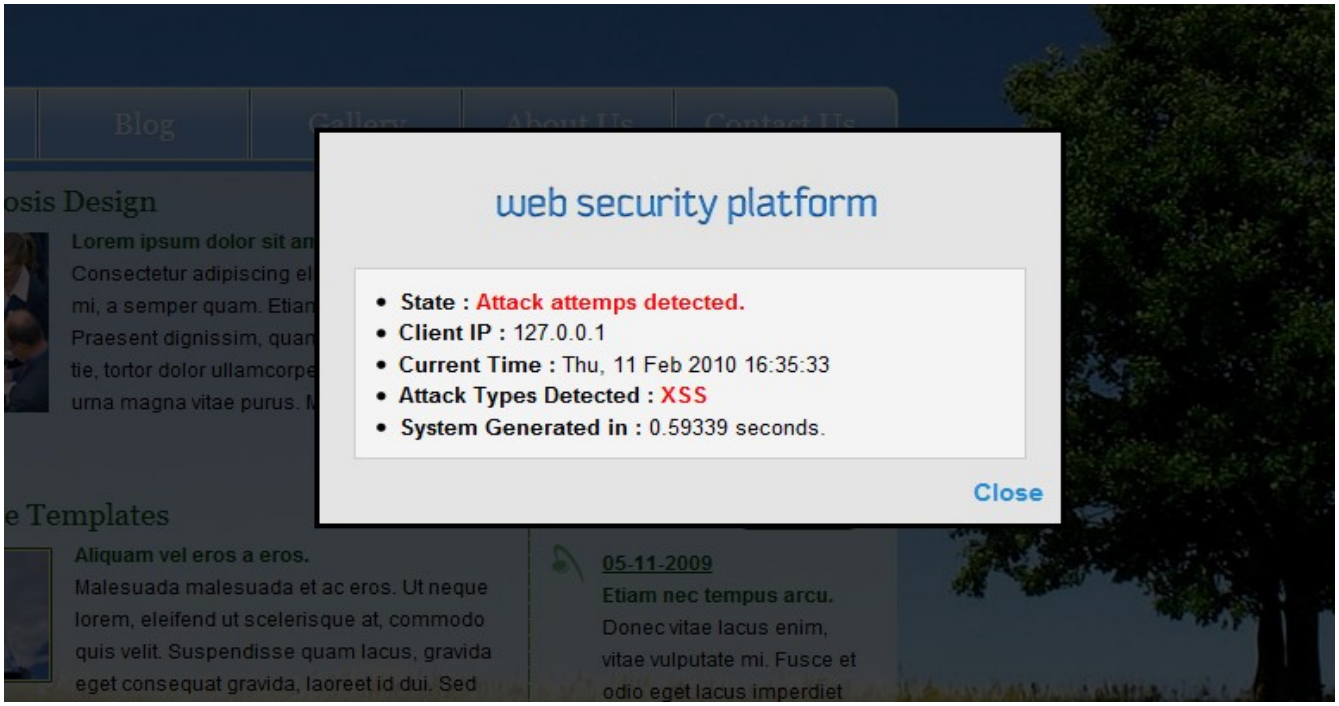
  - **Instalarea automata (neimplementata) –** consta in generarea unui directory management ce ne va ajuta sa alegem care fisiere vor beneficia de instalare automata a platformei. Aceasta metoda este nerecomandata in situatiile in care nu suntem siguri unde incepe/se termina pagina sau care sunt dependentele de fisiere. In cazul in care un fisier nu poate fi editat(lipsa permisiunilor CHMOD) atunci se va recurge la instalare manuala.

- ## Alertele primite de end-user



Alertele care vor fi afisate end-userilor sunt putine si nu urmaresc decat descurajarea hackerului de a continua atacul. In cazul in care unul din sistemele de securitate detecteaza tentative de penetrare a securitatii, pagina va genera in partea dreapta o imagine cu textul *"Web Security Platform"* , care o data apasata va afisa alerta pe pagina userului.Aceste alerte pot fi declansate sau nu, in functie de dorinta administratorului , setarile putand fi facute in *Administrator Control Panel(ACP)* → *Meniu Stanga* → *Settings* → *General Settings* → *Show Attack Alert.*

Mesajul care il va primi atacatorul va fi asemanator cu cel de mai jos :



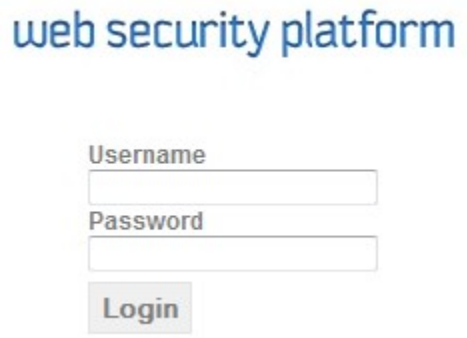
- ## Cerințe de sistem

  - *Apache HTTP Server >= 2.2.3*
  - *PHP >= 4*
  - *MySQL >= 5.0.2.7*

Aceste informații sunt versiunile pe care a fost testat.Este foarte posibil ca platforma sa poata rula în condiții optime și pe servere cu configurări mai slabe, deși în majoritatea cazurilor acest lucru nu va fi necesar deoarece majoritatea hosting providerilor urmaresc sa fie la zi cu update-urile.

Panoul de administrare (ACP) – Web Security Platform

Accesați din browser *http://www.site.com/path_to_WSP/acp* unde introduceti datele de autentificare ce le-ati setat in fisierul de configurare **wspConfig.php**.



- ## Pagina principala și meniul

Pagina principală conține o serie de statistici, alaturi de ultimile loguri ale administratorilor platformei WSP, configurati in fisierul **wspConfig.php** . In partea stanga se afla meniul care va face legatura cu toate membrele platformei WSP , alaturi de extensiile instalate sau ce urmeaza sa fie instalate.Restul documentatiei se va axa pe fiecare sectiune a platformei, prezentand facilitatile acesteia. Pagina principala va afisa si diverse alerte precum Automatic Updates sau schimbarea unor fisiere, detectarea malware etc. Partea dreapta sus ne face legatura rapid cu pagina principala sau ne ofera posibilitatea de a incheia o sesiune.

Dashboard

Stats – Ne reintoarce la pagina principala
Administrator Logs – e pagina care ne ofera logurile actiunilor ce au fost facute de administratorii platformei. Astfel, vom putea vedea daca unul din acestea vor schimba setarile de securitate sau vor sa saboteze platforma.
Internal Logs – stocheaza toate erorile care le intampina platforma pe parcursul rularii la nivel de end-user. Orice eroare a platformei este mascata de o clasa speciala de tratare a erorilor, iar acestea sunt stocate local intr-un fisier : *path_to_WSP/wspLogs/error.logs.php* ce sunt protejate de un sistem de protectie impotriva accesarii directe.

Protected Pages – pagina aceasta contine o lista cu toate paginile care sunt protejate de Web Security Platform alaturi de cateva statistici de baza : numarul de atacuri detectate in cadrul acestei pagini, numarul de afisari, statusul paginii (Cached – pagina nu a mai fost accesata de 30 de zile sau Active).

ID	PAGE	ATTACKS	VIEWS	LAST VISIT	STATE	PROTECTED	ACTIVATE	DELETE
1	/demo/index.php	8	10	Thu, 11 Feb 2010 16:35:34	Active	YES	Deactivate	
2	/test.php	7	809	Thu, 11 Feb 2010 16:31:15	Active	YES	Deactivate	
3	/wspMain.php	0	160	Sun, 01 Nov 2009 19:43:50	Cached	YES	Deactivate	

Plugins

Manage – ne pune la dispozitie toate pluginurile care au configuratia corecta, precum si statusul lor : Active,Dezactivate, Neinstalate alaturi de autor, descriere,numele extensiei etc.

PLUGIN	DESCRIPTION
WSP Anti DDOS Deactivate plugin | Remove plugin	Monitors your website for DDOS attacks on pages. Version 1.0 | By Avadanei Andrei | Visit plugin site
WSP Antivirus Deactivate plugin | Remove plugin	Monitors your website for file infection with content (parasites) that hackers insert into benign web pages using various security holes. Version 1.0 | By Avadanei Andrei | Visit plugin site
Web Security Platform Attacker Cache Deactivate plugin | Remove plugin	Lorem ipsum Version 1.0 | By Avadanei Andrei | Visit plugin site
File Monitor Deactivate plugin | Remove plugin	Monitors your website for added/deleted/changed files. When a change is detected an email alert can be sent to a specified address. Version 1.0 | By Avadanei Andrei | Visit plugin site
Web Security Platform Global Attacks Protection Deactivate plugin | Remove plugin	Lorem ipsum dolor Lorem ipsum dolor Lorem ipsum dolor Lorem ipsum dolor Lorem ipsum dolor Lorem ipsum dolor Lorem ipsum dolor Version 1.0 | By Avadanei Andrei | Visit plugin site

Add new – ne ofera posibilitatea de a instala un plugin dintr-un folder local. Acesta trebuie sa fie valid din punctul de vedere al informatiilor puse la dispozitie, si sa se foloseasca de sablonul unui plugin deja existent.

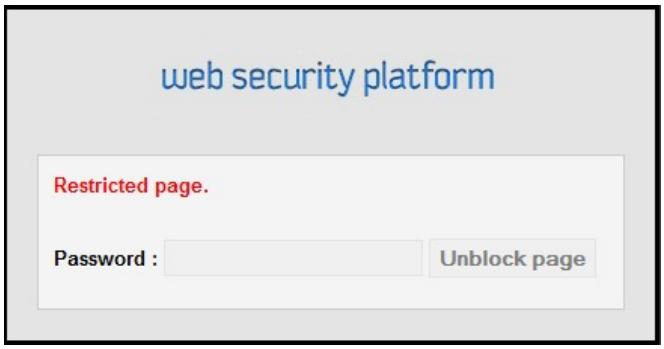
Settings

General Settings – reprezinta setarile generale ale platformei, acestea privesc starea platformei(activa/dezactivata) sau starea alertelor etc.

Restriction

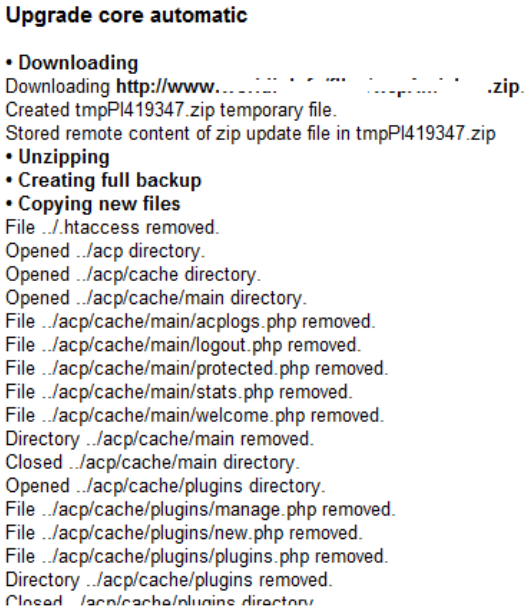
Manage ban list – reprezinta sistemul de restrictii pus la dispozitie de scheletul WSP. Avem posibilitatea de a bana un IP sau o clasa de IP-uri, momentan doar IP v4.Putem stabili durata cat va fi valabila restrictia, alaturi de motivul pentru care a fost luata decizia. Platforma pune la dispozitie si posibilitatea crearii unui White List, atunci cand dorim sa nu restrictionam accesul unor IP-uri sub nici o forma(spre exemplu IP-urile administratorilor).

File access Restriction – o alta facilitate extrem de utila a platformei. Spre exemplu suntem autentificati pe site intr-o sectiune mai sensibila si nu dorim sa ne delogam din aceasta.Platforma WSP ofera posibilitatea de a bloca accesul la pagina si a reactiva acesta doar prin introducerea unei singure parole. Acest sistem poate lucra si ca sistem de autentificare in diferite locatii ale unui site.



Tools

Update Core – singura aplicatie de la Tools pre-instalata este posibilitatea de a verifica daca exista sau nu o noua versiune a platformei. Daca o noua versiune este pusa la dispozitia platforma are posibilitatea de a instala automat.



In momentul in care un upgrade este facut, logurile arata ca in imaginea de mai sus, doar ca aceasta este doar o parte a lor.

Logout

Logout – va inchide sesiunea curenta

Prezentarea extensiilor – Web Security Platform

Tot ce a fost prezentat pana acum reprezinta toate facilitatile puse la dispozitie de denumirea generica a platformei : schelet. Platforma are o structura ce ii confera un dinamism foarte mare, aceasta putand fi dezvoltata de oricine are cunostinte ale structurii platformei si cunostinte in web development. Practic,toate sectiunile sistemului sunt incarcate prin doua modalitati : **default** , in pagina header.php din acp/cache/ sau **dinamic**, cu ajutorul extensiilor. Astfel, orice sectiune,meniu, pagina, poate primi alte pagini sau poate avea dependente. Motorul care pune in miscare toate aceste extensii si functii se bazeaza pe diverse actiuni pentru a alerta diversele aplicatii cand e momentul sa intre ele in joc.

In urmatoarele randuri vor fi prezentate in ordine aleatorie pluginurile ce fac din platforma Web Security Platform un sistem de securitate foarte util si puternic.Fiecare plugin va fi caracterizat prin actiunile la care ruleaza, bazele de date, precum si functiile si facilitatile lui alaturi de injectiile ce le face in panoul de administrare.

WSP Anti DDOS

Actiuni: DA

- init
- pre_start_platform
- post_end_platform

Injectii in ACP: DA

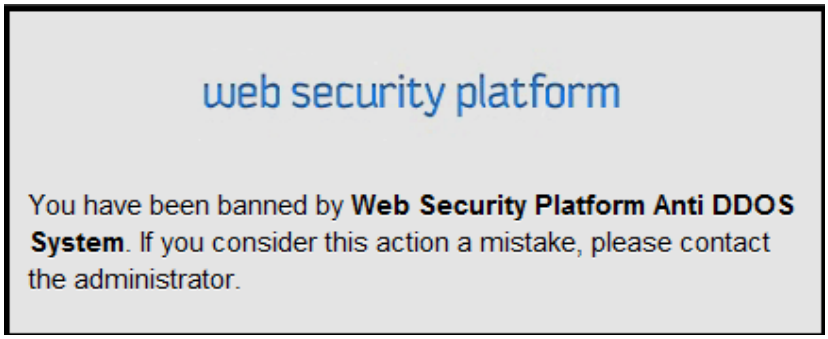
- Settings → Anti DDOS Settings

Baze de date: DA

- iplog

Descriere si prezentare :

Acest plugin reprezinta sistemul de protectie impotriva atacurilor de tip DDOS.Extensia contorizeaza numarul de cereri intr-un interval de timp specificat si configurabil in ACP, iar daca un utilizator depaseste aceasta limita este banat instantaneu de platforma in .htaccess daca are permisiuni de scriere, sau paginile vor primi die() in caz contrar.Platforma se foloseste de tabelul iplog pentru a stoca detaliile ce o ajuta sa stabileasca daca o adresa necesita blocarea accesului. In actiunea “init” isi initializeaza setarile, urmeaza “pre_start_platform” unde testeaza userul si in “post_end_platform” suprascrie contentul HTML generand mesajul de mai jos fortat.



WSP Attacker Cache

Actiuni: DA

- init
- pre_start_platform
- wsp_attack

Injectii in ACP: DA

- Settings → Cache System Setting
- Tools → Manage Attackers
- Tools → Manage Cache

Baze de date: DA

- cache

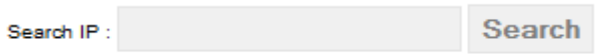
Dependente : DA

- WSP Global Attacks Protection

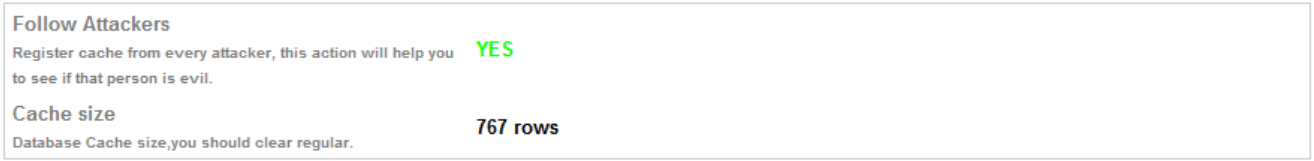
Descriere si prezentare :

Aceasta plugin reprezinta o extensie a unui plugin ce va fi prezentat mai jos (WSP Global Attacks Protection) si se declanseaza in momentul in care respectivul plugin detecteaza un atac web. WSP Attacker Cache reactioneaza la alertele declansate de pluginul de care depinde, activand sistemul de urmarire al unui atacator. Practic, acesta creaza log-uri pentru fiecare persoana care a fost considerata suspecta de celalalt sistem de protectie.Astfel vom avea garantia ca o data un personaj suspect va fi detectat, nu isi va reorganiza atacurile ca sa le poata da bypass la cele ale sistemelor de protectie WSP deoarece oricum toate actiunile lui viitoare vor fi memorate.Pentru site-urile mari trebuie sa aveti grija ca baza de date sa nu se incarce foarte mult. In Tools avem posibilitatea de a analiza Cache-ul atacatorilor, putand vedea toate variabilele de tip GET,POST,SERVER,COOKIE,SESSION care sunt declarate in cadrul unui log.

Extensia isi injecteaza setarile in Meniu → Settings → Cache System Settings iar in Tools cele doua sisteme de management : Tools → Manage Cache , unde avem posibilitatea sa cautam un IP in vederea logurilor sale, iar Tools → Manage Attackers e o injectie creata de WSP Global Attacks Protection. Astfel extensia noastra face o injectie la o injectie. In motorul clasei de protectie, aceasta executa sistemul de logare in actiunea “pre_start_platform” iar inregistrarea unui nou suspect se face imediat dupa ce pluginul de care depinde lanseaza actiunea “wsp_attack”.De aici vine si concluzia ca acest plugin depinde de un altul.



ATTACKER IP	DETECTED DATE	FOLLOW	ATTACKS SIZE	CACHE SIZE	ACTION	ACTION
127.0.0.1	Sat, 06 Feb 2010 15:37:35	YES	35	679	Stop following	Delete all cache



WSP Global Attacks Protection

Actiuni: DA

- init
- pre_start_platform
- scan_global

Injectii in ACP: DA

- Settings → [GAP] Main settings
- Settings → [GAP] Pattern settings
- Settings → [GAP] GVES settings
- Dashboard → Stats → Home
- Tools → Manage Attackers
- Tools → Manage Attacks

Baze de date: DA

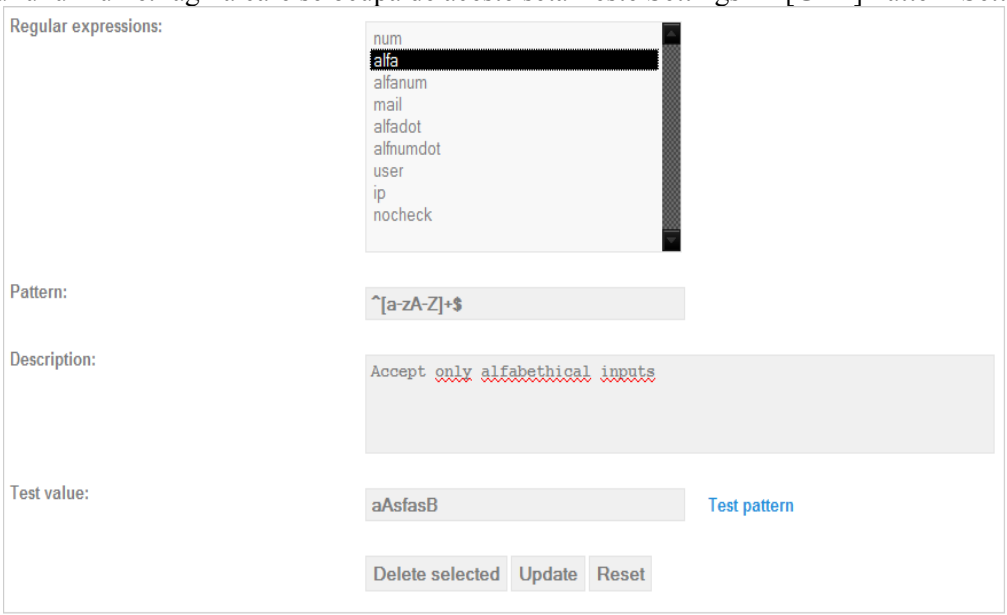
- patterns
- attackers
- attacks
- vectors
- excvars

Descriere si prezentare :

WSP Global Attacks Protection este unul din cele mai complexe extensii ale platformei WSP pana in acest moment, dupa cum observam si in analiza sumara de mai sus.Pluginul acesta este inima sistemului de protectie care are grija de tipurile cunoscute de atacuri web browser based. Practic, acest sistem incearca sa gaseasca si sa rezolve atacurile suspecte initiate de atacatori. Suporta detectarea Cross Side Scripting(XSS), Remote File Inclusion(RFI), Local File Inclusion (LFI),SQL Injection (SQLI), File Path Disclosure (FPD) , Cross Site Request Forgery(CSRF)[**neimplementat inca**] si Remote Code Execution(RCE).

Acesta analizeaza in functie de setari variabilele Globale precum : GET,POST,COOKIE,SESSION,SERVER cautand urme suspecte de atacuri. In cazul in care sunt descoperite, in functie de tipul de atac ce il considera acestea sunt patchuite, devenind inofensive pentru end-user si reducand riscurile de a obtine informatii private de pe urma mesajului malformat.

Pluginul se foloseste de diverse sabloane (expresii regulate de tip perl), care au o pondere diferita pentru a scana diversele variabile globale de orice gen.Aceste expresii pot fi personalizate pentru un management mai usor al lor, cu ajutorul unui nume.Pagina care se ocupa de aceste setari este Settings → [GAP] Pattern Settings .



Fiecare atac are lista lui, ce poate fi updatata de sabloane, cu diverse ponderi ce stabilesc ierarhia si importanta ce o vor avea in stabilirea statutului variabilei scanate : suspecta sau nu.

XSS Vectors :	22 vectors
SQLI Vectors :	11 vectors
RLFI Vectors :	12 vectors
RCE Vectors :	0 vectors
FPD Vectors :	0 vectors

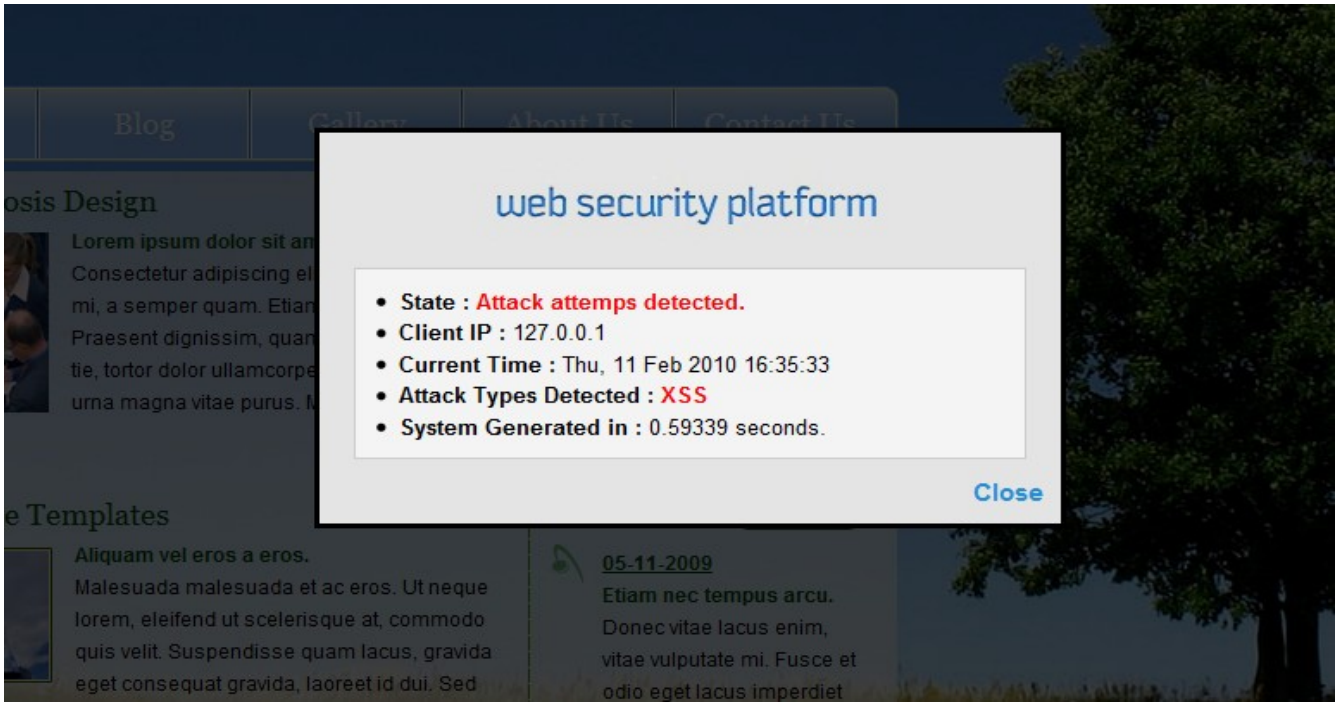
Deoarece acest sistem ar putea multe rezultate false-positive, pluginul are si suportul pentru exceptii.Astfel, poti sa stabilesti tu modul in care sunt scanate unele variabile. Spre exemplu, intr-o variabila asteptam sa fie introdus un e-mail. Alegem patternul e-mail pentru variabila respectiva si pentru pagina dorita si cream o exceptie.Aceasta va ignora restul sabloanelor si se va axa doar pe cele date in exceptii.

ID	PAGE	VARIABLE	PATTERN PROTECTION	EDIT	DELETE
1	/wspMain.php	$_POST[mail]	mail	Edit	

Imediat ce sistemul detecteaza ceva suspect, acesta va anunta atacatorul ca a fost inregistrat printr-un mesaj destul de finut, iar sistemul isi va face treaba mai departe : blocand variabila respectiva sau curatand-o de malware, adaugarea logurilor ce pot fi vizualizate in Tools → Manage Attacks si Tools → Manage Attackers.

ID	IP	BROWSER	TIME	PAGE	ATTACK TYPE	VARIABLE FOCUS	DELETE
1	127.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 6.1; ro; rv:1.	Thu, 11 Feb 2010 17:25:01	/demo/index.php	XSS	$_GET[test] = <script>alert(1)</script>	

ID	ATTACKER IP	DETECTED DATE	BANNED	ATTACKS SIZE	ACTIONS	EXTRA
1	127.0.0.1	Sat, 06 Feb 2010 15:37:35	NO	35	No action	Ban user



WSP File Monitor

Actiuni: DA

- init
- post_start_platform
- filemonitor_temp

Injectii in ACP: DA

- Settings → File Monitor settings
- Dashboard → Stats → File Monitor Alert

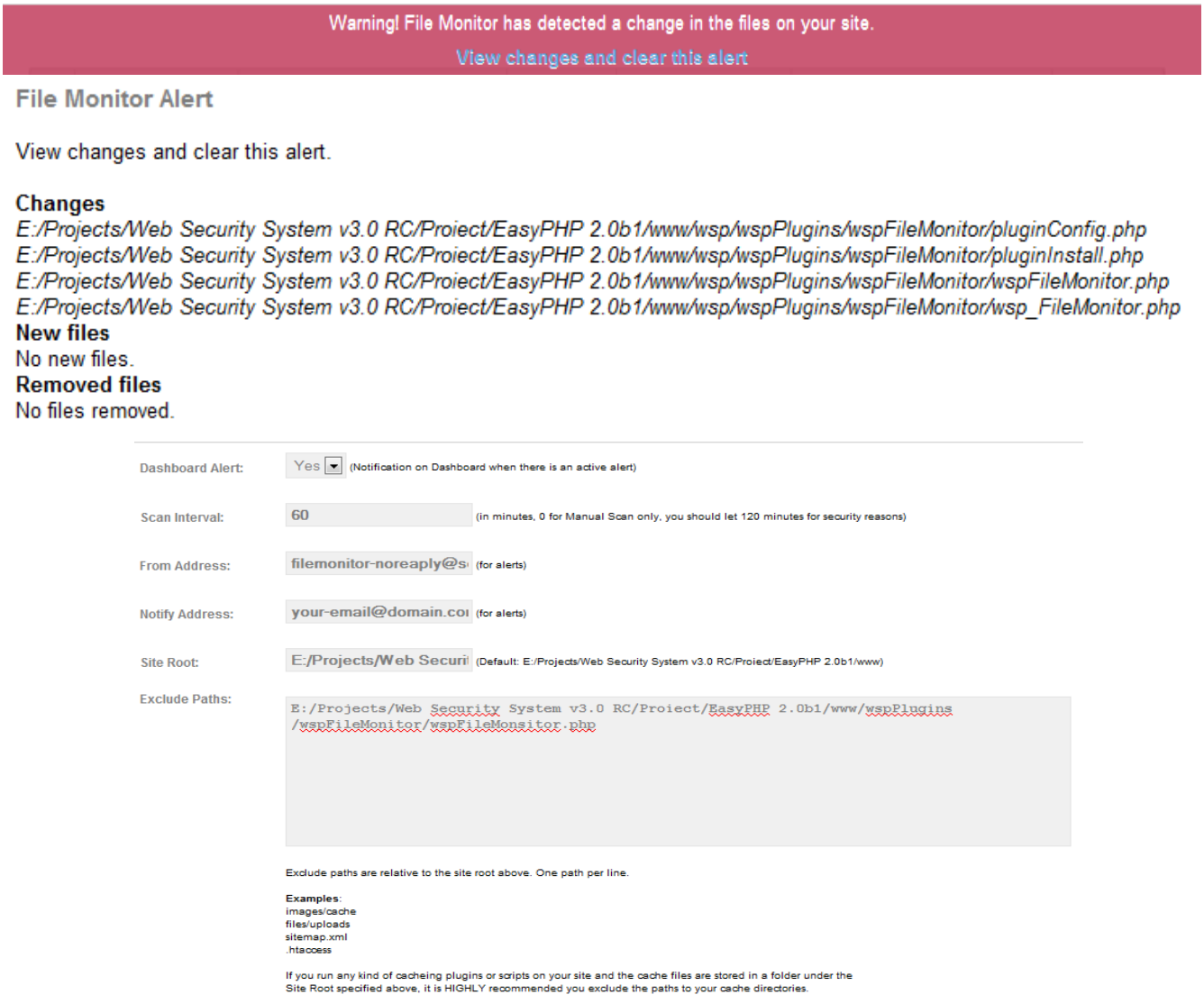
Baze de date: DA

- filemonitor

Descriere si prezentare :

WSP File Monitor este extensia care are grija de integritatea fisierelor. Este inutil sa ne avantam la diverse sisteme de securitate ce vizeaza atacurile web-based daca luam un virus care urca prin FTP diverse aplicatii malware,suprascrie si editeaza fisiere. Pluginul acesta urmareste toate aceste schimbari regulat,in functie de intervalul de scanare ce este setat. Pentru directoarele si fisierele care necesita modificari regulate ar fi inutil sa se fie urmarite (de exemplu cache, sitemap.xml etc.) deoarece la fiecare scanare va genera alerte si ar fi obositor pentru administratori.Extensia suporta si un sistem de alerta prin e-mail(**neimplementat**) in cazul in care apar modificari ,instiintandu-l pe administrator despre acest lucru.

Platforma injecteaza si pe pagina principala o alerta care se declanseaza doar in momentul in care acceseaza pagina unul din administratori si exista modificari ale fisierelor.



WSP Antivirus

Actiuni: DA

- init
- post_start_platform
- antivirus_temp

Injectii in ACP: DA

- Settings → Antivirus settings
- Dashboard → Stats → Antivirus Alert

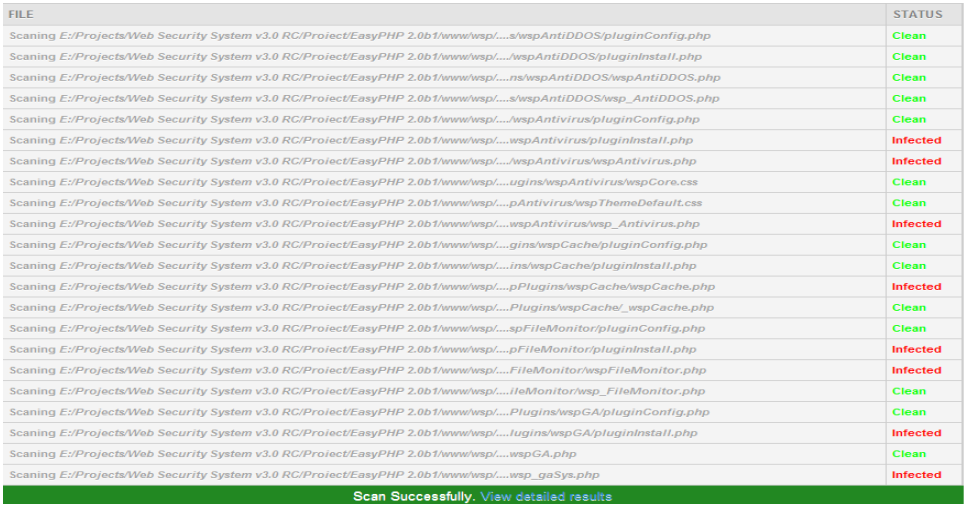
Baze de date: DA

- filemonitor

Descriere si prezentare :

WSP Antivirus este extensia care completeaza ideea pluginului WSP File Monitor. Aceasta va avea grija de diverse linii malware sa nu se gaseasca prin codul fisierelor site-ului. Interfata si setarile sunt extrem de asemanatoare, extensia creand o alerta in Dashboard → Stats daca detecteaza fisiere suspecte. Platforma are posibilitatea de a adauga semnaturi care sunt considerate malware sau domenii de site-uri suspecte. De asemenea, daca apar rezultate false-positive, poti adauga una din liniile unui fisier considerat suspect la exceptii iar linia respectiva nu va mai fi reevaluata decat in urma schimbarii hashului ei.De asemenea, pluginul se injecteaza in codul HTML ,analizandu-l si cautand injectii de iframe-uri, javascript, sau orice cod suspect si care nu respecta normele de securitate.(**neimplementat)**.Atat semnaturile cat si domeniile pot fi adaugate atat de utilizator cat si la viitoarele update-uri ale pluginului.

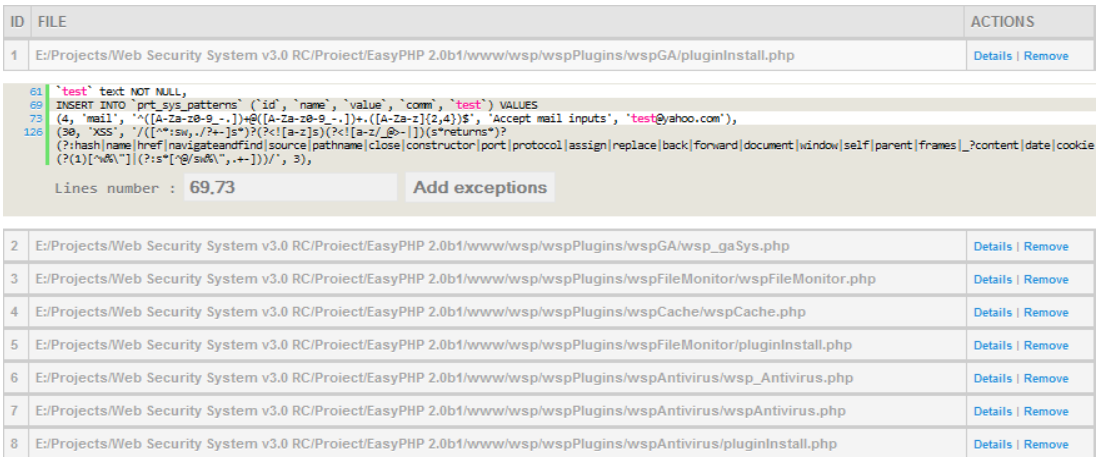
Exemplul de mai jos a cautat in rezultate principalele functii ale virusilor cat si o semnatura denumita sugestiv “test”.



FILE	STATUS
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....s/wspAntiDDOS/pluginConfig.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/..../wspAntiDDOS/pluginInstall.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....ns/wspAntiDDOS/wspAntiDDOS.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....s/wspAntiDDOS/wsp_AntiDDOS.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/..../wspAntivirus/pluginConfig.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....wspAntivirus/pluginInstall.php	Infected
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/..../wspAntivirus/wspAntivirus.php	Infected
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....ugins/wspAntivirus/wspCore.css	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....pAntivirus/wspThemeDefault.css	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....wspAntivirus/wsp_Antivirus.php	Infected
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....gins/wspCache/pluginConfig.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....ins/wspCache/pluginInstall.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....pPlugins/wspCache/wspCache.php	Infected
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....Plugins/wspCache/_wspCache.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....spFileMonitor/pluginConfig.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....pFileMonitor/pluginInstall.php	Infected
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....FileMonitor/wspFileMonitor.php	Infected
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....ileMonitor/wsp_FileMonitor.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....Plugins/wspGA/pluginConfig.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....lugins/wspGA/pluginInstall.php	Infected
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....wspGA.php	Clean
Scaning E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/....wsp_gaSys.php	Infected

Scan Successfully. View detailed results

.



ID	FILE	ACTIONS
1	E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/wspPlugins/wspGA/pluginInstall.php	Details | Remove

```
61  `test` text NOT NULL,
69  INSERT INTO `prt_sys_patterns` (`id`, `name`, `value`, `comm`, `test`) VALUES
73  (4, 'mail', '^([A-Za-z0-9_-.])+@([A-Za-z0-9_-.])+.([A-Za-z]{2,4})$', 'Accept mail inputs', 'test@yahoo.com'),
126 (30, 'XSS', '/([^":sw,./?+-]s*)?(?<![a-z]s)(?<![a-z/_@>-|])(s*returns*)?
    (?:hash|name|href|navigateandfind|source|pathname|close|constructor|port|protocol|assign|replace|back|forward|document|window|self|parent|frames|_?content|date|cookie
    (?(1)[^s&\"]|(?:s*[^@/sw&\",.+-]))/', 3),
```

Lines number : 69,73 Add exceptions

2	E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/wspPlugins/wspGA/wsp_gaSys.php	Details | Remove
3	E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/wspPlugins/wspFileMonitor/wspFileMonitor.php	Details | Remove
4	E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/wspPlugins/wspCache/wspCache.php	Details | Remove
5	E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/wspPlugins/wspFileMonitor/pluginInstall.php	Details | Remove
6	E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/wspPlugins/wspAntivirus/wsp_Antivirus.php	Details | Remove
7	E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/wspPlugins/wspAntivirus/wspAntivirus.php	Details | Remove
8	E:/Projects/Web Security System v3.0 RC/Proiect/EasyPHP 2.0b1/www/wsp/wspPlugins/wspAntivirus/pluginInstall.php	Details | Remove

TO DO

Deoarece timpul nu mi-a permis sa implementez toate facilitatile platformei am decis sa le prezint aici in concept pe cele care vor fi prezente pana la etapa finala in cazul in care sunt acceptat.

Auto-Installer – Alaturi de instalarea manuala, la partea de instalare am precizat si de un sistem care nu este activat in platforma pentru a instala automat platforma in diversele fisiere PHP.Aceasta va analiza fisierele si va incerca sa le gaseasca pe cele care nu au nici un sistem de protectie si sa sugereze instalarea WSP pe ele. Daca acest lucru nu este posibil, platforma va sugersa sa treceti la versiunea manuala de instalare.
E-mail suport – Deoarece doua dintre extensii necsita suport pentru e-mail voi pregati si clasa de e-mail pentru SMTP si astfel voi activa si cele doua facilitati ale WSP File Monitor si WSP Antivirus pentru alertare.
CSRF protection – acesta este singurul tip de atac care nu are nici un mod de protectie. Pentru acesta este nevoie de niste injectii in formularele unei pagini care ne vor asigura validitatea lor si siguranta ca nu sunt bypassed de diverse sisteme de iframeuri.De asemenea va trebui sa am grija ca acest sistem sa nu perturbe buna circulatie a site-ului protejat.
Adaugarea de noi sabloane – la unele atacuri care inca nu am reusit sa le creez expresiile regulate pentru detectie. De asemenea unele din cele de la XSS/SQLI vor trebui imbunatatite.
Rezolvarea unor buguri – exista cateva buguri care nu am reusit sa le repar inca, prezente prin motorul platformei.
Crearea unei baze de date pentru antivirus – in acest moment existand doar sistemul si posibilitatea de a adauga exemple pentru a testa.
Finalizarea sistemului WSP Antivirus – Aici exista mici probleme deoarece inca nu analizeaza pagina in timp real pentru a elimina tagurile suspecte.Spre exemplu trebuie sa caute injectii de javascript suspecte,cod HTML in afara tagurilor etc.

Concluzii – Web Security Platform

Am ajuns la capat de drum, deci cred ca ar fi potrivit sa tragem niste concluzii. Internetul si site-urile web de orice natura prezinta diverse nivele de credibilitate, dar aceasta este doar o aparenta deoarece cu cat au credibilitate mai mare cu atat se afla unui risc mai mare datorat numarul ridicat de vizitatori, care probabil sufera de dorinta de a se afirma prin metode non-etice.
De aceea noi trebuie sa fim cu un pas inaintea lor si sa dezvoltam diverse aplicatii care reduc si mai mult riscul la care ne sunt supuse site-urile. Trebuie sa avem in vedere ca site-urile noastre au o credibilitate,ce poate fi destramata in cateva secunde.Impactul poate dramatic si poate duce la “falimentul” proiectului respectiv. Una din alternativele cele mai indicate pentru acest gen de actiuni este **Web Security Platform**, platforma ce inglobeaza multe sisteme mici si eficiente, formand o aplicatie All in One completa si complexa pentru aproape orice gen de surprize neplacute.