Lesson 7: WEB APPLICATION SECURITY - INTRODUCTION TO SQL INJECTION TECHNIQUES

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Chema Alonso
chema@informatica64.com

Informática 64
Microsoft MVP en Enterprise Security

Video intypedia007en © intypedia 2011 Creative Commons

Security Incidents I: Kaspersky

ChannelWeb

Home | Communities | News

You are not logged into Cha

News | Reviews | Research | Tools | The IT Channel | Networking | Security | Storage

NEW ON CHANNELWEB

- Tech Innovator Winning Products
- Top 100 Executives
- Sign Up For Partner Programs 2010
- Sign Up For Distribution Chiefs 2010
- Sign Up For Channel Chiefs 2010
- FUDWatch Blog
- Coming Up: Women of the Channel Winter Workshop
- Annual Report Cards
- Tech Books Online
- Subscribe to CRN

FEATURED VIDEO

Kaspersky Web Site Hacked With SQL Injection

By Stefanie Hoffman, ChannelWeb
7:51 PM EST lun. feb. 09, 2009

Discuss This

A security vulnerability in Moscow-based Kaspersky Lab's U.S. Web site was made public after a hacker launched a SQL attack and posted listings of tables contained on the security company's site.

The hacker, known as Unu, posted screen shots as well as a list of tables Feb. 7 to a blog after hacking into the security company's Web site via a simple SQL injection attack that allowed information to be exposed by entering secret username and password information.

"Kaspersky is one of the leading companies in the security and antivirus market. It seems as though they are not able to secure their own databases," the hacker said on a hackerblog.org posting. "Alter one of the parameters and you have access to EVERYTHING: users, activation codes, lists of bugs, admins, shop, etc."

Video intypedia007en © intypedia 2011 Creative Commons

Security Incidents II: NASA

SC Magazine Virtual Symposium: Botnets

Home > News > NASA sites hacked via SQL injection

NASA sites hacked via SQL injection

Angela Moscaritolo December 07, 2009

PRINT EMAIL REPRINT PERMISSIONS FONT SIZE: A | A | A

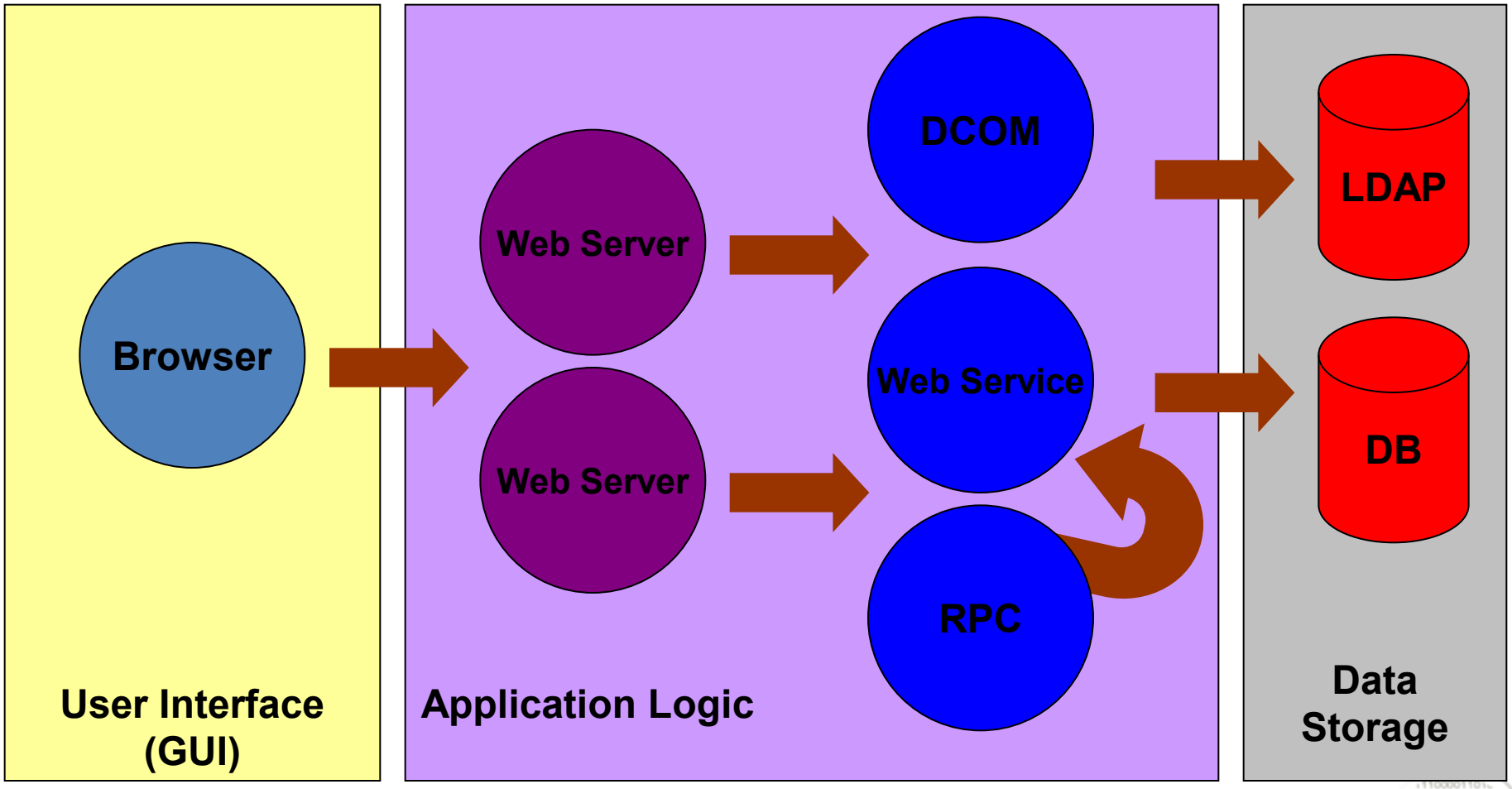
Two NASA sites recently were hacked by an individual wanting to demonstrate that the sites are susceptible to SQL injection.

The websites for NASA's Instrument Systems and Technology Division and Software Engineering Division were accessed by a researcher, who posted to his blog screen shots taken during the hack.

The researcher, using the alias "c0de.breaker," used SQL injection to hijack the sites, Gunter Ollmann, VP of research at security firm Damballa, who recently wrote about the hack, told SCMagazineUS.com on Monday.

Video intypedia007en © intypedia 2011 Creative Commons

Architecture of a Web Application



Video intypedia007en © intypedia 2011 Creative Commons

OWASP Top 10

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross-Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross-Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

Video intypedia007en © intypedia 2011 Creative Commons

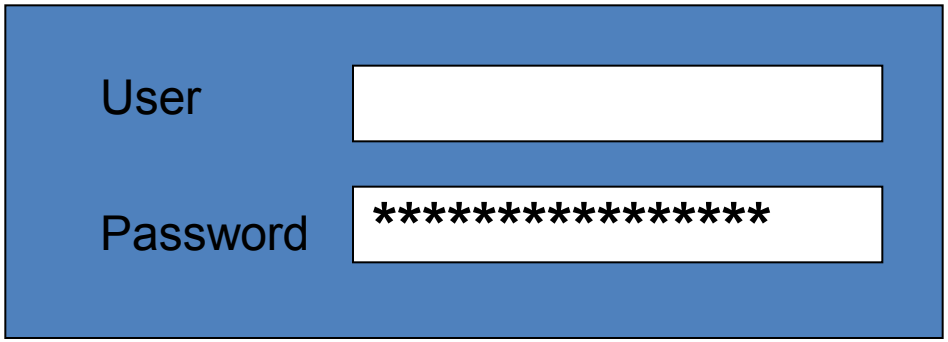
Code Injection

- Applications with poor data input verification
  - User data
    - Forms
    - Cookies
    - ….
  - Data from procedure calls
    - Links
    - Function Scripts
    - Actions
    - …
- User data used in database queries
- Poor construction of queries into databases
- Attacks
  - SQL Injection, LDAP Injection, Xpath Injection
  - ….

Video intypedia007en © intypedia 2011 Creative Commons

Code Injection: Example

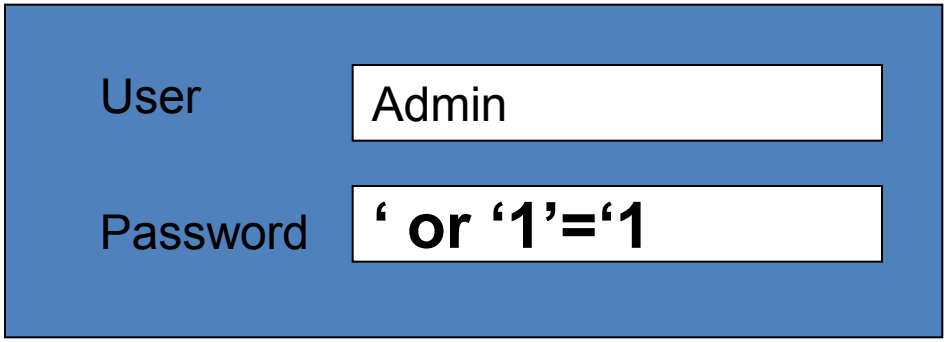
- User authentication against database




```
Select iduser from table_users
Where name_user='$user'
And password='$password';
```


Video intypedia007en © intypedia 2011 Creative Commons

Code Injection: Example



Select iduser from table_users

Where name_user=‘Admin’

And password=‘’ or ‘1’=‘1’;

Video intypedia007en © intypedia 2011 Creative Commons

Impact

- Allow an attacker to:
  - Skip access restrictions
  - Escalate privileges
  - Extract information from the database
  - RDBMS stop
  - Run commands in user context db within the server

Video intypedia007en © intypedia 2011 Creative Commons

Types of Attacks: Inbound

- Access information with listing procedures

  http://www.myweb.com/prog.asp?parameter1=hello

  http://www.myweb.com/prog.asp?parameter1=‘ union select name, password,1,1,1 from table_users; other instruction; xp_cmdshell(“del c:\boot.ini”); shutdown --

  OR

  http://www.myweb.com/prog.asp?parameter1=1

  http://www.myweb.com/prog.asp?parameter1=-1 union select .....; other instruction; --

Video intypedia007en © intypedia 2011 Creative Commons

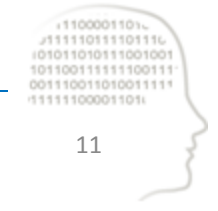
Types of Attacks: Outbound

- The attacker dumps data using the application's error messages and the data repository

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Comilla no cerrada antes de la cadena de caracteres 'd'.

/index.asp, line 23
```



Video intypedia007en © intypedia 2011 Creative Commons

Blind attacks

- The web application doesn't display any error messages
  - An outbound attack isn't possible
- The application doesn't process commands
  - An inbound attack isn't possible
- True and False conditions are injected Examples:
  - http://server/myphp.php?id=1 and 1=1
  - http://server/myphp.php?id=1 and 1=2

Video intypedia007en © intypedia 2011 Creative Commons

Blind Attacks

- How to recognize different behaviours?
  - Gives an error code
  - Gives an error page
  - Changes the signature hash
  - Changes the html tree
  - It takes longer to respond
  - …
- If the page reacts differently to injections of True and False, then you can extract data using Boolean searches
  - http://www.server.com/show_news.php?v_id=1 and (100=(select top 1 ascii(substring(login,1,1)) from users))

Video intypedia007en © intypedia 2011 Creative Commons

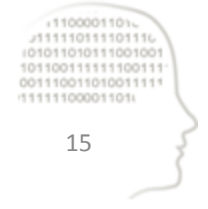
Time-based attacks

- If the content of the answers is identical in both cases, you can still achieve the goal changing the server response time conditionally
  - If the injected condition is true, the application will take a few seconds to answer
  - If the condition is false, the application will return the same answer, but taking the usual time
- The same injection techniques described above can be used

Video intypedia007en © intypedia 2011 Creative Commons

Time-based SQL Injection

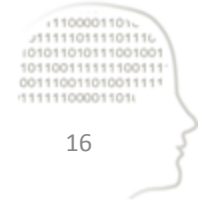
- How can we get the delay?
  - Using delay instructions implemented in the database manager
    - SQL Server: *waitfor delay*
    - Oracle: *dbms_lock.sleep*
    - MySQL: *sleep*
    - *Postgres: pg_sleep*
  - Using heavy queries that consume a lot of the server's resources (CPU or memory)
    - CROSS JOIN involving many tables
  - Any other way (e.g.: xp_cmdshell 'ping…')



Video intypedia007en © intypedia 2011 Creative Commons

Countermeasures

- Not confiding in client based protection measures
- Checking input data
- Creating SQL statements with secure components
- Fortifying the web server
  - Error codes
  - Restriction of verbs, lengths, etc...
  - HTTP Content Filtering in the Firewall (WAF)
- Fortification of DBMS
  - Restriction of motor/user privileges access from the web
  - Isolation of databases



Video intypedia007en © intypedia 2011 Creative Commons

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Video intypedia007en © intypedia 2011 Creative Commons

Contact: info@intypedia.com