OXYGEN
CONSULTING SERVICES
PROGRAMMED FOR PROGRESS

Application Security Flaws, threats and vulnerabilities

Sanjiv Agarwala
CISSP,CISA,CISM,CGEIT,ITIL,MBCI,ISO27001,ISO9001
Director, Trainer and Principal Consultant
Oxygen Consulting Services Pvt. Ltd.
sanjiv.agarwala@o2csv.com
ska262001@yahoo.co.in

Session Topics:

Application and Network threats and vulnerabilities:
Malware, Virus,
Worms, Trojans,
Phishing, Social Engineering,
Mail Attachment,
Personal firewall (zone alarm),
Antivirus

Computer virus and other malicious programs:

A computer virus is a computer program that can replicate itself and spread from one computer to another. This is part of category of programs known as malware, that are software code written for the purpose of causing harm to system and its data.

Viruses attack four parts of the computer:

1. Executable program files
2. The file directory system, which tracks the location of all the computer's files
3. Boot and system areas, which are needed to start the computer
4. Data files

Another variant of a virus frequently encountered is a worm, which, unlike a virus, does not physically attach itself to another program.

To propagate itself to the host systems, a worm typically exploits security weaknesses in operating system configuration.

Virus and worms are easily transmitted

- From downloading files to computers' web browsers
- Attachments to email, so that when the attachment opens, the system becomes infected if not protected
- Files received through other online services
- From sites claiming to be free software, audio and videos etc

How the virus protection works:

Antivirus – policies and procedures

How it works – signature database updated with virus signatures and updated on our systems

Controlling computer virus:

Antivirus management
User awareness
Controlling other malicious programs

Procedures to control virus:

1. Build system from original, clean master copies. Boot only from original media whose write protection has always been in place, if applicable.
2. Scan CD, USB and other electronic media before used on the system
3. Update virus software scanning definitions/signatures frequently.
4. Scan shareware before using them
5. Ensure a sound and effective backup plan is in place
6. Educate users. Hackers relies upon social engineering tactics in getting the user to open the attachment

Social Engineering:

Social engineering, in the context of security, is understood to mean the art of manipulating people into performing actions or divulging confidential information.

While it is similar to a confidence trick or simple fraud, it is typically trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.

"Social engineering" as an act of psychological manipulation had previously been associated with the social sciences, but its usage has caught on among computer professionals.

Phising:

Phishing is a technique of fraudulently obtaining private information.

Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN.

Phone Phising (Vishing):
Phone phishing is also called vishing.

This technique uses a rogue Interactive voice response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted (typically via a phishing e-mail) to call in to the "bank" via a (ideally toll free) number provided in order to "verify" information. A typical system will reject log-ins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems transfer the victim to the attacker posing as a customer service agent for further questioning.

One could even record the typical commands ("Press one to change your password, press two to speak to customer service" ...) and play back the direction manually in real time, giving the appearance of being an IVR without the expense.

Personal Firewall:

A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Typically it works as an application layer firewall.

A personal firewall differs from a conventional firewall in terms of scale. A personal firewall will usually protect only the computer on which it is installed, as compared to a conventional firewall which is normally installed on a designated interface between two or more networks, such as a router or proxy server.

Hence, personal firewalls allow a security policy to be defined for individual computers, whereas a conventional firewall controls the policy between the networks that it connects.

Personal Firewall features:

- Protects the user from unwanted incoming connection attempts
- Alert the user about outgoing connection attempts
- Allows the user to control which programs can and cannot access the local network and/or Internet
- Hide the computer from port scans by not responding to unsolicited network traffic
- Monitor applications that are listening for incoming connections
- Monitor and regulate all incoming and outgoing Internet users
- Prevent unwanted network traffic from locally installed applications
- Provide the user with information about an application that makes a connection attempt
- Provide information about the destination server with which an application is attempting to communicate

ZoneAlarm Personal Firewall:

ZoneAlarm is a personal firewall software application originally developed by Zone Labs, which was acquired in March 2004 by Check Point. It includes an inbound intrusion detection system, as well as the ability to control which programs can create outbound connections. As of June 2011, the newest release is ZoneAlarm Extreme Security 2012. ZoneAlarm was formerly known as Zone Labs.

***** ZoneAlarm Free Firewall: A freeware version that includes a web and local network personal firewall with outbound program control and port stealthing. It is distributed through Download.com.[4]**

***** ZoneAlarm Free Antivirus + Firewall: A freeware version that includes an award-winning Two-Way Firewall, Advanced Firewall, Advanced Download Protection, and Identity Protection, and antivirus protection provided by Kaspersky Labs.**

How ZoneAlarm Works:

In ZoneAlarm, program access is controlled by way of "zones", into which all network connections are divided. The "trusted zone" generally includes the user's local area network and can share resources such as files and printers, while the "Internet zone" includes everything not in the trusted zone.

The user can specify which "permissions" (trusted zone client, trusted zone server, Internet zone client, Internet zone server) to give to a program before it attempts to access the Internet (e.g. before running it for the first time) or, alternatively, ZoneAlarm will ask the user to give the program permission on its first access attempt.

Session Topics:

Web Application Security Flaws:
Injection Flaws
Cross Site Scripting (XSS)
Malicious File Execution
Insecure Direct Object Reference
Cross Site Request Forgery (CSRF)
Information Leakage and Improper Error Handling
Broken Authentication and Session Management
Insecure Cryptographic Storage
Insecure Communications
Failure to Restrict URL Access

Injection Flaws

Injection means…

- Tricking an application into including unintended commands in the data sent to an interpreter

Interpreters…

- Take strings and interpret them as commands
- SQL, OS Shell, LDAP, XPath, Hibernate, etc…

SQL injection is still quite common

- Many applications still susceptible (really don't know why)
- Even though it's usually very simple to avoid

Typical Impact

- Usually severe. Entire database can usually be read or modified
- May also allow full database schema, or account access, or even OS level access

Source: OWASP

Cross-site Scripting

Occurs any time…

- Raw data from attacker is sent to an innocent user’s browser

Raw data…

- Stored in database
- Reflected from web input (form field, hidden field, URL, etc…)
- Sent directly into rich JavaScript client

Virtually every web application has this problem

- Try this in your browser – javascript:alert(document.cookie)

Typical Impact

- Steal user’s session, steal sensitive data, rewrite web page, redirect user to phishing or malware site
- Most Severe: Install XSS proxy which allows attacker to observe and direct all user’s behavior on vulnerable site and force user to other sites

Source: OWASP

Broken Authentication and Session Management:

HTTP is a “stateless” protocol

- Means credentials have to go with every request
- Should use SSL for everything requiring authentication

Session management flaws

- SESSION ID used to track state since HTTP doesn’t
  - and it is just as good as credentials to an attacker
- SESSION ID is typically exposed on the network, in browser, in logs, …

Beware the side-doors

- Change my password, remember my password, forgot my password, secret question, logout, email address, etc…

Typical Impact

- User accounts compromised or user sessions hijacked

Source: OWASP

Insecure Direct Object References:

How do you protect access to your data?

- This is part of enforcing proper "Authorization", along with A7 – Failure to Restrict URL Access

A common mistake …

- Only listing the 'authorized' objects for the current user, or
- Hiding the object references in hidden fields
- … and then not enforcing these restrictions on the server side
- This is called presentation layer access control, and doesn't work
- Attacker simply tampers with parameter value

Typical Impact

- Users are able to access unauthorized files or data

Source: OWASP

Internal Controls

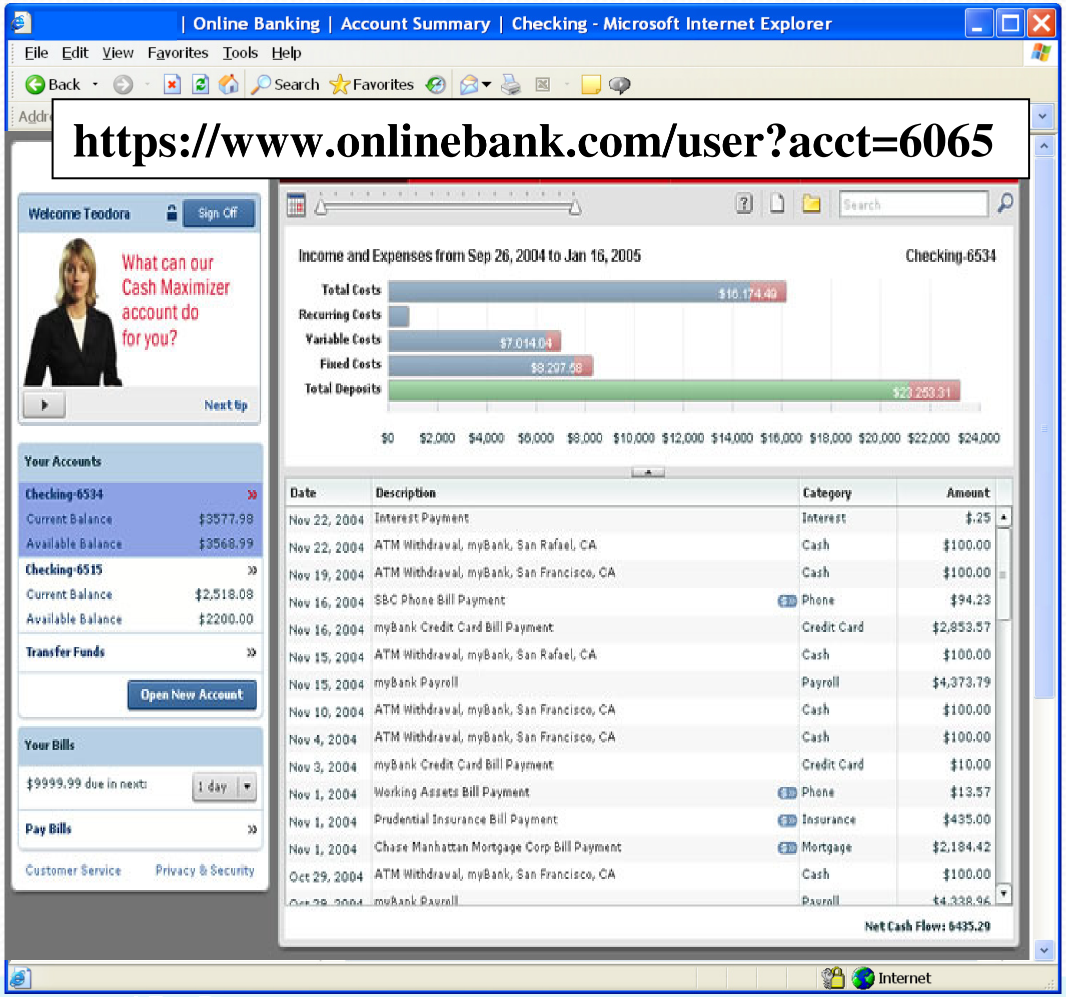
Policies, procedures, practices and organizational structures implemented to reduce risks

Internal controls are developed to provide reasonable assurance that an organization’s business objectives will be achieved and undesired risk events will be prevented, or detected and corrected, based on either compliance or management-initiated concerns.

Control is the means by which control objectives are addressed. Internal control activities and supporting processes are either manual or driven by automated computer information resources. They operate at all levels within an organization to mitigate its exposures to risks that potentially could prevent it from achieving its business objectives.

The board of directors and senior management are responsible for establishing the appropriate culture to facilitate an effective and efficient internal control system.

Insecure Direct Object References Illustrated



https://www.onlinebank.com/user?acct=6065

Income and Expenses from Sep 26, 2004 to Jan 16, 2005

Checking-6534

Your Accounts

Checking-6534	»
Current Balance	$3577.98
Available Balance	$3568.99
Checking-6515	»
Current Balance	$2,518.08
Available Balance	$2200.00
Transfer Funds	»

Open New Account

Your Bills

$9999.99 due in next: 1 day

Pay Bills »

Customer Service Privacy & Security

Date	Description	Category	Amount
Nov 22, 2004	Interest Payment	Interest	$.25
Nov 22, 2004	ATM Withdrawal, myBank, San Rafael, CA	Cash	$100.00
Nov 19, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	$100.00
Nov 16, 2004	SBC Phone Bill Payment	Phone	$94.23
Nov 16, 2004	myBank Credit Card Bill Payment	Credit Card	$2,853.57
Nov 15, 2004	ATM Withdrawal, myBank, San Rafael, CA	Cash	$100.00
Nov 15, 2004	myBank Payroll	Payroll	$4,373.79
Nov 10, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	$100.00
Nov 4, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	$100.00
Nov 3, 2004	myBank Credit Card Bill Payment	Credit Card	$10.00
Nov 1, 2004	Working Assets Bill Payment	Phone	$13.57
Nov 1, 2004	Prudential Insurance Bill Payment	Insurance	$435.00
Nov 1, 2004	Chase Manhattan Mortgage Corp Bill Payment	Mortgage	$2,184.42
Oct 29, 2004	ATM Withdrawal, myBank, San Francisco, CA	Cash	$100.00
Oct 29, 2004	myBank Payroll	Payroll	$4,338.96

Net Cash Flow: 6435.29

- Attacker notices his acct parameter is 6065

  ?acct=6065

- He modifies it to a nearby number

  ?acct=6066

- Attacker views the victim's account information

Cross-site Request Forgery:

Cross Site Request Forgery

- An attack where the victim's browser is tricked into issuing a command to a vulnerable web application
- Vulnerability is caused by browsers automatically including user authentication data (session ID, IP address, Windows domain credentials, ...) with each request

Imagine...

- What if a hacker could steer your mouse and get you to click on links in your online banking application?
- What could they make you do?

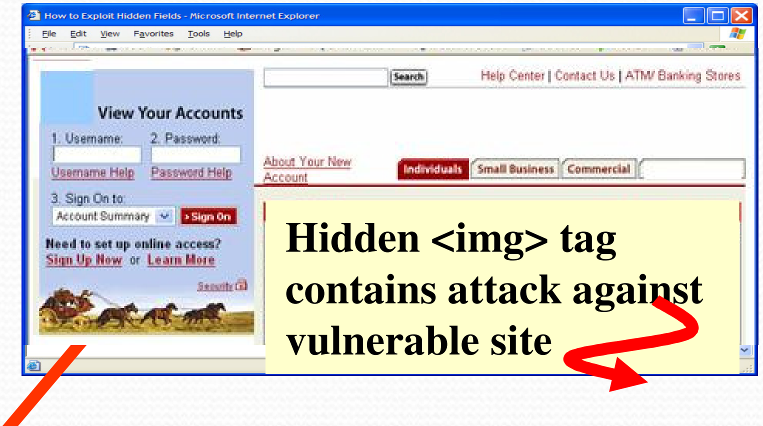
Typical Impact

- Initiate transactions (transfer funds, logout user, close account)
- Access sensitive data
- Change account details

Source: OWASP

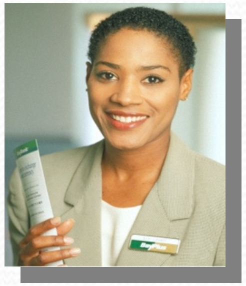
CSRF Illustrated

1 Attacker sets the trap on some website on the internet (or simply via an e-mail)


How to Exploit Hidden Fields - Microsoft Internet Explorer
File Edit View Favorites Tools Help
View Your Accounts
1. Username:
2. Password:
Username Help
Password Help
3. Sign On to:
Account Summary
Sign On
Need to set up online access?
Sign Up Now or Learn More
Security
Search
Help Center | Contact Us | ATM/ Banking Stores
About Your New Account
Individuals
Small Business
Commercial

Hidden <img> tag contains attack against vulnerable site

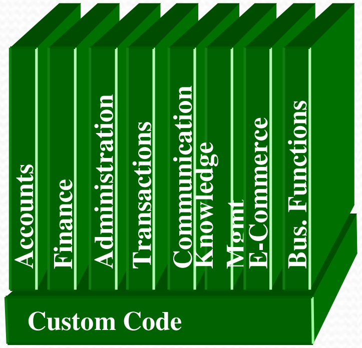
2 While logged into vulnerable site, victim views attacker site



How to Exploit Hidden Fields - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost/WebGoat/attack?Screen=6&menu=51
Go
Logout
How to Exploit Hidden Fields
OWASP WebGoat V4
Hints
Show Params
Show Cookies
Show Java
Lesson Plans
Admin Functions
General
Broken Authentication and Session Management
Broken Access Control
Cross-Site Scripting (XSS)
Unvalidated Parameters
How to Exploit Hidden Fields
How to Bypass Client Side JavaScript Validation
How to Exploit Unchecked Email
Insecure Storage
Injection Flaws
Improper Error Handling
Code Quality
Challenge

<img> tag loaded by browser – sends GET request (including credentials) to vulnerable site

Application with CSRF vulnerability



3 Vulnerable site sees legitimate request from victim and performs the action requested

Security misconfigurations:

Web applications rely on a secure foundation

- Everywhere from the OS up through the App Server
- Don't forget all the libraries you are using!!

Is your source code a secret?

- Think of all the places your source code goes
- Security should not require secret source code

CM must extend to all parts of the application

- All credentials should change in production

Typical Impact

- Install backdoor through missing OS or server patch
- XSS flaw exploits due to missing application framework patches
- Unauthorized access to default accounts, application functionality or data, or unused but accessible functionality due to poor server configuration

Source: OWASP

Insecure Cryptographic Storage:

Storing sensitive data insecurely

- Failure to identify all sensitive data
- Failure to identify all the places that this sensitive data gets stored
  - Databases, files, directories, log files, backups, etc.
- Failure to properly protect this data in every location

Typical Impact

- Attackers access or modify confidential or private information
  - e.g, credit cards, health care records, financial data (yours or your customers)
- Attackers extract secrets to use in additional attacks
- Company embarrassment, customer dissatisfaction, and loss of trust
- Expense of cleaning up the incident, such as forensics, sending apology letters, reissuing thousands of credit cards, providing identity theft insurance
- Business gets sued and/or fined

Source: OWASP

Failure to restrict URL Access:

How do you protect access to URLs (pages)?

- This is part of enforcing proper "authorization", along with A4 – Insecure Direct Object References

A common mistake …

- Displaying only authorized links and menu choices
- This is called presentation layer access control, and doesn't work
- Attacker simply forges direct access to 'unauthorized' pages

Typical Impact

- Attackers invoke functions and services they're not authorized for
- Access other user's accounts and data
- Perform privileged actions

Source: OWASP

Insufficient Transport Layer Protection:

Transmitting sensitive data insecurely

- Failure to identify all sensitive data
- Failure to identify all the places that this sensitive data is sent
  - On the web, to backend databases, to business partners, internal communications
- Failure to properly protect this data in every location

Typical Impact

- Attackers access or modify confidential or private information
  - e.g, credit cards, health care records, financial data (yours or your customers)
- Attackers extract secrets to use in additional attacks
- Company embarrassment, customer dissatisfaction, and loss of trust
- Expense of cleaning up the incident
- Business gets sued and/or fined

Source: OWASP

Unvalidated redirects and forwards:

Web application redirects are very common

- And frequently include user supplied parameters in the destination URL
- If they aren't validated, attacker can send victim to a site of their choice

Forwards (aka Transfer in .NET) are common too

- They internally send the request to a new page in the same application
- Sometimes parameters define the target page
- If not validated, attacker may be able to use unvalidated forward to bypass authentication or authorization checks

Typical Impact

- Redirect victim to phishing or malware site
- Attacker's request is forwarded past security checks, allowing unauthorized function or data access

Source: OWASP

References and links to additional reading:

1. www.owasp.org

2. www.isaca.org

3. www.zonealarm.com

Application Security Flaws, threats and vulnerabilities

Sanjiv Agarwala
CISSP,CISA,CISM,CGEIT,ITIL,MBCI,ISO27001,ISO9001
Director, Trainer and Principal Consultant
Oxygen Consulting Services Pvt. Ltd.
sanjiv.agarwala@o2csv.com
ska262001@yahoo.co.in