

# WIC: Web Integrity Check

S Chansilp

School of Computer Engineering, Institute of Engineering,  
Suranaree University of Technology, Thailand,  
E-mail: sompan@ccs.sut.ac.th

## ABSTRACT

When visiting a Web site by using a vulnerable browser, a serious system security breach may occur. This paper will first try to inform the community of such incidents. The exploitation occurs after a special code has been implanted into the page and is subsequently accessed by a web browser. The main concern to us is the unauthorized alteration of our web pages. The effect of an infected web page of this nature, is often the loss of credibility and reputation with our users. WIC can be used to detect unauthorized changes to web pages. WIC is a detection tool that runs on the web server. It detects changes to web pages made in a selected time span. When a change is detected, WIC provides an incident report and can recover to a known state, by uploading and replacing the faulty page with the original one.

## INTRODUCTION

Nowadays, the Internet has become part of our lives. The World Wide Web has brought a lot of security-unaware users like us into remote access technology (Gollmann, 1999). On our desks, we now have computers connected to the Internet. We use browsers to search for information, much like using a library, but in a much shorter time frame. Most organizations, agencies and companies create web sites to advertise and educate. Educational institutions also use web sites to provide information, utilizing a wide range of communications. Experience provides us with the knowledge that enables us to set up faster, cheaper and simpler connections. A vulnerable network may appear invulnerable for a long period of time, but when an attack is made, the vulnerabilities are soon evident. Examples of hacking and web page defacement are common and regular. For example, in August 1996, United States Department of Justice web-site was hacked and defaced (Hacked: DOJ, 1996) and in January 2001, government Web sites in the United Kingdom, Australia and United States were defaced (Leyden, 2001), and again in December 2003, thirteen NASA Web sites were defaced. Many things that seem impossible can and do happen.

When a web-site is defaced, its Web page is changed. Browser vulnerabilities causing high security risks are commonly reported. McWilliams (2002,para.2) stated that 'By coaxing IE users to view a web page containing the special code, an attacker can silently force Windows 98, Windows 2000, or Windows XP users to run a malicious program of the attacker's choice'. What if the 'attacker's choice' is a program containing a virus, spyware or a backdoor? It has also been shown in a Laboratory that special codes can cause hard disks to be formatted without user consent. There are numerous problems with browsers. A search for IE vulnerabilities at securiteam.com returns 27 reports. It is simple to recognize that defaced web pages can cause loss of confidentiality. It is also obvious that embedded malicious code can also cause our reputation to diminish due to adverse effects, such as viruses being transferred to our users' hardware.

The problem is that securing a web site, free of vulnerabilities is an extremely difficult task. Unfortunately, all browsers are open to some form of vulnerability. When a security solution is found for one problem, another security risk has developed. Imagine what would happen if our students visited our web site and a specially crafted code (malicious in intent), had been inserted into the page by an attacker, causing hard disks to be erased or infecting all their PCs with a virus. Since many respectable web sites have been hacked and defaced (Gaudin, 2003), it might be presumed that an

unauthorized entry into our web sites may not be as difficult as we imagine. We should, therefore, be prepared for such an event. One means of protection is to make periodical checks to determine if our web pages have been altered, and create the necessary incident reports ensuring that the Web Administrator is made aware of such occurrences. With this knowledge the administrator could then repair or replace the damaged files, and maintain a high standard of system integrity. One available tool to aid in these processes is WIC.

## THE ENGINE

We will examine the means of web page integrity checking. According to good security practice, the verifier should not be located on the web server holding the web pages to be monitored. Consequently, we create a validation server. Both administrators, and users, can setup and manage their requirements via the web. This necessitates that not only will the validation server verify web pages on the web server, but it will also validate itself. WIC supports a login page for both administrator and end-user as shown in Figure 1.

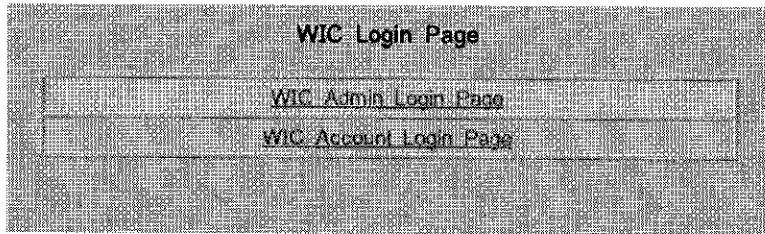


Figure 1: Login Page

Administrators can login via WIC Administrator Login Page and users can login by selecting WIC Account Login Page. At login, the server will display the relevant login page, and will validate the signature of the web page specified by using MD5 (Kaero, 1999). If it is an initial setup, the MD5 value will be stored in the database. Subsequent checkings will be validated against this entry. This entry will be checked periodically and if it has been changed, action will be taken corresponding to the users requirements. Figure 2 shows available actions.

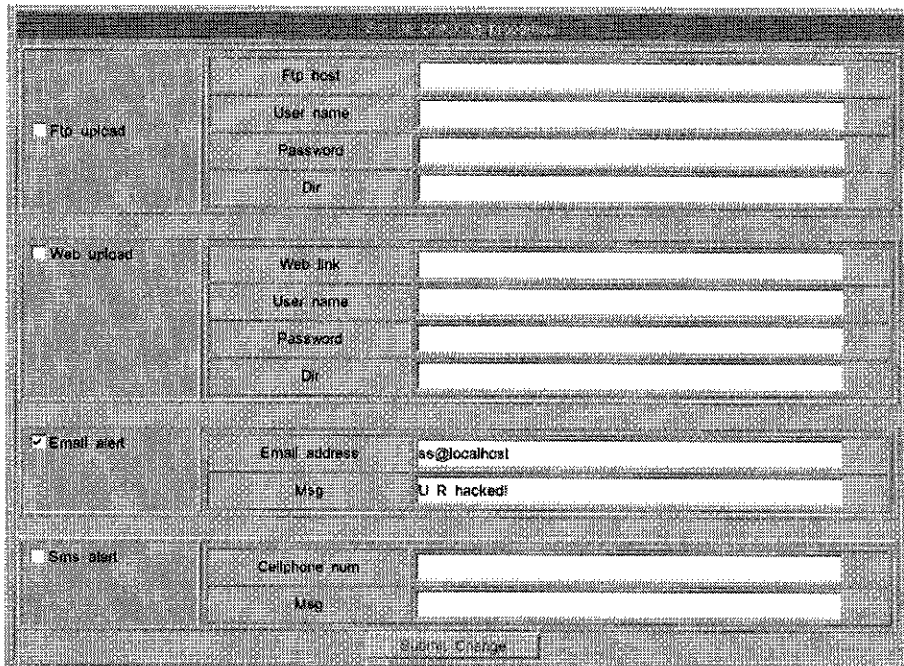
The image shows a web browser window titled "Action when Web page is changed". The form is divided into four main sections, each with a checkbox on the left and a table of input fields on the right. 1. "Ftp upload" (checkbox is unchecked): Fields include "Ftp host", "User name", "Password", and "Dir". 2. "Web upload" (checkbox is unchecked): Fields include "Web link", "User name", "Password", and "Dir". 3. "Email alert" (checkbox is checked): Fields include "Email address" (with the value "ae@localhost") and "Msg" (with the value "U R hacked!"). 4. "Sms alert" (checkbox is unchecked): Fields include "Cellphone num" and "Msg". At the bottom right of the form, there is a "Submit Change" button.

Figure 2: Action when Web page is changed

## ADMINISTRATOR MODE

WIC allows many administrators to be defined, however, only one, the first entry, will be classified as the main administrator. The main administrator can add other WIC administrators by adding WIC administrators and can add users by adding accounts. The main administrator can also backup and restore the WIC system. (See Figure 3).

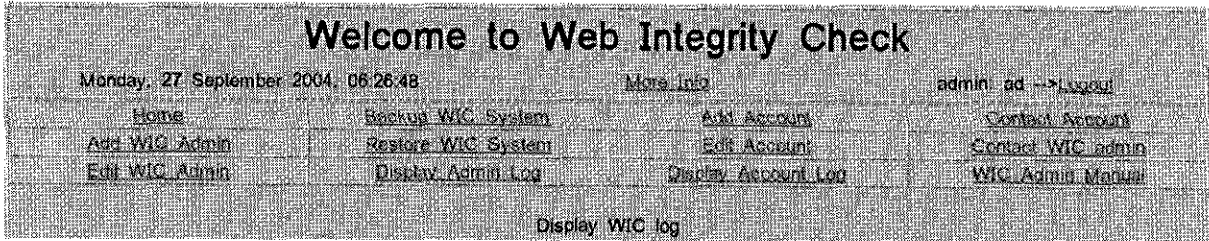


Figure 3: Administrator Menu

Every action the administrator performs is logged and can be displayed (see Figure 4). The administrator can also view other users' logs. The administrator can contact other administrators (Contact WIC admin) and any user (Contact Account). This is performed via e-mail generated by WIC. The primary difference between the main administrator and the other administrators is the ability to backup and restore the WIC program. No secondary administrator has this privilege, however, they are able to backup and restore the database.

No.	Time	From IP	Action
1	Monday, 27 September 2004, 06:27:54	127.0.0.1	Display admin log: main admin ad
2	Monday, 27 September 2004, 06:27:48	127.0.0.1	Display admin log: main admin ad
3	Monday, 27 September 2004, 06:27:25	127.0.0.1	Display admin log: main admin ad
4	Monday, 27 September 2004, 06:25:57	127.0.0.1	Login
5	Monday, 27 September 2004, 06:25:00	localhost	WIC server is up
6	Monday, 27 September 2004, 06:24:10	127.0.0.1	Logout
7	Monday, 27 September 2004, 06:23:20	127.0.0.1	Login
8	Sunday, 19 September 2004, 08:30:00	localhost	WIC server is up
9	Sunday, 19 September 2004, 08:25:00	localhost	WIC server is up
10	Sunday, 19 September 2004, 08:20:00	localhost	WIC server is up

First Page Page 1 of 31 <Last Page> Next Page(2/31)

Figure 4: Administrator Log

## ACCOUNT MODE

The administrator needs to create accounts prior to use. After an account is created, the user for that account can login and setup their checking requirements. After logging in, the user can perform many tasks (see Figure 5). Examples include changing account information, adding and deleting links designated for checking, enabling and disabling checks, displaying the activity log, setting actions for the server to take after a web page has been compromised, setting check schedules (see Figure 6) and contacting administrator by sending e-mail.

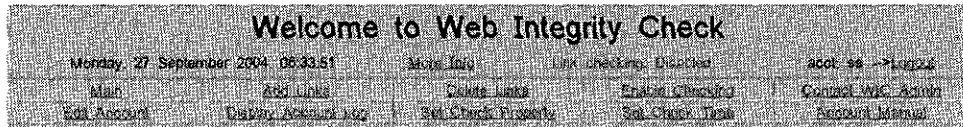


Figure 5: User Menu

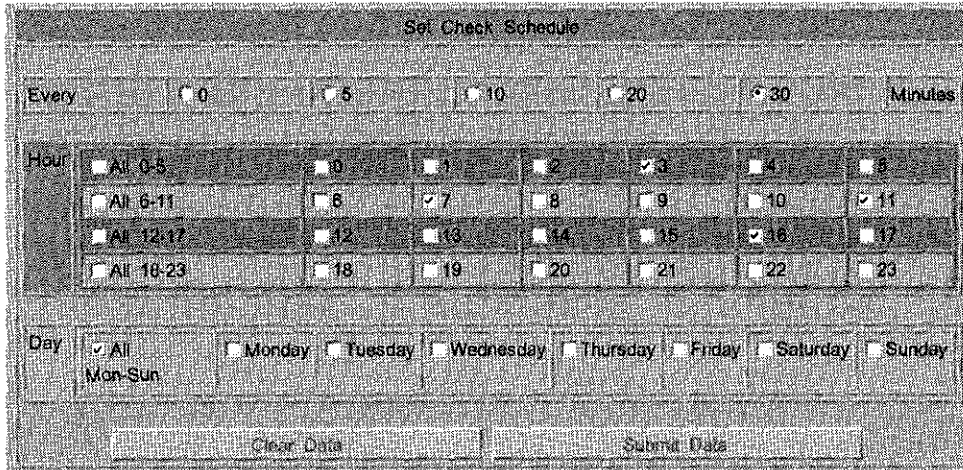


Figure 6: Set Check Time

## DISCUSSION

WIC operates by comparing the signature of the whole web page. Before altering the page, checking should be disabled and when finished, the operator should ensure that checking is re-enabled. WIC, at this stage, does not yet incorporate the ability to check specific sections of a web page. Some pages containing dynamic content such as date, time and banner changes cannot be verified by WIC due to this inability.

## CONCLUSION

Changing a Web page by an attacker may result in serious unimaginable consequence. WIC is a tool to detect such unauthorized change as early as possible and can report and help to recover the attack automatically when the incident occurs.

## REFERENCES

- Gaudin, S. (2003). *NASA Web sites hacked*, [on-line]. Available: <http://www.esecurityplanet.com/trends/article.php/3290791> [2004, 28 September]
- Gollmann, D. (1999). *Computer security*. West Sussex, England: John Wiley & Son Ltd.,
- Hacked: DOJ* (1996). [on-line]. Available: <http://www.actden.com/pp/guide.htmhttp://www.2600.com/hackedphiles/doj/> [2004, 20, September]
- Kaero, M. (1999). *Designing network security*. Indianapolis: Macmillan Technical Publishing.
- Leyden, J. (2001). *Mass hack takes out govt sites*, [on-line]. Available: [http://www.theregister.co.uk/2001/01/22/mass\\_hack\\_takes\\_out\\_govt/](http://www.theregister.co.uk/2001/01/22/mass_hack_takes_out_govt/) [2004, 28 September]
- McWilliams, B. (2002) *Bug triad whacks microsoft browser*, [on-line]. Available: <http://www.securityfocus.com/news/606> [2004, 28 September]