Secure software development for the World Wide Web

Derek Mathieson
Group Leader
Advanced Information Systems
CERN – Geneva, Switzerland

Agenda

- Impact of Security Flaws
- Definitions
- Types of Attack
- Techniques / Solutions

Why Secure Web Application?

Impact of Security Flaws

- **Ping of death**
- **Morris worm (1988)**
  - **~6,000 infected computers**
- **Santy (2004)**
  - **~40,000 infected computers (in 24 hours)**
- **Conficker (2008)**
  - **17,000,000 infected computers**

US Army

- **Computer Virus Hits U.S. Drone Fleet**

SONY PlayStation Network

SonyPictures.com

SONY
PICTURES

Bell Canada

Date: 2nd February 2014

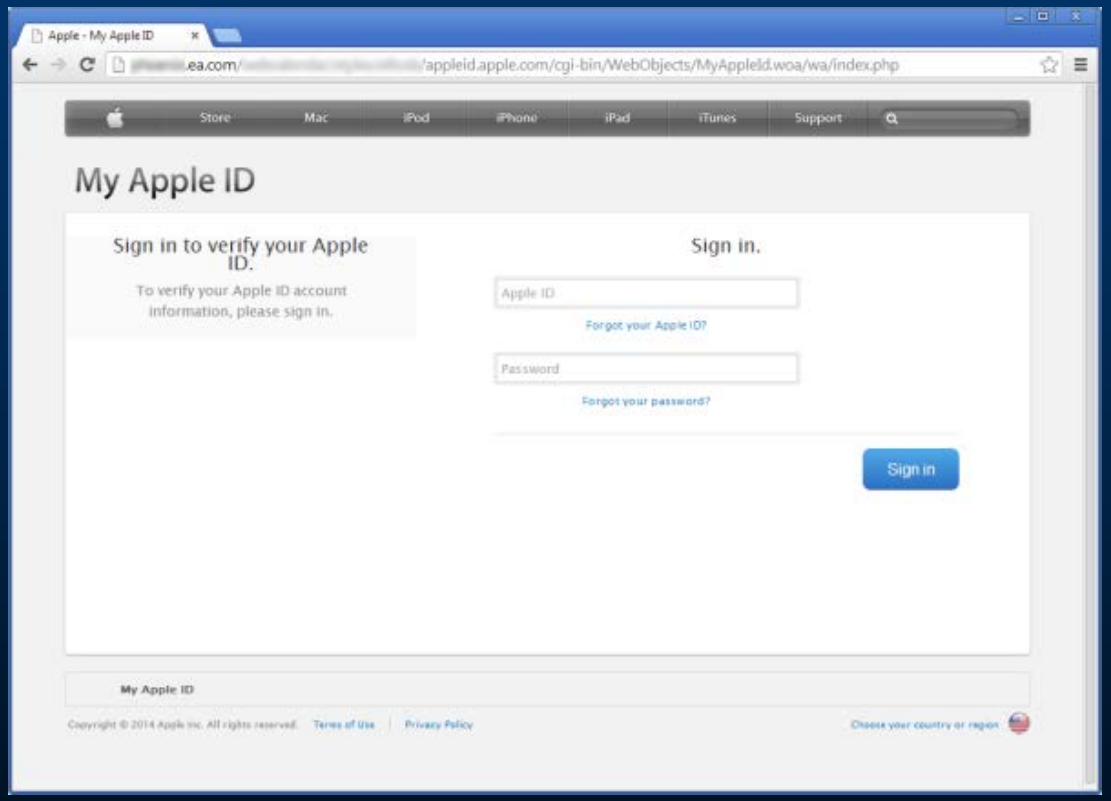
Source: http://www.databreaches.net

Citroën Germany

Date: 17th March 2014

Source: http://www.theguardian.com

EA Games



Date: 19th March 2014

Source: http://news.netcraft.com

Top 25 Software Errors

Top 25 Most Dangerous Software Errors 2011 (CWE/SANS)	
1	SQL Injection
2	OS Command Injection
3	Classic Buffer Overflow
4	Cross-site Scripting
5	Missing Authentication for Critical Function
6	Missing Authorization
7	Use of Hard-coded Credentials
8	Missing Encryption of Sensitive Data
9	Unrestricted Upload of File with Dangerous Type
10	Reliance on Untrusted Inputs in a Security Decision
11	Execution with Unnecessary Privileges
12	Cross-Site Request Forgery (CSRF)
13	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
14	Download of Code Without Integrity Check

Definitions

- **Identification**
- **Authentication**
- **Authorisation**
- **Session Management**

Identification / Authentication

- **How Can You Prove Who You Are?**
  - **Biometric Passport**
  - **Photo ID**
  - **Fingerprint**
  - **Username / Password**

Definitions

- **Entity**
  - A User, another computer system component
- **Identification**
  - Providing credential such that a system can recognise the entity and distinguish it from other entities.
- **Authentication**
  - The process of verifying the identity of an entity.

Authentication *Factors*

- **Something an entity knows:**
  - **Password, PIN**
- **Something an entity has:**
  - **ID Card, ‘Smart key’**
- **Something an entity is:**
  - **Fingerprint, iris scan, …**

Authentication

- **Single / Multi-factor Authentication**
  - **Password only**
  - **Password + Fingerprint**

- **Trade-off between**
  - **Convenience**
  - **Cost**
  - **Complexity**
  - **Security**

Identity Theft

- **Compromised Passwords**
  - **Self Service password reset**
- **Lost ID Cards**
  - **Blocking List**
- **Compromised Private Keys**
  - **CRL**

- **What about Biometrics?**
  - **No easy solution**

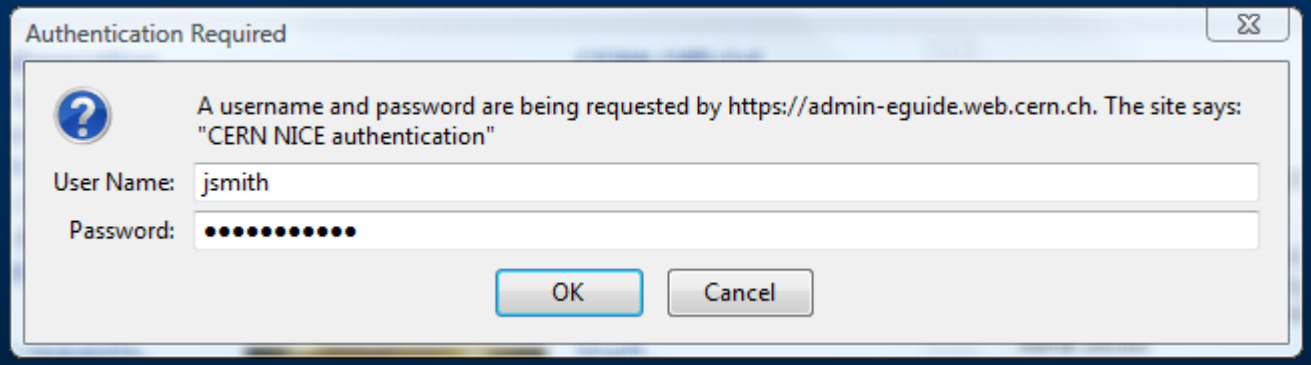
Passwords

- **Server good practices**
  - ***Never*** **store them in 'clear'**
  - **Use encrypted communication protocols (SSL)**
  - **Log authentication failures**
  - **Use generic error messages:**
    - **User/password combination not recognised'**
  - **Show user**
    - **Last login date**
    - **Previous failed login attempts**

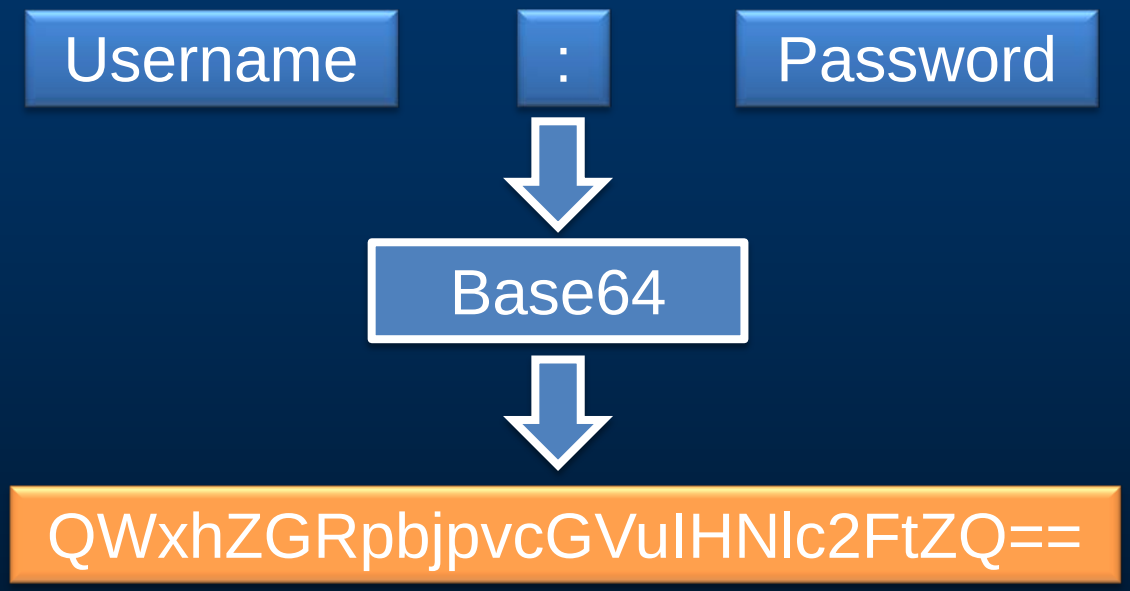
Web Authentication Techniques

- **Basic Authentication**
- **Digest Authentication**
- **Form Authentication**

Basic Authentication

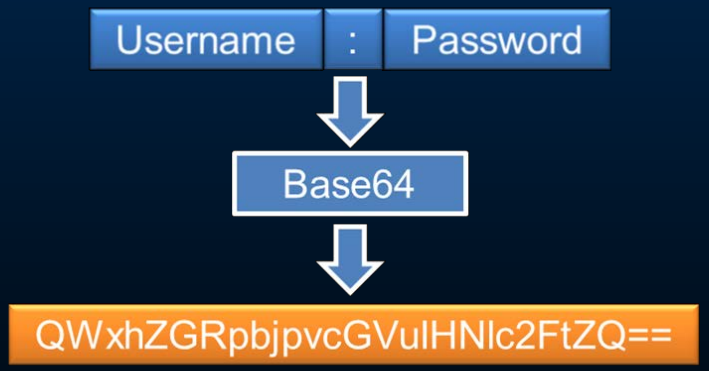


Basic Authentication

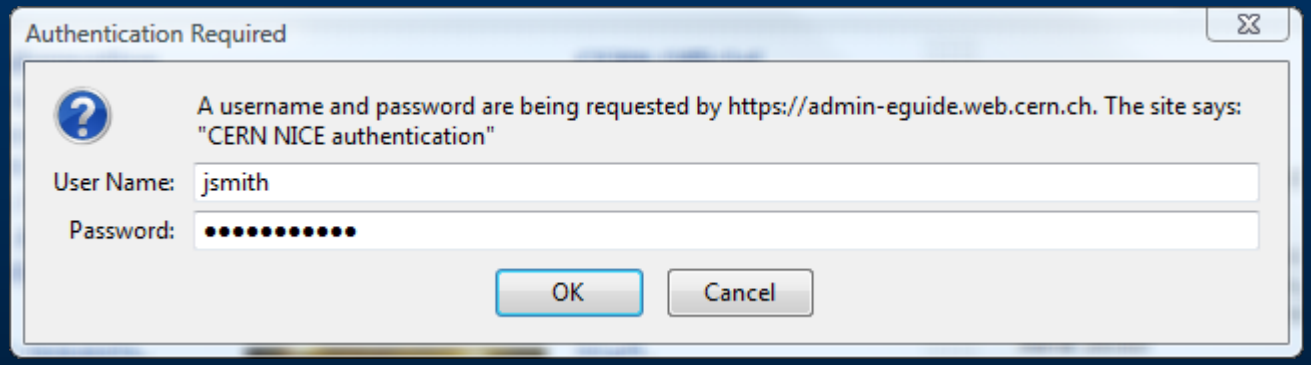


Basic Authentication

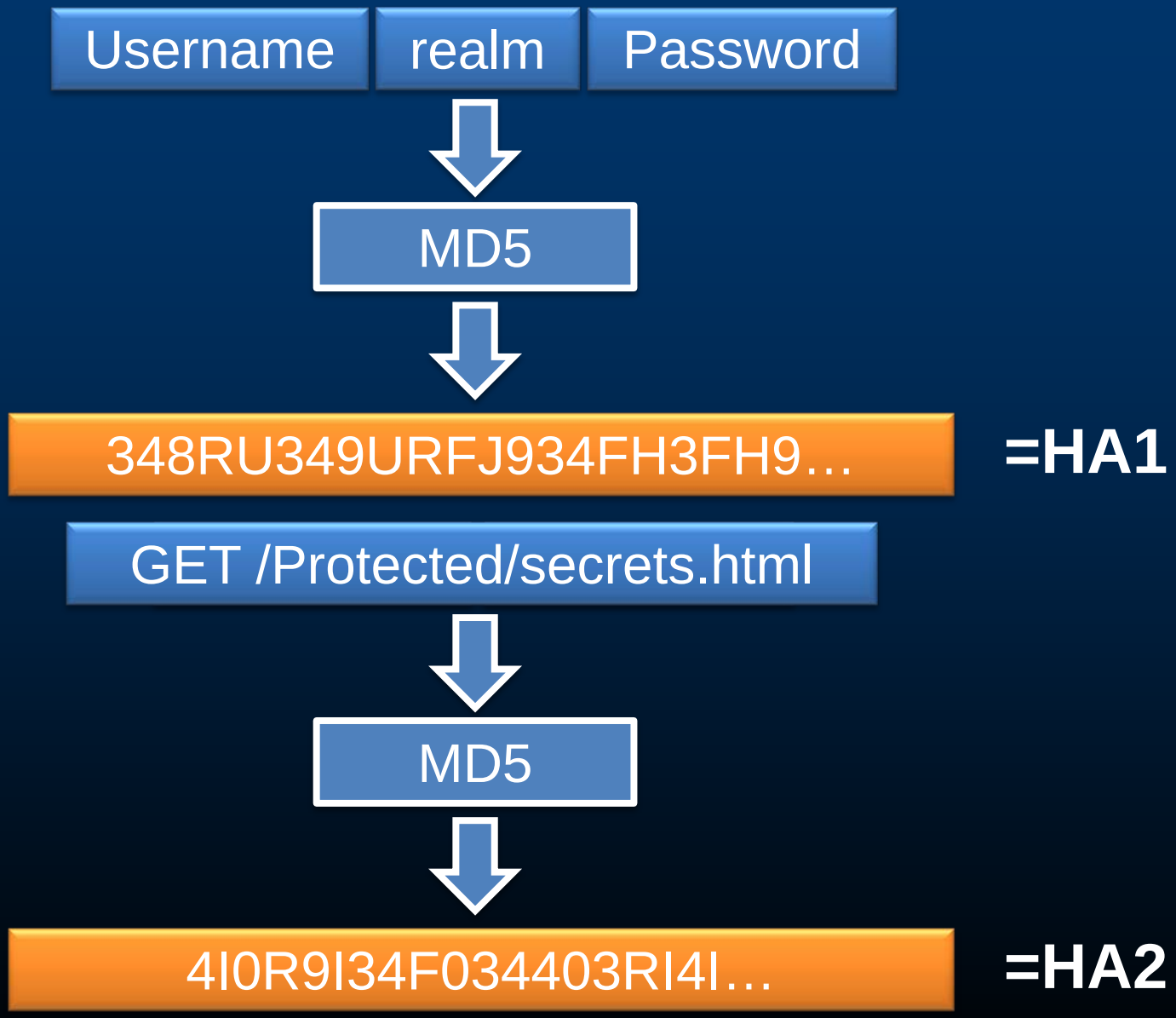
- **No encryption**
  - **Username / Password ‘encoded’**
- **Depends on a secure communication channel**



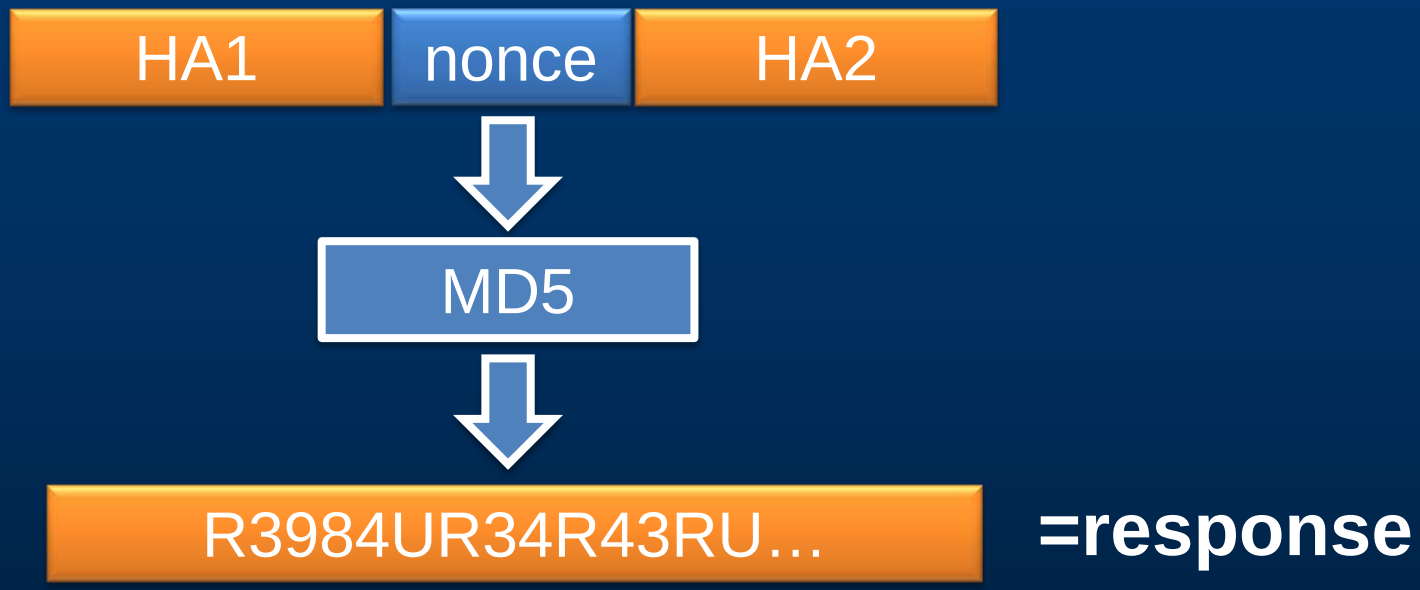
Digest Authentication



Digest Authentication



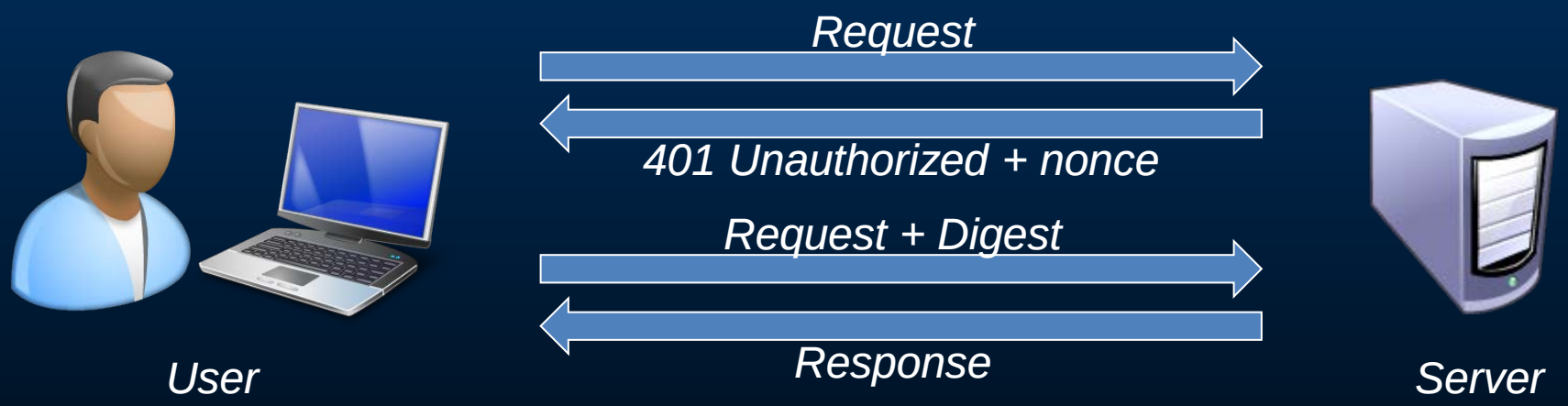
Digest Authentication



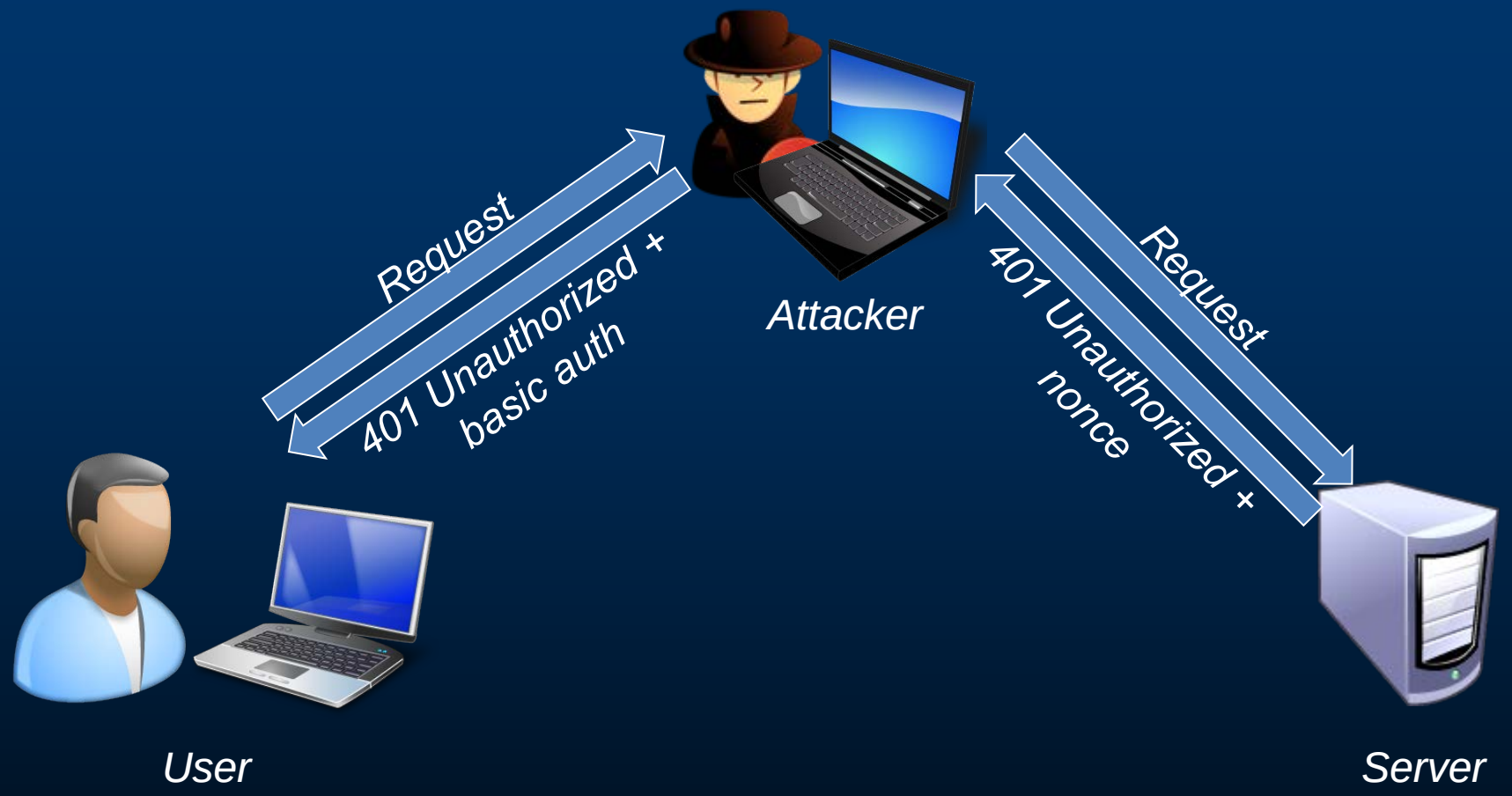
Digest Authentication

- **Advantages**
  - **Communication is more secure**
    - **Some doubts over irreversibility of MD5**
  - **Server *nonce* can avoid replay attacks**
- **Disadvantages**
  - **Server password file is contains usable credentials in plaintext**
  - **Vulnerable to a man-in-the-middle (MitM) attack**

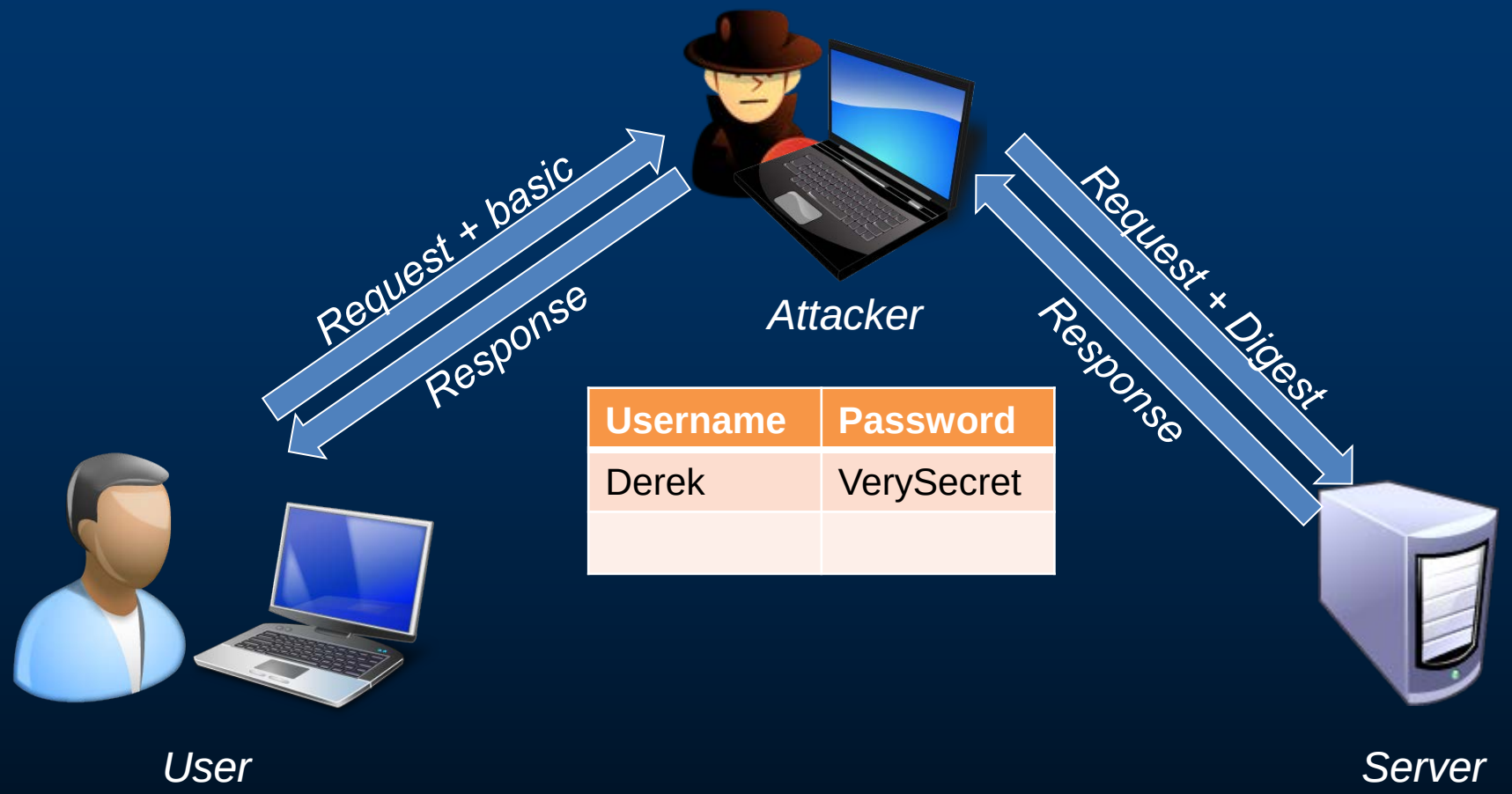
Digest Authentication



Digest Authentication

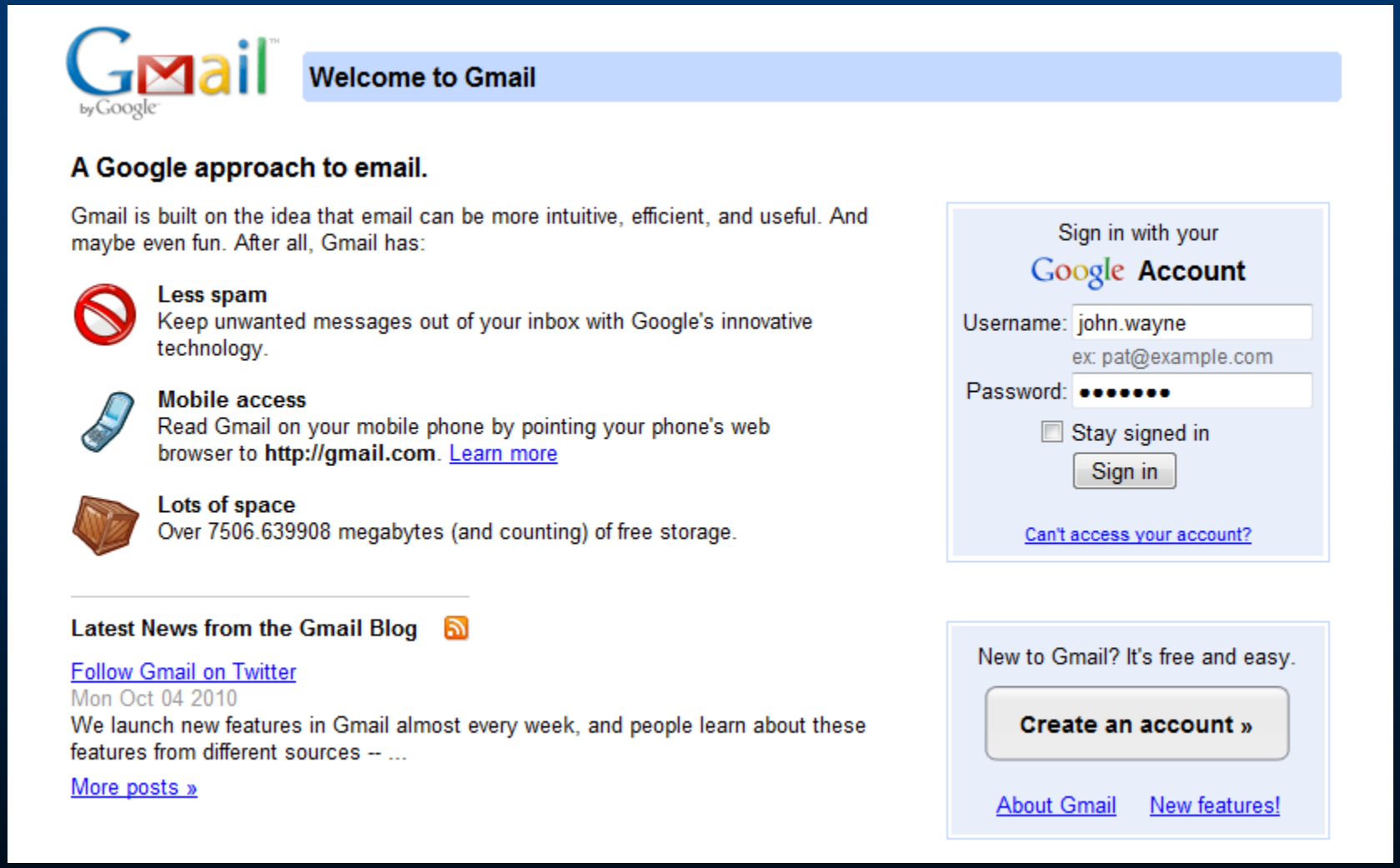


Digest Authentication



Username	Password
Derek	VerySecret

Form Authentication



Form Authentication

- **Advantages**
  - **Simple to develop**
  - **Richer User Interface**
  - **Can use multifactor authentication**
- **Disadvantages**
  - **Depends on a secure communication channel (usually)**

Other Authentication Methods

- **Single Sign-on**
  - **OpenID, Shibboleth, …**
- **Integrated Windows Authentication**
- **Token-based**
  - **One Time Passwords (OTP)**
    - **SecureID, YubiKey**
  - **Public key authentication (SSL client certificates).**

Authorisation

Authorisation

- **An Authorisation system should:**
  - **Allow access to resources to users/systems that are permitted to access them.**
  - **Prevent access to those that are not permitted.**

Authorisation

- **System requirements:**
  - **Who (entity)**
  - **What (resource)**
  - **Which operation (read / update / delete / …)**
  - **Access Policy**

Role Based Access Control

- **Roles are identified**
  - **e.g. administrator, group leader, developer.**
- **Rights are assigned to roles**
  - **group leader can access homepage**
- **Roles are assigned to entities**
  - **Derek is a group leader**

AIS Roles

AIS Roles

User: MATHIESON, Derek Mr. (GS-AIS)
Active role: FOUNDATION MGR

Session ◉ Current time ○ At Date 09-10-2010 16:12:52

Main | Administration

Query Assignments | Query Positions | Info Center |

Selected Person Details

Name **MATHIESON Derek**
Org. Unit GS-AIS
Currently at CERN? **Yes**

Choose View / Filter Results

View: Roles held by MATHIESON Derek
Show Inherited Roles ◉ No ○ Yes
Role Family: All

Role Assignments (max 500 lines displayed - see Help *)

Holder	Org. Unit	Role Type	1st Target	1st Target Type	2nd Target	2nd Target Type
MATHIESON Derek	GS-AIS	ACDNT.READANY	ALL	Scope of EDH access right	-	-
MATHIESON Derek	GS-AIS	ADMIN.ATTACHMENT	ALL	Scope of EDH access right	-	-
MATHIESON Derek	GS-AIS	ADMIN.EDHADMINSUPER	ALL	Scope of EDH access right	-	-
MATHIESON Derek	GS-AIS	ADMIN.MODIFYRIGHTS	ALL	Scope of EDH access right	-	-
MATHIESON Derek	GS-AIS	AIS ADMINISTRATOR	CERN	Organization	-	-
MATHIESON Derek	GS-AIS	ATTACHMENTSIZE.LIMIT	100000000	EDH attachment size limit	-	-
MATHIESON Derek	GS-AIS	AVCL.CREATE	ALL	Scope of EDH access right	-	-
MATHIESON Derek	GS-AIS	AVCL.CREATECANDIDAT	ALL	Scope of EDH access right	-	-
MATHIESON Derek	GS-AIS	AVCL.CREATESTANDINGO	ALL	Scope of EDH access right	-	-
MATHIESON Derek	GS-AIS	AVCLINSTALLATION.CRE	ALL	Scope of EDH access right	-	-
MATHIESON Derek	GS-AIS	Budget Holder	71000	Intersection	-	-
MATHIESON Derek	GS-AIS	Budget Holder	71001	Intersection	-	-

Role Based Access Control

- **Less complex than individual assignment of access rights**
- **Roles can link to organization roles**
  - **Automatic maintenance**
  - **Less administration**

Authorisation: Good Practices

- **Check every access**
- **Centralise rights management**
- **Principal of Least Privilege**

Session Management

Session Management

- **Why do we need it?**
  - **HTTP is state-less**

Session Management

User

Credentials

Session ID: 42

Server

User ID	Session ID
Derek	42
Frank	43
Jim	44
Alex	45
Jane	46
Billy	47
Lilly	48

Session Memory

Session Management

User

Credentials

Session ID: 70457632

Server

User ID	Session ID
Derek	70457632
Frank	67348934
Jim	96734693
Alex	24586424
Jane	33460349
Billy	77349834
Lilly	07256323

Session Memory

Session Management

- **Good Practices**
  - **Keep Session ID secret!**
    - **Use encrypted communications.**
  - **Make them unpredictable**
    - **Based on a random sequence**
    - **Never re-used**
  - **Time limited**

- **Use a standard framework**

Types of Attack

Types of Attack

- **Session**
  - **Session Fixation / Session ID Forgery**
  - **Cross-Site Scripting**
  - **Cross-Site Request Forgery**
- **Injection**
  - **SQL Injection**
  - **Command Injection**
- **Google Hacks**

Session ID Forgery

- **URL Manipulation**
- **POST parameter Manipulation**

Citibank

Citibank customers lost $2.7 million in recent attack

June 2011

PayPal

23-year-old hacker accessed 200,000 PayPal accounts

April 2012

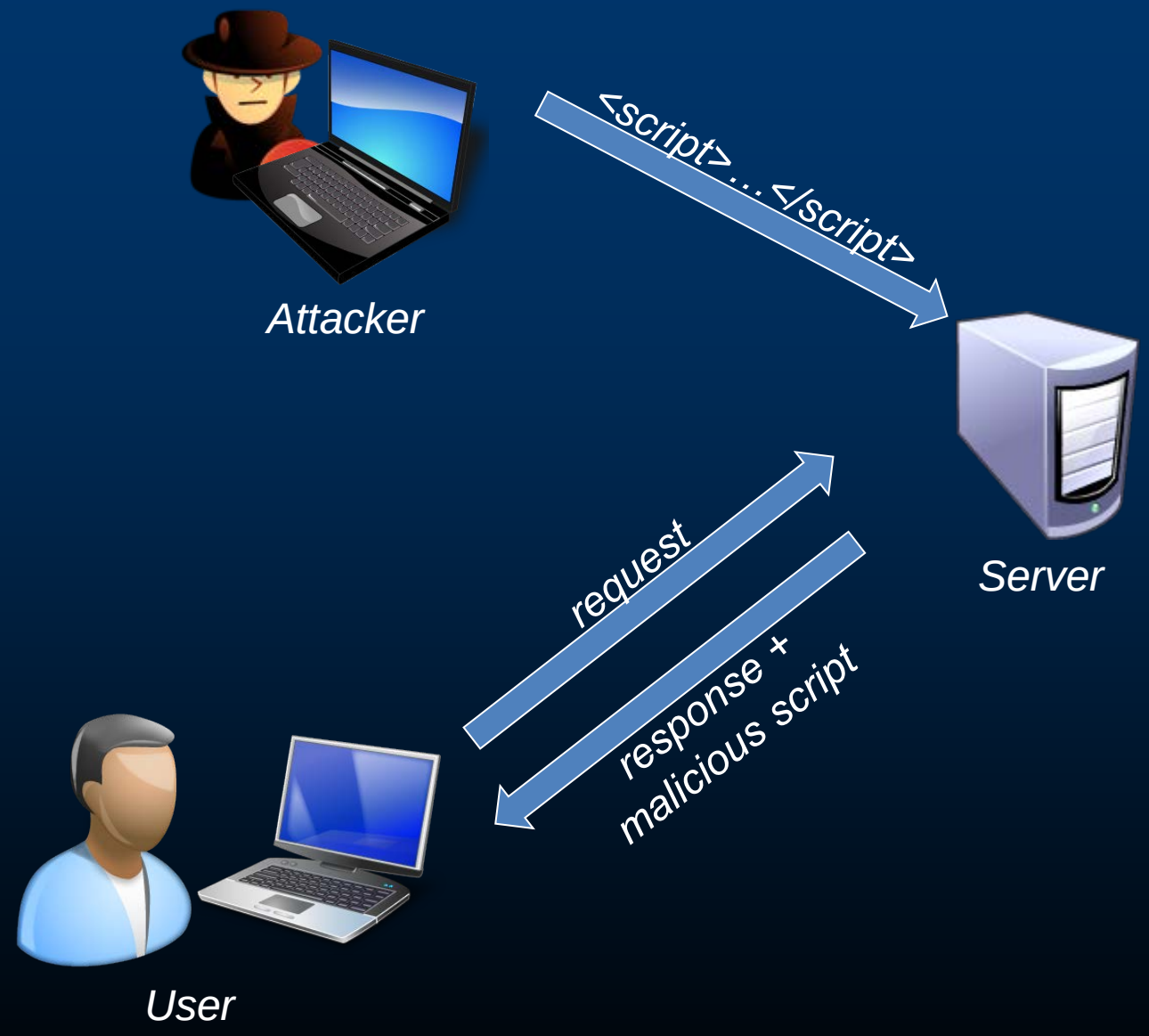
Cross-Site Scripting

XSS

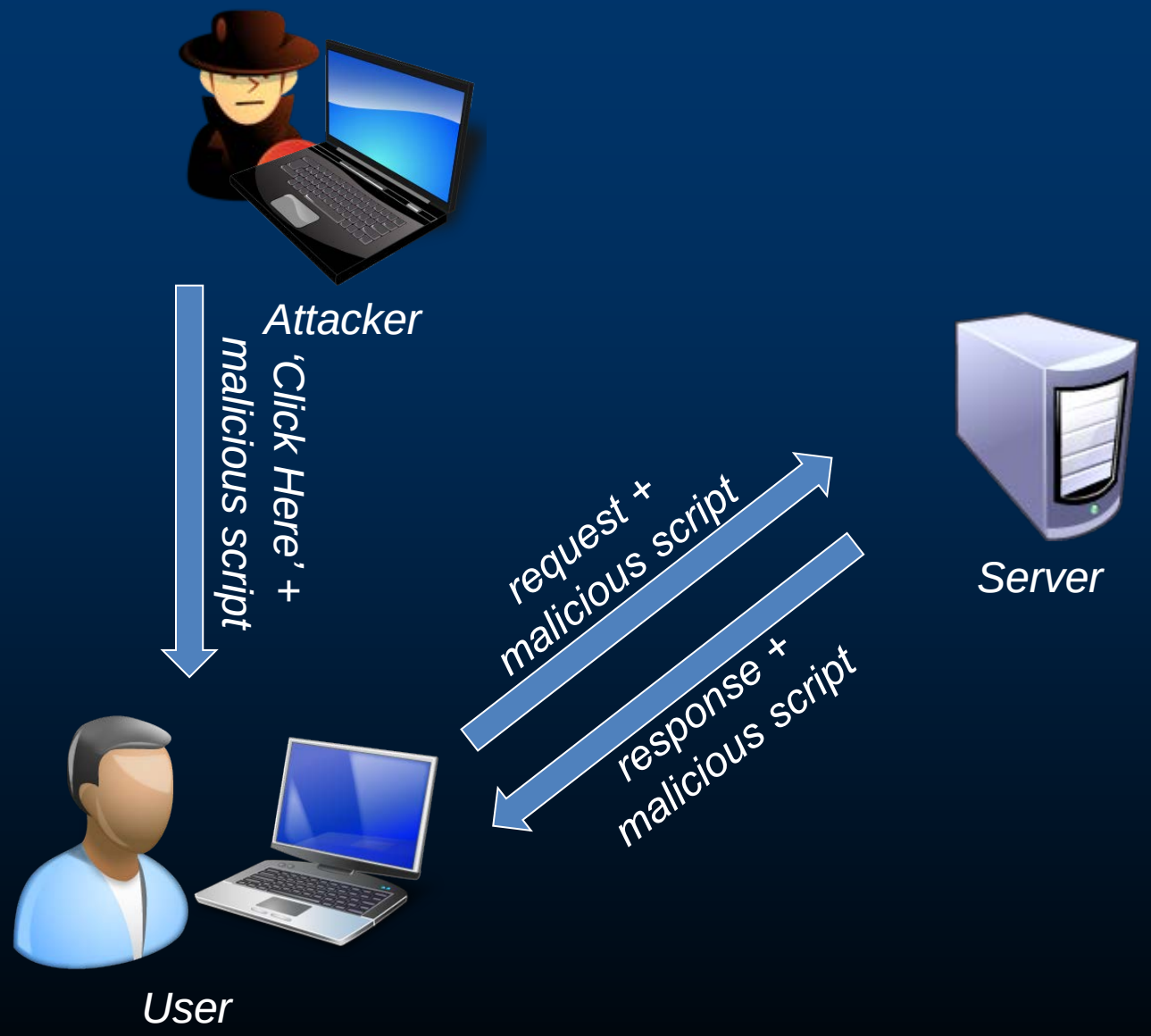
Cross-Site Scripting

- **The most common publicly-reported security vulnerability**
  - **Up to 68% of websites could be vulnerable**

Cross-Site Scripting (Persistent)



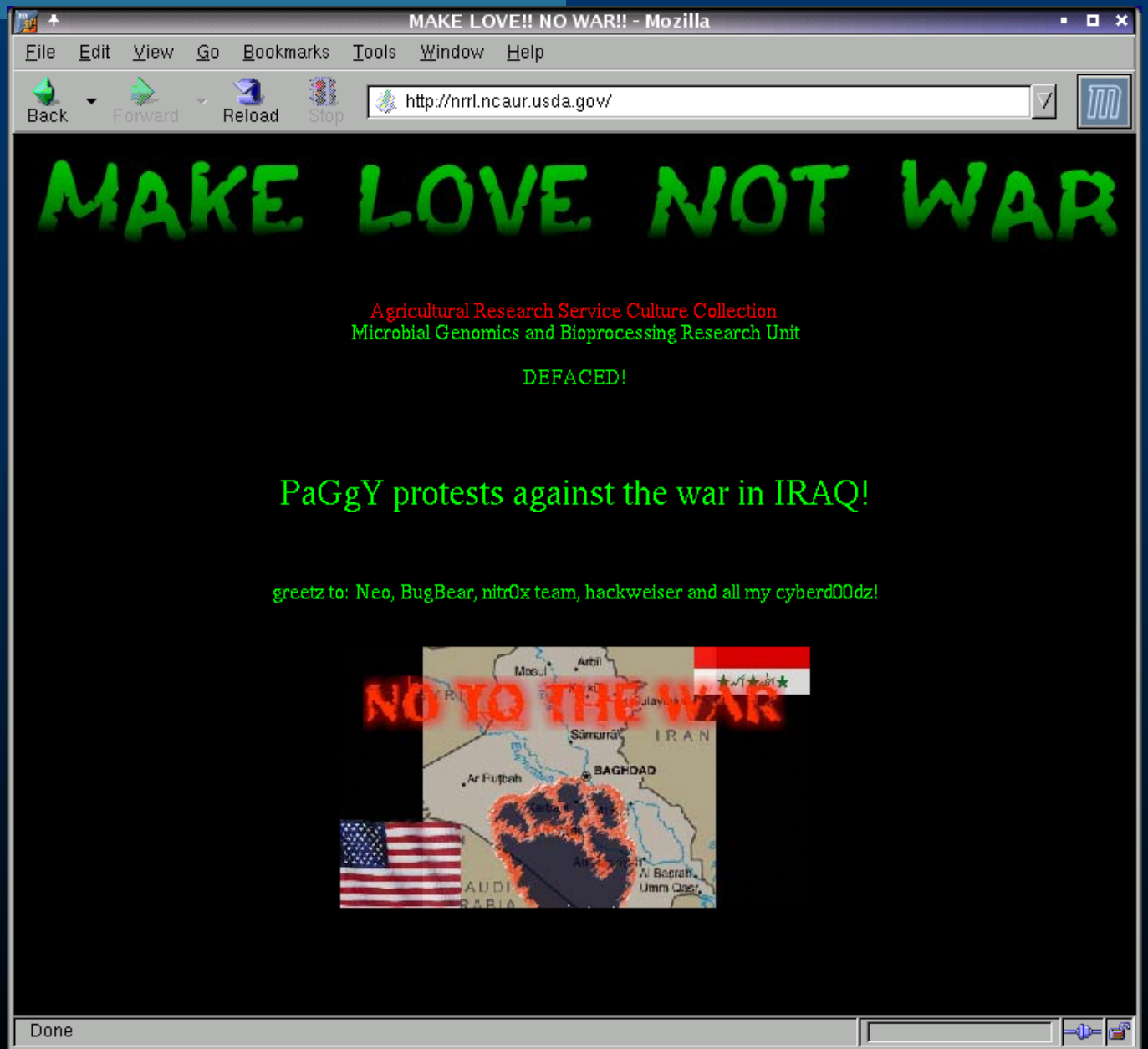
Cross-Site Scripting (non-persistent)



Cross-Site Scripting: Impact

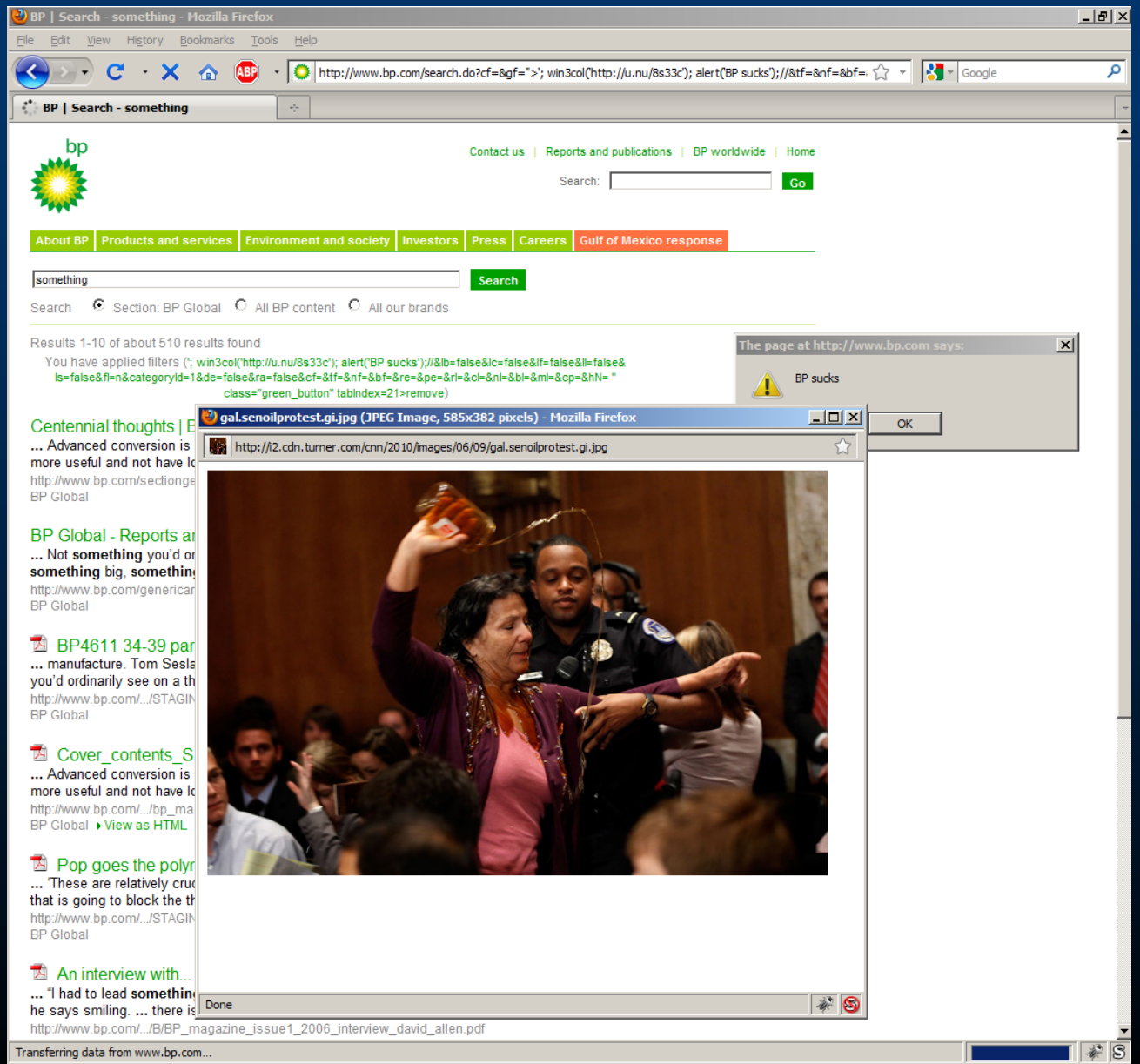
- **Site defacement**

USDA.GOV


MAKE LOVE!! NO WAR!! - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://nrrl.ncaur.usda.gov/
MAKE LOVE NOT WAR
Agricultural Research Service Culture Collection
Microbial Genomics and Bioprocessing Research Unit
DEFACED!
PaGgY protests against the war in IRAQ!
greetz to: Neo, BugBear, nitr0x team, hackweiser and all my cyberd00dz!
NO TO THE WAR
Mosul
Arbil
Sāmurrā'
IRAN
BAGHDAD
Ar Rutbah
Al Basrah
Umm Qasr
Done

EU President

BP.COM



CERN
GS-AIS

Cross-Site Scripting: Impact

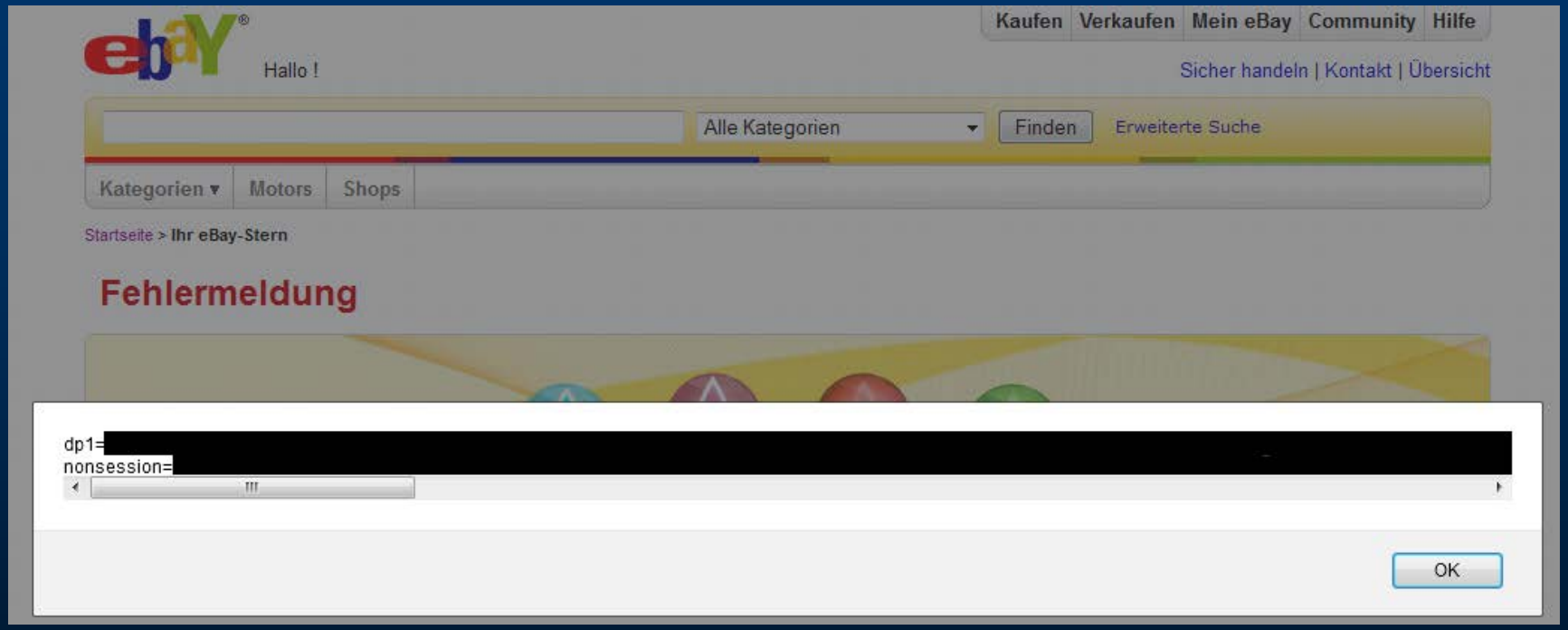
- **Site defacement**
- **Identity Theft**
- **Malware distribution**
- **…**

WordPress

WordPress corrects a cross-site request forgery (CSRF) and cross-site scripting (XSS) in version 3.1.1.

April 2011

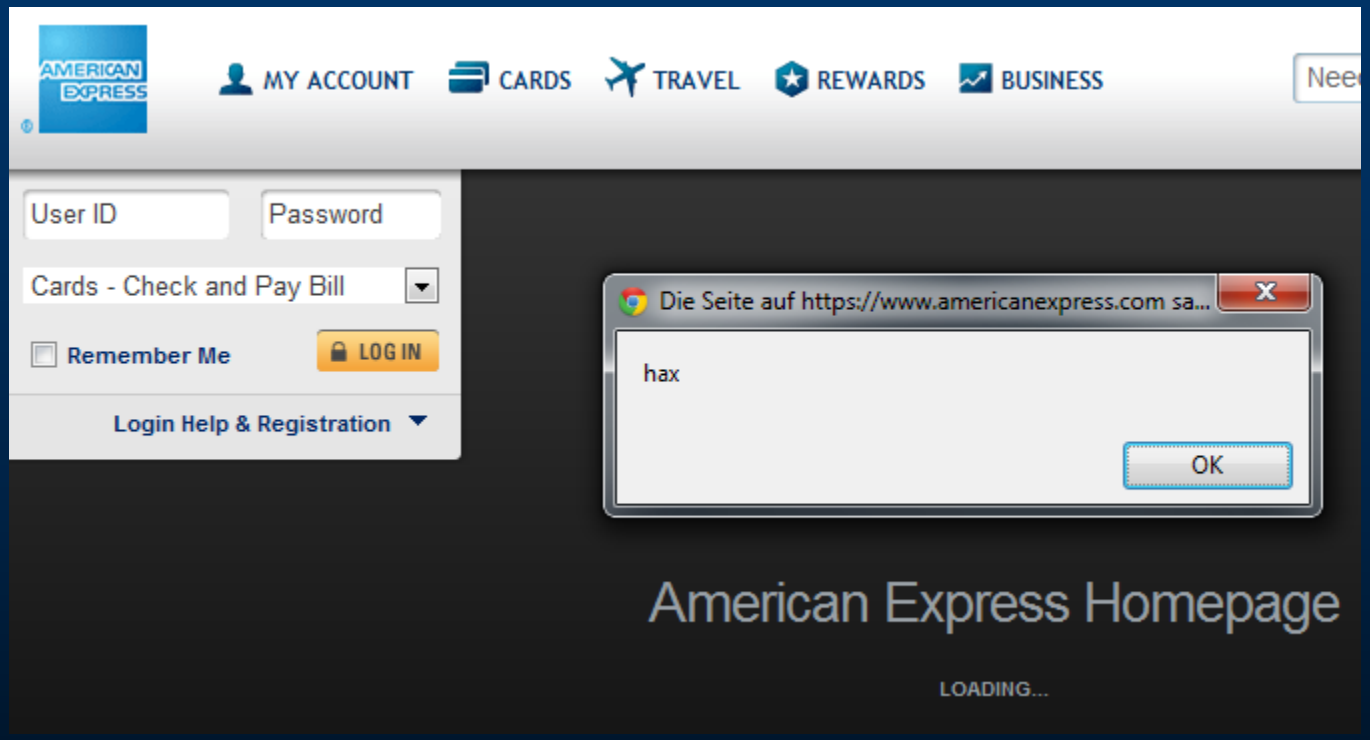
eBay.de



Potential account theft with XSS hole in eBay.de

August 2011

American Express



October 2011

Cross-Site Scripting: Impact

- **'Samy' XSS Worm on MySpace**
  - **Automatically made 'friend request' back to author.**
  - **Within 20 hours of release over 1,000,000 users were affected.**

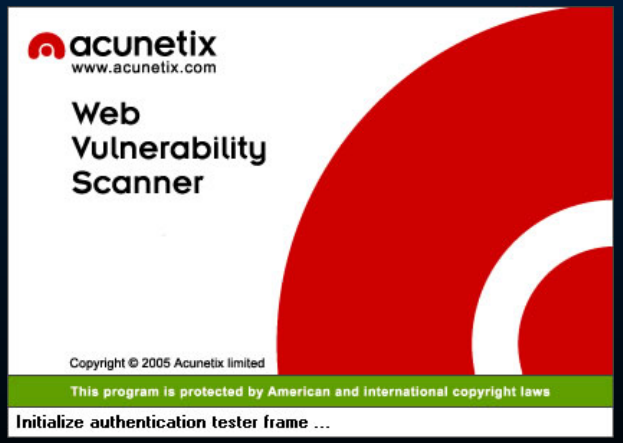
- **Author: Samy Kamkar**
  - **Arrested and on felony charge.**
    - **Sentenced to three years probation, 90 days community service and an undisclosed amount of restitution.**

Cross-Site Scripting: Remedies

- **Do not trust any User Input**
  - **Form Input**
  - **URLs**
  - **Cookies**
  - **HTTP Request Headers**

Cross-Site Scripting: Remedies

- **Remove / replace HTML entities**
  - **'White List' or 'Black List' Filter**
- **Use Non-HTML Lightweight mark-up**
  - **Wiki**
  - **bb-code**
  - **Textile**
- **Use a Site Scanning Tool**
  - **We use Acunetix**



AltoroMutual – Test Site

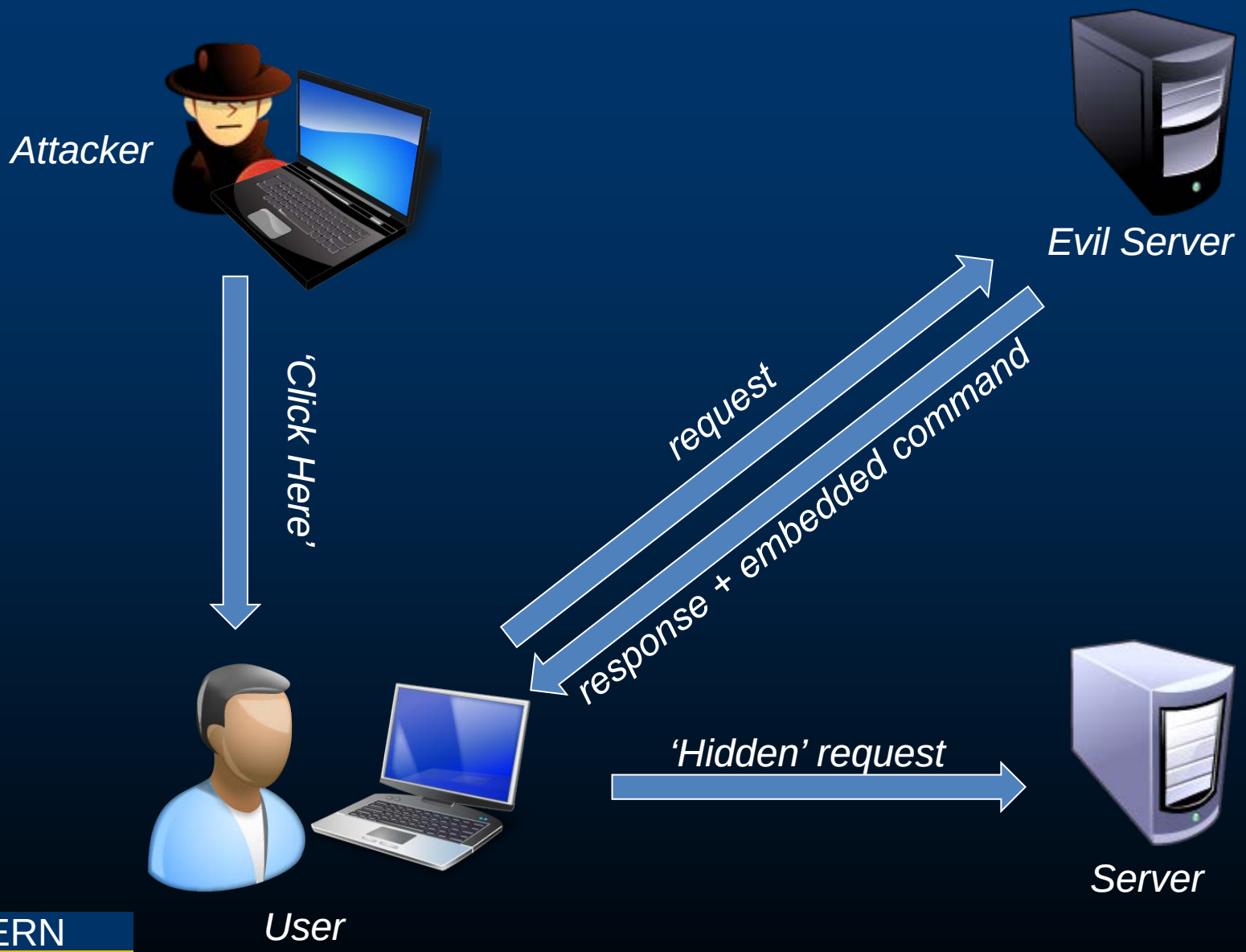
http://demo.testfire.net

- XSS
- XSS 2

Cross-Site Request Forgery

CSRF / XSRF

Cross-Site Request Forgery



Cross-Site Request Forgery

Embedded Image

```
<img src="http://bank.example/withdraw?
            account=bob&amount=1000000&for=mallory">
```

Hidden Form

```
<body onload="document.secretform.submit()">
  <form name="secretform" method="POST"
    action="http:bank.example/account">
    <input type="hidden" name="action" value= "transfer">
    ...
  </form>
</body>
```

CSRF: Remedies

- **For End Users: Very Little!**
  - **Log out before visiting other sites**
  - **Don’t use ‘remember me’ features**
  - **Don’t visit ‘untrustworthy’ sites**

CSRF: Remedies

- **For Website Authors**
  - **Include a hidden ‘nonce’ token in forms**
  - **Ignore GET parameters when processing a POST**
  - **Include Authentication Cookies in POST body (via JavaScript)**

Injection Exploits

SQL Injection

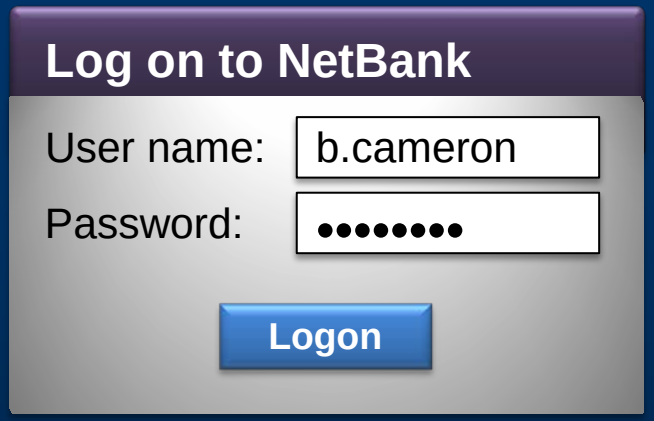
SQL Injection

- **SQL Injection is user input allowed to pass through to the database directly**

SQL Injection: Example

Attacker

X' or '1'='1




```
SELECT id
FROM logins
WHERE username = 'b.cameron'
AND password = 'X' or '1'='1'
```

SQL Injection: Remedies

- **Do not trust any User Input**
  - **Form Input**
  - **URLs**
  - **Cookies**
  - **HTTP Request Headers**

- **Use a Site Scanning Tool**

SQL Injection: Remedies

- **Prepared Statements**

```
SELECT id
FROM logins
WHERE username = ?
AND password = ?
```

  - **Advantages**
    - **Precompiled Query: Faster (usually)**
    - **Database engine does the *bind***
  - **Disadvantages**
    - **(a little) More Complex**

Other Exploits

Heartbleed


April 2014
The Heartbleed Bug attacking over 60% of websites Today.
The bug has the potential to affect the security of all your online accounts and in fact it has had 2 yrs to gather your personal information.
Solutions: Change all your passwords today.
https://www.
THE DEEPER GRAPHIC WEB DESIGN

Command Injection

- **Variation of SQL Injection**
  - **Injects malicious OS command**

```
exec ("ls .; cat /etc/passwd")
```

Google Hacking Database

- http://www.exploit-db.com/google-dorks/

GOOGLE HACKING-DATABASE

Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

Search Goolge Dorks

Category: All Free text search: Search

Latest Google Hacking Entries

Date	Title	Category
2011-10-11	intitle:#k4raeL - sh3LL	Vulnerable Servers
2011-10-11	filetype:php~ (pass|passwd|password|dbpass|db_pass...	Files containing passwords
2011-09-26	+intext:"AWSTATS DATA FILE" filetype:txt	Files containing juicy info
2011-09-26	inurl:ftp "password" filetype:xls	Files containing passwords
2011-09-26	inurl:view.php?board1_sn=	Vulnerable Servers

Summary

- **Do not trust any User Input**
  - **Form Input**
  - **URLs**
  - **Cookies**
  - **HTTP Request Headers**

- **Use a Site Scanning Tool**

Thank You

Q&A

Questions

- **My website is not well known**
  - **No bad people will find it…**

- **http://www.exploit-db.com**

Questions

- **Hacking websites is difficult.**
  - **You need to be an expert programmer.**
- **Metasploit**
- **BeEF**

http://www.1337day.com/

[home] [freelance] [platforms] [shellcode] [pentest] [cracker] [search] [faq] [team] [links] [contact] [style] db: 22116

Contact us:

[authorization] [registration] [restore account] [agreement]

inj3ct0r

Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
Our aim is to collect exploits from submittals and various mailing lists and concentrate them in one, easy-to-navigate database.
This was written solely for educational purposes. Use it at your own risk. The author will be not responsible for any damage. // r0073r

[web applications]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::GOLD	-::AUTHOR
2014-04-12	Comtrend CT 5361T Password Disclosure Vulnerability	hardware	1		R	D	✓	free	TUNISIAN CYBER
2014-04-12	WordPress Quick Page/Post Redirect Plugin 5.0.3 CSRF / XSS	php	180		R	D	✓	free	Tom Adams
2014-04-12	Twitget 3.3.1 Cross Site Request Forgery / Cross Site Scripting	php	65		R	D	✓	free	Tom Adams
2014-04-12	D-Link DAP 1150 Cross Site Request Forgery / Cross Site Scripting D-L..	hardware	89		R	D	✓	free	MustLive
2014-04-12	Sendy 1.1.9.1 - SQL Injection Vulnerability	php	607		R	D	⚠	free	delme
2014-04-10	csChat-R-Box Script Site Cross-Site Scripting Vulnerability	cgi	306		R	D	✓	free	Satanic2000
2014-04-10	XCloner Standalone 3.5 Cross Site Request Forgery Vulnerability	php	166		R	D	✓	free	High-Tech Bridg..
2014-04-10	Orbit Open Ad Server 1.1.0 SQL Injection Vulnerability	php	334		R	D	✓	free	High-Tech Bridg..
2014-04-09	QuickCms 5.4 - Multiple Vulnerabilites	php	254		R	D	✓	free	shpendk
2014-04-09	csUpload Script Site - Authentication Bypass Vulnerability	multiple	506		R	D	✓	free	Satanic2000
2014-04-09	RunCMS 1.6.1 - (pm.class.php) Multiple SQL Injection Vulnerabilities	php	327		R	D	✓	free	The:Paradox
2014-04-08	Halon Security Router (SR) =< v3.2-winter-r1 Multiple Vulnerabiliti..	hardware	406		R	D	✓	free	Juan Manuel Gar..
2014-04-08	XAMPP 3.2.1 & phpMyAdmin 4.1.6 - Multiple Vulnerabilities (XSS &am..	php	969		R	D	✓	free	Mayank Kapoor
2014-04-05	ASUS RT-AC68U Cross Site Scripting Vulnerability	hardware	347		R	D	✓	free	Joaquim Oliveir..
2014-04-05	ASUS RT-AC68U Remote Command Execution Vulnerability	hardware	561		R	D	✓	free	Joaquim Oliveir..
2014-04-04	Oracle Identity Manager 11g R2 SP1 (11.1.2.1.0) - Unvalidated Redirect..	php	235		R	D	⚠	free	Giuseppe D'Amor..
2014-04-04	Wordpress XCloner Plugin 3.1.0 - CSRF Vulnerability	php	554		R	D	✓	free	High-Tech Bridg..
2014-04-03	Kloxo-MR 6.5.0 - CSRF Vulnerability	php	379		R	D	⚠	free	Necmettin
2014-04-02	CIS Manager CMS - SQL Injection Vulnerability	php	660		R	D	⚠	free	felipe andrian
2014-04-02	ICOMM 610 Wireless Modem - CSRF Vulnerability	hardware	315		R	D	✓	free	Blessen Thomas
2014-04-02	Horde Webmail 5.1 - Open Redirect Vulnerability	php	516		R	D	⚠	free	felipe andrian
2014-04-01	AlienVault 4.5.0 SQL Injection Vulnerability	php	783		R	D	⚠	free	Brandon Perry
2014-04-01	EMC Cloud Tiering Appliance v10.0 Unauthenticated XXE Arbitrary File R..	multiple	346		R	D	⚠	free	Brandon Perry

http://www.exploit-db.com/

EXPLOIT DATABASE

blog exploit

Currently Archiving 29113 Exploits

Updated (CVE And Archive): Sat Apr 12 2014

HOME | GHDB | ABOUT | REMOTE | LOCAL | WEB | DOS | SHELLCODE | PAPERS | SEARCH | SUBMIT

Looking for a meaningful Security Certification?

CVE COMPATIBLE cve.mitre.org

The Exploit Database

The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

Remote Exploits

Date	D	A	V	Description		Plat.	Author
2014-04-10		-		Sophos Web Protection Appliance Interface Authenticated Arbitrary Command Execution	68	unix	metasploit
2014-04-10		-		Heartbleed OpenSSL - Information Leak Exploit	114	multiple	Hacker Fantastic
2014-04-10		-		Vtiger Install Unauthenticated Remote Command Execution	51	php	metasploit
2007-07-09		-		Sun Java Runtime Environment 1.6 - Web Start JNLP File Stack Buffer Overflow Vulnerability	95	linux	Daniel Soeder
2008-06-14		-		GSC Client 1.00 2067 - Privilege Escalation Vulnerability	46	multiple	Michael Gray
2014-04-09		-		OpenSSL 1.0.1f TLS Heartbeat Extension - Memory Disclosure (Multiple SSL/TLS versions)	181	multiple	Fitzl Csaba
2014-04-08		-		Bluetooth Text Chat 1.0 iOS - Code Execution Vulnerability	130	ios	Vulnerability-Lab