MODERN WEB SECURITY NEEDS

In today's world just about every part of our society is tied to the internet. As a result, web pages become more and more important for groups and businesses to connect with their target markets. Infrastructures of great importance are susceptible to malcontents, who seek to harm them for a variety of reasons. Hackers have been exploiting the weaknesses of the various online locales since the early days of the internet.

"Data breaches dominated headlines in 2014,… a recent study found that more than 40% of companies experienced a data breach of some sort in the past year – four out of ten companies that maintain your credit card numbers, social security numbers, health information, and other personal information. That number is staggering, and shows no signs of retreat."
-Jay Johnson, Forbes

gethits.com
Vancouver, BC, Canada
Blaine, WA, USA
Tel: 800-652-8182
security@gethits.com

Why Would Someone Attack a Web page?

- **Destruction:** In destructive cyber-attacks someone exploits a website and gains access to the back end of a system, doing damage to both the programming and some physical systems attached to that computer. In some cases hackers have managed to take out whole power grids via an e-mail exploit. Vigilante hackers see themselves as doling out justice on those that have wronged them. Other destructive hackers are just people who enjoy inflicting damage to a system.
- **Personal Gain:** Exploitation of websites occurs to extort or steal money from a site owner or site visitors. Sometimes the profit will be less direct and the hacker will use various methods to mine data about a website's demographics for later use.
- **Defacement:** A hacker may have a political or personal agenda that drives them to alter the appearance of the victim's page to either embarrass or prove a point. This is by far the least destructive to the website; however, the damage done to the site owner's reputation could be irreversible.

How Would They Attack? What Can I do?

Potential Dangers	Protective Solutions
Cross Site Scripting (XSS): A script is placed into a form that accepts user supplied data such as a comments box. XSS is widespread (even Google has to deal with this issue!) XSS can then affect any visitor to the page, tracking their cookies or viewing virtually any information they see while on the web.	Most XSS attacks are preventable via filtering user supplied data. Commercial options are available to automate this task.
SQL Injection: Many user input fields utilize java script to link information to an SQL database. A well versed hacker can put in a line of code to affect the SQL database via the user input field.	Prepared statements can prevent a hacker from adulterating the intent of a query to prevent it from running a script. Stored procedures work similarly, by defining the code and storing the parameters in the database.

Vancouver, BC, Canada
Blaine, WA, USA
Tel: 800-652-8182
security@gethits.com

Potential Dangers	Protective Solutions
ClickJacking: A very simple method where someone creates a malicious, but invisible, clickable object that appears over what the victim thinks they are clicking. Clicking this object will then run whatever script the creator has programmed, often installing malware and keyloggers that can record the victim's web usage and personal data.	Ensure that the current frame is always top level. Set the page to only allow framing from the host domain.
Social Engineering: Is considered by many to be one of the most dangerous forms of "hacking." Sometimes a malicious e-mail will trick someone into providing login information. Often however a savvy hacker can gain login information with just a drink in a bar with an unwitting employee. Social engineering is a dangerous and often overlooked method of web hacking.	Social engineering is prevented by good staffing and employee education around security risks.
Authorization Bypass: Dangerous to servers running a large number of authorization pages with varying levels of security. A hacker will study a network to find the page with the lowest level of login security, and use this page to hack into the entire network. This often creates a backdoor to a more valuable and well protected database.	Easy preventative measures can be taken by ensuring all login systems on the server are uniform.
Google Index Hacks: A surprisingly simple way for a hacker to use Google's search function to uncover unprotected databases containing usernames, passwords, and even administrative accounts.	Harden web servers. Be aware of what is public and searchable.
DDoS Attacks: Designed to simply bring a website down, these attacks are very popular and often reported in the news. All someone really needs to launch such an attack is a credit card and access to a website that will overwhelm the target server with requests when paid to do so. Spoofing DNS queries is easy because of the simplicity of UDP. EDNS0 now also allows large data to travel over DNS so requests can return large encrypted files to create high traffic volumes.	Be aware of max system capacity. Install monitoring systems to alert staff and offset abnormal levels of incoming data by keeping track of average traffic. Use multiple servers on one IP.

Vancouver, BC, Canada
Blaine, WA, USA
Tel: 800-652-8182
security@gethits.com

Potential Dangers	Protective Solutions
Brute Force Password Crack: Software that can be used on a site to try every possible combination of a password until it gains access.	Install a Web Firewall. Lock out accounts after multiple wrong inputs. Require complex passwords.
Semantic Url Attacks: Someone manipulates the text of a url to give them access to something they should not be allowed to get. If the new password request of a site looked like: mywebsite.com/pwreq.php?user1=user0001&mail=personalemail%40company.com and the attacker was able to replace the user name with another account, such as an admin, and leave their own personal email, they could now gain access to that account.	Only allow requests from domain forms. Use a shared secret randomly generated code to assure the origin of the request.

General Protection

Aside from the aforementioned protective measures, anyone wishing to protect themselves should also employ standard practice protections for their infrastructure.

Firewalls are always important to protect servers from unwanted traffic or actions from within and outside of a system.

SSL is an industry standard for creating and encrypting secure connections between a page and its clients and should not be overlooked.

Conclusion

There will always be people who find new ways around the ever-changing systems of the web. It is important to put your clients first, and protect your website security. With good security practices, you will keep the trust of the online community and ensure continued productivity.

Vancouver, BC, Canada
Blaine, WA, USA
Tel: 800-652-8182
security@gethits.com