Website Security

Peter Muia

KENET 22/08/2013

WLAN & BMO Training

Web Security threats

- emergence of Web 2.0, increased information sharing through social networking and increasing business adoption of the means of doing business and delivering service,
- websites are often attacked directly. Hackers either seek to compromise the corporate network or the end-users accessing the website
- As a result, industry is paying increased attention to the security of the web applications themselves in addition to the security of the underlying computer network and operating systems

Web Security Threats

- The majority of web application attacks occur through cross-site scripting (XSS) and SQL injection attacks
- Result from flawed coding, and failure to sanitize input to and output from the web application.

Cross-site scripting

- Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications.
- XSS enables attackers to inject client-side script into Web pages viewed by other users.
- A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.
- Their effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

Cross-site scripting - Types

- The ***non-persistent*** cross-site scripting vulnerability is by far the most common type.
  - A non persistent attack is typically delivered via email or a neutral web site. The bait is an innocent-looking URL, pointing to a trusted site but containing the XSS vector. If the trusted site is vulnerable to the vector, clicking the link can cause the victim's browser to execute the injected script.
- The **persistent** cross-site scripting vulnerability occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing

SQL injection

- **SQL injection** is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.
- SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Denial-of-service attack

- In computing, a **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a machine or network resource unavailable to its intended users.
- Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.
- Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers
- One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable

Handling Denial of Service Attack

- Firewalls
- Switches
- Routers
- Application front end hardwar
- IPS based prevention
- DDS based defense
- Blackholing and sinkholing

Arbitrary code execution

- used to describe an attacker's ability to execute any commands of the attacker's choice on a target machine or in a target process.
- The attacker can potentially take complete control over the machine the process is running on.
- Once the invader can execute arbitrary code directly on the OS, there is often an attempt at a privilege escalation exploit in order to gain additional control.
- This may involve the kernel itself or an account such as Administrator, SYSTEM, or root. With or without this enhanced control, exploits have the potential to do severe

Data breach

- A **data breach** is the intentional or unintentional release of secure information to an untrusted environment.
- Other terms for this phenomenon include **unintentional information disclosure**, **data leak** and also **data spill**. Incidents range from concerted attack by black hats with the backing of organized crime or national governments to careless disposal of used computer equipment or data storage media.

File inclusion vulnerability

- **Remote File Inclusion** (RFI) is a type of vulnerability most often found on websites.
- It allows an attacker to include a remote file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity, to list a few it can lead to:
  - Code execution on the web server
  - Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS).
  - Denial of Service (DoS)
  - Data Theft/Manipulation

- And Many others

Ensure your website is secure

- While security is fundamentally based on people and processes, there are a number of technical solutions to consider when designing, building and testing secure web applications. At a high level, these solutions include:

Black Box Testing

- where an ethical hacker has no knowledge of the system being attacked. The goal of a black-box penetration test is to simulate an external hacking or cyber warfare attack.
  - Web application security scanners
  - vulnerability scanners
  - penetration testing

Web application security scanner

- A **web application security scanner** is a program which communicates with a web application through the web front-end in order to identify potential security vulnerabilities in the web application and architectural weaknesses.
- It performs a black-box test.
- don't have access to the source code and therefore detect vulnerabilities by actually performing attacks.

Example of free Web Scanners

- Nikto
- Paros
- WebScarab

Vulnerability scanner

- A **vulnerability scanner** is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.
- There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets.
- While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the

Vulnarability Scanner Examples

- Port scanner ex: Nmap, Nessus
- Network enumerator
- Network vulnerability scanner ex: BoomScan
- Web application security scanner
- Database security scanner
- ERP security scanner
- Computer worm

Port scanner

- A **port scanner** is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

Other Mechanism

- White Box testing tools such as static source code analyzers FuzzingTools used for input testing Web application firewalls (WAF) used to provide firewall-type protection at the web application layer Password cracking tools for testing password strength and implementation

Penetration test

- A **penetration test**, occasionally **pentest**, is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats. The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures

Penetration Testing

- Penetration tests are valuable for several reasons:[
  - Determining the feasibility of a particular set of attack vectors
  - Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence
  - Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
  - Assessing the magnitude of potential business and operational impacts of successful attacks
  - Testing the ability of network defenders to successfully detect and respond to the attacks
  - Providing evidence to support increased investments in security personnel and technology

Penetration Testing Tools

- Metasploit
- w3af
- Nessus
- Retina Network Security Scanner

Ways To Beef Up Your Website Security

- Keep Your Versions Updated
- Beef Up Your Passwords
- Lock Down Your File Permissions
- Mind Your Links
- Use FTPS For Transfers
- Use SSL To Send Emails
- Known Web Security Vulnerabilities and Unknown Vulnerabilities
- File uploads
- SSL